MANUALE DI GESTIONE DOCUMENTALE

Il Manuale di Gestione Documentale dell'Istituto Comprensivo Ada Negri Motta Visconti descrive il sistema di gestione informatica dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Firmato digitalmente da ROBERTO FRACCIA

SOMMARIO

Firmato digitalmente da ROBERTO FRACCIA

Firmato digitalmente da ROBERTO FRACCIA

Firmato digitalmente da ROBERTO FRACCIA

Firmato digitalmente da ROBERTO FRACCIA

PREMESSA

INTRODUZIONE

Le "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*", emanate dall'AgID, prevedono l'obbligo per le Pubbliche Amministrazioni di redigere con provvedimento formale e pubblicare sul proprio sito istituzionale il Manuale di gestione documentale.
Il Manuale di Gestione documentale (di seguito "**Manuale**"), di cui all'art. 3.5 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, determinazione AGID n. 407/2020 (in seguito "**Linee guida AGID**"), descrive il sistema di gestione e di conservazione dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Nel dettaglio, il Manuale descrive il modello organizzativo adottato dalla scuola per la gestione documentale e il processo di gestione del ciclo di vita del documento, oltre a fornire specifiche istruzioni in merito al documento amministrativo ed al documento informatico, al protocollo informatico e alle tematiche di accesso, trasparenza e privacy.
Il Manuale è destinato alla più ampia diffusione interna ed esterna, in quanto fornisce le istruzioni complete per eseguire correttamente le operazioni di formazione, registrazione, classificazione, fascicolazione e archiviazione dei documenti.
Pertanto, il presente documento si rivolge non solo agli operatori di protocollo ma, in generale, a tutti i dipendenti e ai soggetti esterni che si relazionano con gli organi dell'Istituto.

Nell' Istituto Comprensivo Ada Negri Motta Visconti (di seguito "**Istituto**") è attiva una sola area organizzativa omogenea (di seguito, "**AOO**"), a cui si riferiscono tutti gli uffici operanti nell'Istituto.

L'Istituto:

- nomina con decreto dirigenziale il responsabile del servizio di gestione informatizzata dei flussi documentali e l'amministratore di protocollo della AOO;
- assicura l'adozione (in tempi utili) e l'aggiornamento del Manuale;
- definisce tempi, modalità, misure organizzative e tecniche per la eliminazione dei protocolli settoriali e dei relativi registri, soprattutto se ancora cartacei.

Una volta adottato il manuale a seguito dell'approvazione formale da parte della sovrintendenza ai beni culturali, esso va aggiornato periodicamente effettuando il censimento delle attività e delle prassi in essere, la razionalizzazione delle stesse,

Firmato digitalmente da ROBERTO FRACCIA

l'individuazione e la definizione degli aspetti organizzativi e gestionali in termini di fasi, tempi e risorse umane impegnate nell'automazione dei flussi documentali nel rispetto della normativa vigente.

COMPOSIZIONE

Il Manuale si compone:

- Del presente documento, recante la descrizione del sistema di gestione e conservazione dei documenti e dettante le regole e le procedure di attuazione
- Di tutti gli allegati elencati a fine documento, che caratterizzano l'applicazione del Manuale da parte dell'Istituto e ne definiscono le caratteristiche specifiche e peculiari

RIFERIMENTI

Nella redazione del Manuale sono stati tenuti come riferimento:

- Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, determinazione AGID n. 407/2020
- Linee guida per la gestione documentale nelle Istituzioni scolastiche, Ministero dell'Istruzione
- Format di manuale per la gestione dei flussi documentali delle Istituzioni scolastiche, Ministero dell'Istruzione
- Indicazioni operative pubblicate sul sito governativo del Ministero dell'Istruzione: https://www.istruzione.it/responsabile-transizione-digitale/scuole.html

Firmato digitalmente da ROBERTO FRACCIA

SEZIONE I – DEFINIZIONI, RIFERIMENTI NORMATIVI E AMBITO DI APPLICAZIONE

1.1 GLOSSARIO

Per quanto non previsto dal glossario che segue, si rimanda a quello contenuto nei seguenti atti:

- Linee guida sulla formazione, gestione e conservazione dei documenti informatici, determinazione AGID n. 407/2020 (linee guida AGID).

AA.GG	Autorità giudiziarie
AGID	Agenzia per l'Italia Digitale
AOO	Area Organizzativa Omogenea
ASP	Application Server Provider
AT	Ambito Territoriale
CAD	Codice dell'Amministrazione Digitale (D.Lgs n. 82/2005)
D.G. o D.R.	Direzione Generale o Regionale
D.Lgs	Decreto Legislativo
DPR	Decreto del Presidente della Repubblica
DURC	Documento Unico di Regolarità Contributiva
FF.OO.	Forze dell'Ordine
GdL	Gruppo di Lavoro
MdG	Manuale di Gestione del Protocollo informatico, dei documenti e degli archivi
MIUR	Ministero dell'Istruzione, dell'Università e della Ricerca
OdS	Ordine di Servizio
PA	Pubblica Amministrazione

Firmato digitalmente da ROBERTO FRACCIA

PdP	Prodotto di Protocollo informatico
PEC	Posta elettronica Certificata
PEO	Posta Elettronica Ordinaria
RdP	Responsabile del Procedimento – il dipendente che assume su di se' la responsabilità dell'esecuzione degli adempimenti amministrativi relativi ad un procedimento
RSP	Responsabile della gestione documentale, ovvero della tenuta del Protocollo informatico, della gestione dei flussi documentali, nonché degli archivi e della conservazione
RdU	Responsabile di Ufficio, da intendersi quest'ultimo quale UO
Tab	(o pagina): sezione della scheda documentale con un insieme di informazioni e metadati relativi al documento informatico
TUDA	Testo unico sul Documento Amministrativo (DPR n. 445/2000)
UOP	Unità Organizzativa di registrazione di Protocollo – identifica l'ufficio che svolge attività di registrazione del protocollo
UO	Ai sensi della normativa di riferimento, corrisponde alla Unità Organizzativa Responsabile e di Riferimento – vale a dire un insieme di uffici o un ufficio che, per tipologia di mandato istituzionale e di competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione unitarie e coordinate
SIDI	Sistema informativo dell'Istruzione
S.I.	Sistema Informativo del M.I.U.R.

Firmato digitalmente da ROBERTO FRACCIA

1.2 ESTREMI DEL DOCUMENTO

TITOLO	MANUALE DI GESTIONE DOCUMENTALE
REDATTORE DEL DOCUMENTO	DIRIGENTE PRO TEMPORE
STATO DEL DOCUMENTO	Da approvare / Approvato / Da autorizzare / Autorizzato
ESTREMI AUTORIZZAZIONE	Autorizzazione Soprintendenza del
PROPONENTE	Il Responsabile della Conservazione _____
DATA APPROVAZIONE Da parte del Consiglio di Istituto	xxx
DELIBERA APPROVAZIONE Da parte del Consiglio di Istituto	Delibera numero:
DATA ULTIMA REVISIONE	xxx

1.3 INTRODUZIONE

Il presente manuale disciplina le attività di formazione, registrazione, classificazione, fascicolazione e conservazione dei documenti, oltre che la gestione dei flussi documentali e dei procedimenti dell'Amministrazione
Il Manuale è vincolante per tutti gli operatori e le figure dell'Istituto.

Il Manuale:

- definisce regole e principi della gestione documentale
- fissa termini e modalità d'uso dell'applicativo di protocollo informatico, della posta elettronica (certificata e non), della firma digitale e degli strumenti di dematerializzazione e digitalizzazione delle procedure, in uso presso l'Istituto;
- individua ruoli e responsabilità connesse all'attuazione e monitoraggio delle misure ivi descritte.

Il Manuale richiama, in quanto compatibili, le procedure del Manuale di Gestione MIUR adottato con DDG 240 del 9 ottobre 2015.

Firmato digitalmente da ROBERTO FRACCIA

In prima istanza il Manuale è stato definito e formalizzato con delibera numero _____ in data _____ del Consiglio d'Istituto ed è rivisto, in conformità alla medesima delibera, con Decreto dirigenziale ogni qualvolta se ne rilevi la necessità.

Il Manuale è pubblicato sul sito Internet dell'Istituto, nella sezione *Amministrazione trasparente*.

1.4 STORIA DELLE VERSIONI E REVISIONI DEL DOCUMENTO

Versione	Data	Descrizione	Changelog
1.0		Versione iniziale	Linee Guida AgID 2020

1.5 MODALITA' DI APPROVAZIONE E AGGIORNAMENTO

Il Responsabile della gestione documentale1 si occupa della predisposizione del manuale, che è adottato con provvedimento dal Dirigente Scolastico.
Il manuale deve essere aggiornato periodicamente effettuando il censimento delle attività/prassi in essere, la razionalizzazione delle stesse, l'individuazione e la definizione degli aspetti organizzativi e gestionali in termini di fasi, tempi e risorse umane impegnate nell'automazione dei flussi documentali nel rispetto della normativa.
Ogni evento suscettibile di incidere sull'operatività ed efficacia del manuale medesimo deve essere tempestivamente segnalato al Responsabile della gestione documentale, al fine di prendere gli opportuni provvedimenti in ordine all'eventuale modifica e/o integrazione della procedura stessa.

1.6 FORME DI PUBBLICITA' E DIVULGAZIONE

In coerenza con quanto previsto nelle "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici" (a seguire, anche "Linee Guida"), adottate dall'AgID con Determinazione n. 407/2020 ed in seguito aggiornate con Determinazione n.

Firmato digitalmente da ROBERTO FRACCIA

371/2021 (da attuare entro il 1° gennaio 2022), ovvero che il manuale sia reso pubblico mediante la pubblicazione sul sito istituzionale in una parte chiaramente identificabile dell'area "Amministrazione trasparente", prevista dall'art. 9 del D.Lgs. 33/2013,3 il presente manuale è reso disponibile alla consultazione del pubblico mediante la diffusione sul sito istituzionale dell'Istituzione scolastica.

Firmato digitalmente da ROBERTO FRACCIA

SEZIONE II – ORGANIZZAZIONE DEL SERVIZIO

2.1 AREA ORGANIZZATIVA OMOGENEA

Ai sensi dell'art. 50 del DPR 445 del 28 dicembre 2000, ai fini della gestione dei documenti è individuata una sola area organizzativa omogenea denominata A9B4169 composta dall'insieme di tutte le sue unità organizzative come da elenco allegato (Allegato n. 1 al presente documento).

Il codice identificativo IPA dell'area è: istsc_miic872009

Il sito web istituzionale è: https://www.icmottavisconti.edu.it

Ai sensi della normativa vigente, la casella di posta elettronica certificata associata al registro di protocollo dell'unica AOO è: miic872009@pec.istruzione.it

L'Istituzione scolastica, allo scopo di assicurare un trattamento uniforme dei documenti, una puntuale applicazione delle disposizioni ed un periodico monitoraggio delle modalità d'uso degli strumenti di gestione documentale, deve prevedere al suo interno le seguenti figure:

1 Il **Responsabile della gestione documentale**, ai sensi delle Linee Guida AGID, nella figura di Laura Gilardi, con qualifica di DSGA.
Il Responsabile della gestione documentale è il soggetto in possesso di idonei requisiti professionali o di professionalità tecnico-archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'art. 61 del D.P.R. 28 dicembre 2000, n. 445, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione. Al fine d'agevolare l'assolvimento dei compiti assegnatigli dalla normativa vigente e dal presente Manuale, può individuare, per specifiche attività, un suo delegato, definendo il contesto organizzativo e l'ambito della delega;

2 Il **Referente per l'Indice delle Pubbliche Amministrazioni**, nella figura di Laura Gilardi, con qualifica di DSGA e del Dirigente Scolastico pro tempore; è il soggetto a cui il Dirigente Scolastico affida il compito, sia organizzativo che operativo, di interagire con il gestore dell'iPA per l'inserimento e la modifica dei dati dell'Istituzione scolastica, nonché per ogni altra questione riguardante la presenza della stessa presso l'iPA

3 Il **Referente per la PEC e la PEO** per il coordinamento e la gestione dei sistemi di posta elettronica istituzionale, nella figura di Laura Gilardi, con qualifica di DSGA;

Firmato digitalmente da ROBERTO FRACCIA

4 Il **DPO** (Data Protection Officer / Responsabile per la Protezione dei Dati) nella figura di Ferdinando Bassi.

5 Il **Responsabile per la prevenzione della corruzione e della trasparenza (RPCT)** nella figura di Laura Gilardi, con qualifica di DSGA; è il soggetto al quale può essere presentata l'istanza di accesso civico, qualora la stessa abbia ad oggetto dati, informazioni o documenti oggetto di pubblicazione obbligatoria ai sensi del D.Lgs. 33/2013. Il RPCT, oltre a segnalare i casi di inadempimento o di adempimento parziale degli obblighi in materia di pubblicazione previsti dalla normativa vigente, si occupa delle richieste di riesame dei richiedenti ai quali sia stato negato totalmente o parzialmente l'accesso civico generalizzato, ovvero che non abbiano avuto alcuna risposta entro il termine stabilito.

Le figura di sistema di cui ai punti 2. e 3. sono nominate con decreto del Dirigente, su proposta del Direttore dei Servizi Generali e Amministrativi. In caso di assenza di nomina le funzioni si intendono svolte dal Direttore dei Servizi Generali e Amministrativi.

2.2 SERVIZIO ARCHIVISTICO PER LA GESTIONE INFORMATICA DEL PROTOCOLLO, DEI DOCUMENTI, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

Al fine della gestione unica e coordinata dei documenti, ai sensi dell'art. 50 c. 3 del DPR 445 del 28 dicembre 2000, l'Amministrazione individua una sola struttura di protocollo ed archivio.
Ai sensi dell'articolo 61, comma 1, del DPR 445/2000, si provvederà alla costituzione del Servizio Archivistico per la gestione informatica del protocollo, dei documenti, dei flussi documentali e degli archivi, nell'ambito dell'UO denominata Ufficio del DSGA.
Il servizio, ai sensi dell'articolo 61, comma 3, del DPR 445/2000 ha competenza sulla gestione dell'intera documentazione archivistica, ovunque trattata, distribuita o conservata dall'Amministrazione, ai fini della sua corretta registrazione, classificazione, conservazione, selezione e del suo corretto ordinamento.
Il Responsabile del servizio, ai sensi delle Linee Guida AGID, svolge le funzioni attribuitegli dal DPR 445/2000 e dalle Linee Guida AGID stesse.

Ai sensi delle Linee Guida AGID, è individuato il **Responsabile del procedimento di conservazione della documentazione** generata in formato digitale nella figura di Laura Gilardi, con qualifica di DSGA.

Il Responsabile del procedimento di conservazione della documentazione ha affidato il processo di conservazione, o parte di esso, in outsourcing a Axios dopo aver verificato che quest'ultimo soggetto offra tutte le garanzie organizzative e tecnologiche necessarie.
Il Responsabile del procedimento di conservazione mantiene il compito di vigilare sulla corretta realizzazione del processo di conservazione.

Firmato digitalmente da ROBERTO FRACCIA

Il ruolo del Responsabile della conservazione può essere svolto dal Responsabile della gestione documentale o anche da altre figure.

Qui di seguito, sintetizzate, le principali attività che devono essere svolte dal responsabile della conservazione digitale dei documenti, secondo quanto stabilito nelle nuove regole tecniche attuative del CAD (Codice dell'amministrazione digitale) (articolo 44).

- Redigere il Manuale della Conservazione, che è il documento informatico all'interno del quale è possibile trovare l'organizzazione e il modello di funzionamento del processo di Conservazione digitale a norma, i soggetti che ne sono coinvolti e i loro ruoli, la descrizione delle architetture e delle infrastrutture in uso, le misure di sicurezza e tutte le altre informazioni utili alla gestione e alla verifica del buon andamento, nel tempo, del sistema di Conservazione; cura poi l'aggiornamento periodico di tale Manuale in base ai cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

- Definire le caratteristiche e i requisiti del sistema di conservazione a seconda della tipologia dei documenti da conservare.

- Gestire il processo di conservazione nel suo complesso, garantendone nel tempo la conformità alla normativa vigente e la corretta funzionalità.

- Acquisire e verificare il pacchetto di versamento e generare il rapporto di versamento, secondo le modalità previste dal Manuale di conservazione, quindi preparare il pacchetto di archiviazione, cioè il documento informatico che sancisce il caricamento dei file in un determinato momento e la sua conservazione a norma di legge.

- Creare e sottoscrivere il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, secondo i casi previsti e produrre duplicate e copie informatiche.

- Effettuare lo scarto dei documenti su eventuale indicazione del produttore.

- Verificare periodicamente, o per lo meno ogni cinque anni, l'integrità degli archivi e la leggibilità dei documenti.

- Adottare le misure necessarie per la sicurezza fisica e logica del sistema di conservazione, oltre che per rilevare tempestivamente l'eventuale degrado dei sistemi stessi (inclusa l'obsolescenza dei formati, può infatti accadere che, avendo utilizzato hardware o software non più disponibili dopo un certo periodo di tempo si rischi che le informazioni vadano perdute e non siano più raggiungibili, è quindi necessario che il responsabile della conservazione metta al riparo da tale pericolo).

Firmato digitalmente da ROBERTO FRACCIA

- Assicurare la presenza di un pubblico ufficiale, in ogni caso sia previsto il suo intervento, e assisterlo nelle sue attività fornendogli tutte le risorse utili per svolgere attività di verifica.

- Provvedere, per gli organi giudiziari e amministrativi dello Stato, al versamento dei documenti conservati all'archivio centrale dello Stato e agli archivi di Stato, secondo quanto previsto dalle norme.

2.3 FIGURE DI SISTEMA

Il Codice dell'amministrazione Digitale, le nuove Regole tecniche e le Linee Guida AgID, per la corretta gestione e la tutela di un archivio elettronico prevedono obbligatoriamente la presenza di varie figure che devono interagire tra loro: il responsabile della conservazione, il responsabile della sicurezza, il responsabile del trattamento dei dati e il responsabile del protocollo:

- **Responsabile della Conservazione:** è individuato nella figura di Laura Gilardi, con qualifica di DSGA col compito di coordinare e presidiare i sistemi informatici informativi e documentarli, garantendone una durata nel tempo;

- **Responsabile del trattamento dei dati personali**: è individuato nella figura di Laura Gilardi, con qualifica di DSGA, a cui compete di occuparsi della protezione dei dati nei database e negli archivi digitali, nonché di interfacciarsi con il DPO ogni qualvolta ne ravveda la necessità;

- **Responsabile del protocollo, dei flussi documentali e degli archivi**: è individuato nella figura di Laura Gilardi, con qualifica di DSGA che presidia la componente archivistica di qualsiasi sistema di conservazione dei documenti informatici;

- **Responsabile del procedimento**: è individuato nella figura di Laura Gilardi, con qualifica di DSGA.

2.4 INDIVIDUAZIONE DEL RESPONSABILE DI TENUTA DEL PROTOCOLLO INFORMATICO E DEFINIZIONE DEI COMPITI SPECIFICI

Il **Responsabile di tenuta del protocollo informatico** è individuato nella figura di Laura Gilardi, con qualifica di DSGA.

Il responsabile del servizio di Protocollo Informatico svolge le funzioni attribuitegli dal DPCM 31/10/2000 e dal DPR 445/2000 e dalle Linee guida AGID, e cioè i seguenti compiti:

Firmato digitalmente da ROBERTO FRACCIA

- aggiorna periodicamente il manuale di gestione;
- partecipa ad attività di formazione, dà consulenza e cura la formazione degli assistenti sulla nuova procedura di gestione del protocollo;
- garantisce che le operazioni di assegnazione, registrazione e di segnatura di protocollo si svolgano nel rispetto della normativa vigente;
- garantisce la corretta produzione del registro giornaliero di protocollo;
- garantisce il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali e gestione archivio, escluse le funzionalità di accesso a nuovi utenti;
- vigila sull'osservanza delle disposizioni del presente regolamento;
- cura che le funzionalità del sistema in caso di guasti o anomalie collegate al software siano ripristinate nel più breve tempo possibile, tramite apposita assistenza offerta dalla ditta che fornisce il servizio; guasti e anomalie dell'hardware sono gestiti dall'assistente amministrativo che segue gli acquisti;
- partecipa alla redazione del piano per la sicurezza informatica d'intesa con il responsabile della conservazione, il responsabile dei sistemi informatici e dei dati personali;
- definisce e assicura criteri uniformi di trattamento del documento informatico e, in particolare, di classificazione ed archiviazione, nonché di comunicazione interna tra vari uffici;
- si occupa dell'aggiornamento del titolario di classificazione integrato con le informazioni relative ai tempi, ai criteri ed alle regole di selezione e conservazione;
- indica le modalità di produzione e di conservazione delle registrazioni di protocollo informatico; in particolare, dà l'indicazione delle soluzioni tecnologiche ed organizzative che garantiscono di registrare in modo immodificabile e contemporaneo alla segnatura; definisce le modalità di registrazione delle informazioni annullate o modificate in ogni sessione di registrazione.

Ai sensi delle Linee guida AGID la figura individuata quale responsabile del procedimento di conservazione della documentazione generata in formato digitale, è specificatamente considerato pubblico ufficiale.

2.5 UNICITA' DEL PROTOCOLLO INFORMATICO

Poiché l'Amministrazione gestisce un unico Registro di protocollo, anche la numerazione delle registrazioni di protocollo è unica, progressiva, corrisponde all'anno solare ed è formata da un intero. Essa inizia da uno all'inizio di ogni anno solare e si chiude al 31 dicembre.
Tuttavia a norma dell'articolo 53, comma 5 del DPR 445/2000 sono possibili registrazioni particolari (**Allegato n. 2**). L'Amministrazione non riconosce validità a registrazioni particolari che non siano quelle individuate nell'elenco allegato.

Firmato digitalmente da ROBERTO FRACCIA

Il sistema informatico di gestione del protocollo è sincronizzato per il calcolo dell'ora con i server su cui risiede l'applicativo, a loro volta sincronizzati con un orologio atomico.
Ad ogni documento è assegnato un solo numero, composto da sette cifre, che non può essere utilizzato per la registrazione di altri documenti. (come ad esempio per il protocollo riservato)

2.6 MODELLO ORGANIZZATIVO E MODALITA' DI GESTIONE DEL PROTOCOLLO INFORMATICO

Nell'Amministrazione, la gestione dei flussi documentali e del protocollo informatico avviene a partire dalla data del 11.09.2021 tramite il software gestionale: Nuvola.
Il software in oggetto consente la completa, automazione di un processo di gestione che arriva a coinvolgere tutti gli assistenti amministrativi, il DSGA ed il Dirigente Scolastico, secondo le regole procedurali definite.
L'Istituto è dotato di un archivio digitale all'interno del Cloud del fornitore SaaS Nuvola, dove ogni Assistente Amministrativo, dopo essersi autenticato tramite credenziali personali e univoche, entra nella propria dashboard e trova varie azioni da compiere a seconda della sua profilatura.
La scuola utilizza per l'espletamento delle attività istituzionali la firma digitale rilasciata da un ente certificatore accreditato: Aruba.
Il DS e il DSGA sono anche dotati della firma digitale remota rilasciata dal MIUR (rilasciata per l'utilizzo all'interno del Sistema ministeriale SIDI).
Il DS e il DSGA si dotano, inoltre, del dispositivo di firma digitale remota, abbinato al software ArubaSign.
La scuola dota, inoltre, i suoi assistenti amministrativi e i facenti funzione delle credenziali di accesso al sistema per l'espletamento di tutte le attività connesse all'attuazione delle norme di gestione del Protocollo Informatico, di gestione documentale e di archivistica, ai sensi della normativa vigente in materia di amministrazione digitale.
Tali credenziali di accesso permettono l'identificazione elettronica dell'utente che accede al sistema.

Il modello organizzativo adottato è un modello operativo decentrato, che prevede la partecipazione attiva di più soggetti ed abilitati a svolgere soltanto le operazioni di loro competenza.
In dettaglio:

- le comunicazioni in ingresso sono gestite da tutti gli Uffici abilitati e, successivamente, assegnate per il completamento della pratica
- le comunicazioni in uscita sono trasmesse dai singoli Uffici.

L'archivio storico e di deposito analogico sono conservati presso l'Archivio Generale dell'Istituto, situato nei locali denominati Archivio e ubicati nella sede dell'Istituto; l'archivio corrente è conservato presso le unità organizzative.

Firmato digitalmente da ROBERTO FRACCIA

Le operazioni di consultazione dell'archivio protocollo possono essere effettuate da parte di tutti gli utenti abilitati, non solo per gli atti di propria competenza, ma per tutti gli atti secondo i sistemi di ricerca generale o specifica, fatta eccezione per gli atti protocollati con protocollo riservato, per i quali occorrono specifiche autorizzazioni di profilatura.

Per ciò che concerne la modalità di amministrazione del protocollo informatico, la società fornitrice del software gestisce per conto dell'istituto la conservazione dei dati e dei documenti di protocollo, secondo quanto specificato nel relativo contratto e nell'attestazione di conformità agli standard previsti dalla normativa del protocollo informatico. (**Allegato 3**)

2.7 INDIRIZZI DI POSTA ELETTRONICA

L'indirizzo PEC è utilizzato per la gestione del servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi. L'indirizzo PEC è pubblicato sull'indice delle Pubbliche Amministrazioni (iPA). La casella PEC costituisce l'indirizzo virtuale della sede legale dell'Istituto.
L'Istituto è dotato anche di una casella di posta elettronica ordinaria istituzionale (di seguito PEO) utile a gestire i messaggi di posta elettronica con annessi documenti ed eventuali allegati, aventi rilevanza amministrativa.
Ogni UO, ogni Assistente Amministrativo e il Dirigente Scolastico dell'Istituto sono dotati di una casella di posta elettronica @icmottavisconti.edu.it
Il responsabile della gestione documentale è il custode delle credenziali di accesso alle caselle di posta elettronica istituzionali (certificate e non) dell'Istituto.
Le disposizioni vincolanti inerenti ai termini e modalità d'uso delle PEC e delle PEO sono pubblicati sul sito istituzionale dell'Istituzione scolastica.

2.8 IL CICLO DI VITA DEL DOCUMENTO

Il ciclo di vita del documento è articolato nei processi di produzione, gestione e conservazione:

- il processo di produzione del documento si sostanzia principalmente nell'acquisizione di documenti cartacei, informatici e/o telematici ovvero nella creazione degli stessi;

Firmato digitalmente da ROBERTO FRACCIA

- il processo di gestione interessa tutte le attività a partire dalla registrazione del documento, alla classificazione, assegnazione e fascicolazione/archiviazione corrente;
- il processo di conservazione si sostanzia nel trasferimento dei documenti dall'archivio corrente all'archivio di deposito (dal quale possono eventualmente seguire l'attività di scarto e di delocalizzazione) e dall'archivio di deposito all'archivio storico.

Firmato digitalmente da ROBERTO FRACCIA

SEZIONE III – PRODUZIONE E FORMAZIONE DEI DOCUMENTI INFORMATICI

3.1 – MODALITA' DI FORMAZIONE DEI DOCUMENTI E REQUISITI MINIMI

Le modalità di produzione e formazione dei documenti, del loro contenuto e della loro struttura, sono determinate dalla dirigenza e da quanto previsto dal presente manuale.
Per quanto riguarda i documenti informatici, la loro produzione è regolata sulla base di modelli standard presenti nel sistema informatico di gestione documentale I documenti dell'amministrazione sono prodotti con sistemi informatici, come previsto dalla normativa vigente.

Ogni documento è creato per essere formalmente inoltrato all'esterno o all'interno e possiede parte o tutte le seguenti caratteristiche:

- si riferisce ad un solo protocollo;
- può fare riferimento anche a più pratiche e fascicoli;
- l'oggetto del documento tratta in modo omogeneo e attinente a un argomento.
- Le firme necessarie alla sua redazione e perfezione giuridica devono essere apposte prima della sua protocollazione.
- Il documento deve consentire l'identificazione dell'amministrazione mittente attraverso le seguenti informazioni, presenti nella segnatura del protocollo:
    - la denominazione dell'amministrazione; codice Area Organizzativa Omogenea (AOO); codice Registro di protocollo;
    - numero registrazione di protocollo; data di registrazione protocollo; oggetto del documento;
    - eventuali allegati;
    - estremi identificativi del responsabile del procedimento (l. 241/1990);
    - sottoscrizione elettronica con firma digitale o elettronica del responsabile di gestione

3.2 FORMATO DEI DOCUMENTI INFORMATICI

L'Istituto forma gli originali dei propri documenti con mezzi informatici, secondo le regole tecniche di cui all'articolo 71 del **CAD** e di cui alle **Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici (Allegato 4)**, mediante l'utilizzo di appositi strumenti software.

Firmato digitalmente da ROBERTO FRACCIA

Il documento informatico assume la caratteristica di immodificabilità quando forma e contenuto non sono alterabili durante le fasi di tenuta e accesso e quando sia garantita la staticità nella fase di conservazione. Gli atti formati con strumenti informatici, i dati e i documenti informatici dell'ente costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi tipi di supporto, copie e duplicati per gli usi consentiti dalla legge.
I formati utilizzati sono selezionati sulla base del criterio di maggior garanzia del principio di interoperabilità e nel rispetto delle caratteristiche di apertura, sicurezza, portabilità, funzionalità, supporto allo sviluppo e diffusione, secondo le indicazioni delle Linee Guida dell'Agenzia per l'Italia Digitale (www.agid.gov.it).

Ai fini dell'archiviazione e della conservazione si utilizzano preferibilmente, ove possibile, i formati PDF, PDF/A, TIFF e XML. I messaggi e-mail sono archiviati in formato eml e gli allegati sono mantenuti nel formato originale in cui sono pervenuti all'istituzione scolastica.
L'elenco dei formati accettati è riportato nell'apposito allegato (**Allegato 5**).

3.3 COPIE PER IMMAGINE SU SUPPORTO INFORMATICO DI DOCUMENTI ANALOGICI

La copia per immagine su supporto informatico di un documento analogico è prodotta mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o, nel caso di esigenze di dematerializzazione massiva di documenti analogici, attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia.

Fermo restando quanto previsto dall'art. 22 comma 3 del CAD8 nel caso in cui non vi è l'attestazione di un pubblico ufficiale, la conformità della copia per immagine ad un documento analogico è garantita mediante l'apposizione della firma digitale o firma elettronica qualificata o firma elettronica avanzata o altro tipo di firma ai sensi dell'art. 20 comma 1bis, ovvero del sigillo elettronico qualificato o avanzato da parte di chi effettua il raffronto.

I processi di copia per immagine sono effettuati in osservazione di quanto indicato nel punto *2.2 Copie per immagine su supporto informatico di documenti analogici* delle succitate **Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici**.

3.4 DUPLICATI, COPIE ED ESTRATTI INFORMATICI DI DOCUMENTI INFORMATICI

Un **duplicato informatico** ha lo stesso valore giuridico del documento informatico da cui è tratto se è ottenuto mediante la memorizzazione della medesima evidenza informatica, sullo

Firmato digitalmente da ROBERTO FRACCIA

stesso dispositivo o su dispositivi diversi; ad esempio, effettuando una copia da un PC ad una pen-drive di un documento nel medesimo formato.
La **copia di un documento informatico** è un documento il cui contenuto è il medesimo dell'originale ma con una diversa evidenza informatica rispetto al documento da cui è tratto, come quando si trasforma un documento con estensione ".doc" in un documento ".pdf".
L'estratto di un documento informatico è una parte del documento con una diversa evidenza informatica rispetto al documento da cui è tratto. Tali documenti hanno lo stesso valore probatorio dell'originale da cui hanno origine se la stessa conformità non viene espressamente disconosciuta. In particolare, la validità del documento informatico per le copie e/o estratti di documenti informatici è consentita mediante uno dei due metodi:

- raffronto dei documenti;
- certificazione di processo

I processi di duplicazione, copia ed estrazione sono effettuati in osservazione di quanto indicato nel punto *2.3 Duplicati, copie ed estratti informatici di documenti informatici* delle succitate **Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici**.

3.5 SOTTOSCRIZIONE DEI DOCUMENTI INFORMATICI

La sottoscrizione dei documenti informatici è ottenuta con un processo di firma digitale o avanzata conforme alle disposizioni di legge.
La scuola utilizza per l'espletamento delle attività istituzionali la firma digitale rilasciata dall' ente certificatore accreditato: Aruba.
Il DS e il DSGA sono dotati della firma digitale remota rilasciata dal MIUR (rilasciata per l'utilizzo del Sistema ministeriale SIDI).
Il DS e i l DSGA si dotano, inoltre, del dispositivo di firma digitale remota, abbinato al software ArubaSign.
La scuola dota, inoltre, i suoi assistenti amministrativi e i facenti funzione delle credenziali di accesso al sistema per l'espletamento di tutte le attività connesse all'attuazione delle norme di gestione del Protocollo Informatico, di gestione documentale e di archivistica, ai sensi della normativa vigente in materia di amministrazione digitale.
Tali credenziali di accesso costituiscono la firma elettronica dell'utente che accede al sistema.
I titolari di firma digitale sono abilitati all'utilizzo del dispositivo di firma solo ed esclusivamente nell'esercizio delle proprie funzioni istituzionali, secondo le disposizioni dell'Amministrazione centra- le del MIUR.
Il servizio archivistico è responsabile del controllo della scadenza dei certificati di firma e del loro eventuale rinnovo.

Firmato digitalmente da ROBERTO FRACCIA

3.6 VERIFICA DELLE FIRME DIGITALI

La sequenza delle operazioni previste per la verifica di integrità del documento firmato digitalmente, è la seguente:

- apertura del file firmato
- verifica della validità del certificato e della corrispondenza delle impronte del documento

Queste attività sono realizzate mediante:

- applicazione appositamente fornita da parte dell'ente fornitore dei certificati di firma digitale in dotazione all'Istituto: Aruba.
- software Dike GoSign rilasciato gratuitamente da InfoCert

3.7 TIPOLOGIE PARTICOLARI DI DOCUMENTI PER I QUALI SI STABILISCONO MODALITA' DI TRATTAMENTO SPECIFICHE

Le eventuali modifiche alle tipologie di documentazione sottoposta a trattamento specifico e a registrazione particolare sono evidenziate nell'elenco allegato (**Allegato 6**)

Firmato digitalmente da ROBERTO FRACCIA

SEZIONE IV – RICEZIONE DEI DOCUMENTI

4.1 RICEZIONE DEI DOCUMENTI SU SUPPORTO CARTACEO

I documenti su supporto cartaceo possono arrivare all'istituzione scolastica attraverso:

- il servizio postale;
- la consegna diretta agli uffici;
- fax.

L'Istituto si riserva il diritto a non accettare documenti pervenuti via fax se non sono univocamente riferibili ad un mittente individuato (firma autografata, timbri, punzoni) e non sono accompagnati dalla trasmissione di una copia del documento di identità.
I documenti, esclusi quelli non soggetti a registrazione di protocollo, devono pervenire all'Ufficio Protocollo (postazioni adibite presso l'area amministrativa) per la loro registrazione.
I documenti arrivati via fax sono soggetti alle stesse regole di registrazione degli altri documenti cartacei se rispondono a parametri di autenticità, leggibilità e integrità previsti dalla normativa vigente; in presenza di un sistema informatico che ne consenta l'acquisizione in formato elettronico (fax management) si applicano le procedure previste per la ricezione dei documenti informatici. In caso ciò non fosse possibile, si procederà all'acquisizione informatica secondo quanto stabilito al punto 3.3.

Non è consentita l'identificazione dei documenti mediante l'assegnazione manuale di numeri di protocollo che il sistema ha già attribuito ad altri documenti, anche se questi sono strettamente correlati tra loro.
Non è pertanto consentito, in nessun caso, l'utilizzo di un unico numero di protocollo per il documento in arrivo e il documento in partenza.

La documentazione che non è stata registrata in arrivo o in partenza viene considerata giuridicamente, inesistente, per l'Amministrazione.

I documenti che transitano attraverso il servizio postale tradizionale sono ritirati, ogni giorno lavorativo, a cura del personale collaboratore scolastico addetto, e consegnati al DSGA (o al suo sostituto) che a sua volta li consegna, dopo aver preso visione del contenuto, all'Ufficio Protocollo che avrà cura di mostrarne la visione al Dirigente Scolastico.

I documenti pervenuti ad altri uffici, mediante uno qualunque dei mezzi citati, sono fatti pervenire, a cura del personale che li riceve, all'Ufficio Protocollo.

Firmato digitalmente da ROBERTO FRACCIA

La corrispondenza indirizzata alla cortese attenzione del personale è regolarmente aperta e registrata al protocollo.
Non è ammessa la ricezione di corrispondenza di carattere personale.
Il Responsabile della gestione documentale è in ogni caso tenuto a verificare il contenuto della corrispondenza pervenuta.
La corrispondenza in arrivo viene aperta il giorno lavorativo in cui è pervenuta e contestualmente protocollata.
Laddove, per esigenze interne all'ufficio, non sia possibile registrare la totalità dei documenti pervenuti, il referente del protocollo individua la corrispondenza prioritaria da protocollare immediatamente; i restanti documenti verranno registrati entro il giorno lavorativo successivo.
Non è prevista una gestione associata di servizi (La gestione associata di servizi interessa principalmente i comuni che, associandosi in unione, associazione intercomunale o consorzio ecc., trasferiscono funzioni agli enti associativi al fine di garantirne un migliore funzionamento).

4.2 RICEZIONE DEI DOCUMENTI INFORMATICI ATTRAVERSO PEC E PEO

L'Istituto comunica con le altre Amministrazioni e con gli utenti utilizzando la casella di posta elettronica PEC e la casella di posta elettronica PEO.
Gli indirizzi sono riportati nell'Indice delle Pubbliche Amministrazioni e pubblicizzato sul sito web istituzionale: https://www.icmottavisconti.edu.it/

La ricezione dei documenti informatici soggetti alla registrazione di protocollo trasmessi da posta elettronica ordinaria è garantita dalla casella di posta elettronica ordinaria istituzionale MIIC872009@istruzione.it
Le comunicazioni formali e la trasmissione di documenti informatici, il cui contenuto impegni l'Istituto verso terzi, avvengono tramite le caselle di posta elettronica istituzionali e PEC.

Un documento informatico viene registrato a protocollo se è stato spedito all'indirizzo di posta elettronica certificata (PEC) o all'indirizzo di posta elettronica (PEO) dell'Istituzione Scolastica, ad eccezione delle MAD e del materiale pubblicitario per cui non è prevista protocollazione.
Il responsabile del servizio provvede a renderli pubblici e a trasmetterli all'Agenzia per l'Italia digitale ai sensi delle Linee Guida AGID.

I documenti informatici eventualmente pervenuti ad indirizzi di posta personale degli uffici, devono essere re-inoltrati dal mittente all'indirizzo di posta elettronica certificata PEO per la successiva registrazione a protocollo. Le semplici comunicazioni informali ricevute o trasmesse per posta elettronica, che consistano in scambio di informazioni che non impegnano l'Istituto verso terzi, possono non essere protocollate.

Firmato digitalmente da ROBERTO FRACCIA

L'operazione di ricezione dei documenti informatici avviene con le modalità previste dalle regole tecniche vigenti, attraverso l'utilizzo dell'applicazione di posta elettronica presente nel Sistema di Gestione Documentale fornito da Nuvola.

Il personale addetto alla protocollazione controlla, quotidianamente, i messaggi pervenuti nelle caselle di posta istituzionale non certificata e verifica se il documento ricevuto è da protocollare.
Nel caso in cui il messaggio venga ricevuto su una casella di posta elettronica non istituzionale, il destinatario verifica se il messaggio pervenuto sia da protocollare ed in tal caso vi provvede direttamente oppure trasmette il messaggio con richiesta di protocollazione al Responsabile della Gestione o all'Ufficio protocollo.
Conseguentemente a questa operazione si potrà aprire una pratica o attribuirne una già esistente al documento e al relativo fascicolo di appartenenza.
Il Sistema di Gestione Documentale in uso nell'Istituto supporta la gestione delle pratiche mediante processi automatici di workflow tra le varie figure coinvolte nel processo.

La posta elettronica individuale non può essere utilizzata per la ricezione o la spedizione di documenti a firma digitale per i quali è prevista l'apposita casella di PEC.
Le caselle di posta personale, di cui ogni assistente amministrativo è dotato, vanno utilizzate per comunicazioni a carattere informale e per le comunicazioni di natura non ufficiale o per scambi di documenti non definitivi, per i quali non è necessario acquisire certezza di invio e ricezione.
Non si possono inviare messaggi dalla casella di posta personale quando il contenuto di questi, impegni l'Amministrazione verso terzi.

Nel formato dei messaggi di posta elettronica non certificata è inserito automaticamente il seguente testo: "*Questo messaggio non impegna (nome ente/organizzazione) e contiene informazioni appartenenti al mittente, che potrebbero essere di natura confidenziale, esclusivamente dirette al destinatario sopra indicato. Qualora Lei non sia il destinatario indicato, Le comunichiamo che, ai sensi Regolamento Europeo per il trattamento dei dati personali e sensibili (679/2016 GDPR), sono severamente proibite la revisione, divulgazione, rivelazione, copia, ritrasmissione di questo messaggio nonché ogni azione correlata al contenuto dello stesso*".

4.3 RICEVUTE ATTESTANTI LA RICEZIONE DEI DOCUMENTI

Documenti cartacei
La ricevuta della consegna di un documento cartaceo può essere costituita dalla fotocopia del primo foglio del documento stesso, con un timbro che attesti il giorno della consegna.
A chi ne fa domanda, compatibilmente con le esigenze del servizio, deve essere anche riportato il numero di protocollo assegnato al documento; in questo caso l'operatore deve provvedere immediatamente alla registrazione dell'atto e alla sua acquisizione in formato digitale.

Firmato digitalmente da ROBERTO FRACCIA

Dopo tale registrazione l'operatore può stampare la ricevuta di protocollo dal Sistema di Gestione Documentale, Area Protocollo, dove è prevista una funzione apposita. L'operatore si riserva di inviare, successivamente, via posta elettronica, il file firmato digitalmente con il relativo file .xml dove è indicato anche il numero di protocollo assegnato all'atto.

Documenti informatici
La ricevuta informatica è disponibile nel Sistema di Gestione Documentale immediatamente dopo la protocollazione del documento ricevuto. L'operatore si riserva di inviare, successivamente, via posta elettronica, il file firmato digitalmente con il relativo file .xml dove è indicato anche il numero di protocollo assegnato all'atto.

Posta Elettronica Certificata
Nel caso di ricezione dei documenti informatici tramite Posta Elettronica Certificata, la notifica al mittente dell'avvenuto ricevimento è assicurata dal sistema informatico.

4.4 APERTURA DELLA POSTA

Il Responsabile della gestione documentale apre tutta la corrispondenza cartacea pervenuta all'Istituto e tutta la corrispondenza pervenuta tramite la posta elettronica istituzionale e la posta elettronica PEC. Le buste dei documenti pervenuti non si inoltrano agli uffici destinatari e si conservano per 24 ore; le buste delle assicurate, corrieri, espressi, raccomandate etc. si inoltrano insieme ai documenti.

4.5 ACQUISIZIONE DI DOCUMENTI CARTACEI TRAMITE SCANNER

Tutti i documenti analogici pervenuti al protocollo generale sono acquisiti mediante scanner, compatibilmente con il relativo formato e gli strumenti tecnologici disponibili.
L'immagine digitale così ottenuta è archiviata nel sistema informatico in modo da poter essere sempre consultata ed eventualmente riprodotta in copia.
L'addetto al protocollo deve verificare la leggibilità delle immagini acquisite e la loro esatta corrispondenza con il cartaceo e scandire in formato PDF, ove possibile in formato PDF/A, nel rispetto dei requisiti di accessibilità; occorre sempre rendere accessibili documenti provenienti da altri enti se devono essere pubblicati sul sito scolastico.
Gli originali cartacei sono conservati in apposito fascicolo.
Il processo di acquisizione di documenti cartacei è descritto nella Sezione XI.

4.6 ERRATA RICEZIONE DI DOCUMENTI

Firmato digitalmente da ROBERTO FRACCIA

Nel caso in cui pervengano messaggi/documenti dal cui contenuto si rileva che sono stati erroneamente ricevuti, si provvederà a rispedire il messaggio al mittente utilizzando lo stesso canale tramite il quale il messaggio/documentazione è giunto (mail/mail; Fax/fax etc.). La copia ricevuta erroneamente non sarà conservata.

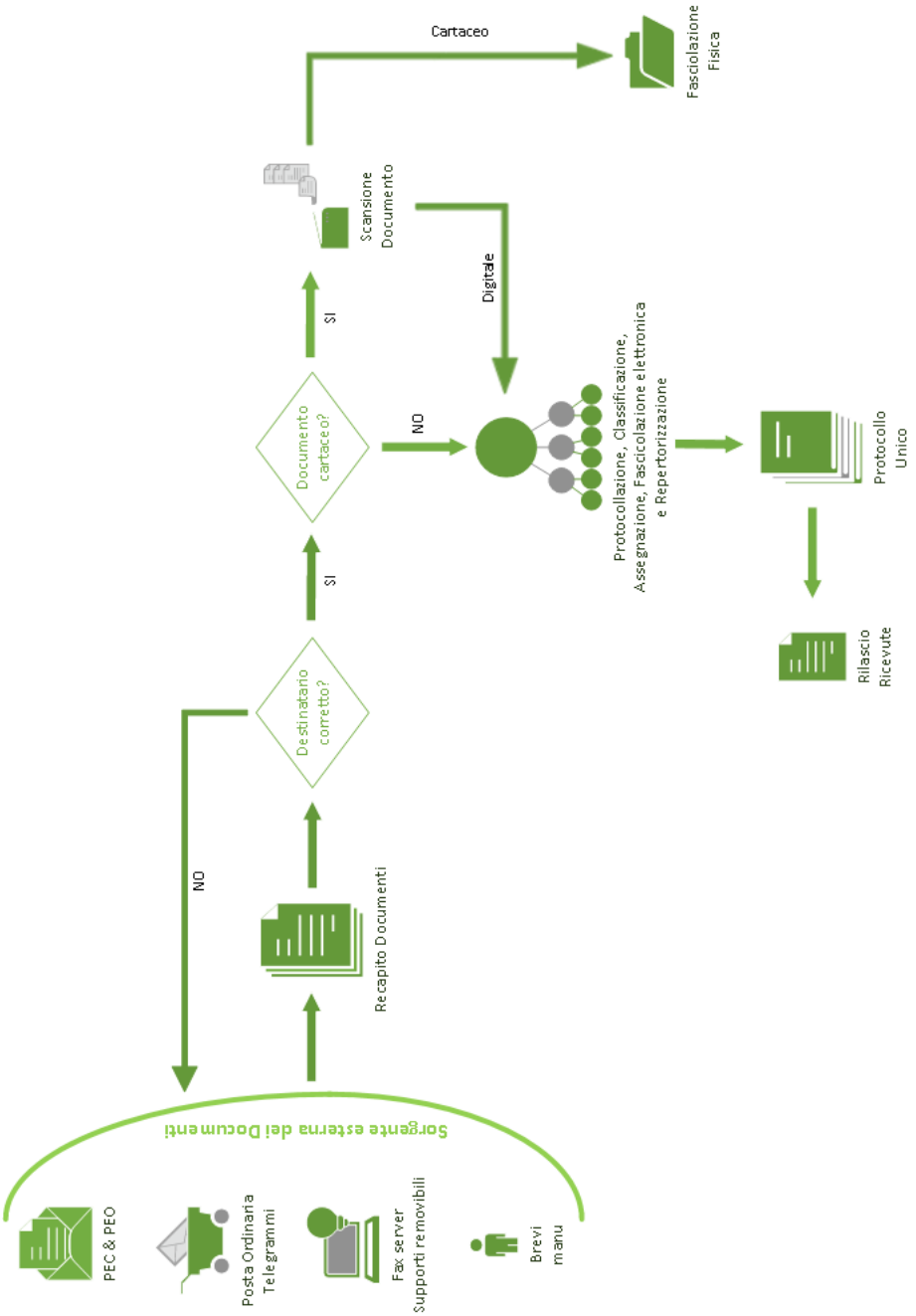
4.7 ORARI DI APERTURA PER IL RICEVIMENTO DELLA DOCUMENTAZIONE CARTACEA

Per la protocollazione dei documenti cartacei in ingresso, l'Ufficio protocollo è aperto con gli orari indicati sul sito web istituzionale.
Gli uffici abilitati al ricevimento dei documenti sono delegati dal Responsabile della gestione documentale all'apertura di tutta la corrispondenza analogica e informatica pervenuta all'ente/organizzazione, salvo i casi particolari specificati nella Sezione VII.

4.8 FLUSSO DI LAVORO DEI DOCUMENTI RICEVUTI DALL'ISTITUTO

Il diagramma di flusso riportato alla pagina successiva descrive il processo di lavoro dei documenti in entrata.

Firmato digitalmente da ROBERTO FRACCIA



4.9 REGISTRAZIONE DEI DOCUMENTI

Se il documento è di competenza dell'Istituzione scolastica ricevente, segue la fase di registrazione in cui l'operatore addetto alla protocollazione:

- valuta se il documento è da protocollare (cfr. par. "4.8. - Protocollabilità di un documento");
- nel caso in cui il documento sia da protocollare procede alla scansione e alla successiva verifica di conformità all'originale della copia informatica (cfr. par. "5.10. - Modalità di svolgimento del processo di scansione");

Firmato digitalmente da ROBERTO FRACCIA

- verifica la presenza di categorie particolari di dati personali, di cui all'articolo 9 del Regolamento UE 679/2016, ai fini dell'attuazione delle misure di sicurezza previste al paragrafo 6.1;
- provvede alla classificazione del documento sulla base del titolario di classificazione;
- provvede alla protocollazione in ingresso del documento;
- appone il timbro contenente i dati contenuti nella segnatura di protocollo tramite l'apposita funzionalità del servizio di protocollo informatico ovvero, solo in caso di impossibilità, procede manualmente.

Per la registrazione dei documenti si veda nel dettaglio la Sezione VI.

Firmato digitalmente da ROBERTO FRACCIA

SEZIONE V – ASSEGNAZIONE, RECAPITO, PRESA IN CARICO DEI DOCUMENTI

5.1 IL PROCESSO DI ASSEGNAZIONE DEI DOCUMENTI

Per assegnazione di un documento si intende l'operazione di individuazione dell'ufficio cui compete la trattazione del relativo affare o procedimento amministrativo. La lavorazione dei documenti ricevuti dall'Amministrazione e la designazione dei relativi responsabili di procedimento sono effettuati in prima istanza dal referente del Protocollo, scegliendo il nominativo o l'ufficio corrispondente all'interno del work flow, e successivamente dal Dirigente o suoi delegati.

5.2 RECAPITO E PRESA IN CARICO DEI DOCUMENTI

I documenti, dopo la fase di protocollo, arrivano nella work list dei responsabili di procedimento, che possono procedere con la lavorazione, creando una pratica o inserendo il file in una pratica già esistente o, semplicemente, prenderne visione.
Il sistema di gestione informatica dei documenti tiene traccia di tutti questi passaggi, memorizzando per ciascuno di essi, l'identificativo dell'utente, lo stato del documento nelle varie fasi: assegnazione, verifica, protocollazione, data e ora di esecuzione, stato del documento, ID di processo e di attività.

Firmato digitalmente da ROBERTO FRACCIA

SEZIONE VI – REGISTRAZIONE DEI DOCUMENTI

6.1 DOCUMENTI SOGGETTI A REGISTRAZIONE DI PROTOCOLLO

Tutti i documenti prodotti e ricevuti dall'Amministrazione, indipendentemente dal supporto sul quale sono formati, ad eccezione di quelli indicati nel successivo articolo, sono registrati al protocollo.

6.2 DOCUMENTI NON SOGGETTI A REGISTRAZIONE DI PROTOCOLLO

Sono esclusi dalla registrazione di protocollo obbligatoria, ai sensi dell'art. 53.5 del T.U. 445/2000 le seguenti tipologie di atti e documenti:

- documenti che, per loro natura, non rivestono alcuna rilevanza giuridico-amministrativa, vale a dire gli inviti, le stampe pubblicitarie, partecipazioni, condoglianze, ringraziamenti, auguri, informative e similari
- le Gazzette ufficiali, i bollettini ufficiali, i notiziari e le riviste scolastiche e della pubblica amministrazione
- le richieste della avvenuta ricevuta, i materiali statistici, i documenti interni preparatori di atti;
- i giornali, le riviste, i libri, i manifesti e i materiali pubblicitari, gli inviti a manifestazioni, i documenti il cui destinatario sia un altro Ente oppure altra persona fisica o giuridica (da trasmettere a chi di competenza o restituire al mittente)
- le bolle di accompagnamento
- le certificazioni che sono soggette ad altra registrazione
- le richieste di intervento di manutenzione ordinarie effettuate tramite invio telematico, dal sito direttamente alle amministrazioni comunali di competenza
- le richieste di viaggi di istruzione, opportunamente conservate nel piano visite d'istruzione del relativo anno scolastico
- i documenti interni di carattere preminentemente informativo (memorie, appunti, brevi comunicazioni tra uffici)
- gli atti o documenti che non danno origine ad un processo
- le offerte di prestazione non richieste
- gli scambi orari tra i dipendenti
- le circolari che si identificano con una registrazione a sé stante.

Firmato digitalmente da ROBERTO FRACCIA

Sono infine non soggetti a protocollazione espressamente individuati ai sensi dell'art. 41 "Documenti soggetti a registrazione particolare" che sono registrati su altri tipi di registri o repertori cartacei o informatici autorizzati.

Per quanto riguarda atti di carattere normativo è sempre obbligatorio il protocollo; ma nel caso di atti a carattere generale, come concorsi per alunni, corsi per il personale e manifestazioni o eventi locali, la loro diffusione avverrà tramite pubblicazione nell'area comunicazioni del sito senza essere protocollati.

Le comunicazioni sindacali non vengono protocollate, ma pubblicate sulla bacheca sindacale; se riguardano scioperi e assemblee vengono diffuse con circolare.

Le domande di messa a disposizione per supplenze vengono registrate a parte in un archivio informatico adibito allo scopo.

6.3 REGISTRAZIONE DI PROTOCOLLO DEI DOCUMENTI RICEVUTI E SPEDITI

La registrazione dei documenti ricevuti o spediti è effettuata in un'unica operazione. I requisiti necessari di ciascuna registrazione di protocollo sono:

a) numero di protocollo generato automaticamente dal sistema e registrato in forma non modificabile;
b) data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
c) mittente o destinatario dei documenti ricevuti o spediti, registrato in forma non modificabile;
d) oggetto del documento, registrato in forma non modificabile;
e) data e numero di protocollo dei documenti ricevuti, se disponibili;
f) impronta del documento informatico, se trasmesso per via telematica, registrato in forma non modificabile;
g) classificazione: categoria, classe, fascicolo (si veda titolario allegato);
h) assegnazione.

Inoltre possono essere aggiunti:

i) data di arrivo;
j) allegati (numero e descrizione);
k) estremi provvedimento, differimento dei termini di registrazione;
l) mezzo di ricezione/spedizione (lettera ordinaria, prioritaria, raccomandata, corriere, fax ecc):
m) ufficio competenza;
n) tipo documento;

Firmato digitalmente da ROBERTO FRACCIA

o) livello di riservatezza;
p) elementi identificativi del procedimento amministrativo, se necessario.

6.4 REGISTRAZIONE DEI DOCUMENTI INTERNI INFORMALI

Nei documenti interni informali sono inclusi tutti quei documenti di lavoro di natura non ufficiale, temporanea ed interlocutoria, a carattere informativo, operativo, preparatorio (ad es.: sono documenti che non possiedono carattere di particolare ufficialità, bozze, appunti, etc...).
Per questa tipologia di documenti che ha rilevanza solo interna, ci si avvale dei sistemi di comunicazione interna con possibilità di sottoscrizione e protocollazione, laddove il Responsabile di Gestione lo ritenga necessario.

6.5 SEGNATURA DI PROTOCOLLO

La segnatura di protocollo apposta o associata al documento è effettuata, contemporaneamente alla registrazione di protocollo, per mezzo di timbri.
I requisiti necessari di ciascuna segnatura di protocollo sono:

- codice identificativo dell'amministrazione, per protocolli informatici;
- codice identificativo dell'area organizzativa omogenea, per protocolli informatici;
- data di protocollo;
- numero di protocollo;
- indice di classificazione.

Per i documenti informatici trasmessi ad altre pubbliche amministrazioni, i dati relativi alla segnatura di protocollo sono contenuti un'unica volta, nell'ambito dello stesso messaggio, in un file conforme alle specifiche dell'Extensibile Markup Language (XML) e compatibile con Document Type Definition (DTD) e comprendono anche:

- oggetto del documento
- mittente/destinatario.

Inoltre possono essere aggiunti:

- persona o ufficio destinatari
- classificazione e fascicolazione di competenza
- identificazione degli allegati
- informazioni sul procedimento e sul trattamento

Firmato digitalmente da ROBERTO FRACCIA

6.6 ANNULLAMENTO DELLE REGISTRAZIONI DI PROTOCOLLO

Le registrazioni di protocollo, tutte o in parte, possono essere annullate con una specifica funzione del sistema di gestione informatica dei documenti e con autorizzazione del Responsabile della gestione documentale, a seguito di motivata richiesta scritta o per iniziativa dello stesso responsabile.
Le registrazioni annullate rimangono memorizzate nel database e sono evidenziate dal sistema. Il sistema, durante la fase di annullamento, registra gli estremi del provvedimento autorizzativo redatto dal Responsabile della gestione documentale. Sui documenti cartacei è apposto un timbro che riporta gli estremi del verbale di annullamento.

Il documento è conservato all'interno del fascicolo di competenza a cura del Responsabile del procedimento. Il Responsabile della gestione documentale mantiene, comunque, un'attività di controllo sull'operato dei Responsabili di procedimento.
Non è possibile annullare il solo numero di protocollo e mantenere valide le altre informazioni della registrazione.

6.7 MODIFICA DELLE REGISTRAZIONI DI PROTOCOLLO

Le registrazioni di protocollo, tutte o in parte, possono essere modificate con una specifica funzione del sistema di gestione informatica dei documenti e con autorizzazione del Responsabile della gestione documentale, a seguito di motivata richiesta scritta o per iniziativa dello stesso responsabile.
Le registrazioni modificate rimangono memorizzate nel database e sono evidenziate dal sistema. Il sistema, durante la fase di modifica, registra gli estremi del provvedimento autorizzativo redatto dal Responsabile della gestione documentale. Sui documenti cartacei è apposto un timbro che riporta gli estremi del verbale di annullamento. Sui documenti cartacei è apposto un timbro che riporta gli estremi del verbale di modifica.

Il documento è conservato all'interno del fascicolo di competenza a cura del Responsabile del procedimento. Il Responsabile della gestione documentale mantiene, comunque, un'attività di controllo sull'operato dei Responsabili di procedimento.
E' possibile modificare le sole registrazioni di protocollo che siano già state trasmesse al sistema di conservazione a norma, per mantenere traccia inalterabile di tutte le variazioni apportate.

6.8 DIFFERIMENTO DEI TERMINI DI PROTOCOLLAZIONE

La registrazione della documentazione pervenuta avviene nell'arco della giornata. Il responsabile del servizio, con apposito provvedimento motivato, può autorizzare la registrazione in tempi successivi, fissando un limite di tempo entro il quale i documenti devono essere protocollati.

Firmato digitalmente da ROBERTO FRACCIA

Ai fini giuridici i termini decorrono dalla data di ricezione riportata sul documento analogico tramite un apposito timbro; il sistema informatico mantiene traccia del ricevimento dei documenti.

6.9 REGISTRO GIORNALIERO ED ANNUALE DI PROTOCOLLO

Ogni giorno il sistema di gestione documentale genera in maniera automatica il registro giornaliero di protocollo informatico, che viene archiviato in una sezione apposita dell'archivio documentale informatico dell'Istituto.
Delle registrazioni del protocollo informatico è sempre possibile estrarre evidenza analogica.
Per quanto riguarda le procedure di conservazione della memoria informatica si veda anche la Sezione 12 (Conservazione e tenuta dei documenti)

6.10 REQUISITI MINIMI DI SICUREZZA DEL SISTEMA DI PROTOCOLLO INFORMATICO

Il sistema di protocollo informatico assicura:

- l'univoca identificazione ed autenticazione degli utenti;
- la protezione delle informazioni relative a ciascun utente nei confronti degli altri;
- la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirne l'identificazione.

Il sistema di protocollo informatico consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti.
Il sistema di protocollo informatico consente il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.
Le registrazioni di protocollo sono protette da modifiche non autorizzate; ogni modifica è tracciata e soggetta ad approvazione da parte del Responsabile.
Il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.

Il sistema di protocollo informatico è fornito dalla software house Nuvola come sistema SaaS ed è certificato AgID SaaS Marketplace.

6.11 REGISTRO DI EMERGENZA

All'inizio di ogni anno, il Responsabile della gestione documentale provvede a istituire il registro di emergenza su supporto cartaceo.

Firmato digitalmente da ROBERTO FRACCIA

Il Responsabile della gestione documentale autorizza lo svolgimento delle operazioni di protocollo su registro di emergenza, a norma dell'articolo 63 del DPR 445/2000, su supporto cartaceo da archiviare a cura del Responsabile della gestione documentale.
Il registro di emergenza su supporto cartaceo è archiviato presso la cassaforte nell'ufficio del DSGA.

6.12 FASCICOLI RISERVATI

Coerentemente alla normativa vigente in materia di protocollo informatico e gestione documentale, è opportuno specificare che alcuni protocolli possono essere classificati come riservati ed il relativo accesso non è consentito a tutti.
La concessione dell'accesso ai protocolli riservati avviene tramite profilatura specifica del singolo utente del sistema di gestione documentale.
Gli eventuali documenti cartacei relativi ai suddetti protocollo vengono conservati nell'ufficio del Dirigente Scolastico.

Firmato digitalmente da ROBERTO FRACCIA

SEZIONE VII – DOCUMENTAZIONE PARTICOLARE

7.1 DETERMINAZIONI DIRIGENZIALI, DECRETI E CONTRATTI

Determinazioni dirigenziali e decreti sono registrati al protocollo.
Il software di produzione e conservazione di questa tipologia particolare di documentazione consente di eseguire su di essi tutte le operazioni previste nell'ambito della gestione dei documenti e del sistema adottato per il protocollo informatico.
In particolare, il flusso di lavoro legato a queste tipologie documentali, prevede:

- firma elettronica da parte del Dirigente Scolastico
- protocollazione
- pubblicazione nella corrispondente sezione di Amministrazione Trasparente, come indicato dalle Linee Guida AgID

Ogni registrazione riporta:

- dati identificativi di ciascun atto (autore, destinatario, oggetto, data: generati in modo non modificabile);
- dati di classificazione;
- numero di repertorio progressivo annuale (generato in modo non modificabile).

I contratti del personale vengono gestiti attraverso la piattaforma SIDI e registrati successivamente all'interno del sistema di gestione documentale dell'Istituto.

7.2 DOCUMENTAZIONE DI GARE D'APPALTO

Qualora non effettuata con le procedure Mepa, la gestione delle offerte di gare d'appalto o altra documentazione da consegnarsi all'Istituto Scolastico in busta chiusa sono registrate al protocollo senza effettuarne l'apertura.
Dopo l'apertura della busta, a cura dell'Ufficio che gestisce la gara, verrà riportato su ciascun documento il medesimo numero di protocollo assegnato alla busta.
A tale scopo sono annotate le seguenti informazioni:

- denominazione dell'Istituto Scolastico
- data apertura busta
- data e numero di protocollo della busta.

Firmato digitalmente da ROBERTO FRACCIA

7.3 GESTIONE DELLE FATTURE

L'ufficio Contabilità è responsabile della gestione delle fatture attraverso la piattaforma SIDI (Sistema di Interscambio).
Le fatture vengono:

- scaricate dal sistema di interscambio
- importate nel sistema di gestione documentale
- protocollate
- classificate e archiviate
- inviate in conservazione a norma

7.4 DOCUMENTI INDIRIZZATI NOMINALMENTE AL PERSONALE DELL'ISTITUTO SCOLASTICO, LETTERE ANONIME E DOCUMENTI NON FIRMATI

La corrispondenza indirizzata nominativamente è regolarmente aperta e registrata al protocollo.
Le lettere anonime vengono protocollate, se intestate genericamente all'Istituto; se specificamente indirizzate, sono consegnate al destinatario, il quale ne potrà disporre la protocollazione.
Le lettere a firma illeggibile, delle quali non sia identificabile in altro modo il mittente, non si registrano a protocollo, ma si inviano al destinatario, il quale ne potrà disporre la protocollazione solo a seguito di eventuali accertamenti, indicando l'identità del mittente.

7.5 CORRISPONDENZA CON PIU' DESTINATARI E COPIE PER CONOSCENZA

Tutte le comunicazioni che abbiano più destinatari si registrano con un solo numero di protocollo. Se in uscita, i destinatari sono descritti nell'elenco dei destinatari associati al documento.
Si faranno copie informatiche dei documenti analogici prodotti/pervenuti di cui necessita la distribuzione interna all'Istituto.

7.6 ALLEGATI

Gli allegati che pervengono via e-mail vengono automaticamente archiviati all'interno del software di archiviazione documentale utilizzato: Nuvola.

Firmato digitalmente da ROBERTO FRACCIA

E’ inoltre possibile l’archiviazione di allegati alle registrazioni di protocollo; tali allegati possono essere gestiti all’interno del flusso di lavoro documentale e vengono archiviati con l’attribuzione dei dati minimi obbligatori.

7.7 DOCUMENTI DI COMPETENZA DI ALTRE AMMINISTRAZIONI

Qualora pervengano all’Istituto documenti di competenza di altre amministrazioni, questi verranno restituiti al destinatario. Se il documento viene erroneamente protocollato, il numero di protocollo sarà annullato ed il documento inviato al destinatario. Nel caso in cui il destinatario non sia individuabile, il documento sarà rimandato al mittente.

7.8 OGGETTI PLURIMI

Qualora un documento in entrata presenti più oggetti relativi a procedimenti diversi e pertanto da assegnare a più fascicoli, occorrerà produrre copie autentiche dello stesso documento e, successivamente, registrarle, classificarle e fascicolarle, indipendentemente una dall'altra.
Lo stesso principio deve essere utilizzato per la protocollazione di documentazione in partenza, pertanto si restituiranno al responsabile di procedimento documenti in uscita con più oggetti.

7.9 PRODUZIONE SERIALE DI DOCUMENTI SULLA BASE DI UN MODELLO GENERALE

Nel caso di produzione in serie di documenti base che abbiano destinatari multipli e parti minime variabili di contenuto (quali la diversità di importi, date, VOTI, ecc.), ogni copia generata serialmente seguirà un proprio flusso di lavoro indipendente dalle altre copie, oppure dipendente per alcune fasi comuni, come ad esempio la firma elettronica.
Sui documenti inviati ai destinatari, ai quali non si vuole apporre singolarmente la sottoscrizione, dovrà essere obbligatoriamente riportata l'indicazione del Responsabile del procedimento o del Sottoscrittore, preceduto dall'acronimo F.to e dalla seguente dicitura:
“La firma autografa è sostituita dall'indicazione del nome a norma del Dlgs n. 39/1993”.

7.10 MODELLI PUBBLICATI

Tutti i modelli di documenti pubblicati sul sito Internet o sulla rete Intranet dell'Istituto sono classificati secondo il piano di classificazione in uso. Non possono essere pubblicati modelli, formulari, etc. che non siano classificati e non contengano l'indicazione del settore/servizio o ufficio.

Firmato digitalmente da ROBERTO FRACCIA

7.11 TRASMISSIONI TELEMATICHE

Trasmissioni verso portali ministeriali

I documenti trasmessi e ricevuti dall'Istituto con immissione diretta sul server del destinatario (es: flussi delle attività didattiche, assenze del personale, contratti del personale, indice trimestrale di tempestività dei pagamenti, flussi di bilancio), non richiedono la produzione e la conservazione dell'originale cartaceo; tali documenti sono trasmessi senza firma digitale, in quanto inviati tramite linee di comunicazione sicure, riservate ad identificazione univoca attivati con singoli Enti destinatari.

Gli invii telematici sostituiscono integralmente gli invii cartacei della medesima documentazione.

Atti e provvedimenti amministrativi

Gli atti e provvedimenti amministrativi vengono pubblicati sul sito dell'Istituto nella sezione “Albo on line”, secondo quanto previsto dalla normativa vigente.

La pubblicazione di Atti all'Albo on line ha lo scopo di fornire presunzione di conoscenza legale degli stessi, a qualunque effetto giuridico specifico essa assolva (pubblicità, notizia, dichiarativa, costitutiva, integrativa dell'efficacia, etc.). Sono soggetti alla pubblicazione all'Albo Pretorio on line tutti gli atti per i quali la legge ne prevede l'adempimento.

Salvo casi specifici la durata è di quindici giorni.

Fatture elettroniche

Col decreto 3 aprile 2013, n. 55 del Ministero dell'Economia e delle Finanze entrato in vigore il 6 giugno 2013, è stato approvato il regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica, ai sensi dell'articolo 1, commi da 209 a 213, della legge 24 dicembre 2007, n 244.

Dal 6 giugno 2014 i fornitori devono produrre, nei confronti dell'Istituto, esclusivamente fatture elettroniche, nel rispetto delle specifiche tecniche reperibili sul sito www.fatturarapa.gov.it.

Le fatture elettroniche così ricevute vengono gestite per il tramite di apposite funzioni del sistema SIDI, che provvede automaticamente a ricevere le fatture indirizzate dai fornitori all'Istituto, riconoscibili tramite il codice univoco di fatturazione.

Dalla data di ricezione decorrono i termini per il pagamento della fattura, pari a 30 giorni, salvo patti contrari tra le parti.

Le fatture, in prima fase, vengono protocollate con ordinaria modalità.

Il DSGA, ovvero un suo delegato, è responsabile della gestione delle fatture per l’intero ciclo di lavorazione.

Il DSGA, ovvero un suo delegato, provvede a:

- riconoscere/rifiutare la fattura mediante il sistema SIDI entro 15 giorni dalla ricezione della medesima;

Firmato digitalmente da ROBERTO FRACCIA

- adottare gli atti di spesa, avvalendosi delle usuali funzioni del programma utilizzato per la gestione del Bilancio dell'Istituto, a estinzione totale/parziale del debito corrispondente alla fattura;
- effettuare la conservazione sostitutiva delle fatture elettroniche caricate nel sistema di gestione documentale.

In base alla legge n. 190/2012, l'Istituto è tenuto a rendere noti all'ANAC, tutti i dati relativi all'espletamento di gare e bandi. Annualmente (entro il 31 gennaio dell'anno successivo a quello di riferimento) i dati devono essere trasferiti direttamente in formato aperto utilizzando lo standard XML. L'Istituto ha predisposto sul proprio sito web una sezione apposita denominata "*Amministrazione Trasparenza/ Bandi di gara e contratti*", all'interno della quale vengono caricati i file XML che descrivono le gare espletate.
L'indirizzo viene comunicato via PEC all'Autorità, in modo che possa provvedere al recupero automatico delle informazioni contenute.

Trasmissione verso sistemi centralizzati
Tutti i documenti (DURC, denunce di infortunio, certificati di malattia, …) che sono ricevuti dall'Istituto con immissione diretta dei dati via web nel sistema dell'ente/organizzazione destinatario sostituiscono integralmente gli invii cartacei della medesima documentazione.
I documenti possono essere trasmessi senza firma digitale in quanto inviati tramite linee di comunicazione sicure, riservate e ad identificazione univoca, attivate con i singoli destinatari.

7.12 DOCUMENTI INFORMATICI CON CERTIFICATO DI FIRMA SCADUTO O REVOCATO

Nel caso in cui l'Istituto riceva documenti informatici firmati digitalmente il cui certificato di firma risulta scaduto o revocato prima della sottoscrizione, questi verranno protocollati e inoltrati al responsabile di procedimento che farà opportuna comunicazione al mittente.

7.13 DOCUMENTI RICEVUTI VIA FAX

La normativa vigente prevede l'esclusione della corrispondenza via fax fra pubbliche amministrazioni. La trasmissione di documenti via fax con cittadini o altri soggetti privati non aventi l'obbligo di comunicazione in forma telematica con la pubblica amministrazione richiede la registrazione di protocollo.
L'Istituto acquisisce i fax ricevuti tramite scanner, secondo la procedura individuata nella Sezione XI.
Di norma al fax non segue mai l'originale. Qualora successivamente arrivasse anche l'originale del documento, questo sarà considerato allegato alla registrazione di protocollo e sarà attribuito lo stesso numero di protocollo.

Firmato digitalmente da ROBERTO FRACCIA

7.14 DOCUMENTAZIONE PRODOTTA TRAMITE APPOSITI GESTIONALI

L'Istituto è dotato di software gestionale in grado di acquisire automaticamente la registrazione di protocollo, mediante specifico collegamento tra i sistemi, nell'ambito di procedimenti riguardanti determinate attività. Il software gestionale consente la registrazione automatica di protocollo solo dopo opportuna configurazione del procedimento che si intende automatizzare.

7.15 GESTIONE DELLE PASSWORD

Il sistema garantisce la gestione e conservazione delle password di accesso al sistema stesso e ai servizi online degli utenti interni e esterni secondo le modalità descritte nel Piano per la sicurezza informatica (Allegato 10).

Firmato digitalmente da ROBERTO FRACCIA

SEZIONE VIII – ASSEGNAZIONE DEI DOCUMENTI

8.1 ASSEGNAZIONE

L'assegnazione dei documenti ai responsabili e ai referenti di procedimento è effettuata dal Responsabile della gestione documentale sulla base degli uffici definiti nella AOO.
L'assegnatario può a sua volta smistare i documenti a unità organizzative afferenti attraverso apposita funzione del software di gestione documentale.
Qualora sia necessario consegnare un documento analogico originale, questo dovrà essere consegnato all'ufficio che risulta assegnatario nel sistema di gestione documentale.
Le assegnazioni per conoscenza devono essere effettuate tramite il sistema di gestione documentale.

8.2 MODIFICA DELLE ASSEGNAZIONI

Nel caso di un'assegnazione errata, l'Ufficio che riceve il documento lo rinvia al Responsabile della gestione documentale, che provvederà alla riassegnazione per poi trasmetterlo al nuovo assegnatario. La responsabilità del mancato rispetto di quanto sopra descritto è da attribuirsi all'Ufficio che non ha rimandato al Responsabile della gestione documentale.
Delle operazioni di riassegnazione e degli estremi del Provvedimento di autorizzazione è lasciata traccia nel sistema informatico di gestione dei documenti.
Il software di gestione documentale provvederà automaticamente a rendere visibile il documento riassegnato al destinatario di competenza.

Firmato digitalmente da ROBERTO FRACCIA

SEZIONE XI – ARCHIVIAZIONE, CLASSIFICAZIONE E FASCICOLAZIONE DEI DOCUMENTI

9.1 CLASSIFICAZIONE DEI DOCUMENTI

Gli addetti al servizio di ricezione eseguono la prima classificazione del documento e provvedono ad inserirlo nell'archivio digitale dove verranno attribuiti al documento i campi di ricerca e metadati, necessari, per la corretta gestione (l'inserimento è automatico per i documenti informatici ricevuti via mail; manuale con parametri preimpostati e/o impostabili dal singolo operatore per tutti gli altri casi). I campi di ricerca e metadati sono consultabili nella sezione “Proprietà “del raccoglitore cliccando al di sopra di esso con tasto destro del mouse.
Gli addetti al servizio di ricezione, inoltre, provvedono ad inviare il documento tramite uno specifico flusso di lavoro al Responsabile della Gestione che:

- esegue una verifica di congruità;
- in caso di errore ne dà immediata comunicazione all'addetto che ha ricevuto il documento;
- in caso di verifica positiva, assegna all'Area Utente responsabile l'operazione di presa in carico del documento e provvede ad affidare la gestione della pratica, della fascicolazione e delle altre fasi di lavorazione specifiche della pratica trattata.

Al fine della corretta presa in carico dei documenti, tutto il personale amministrativo profilato per l’accesso alle Aree Utenti di pertinenza ha il compito di consultare giornalmente l'applicativo in dotazione ed avviare i processi di gestione documentale assegnati.
I tempi di lavorazione standard delle pratiche sono dichiarati nei modelli di procedimento definiti all’interno del sistema di gestione documentale.

9.2 FORMAZIONE E IDENTIFICAZIONE DEI FASCICOLI

Tutti i documenti registrati al protocollo informatico e classificati, indipendentemente dal supporto sul quale sono forniti, sono riuniti in fascicoli elettronici, attraverso le opportune funzioni del sistema di gestione documentale.

La formazione di un nuovo fascicolo è effettuata dal Responsabile del procedimento ed avviene attraverso l'operazione di apertura, oppure, se informatica, regolata dal manuale operativo del sistema, che prevede la registrazione sul repertorio/elenco dei fascicoli o nel sistema informatico delle seguenti informazioni:

- categoria e classe del titolario di classificazione;

Firmato digitalmente da ROBERTO FRACCIA

- numero del fascicolo (la numerazione dei fascicoli è annuale, assegnata automaticamente dal sistema ed indipendente per ogni classe)
- oggetto del fascicolo;
- intestatario del fascicolo;
- data di apertura;
- ufficio a cui è assegnato;
- responsabile del procedimento;
- tempo previsto di conservazione.

All'interno dei fascicoli è possibile creare dei sotto-fascicoli.

Il sistema di protocollo informatico provvede, automaticamente, ad aggiornare il repertorio/elenco dei fascicoli.

9.3 PROCESSO DI FORMAZIONE DEI FASCICOLI

I documenti in arrivo sono fascicolati dai Responsabili di Procedimento. Il software di gestione documentale non permette la gestione della documentazione senza che prima la stessa venga fascicolata.
I documenti in partenza sono fascicolati dai Responsabili di Procedimento che hanno cura di inserirli fisicamente nel fascicolo, in caso di documenti cartacei; nel caso di documenti informatici, il sistema provvede, automaticamente, dopo l'assegnazione del numero di fascicolo, ad inserire il documento nel fascicolo informatico stesso. I documenti pertanto verranno protocollati già con l'indicazione del numero/identificativo di fascicolo. Ai documenti informatici prodotti nei software gestionali tramite l'utilizzo di modelli standard, sono associati automaticamente dal sistema di gestione documentale i metadati minimi del fascicolo informatico
Se il documento processato prevede l'avvio di un nuovo affare, i Responsabili di Procedimento aprono un nuovo fascicolo (con le procedure sopra descritte)

9.4 FASCICOLO IBRIDO

Il fascicolo ibrido è composto da documenti formati su due supporti, quello cartaceo e quello informatico, afferenti ad un affare o a un procedimento amministrativo che dà quindi origine a due unità archivistiche di conservazione differenti; l'unitarietà del fascicolo è garantita dal sistema mediante l'indice di classificazione ed il numero di repertorio.
Alla chiusura del fascicolo, ai sensi del Codice dell'Amministrazione digitale (D. Lgs.n.82/2005), sono previste due possibilità':

- stampa e copia conforme e cartacea dell'originale informatico;
- scansione e copia conforme informatica dell'originale cartaceo.

Firmato digitalmente da ROBERTO FRACCIA

È compito dei Responsabili di procedimento scegliere la soluzione ritenuta più idonea. Il Responsabile della gestione documentale mantiene, comunque, un'attività di controllo sulle procedure suddette.
Saranno quindi i Responsabili di Procedimento ad apporre la propria firma autografa in caso di produzione di copie conformi cartacee oppure la propria firma digitale/avanzata in caso di copie conformi informatiche.
I documenti originali informatici saranno sottoposti al procedimento di conservazione sostitutiva. I documenti originali cartacei saranno inviati in archivio di deposito in apposite scatole contenenti l'indicazione della classificazione e dell'anno di produzione/ricevimento.

9.5 PROCESSO DI GESTIONE E ARCHIVIAZIONE

Le Istituzioni scolastiche definiscono nel proprio manuale la gestione degli archivi rifacendosi alla seguente articolazione archivistica:

- archivio corrente: riguarda i documenti necessari alle attività correnti;
- archivio di deposito: riguarda i documenti ancora utili per finalità amministrative o giuridiche, ma non più indispensabili per la trattazione delle attività correnti;
- archivio storico: riguarda i documenti storici selezionati per la conservazione permanente.

L'archiviazione, per alcune fattispecie di documenti, può avvenire presso archivi gestiti a livello centrale dal Ministero dell'Istruzione. A titolo esemplificativo, le istanze che pervengono alla scuola mediante il Servizio Istanze OnLine, che permette di effettuare in modalità digitale la presentazione delle domande connesse ai principali procedimenti amministrativi dell'Amministrazione, sono protocollate in ingresso dalla AOO appositamente costituita presso il Ministero dell'Istruzione, e sono rese disponibili alle Istituzioni scolastiche.
Tenendo conto che l'archivio corrente è organizzato su base annuale e che il passaggio dall'archivio corrente all'archivio di deposito è possibile solo qualora il fascicolo contenga documenti afferenti a procedimenti conclusi,

9.6 TENUTA DEI FASCICOLI DELL'ARCHIVIO CORRENTE

I fascicoli dell'archivio corrente sono formati a cura dei responsabili o dei referenti di procedimento e conservati, fino al trasferimento nell'archivio di deposito, presso gli uffici di competenza.

Firmato digitalmente da ROBERTO FRACCIA

9.7 MOVIMENTAZIONE DEI FASCICOLI DA E VERSO L'ARCHIVIO

Annualmente, gli uffici devono redigere un apposito piano di versamento costituito dall'elenco dei fascicoli relativi ad affare ed a procedimenti conclusi, a seguito del quale consegneranno al Responsabile della gestione documentale i fascicoli da depositare nell'archivio di deposito.
Periodicamente e secondo un apposito piano di versamento (di norma una volta all'anno), il Responsabile di procedimento deve consegnare all'archivio i fascicoli relativi ad affari e a procedimenti amministrativi non più necessari ad una trattazione corrente corredati dal relativo elenco di versamento. Le serie Archivistiche ed i relativi registri o repertori sono conservati per cinque anni presso la struttura che cura i rispettivi procedimenti; trascorso tale termine vengono versati all'Archivio di deposito.

È fatto divieto di prelevare, anche temporaneamente, gli atti dall'archivio di deposito senza l'autorizzazione del Responsabile della gestione documentale e la collocazione di apposita scheda di prelevamento.
Il trasferimento deve essere attuato rispettando l'organizzazione che i fascicoli avevano nell'archivio corrente.

Prima di effettuare il conferimento di cui sopra, il Responsabile del procedimento verifica:

- l'effettiva conclusione ordinaria della pratica
- l'effettiva trascrizione dell'esaurimento della pratica nel registro di repertorio dei fascicoli;
- il corretto aggiornamento della data di chiusura sulla camicia del fascicolo (in caso di documentazione cartacea). In caso di documentazione informatica, la data di chiusura del fascicolo elettronico viene assegnata automaticamente dal software di gestione documentale in uso;
- lo scarto di eventuali copie e fotocopie di documentazione passibile di scarto al fine di garantire la presenza di tutti e soli documenti pertinenti alla pratica.

I fascicoli del personale sono conservati presso la competente U.O. e devono essere versati all'archivio di deposito dopo un anno dalla cessazione (e conclusione dei relativi adempimenti) dal servizio del dipendente.

Firmato digitalmente da ROBERTO FRACCIA

SEZIONE X – SPEDIZIONE DEI DOCUMENTI DESTINATI ALL'ESTERNO

10.1 SPEDIZIONE DI DOCUMENTI ANALOGICI

I documenti da spedire sono trasmessi all'incaricato della spedizione in busta chiusa, completi dalla firma autografa del Responsabile della gestione documentale, della classificazione e del numero di fascicolo, nonché delle eventuali indicazioni necessarie ad individuare il procedimento amministrativo di cui fanno parte. Nel caso di spedizione che utilizzi pezze di accompagnamento (raccomandata o altro mezzo di spedizione tracciata), queste devono essere compilate a cura dell'ufficio produttore.
Eventuali situazioni di urgenza che modifichino la procedura descritta devono essere valutate ed autorizzate dal Responsabile della gestione documentale.

10.2 SPEDIZIONE DEI DOCUMENTI INFORMATICI

La spedizione dei documenti informatici avviene all'interno del sistema informatico di gestione dei documenti, dopo che gli stessi sono stati classificati, fascicolati e protocollati con le procedure adottate dal manuale operativo stesso, e comunque secondo i seguenti criteri generali:

- i documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari abilitato alla ricezione della posta per via elettronica; se l'indirizzo è abilitato alla ricezione di posta elettronica certificata, la trasmissione viene effettuata tramite casella di posta elettronica certificata
- ogni qualvolta sia possibile, per la spedizione l'amministrazione si avvale di una casella di posta elettronica certificata
- l'Ufficio protocollo provvede:
    - a effettuare l'invio elettronico utilizzando i servizi di autenticazione e marcatura temporale forniti dal sistema informatico di gestione documentale
    - a verificare l'avvenuto recapito dei documenti spediti per via elettronica
    - ad archiviare le ricevute elettroniche collegandole alle registrazioni di protocollo o al fascicolo elettronico interessato dal procedimento.

Per la riservatezza delle informazioni contenute nei documenti elettronici, chi spedisce si attiene a quanto prescritto dall'articolo 49 del CAD dlgs 235/10.

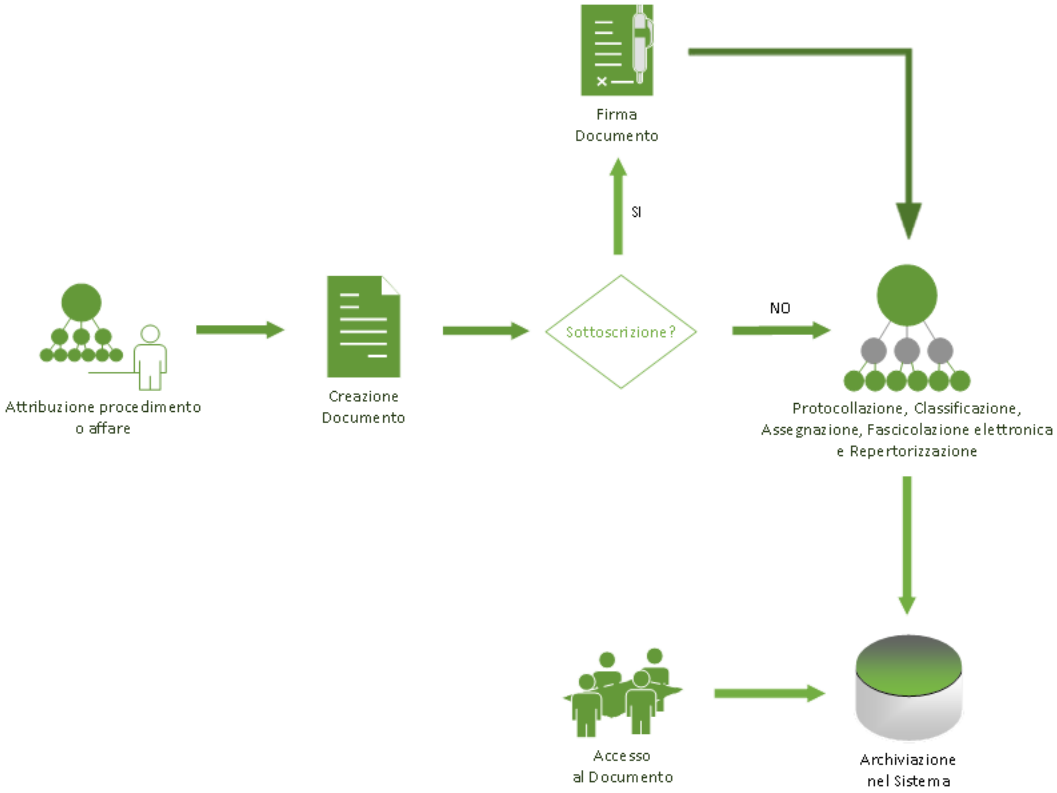
Firmato digitalmente da ROBERTO FRACCIA

La spedizione di documenti informatici al di fuori dei canali istituzionali descritti è considerata una mera trasmissione di informazioni senza che a queste l'amministrazione riconosca un carattere giuridico-amministrativo che la impegni verso terzi.

10.3 TRASMISSIONE DI DOCUMENTI INFORMATICI IN INTEROPERABILITA' E IN COOPERAZIONE APPLICATIVA (TRASMISSIONI TELEMATICHE)

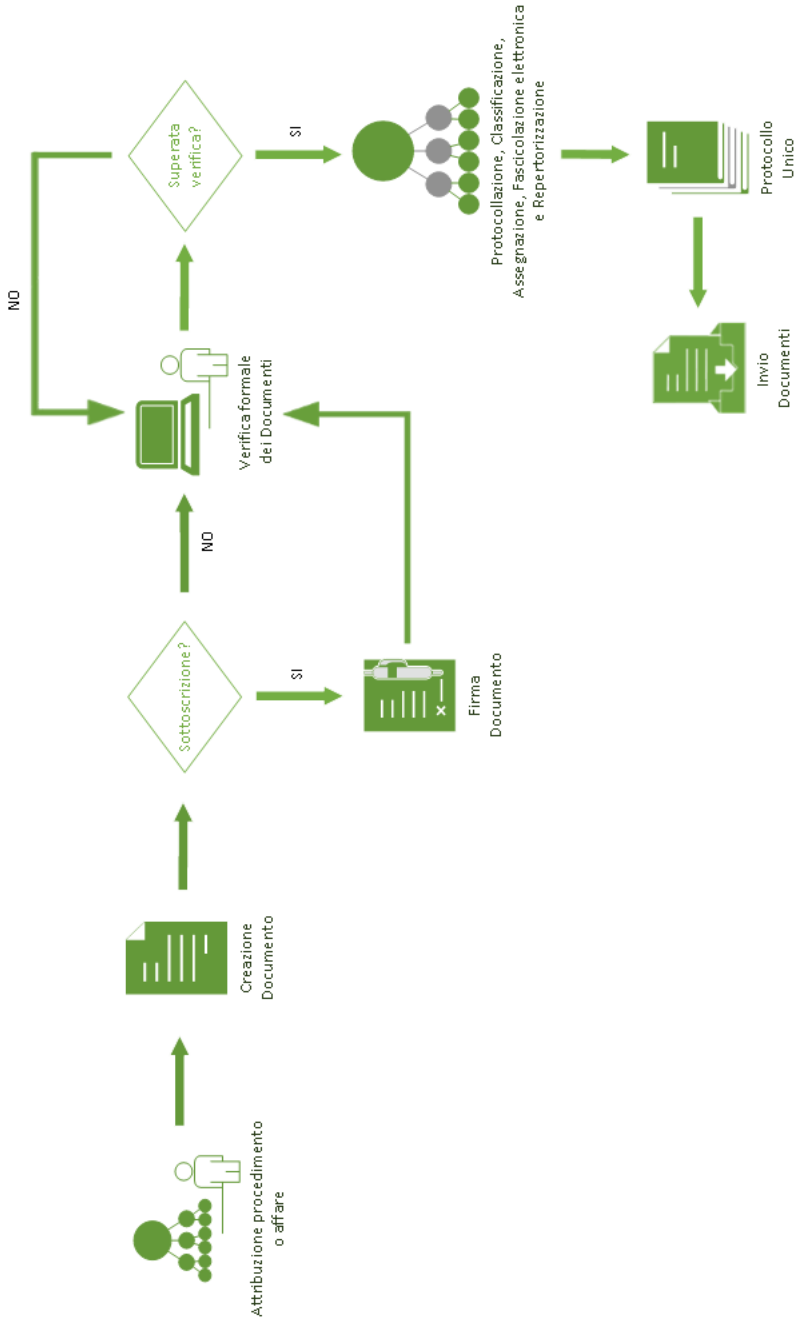
L'Istituto effettua lo scambio di informazioni, dati e documenti soggetti a registrazione di protocollo attraverso messaggi trasmessi in cooperazione applicativa.
I documenti sono trasmessi dall'Istituto con immissione diretta dei dati nel sistema informatico dell'ente/organizzazione destinatario, senza la produzione e conservazione dell'originale cartaceo. documentazione
I documenti possono essere trasmessi senza firma digitale in quanto inviati tramite linee di comunicazione sicure, riservate e ad identificazione univoca attivati con i singoli enti destinatari.
Per maggiori dettagli si veda la sezione 7.11

10.4 FLUSSO DI LAVORO DEI DOCUMENTI INTERNI INFORMALI



Firmato digitalmente da ROBERTO FRACCIA

10.5 FLUSSO DI LAVORO DEI DOCUMENTI IN USCITA



Firmato digitalmente da ROBERTO FRACCIA

SEZIONE XI – SCANSIONE DI DOCUMENTI SU SUPPORTO CARTACEO

11.1 DOCUMENTI SOGGETTI A SCANSIONE

I documenti cartacei che pervengono all'Organizzazione per mezzo di posta ordinaria, fax o tele- gramma vengono sottoposti ad un processo di dematerializzazione tramite scansione ed acquisizione di immagine.

11.2 PROCESSO DI SCANSIONE

Le copie per immagine sono prodotte mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto. Le copie per immagine di uno o più documenti analogici possono essere sottoscritte con firma digitale o firma elettronica qualificata da chi effettua la copia. Affinché le copie non siano disconoscibili esse devono essere firmate da un pubblico ufficiale.
Dei documenti analogici ricevuti viene effettuata copia conforme digitale e il documento originale viene trattenuto presso la postazione di protocollo24.
La copia informatica di un documento analogico, è acquisita nel sistema mediante processi e strumenti che assicurino che il documento informatico abbia contenuto identico a quello del documento analogico da cui è tratto.
L'unitarietà è garantita dal sistema mediante il numero di protocollo, l'indice di classificazione e il numero di repertorio del fascicolo.

Il processo di scansione si articola di massima nelle seguenti fasi:

- acquisizioni delle immagini in modo che ad ogni documento, anche composto da più fogli, corrisponda ad un unico file in un formato standard abilitato alla conservazione (PDF/PDF-A)
- verifica della leggibilità delle immagini acquisite e della loro esatta corrispondenza con gli originali cartacei
- collegamento del documento alla registrazione di protocollo, in modo non modificabile
- memorizzazione e archiviazione del documento, in modo non modificabile.
- autenticazione, attraverso sottoscrizione digitale, di ogni singolo file, o comunque secondo quanto previsto dalla legge

Firmato digitalmente da ROBERTO FRACCIA

I documenti analogici soggetti a riproduzione sostitutiva si conservano nell'archivio dell'ente/organizzazione fino a procedimento legale di scarto.

Firmato digitalmente da ROBERTO FRACCIA

SEZIONE XII – CONSERVAZIONE E TENUTA DEI DOCUMENTI

12.1 CONSERVAZIONE DEI DOCUMENTI INFORMATICI

La documentazione corrente è conservata a cura del responsabile del procedimento fino al trasferimento in archivio di deposito.
A far data dal 11.09.2021, i documenti informatici dell'Istituto sono conservati a cura del Responsabile della Conservazione in modo conforme a quanto previsto dalle Linee Guida AGID del 2020.
Al termine delle operazioni di archiviazione, registrazione e segnatura di protocollo, il Responsabile della Conservazione provvede quindi, in collaborazione con i Sistemi Informativi e con il supporto della tecnologia disponibile, a conservare i documenti informatici in modo non modificabile e garantendone la leggibilità nel tempo, in appositi archivi informatici e a controllare periodicamente a campione la leggibilità dei documenti stessi.
L'intervento del Responsabile della conservazione provvede alla conservazione integrata dei documenti e delle informazioni di contesto generale (metadati), prodotte sia nelle fasi di gestione sia in quelle di conservazione degli stessi.

12.2 CENSIMENTO DEI DEPOSITI DOCUMENTARI, DELLE BANCHE E DEI SOFTWARE

Ogni anno il Responsabile della gestione documentale provvede ad effettuare il censimento dei depositi documentari, dei registri particolari, delle banche dati e dei software di gestione documentale in uso all'ente, per programmare i versamenti dei documenti cartacei all'archivio di deposito e per verificare la corretta conservazione dei documenti informatici.

12.3 SELEZIONE E CONSERVAZIONE DEI DOCUMENTI

Ogni anno, in base al massimario di scarto, viene effettuata la procedura di selezione della documentazione da proporre allo scarto e attivato il procedimento amministrativo di scarto documentale con l'invio della proposta alla competente Soprintendenza archivistica e bibliografica di competenza.
I fascicoli non soggetti a operazioni di scarto sono trasferiti nell'archivio storico per la conservazione permanente, sia essa analogica o digitale. Il manuale di gestione e i relativi aggiornamenti devono essere conservati integralmente e perennemente nell'archivio

Firmato digitalmente da ROBERTO FRACCIA

dell'ente. Il piano di conservazione dell'archivio, sia esso cartaceo che informatico, comprende il Titolario di classificazione e il Massimario di scarto. Si rinvia allo specifico **Massimario di scarto** adottato dall'Istituto per la conservazione dei documenti informatici, il cui scarto è ivi disciplinato (**Allegato 9**).

12.4 MEMORIZZAZIONE DEI DATI E SALVATAGGIO DELLA MEMORIA INFORMATICA

I dati e i documenti informatici sono memorizzati nel sistema di gestione documentale al termine delle operazioni di registrazione.

12.5 PACCHETTI DI VERSAMENTO

Il Responsabile della gestione documentale/conservazione assicura la trasmissione del contenuto del pacchetto di versamento al sistema di conservazione secondo le modalità operative definite nel Manuale di conservazione (**Allegato 13**).
Il Responsabile della conservazione genera il rapporto di versamento relativo ad uno o più pacchetti di versamento e una o più impronte relative all'intero contenuto del pacchetto, secondo le modalità descritte nel Manuale di conservazione.

12.6 CONSERVAZIONE IN OUTSOURCING

L'ente/organizzazione, per la conservazione di tutto l'archivio documentale si avvale del sistema di conservazione fornito da Aruba.

Le modalità di conservazione e accesso ai documenti, analogici o digitali, sono specificate con riferimento al Manuale di conservazione dell'outsourcer (Allegato n. 13).

Il Responsabile della conservazione dell'ente/organizzazione vigila affinché il soggetto individuato come conservatore esterno provveda alla conservazione integrata dei documenti e delle informazioni di contesto generale, prodotte sia nelle fasi di gestione sia in quelle di conservazione degli stessi.

12.7 CONSERVAZIONE A NORMA

La Scuola, ai sensi dell'art. 5 comma 3 delle Regole tecniche per la conservazione, si affida ad un ente conservatore accreditato esterno, per la conservazione dei propri documenti.

Firmato digitalmente da ROBERTO FRACCIA

La Scuola si avvale della soluzione di conservazione a norma messa a disposizione da Nuvola che si interfaccia con un conservatore a norma accreditato specifico: Aruba.
Le regole tecniche in materia di conservazione a norma sono descritte nel Manuale di Conservazione del conservatore a norma specificato qui sopra (**Allegato 13**)

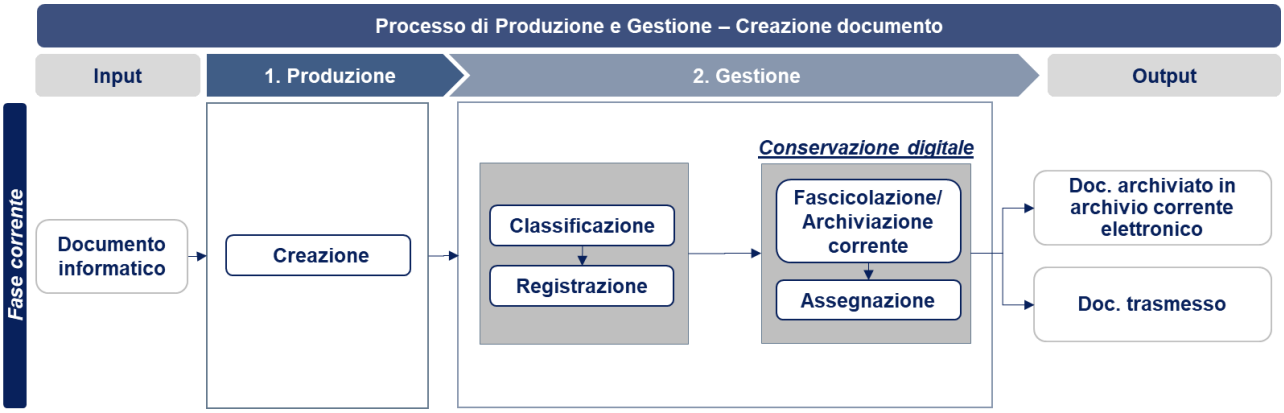
Firmato digitalmente da ROBERTO FRACCIA

SEZIONE XIII – SCHEMA FLUSSI DI LAVORO

13.1 PROCESSO DI ACQUISIZIONE DOCUMENTO INFORMATICO

13.2 PROCESSO DI ACQUISIZIONE DOCUMENTO CARTACEO

13.3 PROCESSO DI CREAZIONE DOCUMENTO



Firmato digitalmente da ROBERTO FRACCIA

13.4 PROCESSO DI CONSERVAZIONE DOCUMENTO

Firmato digitalmente da ROBERTO FRACCIA

SEZIONE XIV – DISPOSIZIONI FINALI

14.1 APPROVAZIONE

Il manuale viene approvato dal Consiglio d'Istituto, su proposta del Dirigente Scolastico.

14.2 REVISIONE

Tenuto conto del carattere dinamico del processo di dematerializzazione e della costante evoluzione dei sistemi di gestione documentale, il Dirigente Scolastico può provvedere alle modifiche del manuale ritenute maggiormente idonee a garantire l'adeguamento delle procedure e dei sistemi informativi alla normativa vigente.
Se sono state apportate modifiche al manuale, con cadenza almeno annuale il Dirigente sottopone la versione rivista del manuale di gestione al Consiglio d'Istituto.
Sono escluse dal passaggio in Consiglio di Istituto le modifiche apportate agli aggiornamenti degli incarichi, di cui all'**Allegato 16**, che non comportano cambiamenti strutturali al presente Manuale e che l'Istituto avrà cura di aggiornare entro il 31 dicembre di ogni anno.

14.3 PUBBLICAZIONE

Il presente manuale è pubblicato sul sito web dell'Istituzione scolastica, nella sezione Amministrazione Trasparente. Per tutto quanto non espressamente previsto dal presente Manuale, si rinvia alle linee guida AGID (**Allegato 4**), al CAD e alle altre norme attuative.

Firmato digitalmente da ROBERTO FRACCIA

SEZIONE XV – ELENCO ALLEGATI

15.1 ELENCO ALLEGATI

Di seguito gli allegati che completano il presente Manuale di Gestione Documentale dell'Istituto:

- Allegato 1: Funzionigramma e Unità Organizzative
- Allegato 2: registrazioni di protocollo particolari
- Allegato 3: conformità protocollo informatico
- Allegato 4: Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici
- Allegato 5: Elenco dei formati accettati
- Allegato 6: Tipologie particolari di documenti
- Allegato 7: Tipologie di fascicoli elettronici
- Allegato 8: Tipologie di classificazione documentale
- Allegato 9: Massimario di scarto
- Allegato 10: Piano per la sicurezza informatica
- Allegato 11: Regolamento di accesso agli atti
- Allegato 12: Piano di classificazione e Titolario
- Allegato 13: Manuale di Conservazione a cura del Conservatore
- Allegato 14: Formati di file e riversamenti
- Allegato 15: Delibera di approvazione del Manuale di Gestione Documentale
- Allegato 16: Modello per l'aggiornamento degli incarichi

Firmato digitalmente da ROBERTO FRACCIA

- Allegato 17: Linee guida per la gestione documentale del Ministero dell'Istruzione
- Allegato 18: Format di manuale per la gestione dei flussi documentali a cura del Ministero dell'Istruzione

Firmato digitalmente da ROBERTO FRACCIA

ISTITUTO COMPRENSIVO STATALE
"ADA NEGRI"
Via Don Milani 4 - 20086 MOTTA VISCONTI (MILANO)
Tel./Fax02.90000266
E- mail : miic872009@istruzione.it - miic872009@pec.istruzione.it
www.icmottavisconti.edu.it
C.F. 90015610158 – C.M. MIIC872009

FUNZIONIGRAMMA

FUNZIONE	INCARICATO
DATA PROTECTION OFFICER (DPO)	FERDINANDO BASSI
RESPONSABILE DELLA CONSERVAZIONE	DIRETTORE SS.GG.AA. Laura Gilardi
RESPONSABILE TRATTAMENTO DATI PERSONALI	DIRETTORE SS.GG.AA. Laura Gilardi
RESPONSABILE DEL PROTOCOLLO	DIRETTORE SS.GG.AA. Laura Gilardi
RESPONSABILE DEL PROCEDIMENTO	DIRETTORE SS.GG.AA. Laura Gilardi

Firmato digitalmente da ROBERTO FRACCIA

UNITA' ORGANIZZATIVE PRESENTI NELLA AOO

Nell'unica AOO dell'Istituto sono presenti le seguenti unità organizzative:

- Ufficio di presidenza
- Ufficio del D.S.G.A.
- Ufficio Didattica
- Ufficio Personale
- Ufficio Contabilità
- Ufficio Magazzino e Protocollo
- Ufficio Affari Generali

Firmato digitalmente da ROBERTO FRACCIA

REGISTRAZIONI DI PROTOCOLLO PARTICOLARI

I seguenti documenti:

- comunicazioni ordinarie alle famiglie da parte dei Coordinatori di classe e dei moduli;
- registrazioni in elenchi e albi tenuti dall'Istituto;
- delibere degli Organi Collegiali, determine dirigenziali, mandati, reversali, egistri dei verbali degli Organi Collegiali, registro degli accessi, contratti;
- decreti e ordinanze;
- verbali della polizia locale e altri tipi di verbalizzazioni previsti dalla legge o da regolamenti;

se sono documenti già soggetti a registrazione particolare da parte dell'Istituto possono non essere registrati al protocollo. Il software di produzione e conservazione di questa tipologia particolare di documentazione deve consentire di eseguire su di essi tutte le operazioni previste nell'ambito della gestione dei documenti e del sistema adottato per il protocollo informatico

Firmato digitalmente da ROBERTO FRACCIA

POLITICA INTEGRATA DELLA QUALITA' E DELLA SICUREZZA DELLE INFORMAZIONI

Motivazione

MADISOFT S.P.A., data la natura delle proprie attività, considera la qualità e la sicurezza delle informazioni un fattore irrinunciabile per la protezione del proprio patrimonio informativo ed un fattore di valenza strategica facilmente trasformabile in vantaggio competitivo.

Per quanto riguarda la qualità, essa costituisce il riferimento generale per la gestione di tutte le attività aventi influenza sui processi dell'Organizzazione. Tutto il Personale è tenuto a basare le proprie attività sui principi contenuti nella presente politica in un'ottica di continuo miglioramento tecnico, economico e qualitativo.

Attraverso l'impostazione del Sistema Garanzia Integrato, in conformità alle norme UNI EN ISO 9001 e serie di norme ISO 27001, vogliamo migliorare la nostra immagine in materia di qualità e sicurezza delle informazioni, le performance aziendali e le relazioni con i nostri stakeholder. Con la Certificazione del Sistema di Gestione Integrato da parte di un Istituto accreditato a livello internazionale vogliamo inoltre dare garanzia a tutti i Clienti delle nostre capacità di erogare dei servizi di elevato standard sia in termini qualitativi che di sicurezza delle informazioni.

La direzione svolge direttamente il ruolo di Rappresentante della Direzione

Obiettivi

L'obiettivo del Sistema di Gestione Integrato per la Qualità e per la Sicurezza delle Informazioni di MADISOFT S.P.A. è di garantire un adeguato livello di sicurezza dei dati e delle informazioni nell'ambito della progettazione, sviluppo ed erogazione dei servizi aziendali, attraverso l'identificazione, la valutazione ed il trattamento dei rischi ai quali i servizi stessi sono soggetti.

Inoltre, la Direzione ha fissato i seguenti obiettivi generali:

- disporre di un'organizzazione certificata;
- migliorare continuamente la soddisfazione dei Clienti e le aspettative degli Stakeholder;
- coinvolgere creativamente ed organizzativamente il Personale
- rispettare le norme applicabili sia di natura cogente che volontaria
- disporre di un parco fornitori affidabili ed efficienti;
- migliorare continuamente i processi di erogazione del servizio;
- disporre di indicatori di monitoraggio che permettano di misurare periodicamente il grado di soddisfacimento degli obiettivi suddetti, anche in ottica di miglioramento continuo.

Il Sistema di Gestione Integrato per la Sicurezza delle Informazioni definisce un insieme di misure organizzative, tecniche e procedurali a garanzia del soddisfacimento dei sottoelencati requisiti di sicurezza di base:

- Riservatezza, ovvero la proprietà dell'informazione di essere nota solo a chi ne ha i privilegi

Firmato digitalmente da ROBERTO FRACCIA

- Integrità, ovvero la proprietà dell'informazione di essere modificata solo ed esclusivamente da chi ne possiede i privilegi
- Disponibilità, ovvero la proprietà dell'informazione di essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti che ne godono i privilegi

Inoltre, con la presente Politica, MADISOFT S.P.A. intende formalizzare i seguenti obiettivi nell'ambito della sicurezza delle informazioni:

- ✔ preservare al meglio l'immagine dell'azienda quale fornitore affidabile e competitivo
- ✔ proteggere il proprio patrimonio informativo
- ✔ evitare al meglio ritardi nella delivery
- ✔ adottare le misure atte a garantire la fidelizzazione del personale e la sua professionalizzazione
- ✔ rispondere pienamente alle indicazioni della normativa vigente e cogente
- ✔ aumentare, nel proprio personale, il livello di sensibilità e la competenza sui temi della sicurezza

Contenuto della Politica

Il SGSI si applica a tutte le attività di analisi, progettazione, sviluppo e manutenzione, ai servizi e ai dati ad esse collegate: tutte le informazioni che vengono create o utilizzate da MADISOFT S.P.A. sono da salvaguardare e debbono essere protette, secondo la classificazione attribuita, dalla loro creazione, durante il loro utilizzo, fino alla loro eliminazione. Le informazioni debbono essere gestite in modo sicuro, accurato e affidabile e debbono essere prontamente disponibili per gli usi consentiti. È qui da intendersi con "utilizzo dell'informazione" qualsiasi forma di trattamento che si avvalga di supporti elettronici, cartacei o consenta, in una qualsiasi forma, la comunicazione verbale.

Relativamente all'ambito della progettazione e sviluppo, tale sistema prevede – in conformità alla NORMA ISO/IEC 27001:2017 - che il Responsabile per la Sicurezza della Informazioni svolga periodicamente un'analisi dei rischi che tenga in considerazione gli obiettivi strategici espressi nella presente Politica, degli incidenti eventualmente occorsi e dei cambiamenti strategici, di business e tecnologici avvenuti; l'analisi dei rischi ha lo scopo di valutare il rischio associato ad ogni asset da proteggere rispetto alle minacce individuate. La Direzione condivide con il Responsabile della Sicurezza delle informazioni la metodologia da impiegare per la valutazione del rischio, approvando il relativo documento; nella relazione della metodologia, la Direzione partecipa anche alla definizione delle scale di valore da impiegare per valorizzare i parametri che concorrono alla valutazione del rischio. In seguito alla elaborazione dell'analisi dei rischi, la Direzione valuta i risultati ottenuti accettando la soglia di rischio accettabile, il trattamento di mitigazione dei rischi oltre tale soglia e il rischio residuo in seguito al trattamento.

Tale analisi sarà ponderata anche rispetto al valore di business dei singoli beni da proteggere e dovrà identificare chiaramente le azioni da intraprendere, classificate secondo una scala di priorità che rispetti gli obiettivi aziendali, il

budget a disposizione e la necessità di mantenere la conformità alle norme e alle leggi vigenti. Detta analisi dovrà essere effettuata anche a fronte di eventi che possano modificare il profilo di rischio complessivo del sistema.

Firmato digitalmente da ROBERTO FRACCIA

Responsabilità

Tutto il Personale di che, a qualsiasi titolo, collabora con MADISOFT S.P.A. è responsabile dell'osservanza di questa policy e della segnalazione di anomalie, anche non formalmente codificate, di cui dovesse venire a conoscenza.

Comitato della Sicurezza delle Informazioni

Viene istituito un comitato della sicurezza che si incontrerà con cadenza almeno semestrale. È composto, in forma stabile, dalla Direzione e dal responsabile della Sicurezza delle Informazioni. Ha il compito di fissare gli obiettivi, assicurare un indirizzo chiaro e condiviso con le strategie aziendali e un supporto visibile alle iniziative di sicurezza. Promuove la sicurezza garantendo la congruità dei singoli budget destinati alla sicurezza coerentemente alle politiche e alle linee strategiche aziendali.

Responsabile della Sicurezza delle Informazioni: si occupa della progettazione del Sistema di Gestione per la Sicurezza delle informazioni e, in particolare di:

- ✔ emanare tutte le procedure necessarie, ivi inclusa la tipologia di classificazione dei documenti affinché l'organizzazione aziendale possa condurre, in modo sicuro, le proprie attività;
- ✔ adottare criteri e metodologie per l'analisi e la gestione del rischio;
- ✔ suggerire le misure di sicurezza organizzative, procedurali e tecnologiche a tutela della sicurezza e continuità delle attività di MADISOFT S.P.A.;
- ✔ pianificare un percorso formativo, specifico e periodico in materia di sicurezza delle informazioni per il personale;
- ✔ controllare periodicamente l'esposizione dei servizi aziendali alle principali minacce verificare gli incidenti di sicurezza e adottare le opportune contromisure;
- ✔ promuovere la cultura relativa alla sicurezza delle informazioni.

Tutti i soggetti esterni, che intrattengono rapporti con MADISOFT S.P.A. devono garantire il rispetto dei requisiti di sicurezza esplicitati nella presente Politica per la Sicurezza, anche attraverso la sottoscrizione di un "Patto per la Riservatezza" all'atto del conferimento del conferimento d'incarico (quando questo tipo di vincolo non sia espressamente citato negli accordi).

Applicabilità

La presente Politica si applica indistintamente a tutti gli organi dell'azienda. La sua attuazione è obbligatoria per il personale e va inserita nell'ambito della regolamentazione degli accordi nei confronti di qualsiasi soggetto esterno che, a qualsivoglia titolo, possa venire a conoscenza delle informazioni gestite in azienda.

MADISOFT S.P.A. consente la comunicazione e la diffusione delle informazioni verso l'esterno solo per il corretto svolgimento delle attività aziendali, che devono avvenire nel rispetto delle regole e delle norme cogenti.

Firmato digitalmente da ROBERTO FRACCIA

Riesame

MADISOFT S.P.A. verificherà periodicamente l'efficacia e l'efficienza del Sistema di Gestione per la Sicurezza delle Informazioni, garantendo l'adeguato supporto per l'adozione delle necessarie migliorie al fine di consentire l'attivazione di un processo continuo che controlli il variare delle condizioni o degli obiettivi di business aziendali al fine di garantire il suo corretto adeguamento.

Pollenza, lì 02.01.2020

Il Direttore Generale

Firmato digitalmente da ROBERTO FRACCIA

AGID | Agenzia per l'Italia Digitale

Linee Guida sulla formazione, gestione e conservazione dei documenti informatici

Maggio 2021

AGID | via Liszt, 21 – 00144 Roma | protocollo@pec.agid.gov.it | www.agid.gov.it | tel. 06 85264.1

Presidenza del Consiglio dei Ministri

Firmato digitalmente da ROBERTO FRACCIA

Sommario

Firmato digitalmente da ROBERTO FRACCIA

Firmato digitalmente da ROBERTO FRACCIA

Questo documento raccoglie il testo delle linee guida sulla *Formazione, gestione e conservazione dei documenti informatici*.

Firmato digitalmente da ROBERTO FRACCIA

CAPITOLO 1 Introduzione, strumenti di lettura e disposizioni comuni

1.1. Scopo del documento

Lo scopo delle presenti linee guida è duplice:

a) aggiornare le attuali regole tecniche in base all'art. 71 del Codice dell'amministrazione digitale[1] (da ora in avanti CAD), concernenti la formazione, protocollazione, gestione e conservazione dei documenti informatici;

b) incorporare in un'unica linea guida le regole tecniche e le circolari in materia, addivenendo ad un "unicum" normativo che disciplini gli ambiti sopracitati, nel rispetto della disciplina in materia di Beni culturali.

1.2. Ambito soggettivo di applicazione

Le presenti Linee Guida sono applicabili ai soggetti indicati nell'art. 2 commi 2 e 3 del CAD[2], fatti salvi gli specifici riferimenti alla Pubblica Amministrazione.

[1] L'art. 71, comma 1, del CAD prevede che "L'AgID, previa consultazione pubblica da svolgersi entro il termine di trenta giorni, sentiti le amministrazioni competenti e il Garante per la protezione dei dati personali nelle materie di competenza, nonché acquisito il parere della Conferenza unificata, adotta Linee guida contenenti le regole tecniche e di indirizzo per l'attuazione del presente Codice".

[2] L'art. 2, comma 2, del CAD prevede che le disposizioni del Codice si applicano:
"a) alle pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, nel rispetto del riparto di competenza di cui all'articolo 117 della Costituzione, ivi comprese le autorità di sistema portuale, nonché alle autorità amministrative indipendenti di garanzia, vigilanza e regolazione;
b) ai gestori di servizi pubblici, ivi comprese le società quotate, in relazione ai servizi di pubblico interesse;
c) alle società a controllo pubblico, come definite nel decreto legislativo 19 agosto 2016, n. 175, escluse le società quotate di cui all'articolo 2, comma 1, lettera p), del medesimo decreto che non rientrino nella categoria di cui alla lettera b)".
Il successivo comma 3 prevede che le disposizioni del Codice e le relative Linee guida "concernenti il documento informatico, le firme elettroniche e i servizi fiduciari di cui al Capo II, la riproduzione e conservazione dei documenti di cui agli articoli 43 e 44, il domicilio digitale e le comunicazioni elettroniche di cui all'articolo 3-bis e al Capo IV, l'identità digitale di cui agli articoli 3-bis e 64 si applicano anche ai privati, ove non diversamente previsto".

Firmato digitalmente da ROBERTO FRACCIA

1.3. Ambito oggettivo di applicazione

Le presenti Linee Guida contengono le regole tecniche sugli ambiti disciplinati dalle seguenti disposizioni del CAD:

- Art. 20, *Validità ed efficacia probatoria dei documenti informatici*, fatte salve le norme in materia di generazione, apposizione e verifica di qualsiasi tipo di firma elettronica
- Art. 21, *Ulteriori disposizioni relative ai documenti informatici, sottoscritti con firma elettronica avanzata, qualificata o digitale*
- Art. 22, commi 2 e 3, *Copie informatiche di documenti analogici*
- Art. 23, *Copie analogiche di documenti informatici*
- Art. 23-bis, *Duplicati e copie informatiche di documenti informatici*
- Art. 23-ter, *Documenti amministrativi informatici*
- Art. 23-quater, *Riproduzioni informatiche*
- Art. 34, *Norme particolari per le Pubbliche Amministrazioni*
- Art. 40, *Formazione di documenti informatici*
- Art. 40-bis, *Protocollo informatico*
- Art. 41, *Procedimento e fascicolo informatico*
- Art. 42, *Dematerializzazione dei documenti delle Pubbliche Amministrazioni*
- Art. 43, *Conservazione ed esibizione dei documenti*
- Art. 44, *Requisiti per la conservazione dei documenti informatici*
- Art. 45, *Valore giuridico della trasmissione*
- Art. 46, *Dati particolari contenuti nei documenti trasmessi*
- Art. 47, *Trasmissione dei documenti tra le Pubbliche Amministrazioni*
- Art. 49, *Segretezza della corrispondenza trasmessa per via telematica*
- Art. 50, *Disponibilità dei dati delle Pubbliche Amministrazioni*
- Art. 51, *Sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture delle Pubbliche Amministrazioni*
- Art. 64-bis, *Accesso telematico ai servizi della Pubblica Amministrazione*
- Art. 65, *Istanze e dichiarazioni presentate alle Pubbliche Amministrazioni per via telematica*

1.4. Abrogazioni e norme transitorie

Le presenti Linee Guida entrano in vigore il giorno successivo a quello della loro pubblicazione sul sito istituzionale di AGID, di cui si darà notizia sulla Gazzetta Ufficiale.

Esse si applicano a partire dal duecento settantesimo giorno successivo alla loro entrata in vigore.

A partire da questo termine i soggetti di cui all' art. 2 commi 2 e 3 del CAD formano i loro documenti esclusivamente in conformità alle presenti Linee Guida.

A partire dalla data di applicazione delle presenti Linee Guida, sono abrogati:

- il DPCM 13 novembre 2014, contenente "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici";
- il DPCM 3 dicembre 2013, contenente "Regole tecniche in materia di sistema di conservazione".

Firmato digitalmente da ROBERTO FRACCIA

Per quanto concerne il DPCM 3 dicembre 2013, contenente "Regole tecniche per il protocollo informatico", a partire dalla data di applicazione delle presenti Linee guida sono abrogate tutte le disposizioni fatte salve le seguenti:

- art. 2 comma 1, *Oggetto e ambito di applicazione*;
- art. 6, *Funzionalità*;
- art. 9, *Formato della segnatura di protocollo*;
- art. 18 commi 1 e 5, *Modalità di registrazione dei documenti informatici*;
- art. 20, *Segnatura di protocollo dei documenti trasmessi*;
- art. 21, *Informazioni da includere nella segnatura*.

Sempre a far data dalla data di applicazione delle presenti Linee guida, la circolare n. 60 del 23 gennaio 2013 dell'AgID in materia di "Formato e definizione dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le Pubbliche Amministrazioni" è abrogata e sostituita dall'allegato 6 "Comunicazione tra AOO di documenti amministrativi protocollati" del presente documento.

1.5. Principali riferimenti normativi

I principali riferimenti normativi presi in considerazione ai fini della redazione delle presenti Linee Guida sono i seguenti:

a) RD 1163/1911, *Regolamento per gli archivi di Stato*;
b) DPR 1409/1963, *Norme relative all'ordinamento ed al personale degli archivi di Stato*;
c) Legge 241/1990, *Nuove norme sul procedimento amministrativo*;
d) DPR 445/2000, *Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*;
e) DPR 37/2001, *Regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli uffici dello Stato*;
f) D.lgs 196/2003 *recante il Codice in materia di protezione dei dati personali*;
g) D.lgs 42/2004, *Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137*;
h) Legge 9 gennaio 2004, n. 4 aggiornata dal decreto legislativo 10 agosto 2018, n. 106, *Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici;*
i) D.lgs 82/2005 e ss.mm.ii., *Codice dell'amministrazione digitale*;
j) D.lgs 33/2013, *Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*;
k) DPCM 22 febbraio 2013, *Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71*;
l) DPCM 21 marzo 2013, *Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente*

Firmato digitalmente da ROBERTO FRACCIA

ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni;

n) Reg. UE 910/2014, *in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE - Regolamento eIDAS*;
o) Circolare 40 e 41 del 14 dicembre 2015 della Direzione generale degli archivi, *Autorizzazione alla distruzione di originali analogici riprodotti secondo le regole tecniche di cui al DPCM 13.11.2014 e conservati secondo le regole tecniche di cui al DPCM 13.12.2013*;
p) Reg. UE 679/2016 (GDPR), *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*;
q) Circolare 18 aprile 2017, n. 2/2017 dell'Agenzia per l'Italia Digitale, *recante le misure minime di sicurezza ICT per le pubbliche amministrazioni*;
r) Circolare n. 2 del 9 aprile 2018, *recante i criteri per la qualificazione dei Cloud Service Provider per la PA;*
s) Circolare n. 3 del 9 aprile 2018, *recante i criteri per la qualificazione di servizi SaaS per il Cloud della PA*;
t) Reg. UE 2018/1807, *relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea;*
u) DPCM 19 giugno 2019, n. 76, *Regolamento di organizzazione del Ministero per i beni e le attività culturali, degli uffici di diretta collaborazione del Ministro e dell'Organismo indipendente di valutazione della performance.*

1.6. Linee guida AGID richiamate

a) Linee guida del 15 aprile 2019 *dell'indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi*;
b) Linee guida del 6 giugno 2019 *contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate.*
c) Linee guida del 09/01/2020 *sull'Accessibilità degli strumenti informatici.*

1.7. Gruppo di lavoro

Il presente documento è stato redatto dal Tavolo di lavoro dell'Agenzia per l'Italia Digitale, istituito con determinazione del Direttore Generale n. 137 del 2 maggio 2018. Al Tavolo di lavoro, coordinato da Patrizia Gentili, hanno partecipato Alessandra Antolini, Gaetano Bruno, Matteo Carabellese, Antonio Florio, Enrica Massella Ducci Teri, Guido Pera, Vincenzo Travascio, Cristina Valiante. A titolo di esperti hanno partecipato inoltre Walter Arrighetti, Pietro Falletta Giacomo Massi e Luigi Avena, sentito anche il MIC come da art. 23 ter comma 4 del CAD[3].

[3] L'art. 23 ter comma 4 del CAD prevede che "In materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni, le Linee guida sono definite anche sentito il Ministero dei beni e delle attività culturali e del turismo".

Firmato digitalmente da ROBERTO FRACCIA

1.8. Allegati

Costituiscono parte integrante delle presenti Linee Guida i seguenti allegati:

1. Glossario dei termini e degli acronimi
2. Formati di file e riversamento
3. Certificazione di processo
4. Standard e specifiche tecniche
5. Metadati
6. Comunicazione tra AOO di Documenti Amministrativi Protocollati, che sostituisce la circolare 60/2013 dell'AgID.

1.9. Premessa metodologica

Le presenti linee guida costituiscono la nuova versione aggiornata delle regole tecniche in materia di formazione, protocollazione, gestione e conservazione del documento, già precedentemente regolate nei DPCM del 2013 e 2014. Obiettivo generale del documento è che la gestione complessiva del documento informatico risulti semplificata attraverso una visione d'insieme che aggrega in un "corpo unico" materie prima disciplinate separatamente.

L'approccio utilizzato è di tipo olistico, ossia diretto a mettere in evidenza e a rappresentare le interdipendenze funzionali tra le varie fasi della gestione documentale dal momento della formazione fino alla selezione per lo scarto o la conservazione permanente.

La tecnica redazionale – stante la natura prescrittiva del testo - ha privilegiato uno stile chiaro e fruibile per il lettore, indipendentemente dalla natura pubblica o privata di quest'ultimo e dalle sue competenze in materia.

Considerata la velocità dell'innovazione, le linee guida devono garantire un adattamento costante ai cambiamenti imposti dall'incessante rivoluzione digitale. Di qui la scelta di prevedere un testo "statico" che contenga la base normativa della materia e una serie di "allegati" i cui contenuti più "flessibili" potranno adeguarsi agevolmente all'evoluzione tecnologica. Tale processo di costante adeguamento degli "allegati" è realizzato in coerenza con il quadro normativo e attuativo in materia di digitalizzazione. Relativamente ai temi della trasmissione di contenuti digitali tra e con le pubbliche amministrazioni si assicura la conformità al Modello di interoperabilità definito da AgID e alle tecnologie introdotte dallo stesso.

Firmato digitalmente da ROBERTO FRACCIA

1.10. Natura vincolante delle Linee Guida

Come precisato dal Consiglio di Stato - nell'ambito del parere reso sullo schema di decreto legislativo del correttivo al CAD, n. 2122/2017 del 10.10.2017 - le Linee Guida adottate da AGID, ai sensi dell'art. 71 del CAD, hanno carattere vincolante e assumono valenza *erga omnes*.

Ne deriva che, nella gerarchia delle fonti, anche le presenti Linee Guida sono inquadrate come un atto di regolamentazione, seppur di natura tecnica, con la conseguenza che esse sono pienamente azionabili davanti al giudice amministrativo in caso di violazione delle prescrizioni ivi contenute. Nelle ipotesi in cui la violazione sia posta in essere da parte dei soggetti di cui all'art. 2, comma 2 del CAD, è altresì possibile presentare apposita segnalazione al difensore civico, ai sensi dell'art. 17 del CAD[4].

1.11. Principi generali della gestione documentale

La gestione documentale è un processo che può essere suddiviso in tre fasi principali: formazione, gestione e conservazione. Nell'ambito di ognuna delle suddette fasi si svolgono una serie di attività che si distinguono per complessità, impatto, natura, finalità e/o effetto, anche giuridico, alle quali corrispondono approcci metodologici e prassi operative distinte.

Il sistema di gestione informatico dei documenti, la cui tenuta può anche essere delegata a terzi, affinché possa essere efficiente e sicuro deve essere necessariamente presidiato da specifiche procedure e strumenti informatici, in grado di governare con efficacia ogni singolo accadimento che coinvolge la vita del documento ed effettuata secondo i principi generali applicabili in materia di trattamento dei dati personali anche mediante un'adeguata analisi del rischio.

Una corretta gestione dei documenti sin dalla loro fase di formazione rappresenta inoltre la migliore garanzia per il corretto adempimento degli obblighi di natura amministrativa, giuridica e archivistica tipici della gestione degli archivi pubblici.

Dal punto di vista archivistico, si distinguono tradizionalmente tre fasi di gestione in ragione delle diverse modalità di organizzazione ed utilizzo dei documenti:

- archivio corrente: riguarda i documenti necessari alle attività correnti;
- archivio di deposito: riguarda i documenti ancora utili per finalità amministrative o giuridiche, ma non più indispensabili per la trattazione delle attività correnti;
- archivio storico: riguarda i documenti storici selezionati per la conservazione permanente.

Nella fase di formazione devono essere perseguiti obiettivi di qualità, efficienza, razionalità, sistematicità, accessibilità e coerenza alle regole tecniche che presidiano la formazione dei documenti

[4] L'art. 17 comma 1-quater del CAD prevede che "È istituito presso l'AgID l'ufficio del difensore civico per il digitale, a cui è preposto un soggetto in possesso di adeguati requisiti di terzietà, autonomia e imparzialità. Chiunque può presentare al difensore civico per il digitale, attraverso apposita area presente sul sito istituzionale dell'AgID, segnalazioni relative a presunte violazioni del presente Codice e di ogni altra norma in materia di digitalizzazione ed innovazione della pubblica amministrazione da parte dei soggetti di cui all'articolo 2, comma 2. Ricevuta la segnalazione, il difensore civico, se la ritiene fondata, invita il soggetto responsabile della violazione a porvi rimedio tempestivamente e comunque non oltre trenta giorni".

Firmato digitalmente da ROBERTO FRACCIA

informatici, tenendo in debito conto le esigenze e i bisogni pratici del lavoro quotidiano. Al tal fine, risulta decisivo avvalersi di un valido e completo manuale di gestione documentale, di workflow documentali e sistemi di Document & Content Management e di applicativi informatici, per la PA ai sensi degli articoli 68[5] e 69[6] del CAD, che si basino su elevati livelli di automazione ed interoperabilità in grado di operare nel web. In un contesto in continua trasformazione, il manuale di gestione documentale deve essere sottoposto a continuo aggiornamento, in ragione dell'evoluzione tecnologica e dell'obsolescenza degli oggetti e degli strumenti digitali utilizzati. Allo stesso modo, anche i processi e le attività che governano la fase di formazione dei documenti informatici devono essere sottoposti ad un costante lavoro di valutazione, monitoraggio, ri-progettazione e reingegnerizzazione. L'adozione del manuale di gestione documentale e del manuale di conservazione non risponde solo ad esigenze pratico-operative, ma rappresenta un preciso obbligo come specificato ai paragrafi 3.5 e 4.7, al quale per la PA fa seguito l'ulteriore obbligo della loro pubblicazione sul sito istituzionale dell'ente.

La gestione dei documenti informatici prosegue con il suo trasferimento in un sistema di conservazione da realizzarsi in ottemperanza a quanto disposto dal CAD e dalle presenti Linee guida.

La conservazione dei documenti è tipicamente svolta all'interno di un sistema di conservazione dedicato a questa funzione.

Tuttavia, l'attenzione al profilo conservativo deve essere posta fin dal momento della formazione del documento, al fine di garantirne la tenuta all'interno del sistema di gestione informatica dei documenti e di eventuale conservazione a lungo termine all'interno di sistemi dedicati.

Nell'ambito della gestione documentale possono essere necessarie attività di riversamento dei documenti in altro formato diverso da quello originale, come specificato al paragrafo 3.7. Tale riversamento può avvenire più volte nella gestione del documento informatico e in diversi momenti per finalità gestionali o conservative.

In ambito digitale, infine, gli obblighi di pubblicazione di atti e provvedimenti amministrativi aventi effetto di pubblicità legale o comunque derivanti dalla normativa in materia di trasparenza devono essere assolti con la pubblicazione nei rispettivi siti web istituzionali. Affinché il processo di pubblicazione on line possa generare un prodotto atto ad assolvere i predetti obblighi è necessario che esso garantisca la conformità di quanto pubblicato all'originale, l'autorevolezza dell'ente emanatore e del sito web, la validità giuridica dei documenti e quindi la loro veridicità, efficacia e perdurabilità nel tempo.

---

[5] L'art. 68 del CAD prevede che "Le pubbliche amministrazioni acquisiscono programmi informatici o parti di essi nel rispetto dei principi di economicità e di efficienza, tutela degli investimenti, riuso e neutralità tecnologica, a seguito di una valutazione comparativa di tipo tecnico ed economico tra le seguenti soluzioni disponibili sul mercato:
a) software sviluppato per conto della pubblica amministrazione;
b) riutilizzo di software o parti di esso sviluppati per conto della pubblica amministrazione;
c) software libero o a codice sorgente aperto;
d) software fruibile in modalità cloud computing;
e) software di tipo proprietario mediante ricorso a licenza d'uso;
f) software combinazione delle precedenti soluzioni".

[6] L'art. 69 del CAD prevede che "Le pubbliche amministrazioni che siano titolari di soluzioni e programmi informatici realizzati su specifiche indicazioni del committente pubblico, hanno l'obbligo di rendere disponibile il relativo codice sorgente, completo della documentazione e rilasciato in repertorio pubblico sotto licenza aperta, in uso gratuito ad altre pubbliche amministrazioni o ai soggetti giuridici che intendano adattarli alle proprie esigenze, salvo motivate ragioni di ordine e sicurezza pubblica, difesa nazionale e consultazioni elettorali".

Firmato digitalmente da ROBERTO FRACCIA

CAPITOLO 2 Formazione dei documenti informatici

2.1. Documento informatico

2.1.1. Formazione del documento informatico

Il contenuto del presente capitolo si applica, salvo ove diversamente specificato, ai soggetti di cui all'art. 2 commi 2 e 3 del CAD.

Il documento informatico è formato mediante una delle seguenti modalità:

a) creazione tramite l'utilizzo di strumenti software o servizi cloud qualificati che assicurino la produzione di documenti nei formati e nel rispetto delle regole di interoperabilità di cui all'allegato 2;
b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;
c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;
d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

Il documento informatico deve essere identificato in modo univoco e persistente. Nel caso della Pubblica Amministrazione[7], l'identificazione dei documenti oggetto di registrazione di protocollo è rappresentata dalla segnatura di protocollo univocamente associata al documento. L'identificazione dei documenti non protocollati è affidata alle funzioni del sistema di gestione informatica dei documenti. In alternativa l'identificazione univoca può essere realizzata mediante associazione al documento di una sua impronta crittografica basata su funzioni di *hash* che siano ritenute crittograficamente sicure, e conformi alle tipologie di algoritmi previsti nell'allegato 6 delle linee guida nella tabella 1 del paragrafo 2.2 regole di processamento.

[7]Si fa riferimento ai soggetti di cui all'art. 2 comma 2, lettera a) del CAD.

Firmato digitalmente da ROBERTO FRACCIA

Il documento informatico è immodificabile se la sua memorizzazione su supporto informatico in formato digitale non può essere alterata nel suo accesso, gestione e conservazione.

Nel caso di documento informatico formato secondo la sopracitata lettera a), l'immodificabilità e l'integrità sono garantite da una o più delle seguenti operazioni:

- apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
- memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza in accordo con quanto riportato al § 3.9;
- il trasferimento a soggetti terzi attraverso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal regolamento (UE) 23 luglio 2014 n. 910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (regolamento eIDAS), valido ai fini delle comunicazioni elettroniche aventi valore legale;
- versamento ad un sistema di conservazione.

Nel caso di documento informatico formato secondo la sopracitata lettera b) l'immodificabilità ed integrità sono garantite da una o più delle seguenti operazioni mediante:

- apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
- memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza in accordo con quanto riportato al § 3.9;
- versamento ad un sistema di conservazione.

Nel caso di documento informatico formato secondo le sopracitate lettere c) e d) le caratteristiche di immodificabilità e di integrità sono garantite da una o più delle seguenti operazioni:

- apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata
- registrazione nei log di sistema dell'esito dell'operazione di formazione del documento informatico, compresa l'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema;
- produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.

Al momento della formazione del documento informatico immodificabile, devono essere generati e associati permanentemente ad esso i relativi metadati. L'insieme dei metadati del documento informatico è definito nell'allegato 5 "Metadati" alle presenti linee guida. Potranno essere individuati ulteriori metadati da associare a particolari tipologie di documenti informatici. A tal proposito si ricorda che nel manuale di gestione devono essere riportati i metadati definiti per ogni tipologia di documento.

La disponibilità e la riservatezza delle informazioni contenute nel documento informatico sono garantite attraverso l'adozione di specifiche politiche e procedure predeterminate dall'ente, in

Firmato digitalmente da ROBERTO FRACCIA

conformità con le disposizioni vigenti in materia di accesso e protezione dei dati personali. Nel caso della Pubblica Amministrazione, tali politiche e procedure sono contenute nel manuale di gestione documentale di cui al paragrafo 3.5. L'evidenza informatica corrispondente al documento informatico immodificabile è prodotta in uno dei formati contenuti nell'Allegato 2 "Formati di file e riversamento" alle presenti linee guida ove sono specificate, anche, le caratteristiche e i criteri di scelta del formato stesso.

2.2. Copie per immagine su supporto informatico di documenti analogici

La copia per immagine su supporto informatico di un documento analogico è prodotta mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o, nel caso di esigenze di dematerializzazione massiva di documenti analogici, attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia.

I requisiti tecnici per la certificazione di processo sono individuati nell'allegato 3 "Certificazione di Processo".

Fermo restando quanto previsto dall'art. 22 comma 3 del CAD[8] nel caso in cui non vi è l'attestazione di un pubblico ufficiale, la conformità della copia per immagine ad un documento analogico è garantita mediante l'apposizione della firma digitale o firma elettronica qualificata o firma elettronica avanzata o altro tipo di firma ai sensi dell'art. 20 comma 1bis, ovvero del sigillo elettronico qualificato o avanzato da parte di chi effettua il raffronto.

Laddove richiesta dalla natura dell'attività, l'attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico può essere inserita nel documento informatico contenente la copia per immagine o essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o firma elettronica qualificata o avanzata del notaio o del pubblico ufficiale a ciò autorizzato.

La distruzione degli originali analogici potrà essere effettuata in accordo con le previsioni di cui all'art. 22, commi 4 e 5 del CAD[9].

---

[8] L'art. 22 comma 4 del CAD prevede "Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico nel rispetto delle regole tecniche di cui all'articolo 71 hanno la stessa efficacia probatoria degli originali da cui sono tratte se la loro conformità all'originale non è espressamente disconosciuta."

[9] L'art. 22 commi 4 e 5 del CAD prevedono "4. Le copie formate ai sensi dei commi 1, 1 bis, 2 e 3 sostituiscono ad ogni effetto di legge gli originali formati in origine su supporto analogico, e sono idonee ad assolve-re gli obblighi di conservazione previsti dalla legge, salvo quanto stabilito dal comma 5.
5.Con decreto del Presidente del Consiglio dei Ministri possono essere individuate particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico."

Firmato digitalmente da ROBERTO FRACCIA

2.3. Duplicati, copie ed estratti informatici di documenti informatici

Un duplicato informatico ha lo stesso valore giuridico del documento informatico da cui è tratto se è ottenuto mediante la memorizzazione della medesima evidenza informatica, sullo stesso dispositivo o su dispositivi diversi; ad esempio, effettuando una copia da un PC ad una pen-drive di un documento nel medesimo formato.

La copia di un documento informatico è un documento il cui contenuto è il medesimo dell'originale ma con una diversa evidenza informatica rispetto al documento da cui è tratto, come quando si trasforma un documento con estensione ".doc" in un documento ".pdf". L'estratto di un documento informatico è una parte del documento con una diversa evidenza informatica rispetto al documento da cui è tratto. Tali documenti hanno lo stesso valore probatorio dell'originale da cui hanno origine se la stessa conformità non viene espressamente disconosciuta. In particolare, la validità del documento informatico per le copie e/o estratti di documenti informatici è consentita mediante uno dei due metodi:

- raffronto dei documenti;
- certificazione di processo.

I requisiti tecnici per la certificazione di processo sono individuati nell'allegato 3 "Certificazione di Processo".

Il ricorso ad uno dei due metodi sopracitati assicura la conformità del contenuto della copia o dell'estratto informatico alle informazioni del documento informatico di origine.

Fatto salvo quanto previsto dall'art. 23bis comma 2 del CAD[10] nel caso in cui non vi è l'attestazione di un pubblico ufficiale, la conformità della copia o dell'estratto informatico ad un documento informatico è garantita mediante l'apposizione della firma digitale o firma elettronica qualificata o firma elettronica avanzata, nonché del sigillo elettronico qualificato e avanzato da parte di chi effettua il raffronto.

Laddove richiesta dalla natura dell'attività, l'attestazione di conformità delle copie o estratti informatici di documenti informatici può essere inserita nel documento informatico contenente la copia o l'estratto. L'attestazione di conformità delle copie o dell'estratto informatico di uno o più documenti informatici può essere altresì prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia o estratto informatico. Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o con firma elettronica qualificata o avanzata del notaio o del pubblico ufficiale a ciò autorizzato.

[10] Le copie e gli estratti informatici del documento informatico, se prodotti in conformità alle vigenti regole tecniche di cui all'articolo 71, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale, in tutti le sue componenti, è attestata da un pubblico ufficiale a ciò autorizzato o se la conformità non è espressamente disconosciuta. Resta fermo, ove previsto, l'obbligo di conservazione dell'originale informatico.

Firmato digitalmente da ROBERTO FRACCIA

2.4. Il documento amministrativo informatico

2.4.1. Formazione del documento amministrativo informatico

Al documento amministrativo informatico si applicano le stesse regole valide per il documento informatico, salvo quanto specificato nel presente paragrafo.

La Pubblica Amministrazione forma gli originali dei propri documenti attraverso gli strumenti informatici riportati nel manuale di gestione documentale oppure acquisendo le istanze, le dichiarazioni e le comunicazioni di cui agli articoli 5 -bis[11], 40 -bis[12] e 65[13] del CAD.

Il documento amministrativo informatico è identificato e trattato nel sistema di gestione informatica dei documenti con le modalità descritte nel manuale di gestione documentale.

Le istanze, le dichiarazioni e le comunicazioni di cui agli articoli 5-bis, 40-bis e 65 del CAD sono identificate e trattate come i documenti amministrativi informatici. Se soggette a norme specifiche che prevedono la sola tenuta di estratti per riassunto sono memorizzate in specifici archivi informatici dettagliatamente descritti nel manuale di gestione documentale.

Il documento amministrativo informatico assume le caratteristiche di immodificabilità e di integrità, oltre che con le modalità di cui al paragrafo 2.1.1, anche con la sua registrazione nel registro di protocollo, negli ulteriori registri, nei repertori, negli albi, negli elenchi, negli archivi o nelle raccolte di dati contenute nel sistema di gestione informatica dei documenti con le modalità descritte nel manuale di gestione documentale.

Al documento amministrativo informatico viene associato l'insieme dei metadati previsti per la registrazione di protocollo ai sensi dell'art 53 del TUDA[14], nonché i metadati relativi alla

[11] L'art. 5-bis, comma 1, del CAD prevede che "La presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti, anche a fini statistici, tra le imprese e le amministrazioni pubbliche avviene esclusivamente utilizzando le tecnologie dell'informazione e della comunicazione. Con le medesime modalità le amministrazioni pubbliche adottano e comunicano atti e provvedimenti amministrativi nei confronti delle imprese".

[12] L'art. 40-bis del CAD prevede che "Formano comunque oggetto di registrazione di protocollo ai sensi dell'articolo 53 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, le comunicazioni che provengono da o sono inviate a domicili digitali eletti ai sensi di quanto previsto all'articolo 3-bis, nonché le istanze e le dichiarazioni di cui all'articolo 65 in conformità alle regole tecniche di cui all'articolo 71".

[13] L'art. 65 del CAD disciplina "Le istanze e le dichiarazioni presentate per via telematica alle pubbliche amministrazioni e ai gestori dei servizi pubblici".

[14] L'art. 53, comma 1, del TUDA prevede che "La registrazione di protocollo per ogni documento ricevuto o spedito dalle pubbliche amministrazioni è effettuata mediante la memorizzazione delle seguenti informazioni: a) numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile; b) data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile; c) mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile; d) oggetto del documento, registrato in forma non modificabile; e) data e protocollo del documento ricevuto, se disponibili; f) l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile".

Firmato digitalmente da ROBERTO FRACCIA

classificazione, ai sensi dell'articolo 56 del TUDA[15], e ai tempi di conservazione, in coerenza con il piano di conservazione, e quelli relativi alla relazione con l'aggregazione documentale informatica d'appartenenza.

Al documento amministrativo informatico sono associati ulteriori metadati rilevanti ai fini amministrativi o per finalità gestionali o conservative, definiti, per ogni tipologia di documento, nell'ambito del contesto a cui esso si riferisce, secondo quanto previsto dall'Allegato 5 alle presenti Linee guida.

Sarà cura dell'Amministrazione individuare ulteriori metadati (ad es. metadati relativi al Registro giornaliero di protocollo ecc.) da associare a particolari tipologie di documenti amministrativi informatici. A tal proposito si ricorda che nel manuale di gestione devono essere riportati i metadati definiti per ogni tipologia di documento.

Sono inclusi i documenti soggetti a registrazione particolare, come identificati nel manuale di gestione documentale, che comunque devono contenere al proprio interno o avere associati l'insieme minimo dei metadati previsti per il documento amministrativo informatico.

In applicazione dell'art.23-ter comma 5-bis del CAD[16], i documenti amministrativi informatici devono essere accessibili secondo le regole previste dall'art. 11 della legge n. 4/2004.

2.5. Copie su supporto informatico di documenti amministrativi analogici

Alle copie su supporto informatico di documenti amministrativi analogici si applicano le disposizioni di cui al paragrafo 2.2.

L'attestazione di conformità della copia informatica di un documento amministrativo analogico, formato dalla Pubblica Amministrazione, ovvero da essa detenuto, può essere inserita nel documento informatico contenente la copia informatica o essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o con firma elettronica qualificata o avanzata del funzionario delegato.

[15] L'art. 56 del TUDA prevede che "Le operazioni di registrazione indicate all'articolo 53 e le operazioni di segnatura di protocollo di cui all'articolo 55 nonché le operazioni di classificazione costituiscono operazioni necessarie e sufficienti per la tenuta del sistema di gestione informatica dei documenti da parte delle pubbliche amministrazioni".

[16] L'art. 23-ter comma 5-bis prevede che "I documenti di cui al presente articolo devono essere fruibili indipendentemente dalla condizione di disabilità personale, applicando i criteri di accessibilità definiti dai requisiti tecnici di cui all'articolo 11 della legge 9 gennaio 2004, n. 4".

Firmato digitalmente da ROBERTO FRACCIA

CAPITOLO 3 Gestione documentale

3.1. Registrazione informatica dei documenti

3.1.1. Ambito di applicazione

Il presente capitolo individua le regole tecniche, i criteri e le specifiche delle informazioni previste nelle operazioni di registrazione e segnatura di protocollo, di cui agli articoli da 50 a 57 e da 61 a 66 del TUDA[17].

Il presente capitolo stabilisce inoltre le regole tecniche, i criteri e le specifiche delle informazioni previste nelle operazioni di registrazione e segnatura di protocollo di cui agli articoli 40-bis, 41 e 47 del CAD[18].

3.1.2. Adeguamento organizzativo e funzionale

Le Pubbliche Amministrazioni, nell'ambito del proprio ordinamento, provvedono a:

A. individuare le aree organizzative omogenee (di seguito AOO) e i relativi uffici di riferimento ai sensi dell'art. 50, comma 4, del TUDA[19];

B. nominare, in ciascuna delle AOO, il responsabile della gestione documentale e un suo vicario, in possesso di idonee competenze giuridiche, informatiche ed archivistiche;

[17] Gli articoli da 50 a 57 e da 61 a 66 del TUDA sono compresi nel Capo IV "Sistemi di gestione informatica del documento".
[18] Gli articoli 40-bis, 41 e 47 del CAD disciplinano, rispettivamente, in materia di protocollo informatico, procedimento e fascicolo informatico, trasmissione dei documenti tra le pubbliche amministrazioni.
[19] L'art. 50, comma 4, del TUDA prevede che "Ciascuna amministrazione individua, nell'ambito del proprio ordinamento, gli uffici da considerare ai fini della gestione unica o coordinata dei documenti per grandi aree organizzative omogenee, assicurando criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna tra le aree stesse".

Firmato digitalmente da ROBERTO FRACCIA

C. per le amministrazioni con più AOO, nominare il coordinatore della gestione documentale e un suo vicario, in possesso di idonee competenze giuridiche, informatiche ed archivistiche;

D. adottare per ogni AOO il manuale di gestione documentale, su proposta del responsabile della gestione documentale oppure, ove nominato, dal coordinatore della gestione documentale.

Secondo quanto previsto dal CAD e dalle Linee guida AGID del 15 aprile 2019[20], l'Indice dei domicili digitali delle Pubbliche Amministrazioni e dei gestori di pubblici servizi, di seguito indicato con l'acronimo IPA, include, tra gli indirizzi telematici degli Enti ivi iscritti, il domicilio digitale da cui provengono, o sono inviate, comunicazioni, istanze, dichiarazioni e notifiche che formano oggetto di registrazione di protocollo.

3.1.3. Registrazione di protocollo e altre forme di registrazione

La registrazione informatica dei documenti è rappresentata dall'insieme di dati in forma elettronica allegati o connessi al documento informatico al fine dell'identificazione univoca di tutti i documenti prodotti e acquisiti. Per la Pubblica Amministrazione vale quanto disposto ai sensi dell'articolo 53 comma 5 del TUDA[21].

Al termine della registrazione, il documento è identificato da un insieme di dati in forma elettronica che può includere sin da questa fase la classificazione e si integra con il piano di organizzazione delle aggregazioni documentali, definito dal Responsabile della gestione documentale di cui al paragrafo 3.4, nell'ambito del manuale di gestione.

La Pubblica Amministrazione, al fine di dare attuazione alle disposizioni introdotte dal CAD stesso in materia di sistema di gestione informatica dei documenti realizza le funzionalità di gestione dell'archivio corrente, dell'archivio di deposito, dei flussi documentali, automatizzazione dei procedimenti amministrativi sulla base dei propri obiettivi di miglioramento dei servizi e di incremento dell'efficienza operativa, tenuto conto del rapporto costi e benefici, nel rispetto degli articoli 53 e 55 del TUDA[22] e dei requisiti del sistema di gestione informatica dei documenti e dei flussi documentali" definiti negli articoli 52, 65 e 67 del TUDA[23], applicando ove possibile i requisiti fissati per la registrazione di protocollo anche alle altre forme di registrazione informatica dei documenti, fatto salvo quanto disposto per esse da eventuali norme vigenti".

---

[20] Linee Guida dell'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi.

[21] L'art. 53, comma 5, del TUDA prevede che "Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici. Ne sono esclusi le gazzette ufficiali, i bollettini ufficiali e i notiziari della pubblica amministrazione, le note di ricezione delle circolari e altre disposizioni, i materiali statistici, gli atti preparatori interni, i giornali, le riviste, i libri, i materiali pubblicitari, gli inviti a manifestazioni e tutti i documenti già soggetti a registrazione particolare dell'amministrazione".

[22] Gli articoli 53 e 55 del TUDA disciplinano, rispettivamente, in materia di registrazioni di protocollo e segnatura di protocollo.

[23] Gli articoli 52, 65 e 67 del TUDA disciplinano, rispettivamente, in materia di sistema di gestione informatica dei documenti, requisiti del sistema per la gestione dei flussi documentali e trasferimento dei documenti all'archivio di deposito.

Firmato digitalmente da ROBERTO FRACCIA

3.1.4. Formato della registrazione e della segnatura di protocollo

La registrazione di protocollo è l'insieme dei metadati che il registro di protocollo deve memorizzare, per tutti i documenti ricevuti o spediti dalla Pubblica Amministrazione e per tutti i documenti informatici che non rientrano tra le tipologie specificate dall'art. 53, comma 5 del TUDA[24] e che non sono oggetto di registrazione particolare da parte dell'amministrazione, al fine di garantirne l'identificazione univoca e certa. In merito, l'articolo 53, comma 1, del TUDA indica le informazioni che caratterizzano il registro di protocollo[25], a cui si aggiungono le informazioni inerenti l'assegnazione interna all'amministrazione e la eventuale classificazione.

La segnatura di protocollo è l'associazione ai documenti amministrativi informatici in forma permanente e non modificabile di informazioni riguardanti i documenti stessi, in ingresso e in uscita al sistema di protocollo, utile alla sua identificazione univoca e certa.

In merito l'articolo 55, comma 1, del TUDA individua le informazioni che caratterizzano la segnatura di protocollo[26].

Le operazioni di segnatura e registrazione di protocollo sono effettuate contemporaneamente.

Gli "standard, le modalità di trasmissione, il formato e le definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le Pubbliche Amministrazioni e associate ai documenti protocollati" sono definiti nell'allegato 6 "Comunicazione tra AOO di Documenti Amministrativi Protocollati".

---

[24] L'art. 53, comma 5 del TUSA prevede che: "Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici. Ne sono esclusi le gazzette ufficiali, i bollettini ufficiali e i notiziari della pubblica amministrazione, le note di ricezione delle circolari e altre disposizioni, i materiali statistici, gli atti preparatori interni, i giornali, le riviste, i libri, i materiali pubblicitari, gli inviti a manifestazioni e tutti i documenti già soggetti a registrazione particolare dell'amministrazione".

[25] L'art. 53, comma 1, del TUDA prevede che: "La registrazione di protocollo per ogni documento ricevuto o spedito dalle pubbliche amministrazioni è effettuata mediante la memorizzazione delle seguenti informazioni:
a) numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile;
b) data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile;
c) mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile;
d) oggetto del documento, registrato in forma non modificabile;
e) data e protocollo del documento ricevuto, se disponibili;
f) l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile".

[26] L'art. 55, comma 1, del TUDA prevede che: "La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso. Essa consente di individuare ciascun documento in modo inequivocabile. Le informazioni minime previste sono:
a) il progressivo di protocollo, secondo il formato disciplinato all'articolo 57;
b) la data di protocollo;
c) l'identificazione in forma sintetica dell'amministrazione o dell'area organizzativa individuata ai sensi dell'articolo 50, comma 4".

Firmato digitalmente da ROBERTO FRACCIA

3.1.5. Annullamento delle informazioni registrate in forma immodificabile

Il protocollo informatico deve assicurare il tracciamento e la storicizzazione di ogni operazione, comprese le operazioni di annullamento, e la loro attribuzione all'operatore. Il sistema di protocollo informatico assicura che:

- le informazioni relative all'oggetto, al mittente e al destinatario di una registrazione di protocollo, non possano essere modificate, ma solo annullate con la procedura prevista dall'art. 54 del TUDA[27];
- le uniche informazioni modificabili di una registrazione di protocollo siano l'assegnazione interna all'amministrazione e la classificazione;
- le azioni di annullamento provvedano alla storicizzazione dei dati annullati attraverso le informazioni oggetto della stessa;
- per ognuno di questi eventi, anche nel caso di modifica di una delle informazioni di cui al punto precedente, il sistema storicizzi tutte le informazioni annullate e modificate rendendole entrambe visibili e comparabili, nel rispetto di quanto previsto dall'art. 54, comma 2 del TUDA.

3.1.6. Requisiti minimi di sicurezza dei sistemi di protocollo informatico

Il sistema di protocollo informatico, eventualmente integrato in un sistema di gestione informatica dei documenti, assicura il rispetto delle disposizioni in materia di sicurezza predisposte dall'AgID di cui al paragrafo 3.9 e dagli altri organismi preposti e delle disposizioni in materia di protezione dei dati personali.

In particolare, il sistema di protocollo informatico deve garantire:

a) l'univoca identificazione ed autenticazione degli utenti;
b) la garanzia di accesso alle risorse esclusivamente agli utenti abilitati e/o a gruppi di utenti secondo la definizione di appositi profili;
c) il tracciamento permanente di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.

Il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.

[27] L'art. 54, comma 2, del TUDA prevede che: "La procedura per indicare l'annullamento riporta, secondo i casi, una dicitura o un segno in posizione sempre visibile e tale, comunque, da consentire la lettura di tutte le informazioni originarie unitamente alla data, all'identificativo dell'operatore ed agli estremi del provvedimento d'autorizzazione".

Firmato digitalmente da ROBERTO FRACCIA

3.2. Classificazione dei documenti informatici

La classificazione ha il fine di organizzare logicamente tutti i documenti amministrativi informatici prodotti o ricevuti da un ente nell'esercizio delle sue funzioni. L'attività di classificazione si avvale del piano di classificazione che mappa, su più livelli gerarchici, tutte le funzioni dell'ente.

La classificazione è un'attività obbligatoria nel sistema di gestione informatica dei documenti dell'AOO e si applica a tutti i documenti prodotti e acquisiti dalla stessa AOO sottoposti o meno alla registrazione di protocollo, ai sensi degli articoli 56[28] e 64, comma 4[29], del TUDA. Le informazioni relative alla classificazione nei casi dei documenti amministrativi informatici costituiscono parte integrante dei metadati previsti per la formazione dei documenti medesimi.

Il Responsabile della gestione documentale o il coordinatore della gestione documentale, ove nominato, verifica periodicamente la rispondenza del piano di classificazione ai procedimenti amministrativi e agli affari in essere e procede al suo aggiornamento.

Nel sistema di gestione informatica dei documenti dell'AOO l'attività di classificazione guida la formazione dell'archivio mediante il piano di organizzazione delle aggregazioni documentali.

3.3. Aggregazioni documentali informatiche

La Pubblica Amministrazione documenta la propria attività tramite funzioni del sistema di gestione informatica dei documenti finalizzate alla produzione, alla gestione e all'uso delle aggregazioni documentali informatiche, corredate da opportuni metadati, così come definiti nell'allegato 5 "Metadati" alle presenti Linee guida.

3.3.1. Fascicoli informatici

Nelle Pubbliche Amministrazioni l'AOO gestisce i flussi documentali mediante fascicoli informatici predisposti secondo il piano di classificazione e relativo piano di organizzazione delle aggregazioni documentali ai sensi dell'art. 64 del TUDA, anche con riferimento a fascicoli non afferenti a procedimenti.

[28] L'articolo 56 del TUDA prevede che: "Le operazioni di registrazione indicate all'articolo 53 e le operazioni di segnatura di protocollo di cui all'articolo 55 nonché le operazioni di classificazione costituiscono operazioni necessarie e sufficienti per la tenuta del sistema di gestione informatica dei documenti da parte delle pubbliche amministrazioni".

[29] L'articolo 64, comma 4, del TUDA prevede che: "Le amministrazioni determinano autonomamente e in modo coordinato per le aree organizzative omogenee, le modalità di attribuzione dei documenti ai fascicoli che li contengono e ai relativi procedimenti, definendo adeguati piani di classificazione d'archivio per tutti i documenti, compresi quelli non soggetti a registrazione di protocollo".

Firmato digitalmente da ROBERTO FRACCIA

La produzione, il mantenimento e l'uso dei fascicoli informatici sono conformi a quanto stabilito dall'art. 65[30] del TUDA e dell'art 41[31] del CAD.

3.3.2. Altre aggregazioni documentali informatiche

All'interno del sistema di gestione informatica dei documenti la Pubblica Amministrazione forma, gestisce e utilizza tipologie di aggregazioni documentali informatiche diverse dai fascicoli: serie che aggregano documenti e serie che aggregano fascicoli.

Le serie documentarie sono costituite da documenti singoli accorpati per ragioni funzionali in base alla tipologia di riferimento.

Le serie di fascicoli sono costituite da fascicoli accorpati per ragioni funzionali in base alla classe di riferimento o alla tipologia di fascicoli.

I fascicoli appartenenti a serie diverse possono essere collegati tra loro.

---

[30] L'articolo 65 del TUDA prevede che: "Oltre a possedere i requisiti indicati all'articolo 52, il sistema per la gestione dei flussi documentali deve:

a) fornire informazioni sul legame esistente tra ciascun documento registrato, il fascicolo ed il singolo procedimento cui esso è associato;
b) consentire il rapido reperimento delle informazioni riguardanti i fascicoli, il procedimento ed il relativo responsabile, nonché la gestione delle fasi del procedimento;
c) fornire informazioni statistiche sull'attività dell'ufficio;
d) consentire lo scambio di informazioni con sistemi per la gestione dei flussi documentali di altre amministrazioni al fine di determinare lo stato e l'iter dei procedimenti complessi".

[31] L'art. 41, comma 2-ter, del CAD prevede che: "Il fascicolo informatico reca l'indicazione:

a) dell'amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
2. delle altre amministrazioni partecipanti;
3. del responsabile del procedimento;
4. dell'oggetto del procedimento;
e) dell'elenco dei documenti contenuti, salvo quanto disposto dal comma 2-quater;
e-bis) dell'identificativo del fascicolo medesimo apposto con modalità idonee a consentirne l'indicizzazione e la ricerca attraverso il sistema di cui all'articolo 40-ter nel rispetto delle Linee guida".

Il successivo comma 2-quater prevede che: "Il fascicolo informatico può contenere aree a cui hanno accesso solo l'amministrazione titolare e gli altri soggetti da essa individuati; esso è formato in modo da garantire la corretta collocazione, la facile reperibilità e la collegabilità, in relazione al contenuto ed alle finalità, dei singoli documenti. Il fascicolo informatico è inoltre costituito in modo da garantire l'esercizio in via telematica dei diritti previsti dalla citata legge n. 241 del 1990 e dall'articolo 5, comma 2, del decreto legislativo 14 marzo 2013, n. 33, nonché l'immediata conoscibilità anche attraverso i servizi di cui agli articoli 40-ter e 64-bis, sempre per via telematica, dello stato di avanzamento del procedimento, del nominativo e del recapito elettronico del responsabile del procedimento. AgID detta, ai sensi dell'articolo 71, Linee guida idonee a garantire l'interoperabilità tra i sistemi di gestione dei fascicoli dei procedimenti e i servizi di cui agli articoli 40-ter e 64-bis".

Firmato digitalmente da ROBERTO FRACCIA

Il sistema di gestione informatica dei documenti dell'AOO, individuata ai sensi dell'art. 50, comma 4, del TUDA[32], permette la gestione, formazione, utilizzo di serie secondo il piano di classificazione o di fascicolatura, sulla base delle indicazioni contenute nel manuale di gestione.

3.3.3. Registri e repertori informatici

Il registro di protocollo e i registri dei documenti soggetti a registrazione particolare, i repertori, gli albi, gli elenchi e ogni raccolta di dati concernente stati, qualità personali e fatti realizzati dalle amministrazioni su supporto informatico in luogo dei registri cartacei sono formati attraverso la generazione o il raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti che operano fra loro, secondo una struttura logica predeterminata e memorizzata in forma statica.

3.4. Compiti del responsabile della gestione documentale

Le Pubbliche Amministrazioni definiscono le attribuzioni del responsabile della gestione documentale ovvero, ove nominato, del coordinatore della gestione documentale.

Il responsabile della gestione documentale è preposto al servizio di cui all'articolo 61 del TUDA[33] e, d'intesa con il responsabile della conservazione, il responsabile per la transizione digitale di cui

---

[32] L'art. 50, comma 4, del TUDA, prevede che: "Ciascuna amministrazione individua, nell'ambito del proprio ordinamento, gli uffici da considerare ai fini della gestione unica o coordinata dei documenti per grandi aree organizzative omogenee, assicurando criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna tra le aree stesse".

[33] L'articolo 61 del TUDA prevede che "1. Ciascuna amministrazione istituisce un servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi in ciascuna delle grandi aree organizzative omogenee individuate ai sensi dell'articolo 50. Il servizio è posto alle dirette dipendenze della stessa area organizzativa omogenea.
2. Al servizio è preposto un dirigente ovvero un funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica acquisita a seguito di processi di formazione definiti secondo le procedure prescritte dalla disciplina vigente. 3. Il servizio svolge i seguenti compiti:
a) attribuisce il livello di autorizzazione per l'accesso alle funzioni della procedura, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;
b) garantisce che le operazioni di registrazione e di segnatura di protocollo si volgano nel rispetto delle disposizioni del presente testo unico;
c) garantisce la corretta produzione e la conservazione del registro giornaliero di protocollo di cui all'articolo 53;
d) cura che le funzionalità del sistema in caso di guasti o anomalie siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
e) conserva le copie di cui agli articoli 62 e 63, in luoghi sicuri differenti;
f) garantisce il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso di cui agli articoli 59 e 60 e le attività di gestione degli archivi di cui agli articoli 67, 68 e 69;
g) autorizza le operazioni di annullamento di cui all'articolo 54;
h) vigila sull'osservanza delle disposizioni del presente testo unico da parte del personale autorizzato e degli incaricati.

Firmato digitalmente da ROBERTO FRACCIA

all'art.17 del CAD[34] e acquisito il parere del responsabile della protezione dei dati personali, di cui agli artt. 37 "Designazione del responsabile della protezione dei dati" e 39 "Compiti del responsabile della protezione dei dati" del Regolamento UE 679/2016, predispone:

- il manuale di gestione documentale relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso ai documenti informatici nel rispetto della normativa in materia di trattamenti dei dati personali ed in coerenza con quanto previsto nel manuale di conservazione;

Tale manuale conterrà inoltre, come parte integrante dello stesso, il piano per la sicurezza informatica, per la quota parte di competenza, nel rispetto delle:

- misure di sicurezza predisposte dall'AgID e dagli altri organismi preposti;
- delle disposizioni in materia di protezione dei dati personali in linea con l'analisi del rischio fatta;
- indicazioni in materia di continuità operativa dei sistemi informatici predisposti dall'AGID.

Per l'Amministrazione con più AOO il coordinatore della gestione, sentiti i responsabili della gestione documentale, assicura l'adozione di criteri uniformi per la gestione informatica dei documenti.

Il responsabile della gestione documentale ovvero, ove nominato, il coordinatore della gestione documentale, verifica l'avvenuta eliminazione dei protocolli di settore, dei protocolli multipli e, più in generale, dei protocolli diversi dal protocollo informatico previsto dal TUDA.

3.5. Manuale di gestione documentale

Il manuale di gestione documentale descrive il sistema di gestione informatica dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Nel manuale di gestione documentale sono riportati, in particolare:

1. relativamente agli aspetti organizzativi:
   a) le modalità di utilizzo degli strumenti informatici per la formazione dei documenti informatici e per lo scambio degli stessi all'interno ed all'esterno dell'AOO, applicando le modalità di trasmissione indicate nell'allegato 6 "Comunicazione tra AOO di Documenti Amministrativi Protocollati";
   b) l'indicazione delle unità organizzative responsabili (UOR) delle attività di registrazione di protocollo, di archiviazione dei documenti all'interno dell'AOO;
   c) l'indicazione delle regole di assegnazione dei documenti ricevuti con la specifica dei criteri per l'ulteriore eventuale inoltro dei documenti verso aree organizzative omogenee della stessa amministrazione o verso altre amministrazioni;
   d) i criteri e le modalità per il rilascio delle abilitazioni di accesso, interno ed esterno all'Amministrazione, al sistema di gestione informatica dei documenti;

[34] L'art. 17 del CAD prevede che:" …ciascuna pubblica amministrazione affida a un unico ufficio dirigenziale generale, fermo restando il numero complessivo di tali uffici, la transizione alla modalità operativa digitale".

Firmato digitalmente da ROBERTO FRACCIA

2. relativamente ai formati dei documenti:
   a) l'individuazione dei formati utilizzati per la formazione del documento informatico, come introdotti nel paragrafo 3.6, tra quelli indicati nell'Allegato 2 "Formati di file e riversamento";
   b) la descrizione di eventuali ulteriori formati utilizzati per la formazione di documenti in relazione a specifici contesti operativi che non sono individuati nell'Allegato 2 "Formati di file e riversamento";
   c) le procedure per la valutazione periodica di interoperabilità dei formati e per le procedure di riversamento previste come indicato al paragrafo 3.7 e nell'Allegato 2 "Formati di file e riversamento";

3. relativamente al protocollo informatico e alle registrazioni particolari:
   a) le modalità di registrazione delle informazioni annullate o modificate nell'ambito delle attività di registrazione;
   b) la descrizione completa e puntuale delle modalità di utilizzo della componente «sistema di protocollo informatico» del sistema di gestione informatica dei documenti;
   c) le modalità di utilizzo del registro di emergenza ai sensi dell'art. 63 del TUDA[35], inclusa la funzione di recupero dei dati protocollati manualmente;
   d) l'elenco dei documenti esclusi dalla registrazione di protocollo, per cui è prevista registrazione particolare ai sensi dell'art. 53, comma 5, del TUDA[36];
   e) determinazione dei metadati da associare ai documenti soggetti a registrazione particolare individuati, assicurando almeno quelli obbligatori previsti per il documento informatico dall'Allegato 5 alle presenti Linee Guida;
   f) i registri particolari individuati per la gestione del trattamento delle registrazioni particolari informatiche anche associati ad aree organizzative omogenee definite dall'amministrazione sull'intera struttura organizzativa e gli albi, gli elenchi e ogni raccolta di dati concernente stati, qualità personali e fatti, riconosciuti da una norma;

4. relativamente alle azioni di classificazione e selezione:
   a) il piano di classificazione adottato dall'Amministrazione, con l'indicazione delle modalità di aggiornamento, integrato con le informazioni relative ai tempi, ai criteri e alle regole di selezione e conservazione, con riferimento alle procedure di scarto;

5. relativamente alla formazione delle aggregazioni documentali
   a) le modalità di formazione, gestione e archiviazione dei fascicoli informatici e delle aggregazioni

---

[35] L'art. 63 del TUDA prevede che: "1. Il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi autorizza lo svolgimento anche manuale delle operazioni di registrazione di protocollo su uno o più registri di emergenza, ogni qualvolta per cause tecniche non sia possibile utilizzare la normale procedura informatica. Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema. 2. Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre ventiquattro ore, per cause di eccezionale gravità, il responsabile per la tenuta del protocollo può autorizzare l'uso del registro di emergenza per periodi successivi di non più di una settimana. Sul registro di emergenza vanno riportati gli estremi del provvedimento di autorizzazione. 3. Per ogni giornata di registrazione di emergenza è riportato sul registro di emergenza il numero totale di operazioni registrate manualmente. 4. La sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'area organizzativa omogenea. 5. Le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico, utilizzando un'apposita funzione di recupero dei dati, senza ritardo al ripristino delle funzionalità del sistema. Durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, che provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza".

[36] L'art. 53, comma 5, del TUDA prevede che: "Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici. Ne sono esclusi le gazzette ufficiali, i bollettini ufficiali e i notiziari della pubblica amministrazione, le note di ricezione delle circolari e altre disposizioni, i materiali statistici, gli atti preparatori interni, i giornali, le riviste, i libri, i materiali pubblicitari, gli inviti a manifestazioni e tutti i documenti già soggetti a registrazione particolare dell'amministrazione".

Firmato digitalmente da ROBERTO FRACCIA

documentali informatiche con l'insieme minimo dei metadati ad essi associati;

6. relativamente ai flussi di lavorazione dei documenti in uso:
   a) la descrizione dei flussi di lavorazione interni all'Amministrazione, anche mediante la rappresentazione formale dei processi attraverso l'uso dei linguaggi indicati da AgID, applicati per la gestione dei documenti ricevuti, inviati o ad uso interno;

7. relativamente alla organizzazione dei documenti informatici, dei fascicoli informatici e delle serie informatiche:

   a) la definizione della struttura dell'archivio all'interno del sistema di gestione informatica dei documenti. L'archivio informatico - formato ai sensi del capo IV "Sistema di gestione informatica dei documenti" del DPR 445/2000 - deve essere progettato in modo da assicurare certezza e trasparenza all'attività giuridico amministrativa;

8. relativamente alle misure di sicurezza e protezione dei dati personali adottate:
   a) le opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio anche in materia di protezione dei dati personali;

9. relativamente alla conservazione:
   a) per le Pubbliche Amministrazioni il piano di conservazione è allegato al manuale di gestione documentale, con l'indicazione dei tempi entro i quali le diverse tipologie di oggetti digitali devono essere trasferite in conservazione ed eventualmente scartate;
   b) per i soggetti diversi dalle Pubbliche Amministrazioni che sono sprovvisti di piano di conservazione, qualora si renda necessario redigere un Manuale di gestione per la complessità della struttura organizzativa e della documentazione prodotta, dovrebbero essere definiti i criteri di organizzazione dell'archivio, di selezione periodica e di conservazione dei documenti, ivi compresi i tempi entro i quali le diverse tipologie di oggetti digitali devono essere trasferite in conservazione ed eventualmente scartate.

La Pubblica Amministrazione è tenuta a redigere, adottare con provvedimento formale e pubblicare sul proprio sito istituzionale il Manuale di gestione documentale. La pubblicazione è realizzata in una parte chiaramente identificabile dell'area "Amministrazione trasparente" prevista dall'art. 9 del d.lgs. 33/2013[37].

3.6. Formati di file

I formati da utilizzare nell'ambito delle presenti Linee guida sono quelli previsti dall'Allegato 2 "Formati di file e riversamento". Nello scegliere i formati di file di cui sopra, da utilizzare per i propri documenti informatici, i soggetti di cui all'art. 2 comma 2 e comma 3 del CAD possono effettuare una valutazione di interoperabilità che tenga conto dei seguenti fattori: formati aperti, non proprietari, standard *de iure*, estendibili, parlanti, completamente robusti, indipendenti dal dispositivo.

[37] L'art. 9, comma 1, del d.lgs. 33/2013, prevede che: "Ai fini della piena accessibilità delle informazioni pubblicate, nella home page dei siti istituzionali è collocata un'apposita sezione denominata «Amministrazione trasparente», al cui interno sono contenuti i dati, le informazioni e i documenti pubblicati ai sensi della normativa vigente. Le amministrazioni non possono disporre filtri e altre soluzioni tecniche atte ad impedire ai motori di ricerca web di indicizzare ed effettuare ricerche all'interno della sezione «Amministrazione trasparente»".

Firmato digitalmente da ROBERTO FRACCIA

Le pubbliche amministrazioni garantiscono sempre la gestione dei formati classificati nell'Allegato 2 "Formati di file e riversamento" come "generici", secondo la distinzione introdotta nell'Allegato 2 tra formati di file generici e specifici.

Qualora l'ordinamento giuridico preveda, per particolari categorie di documenti elettronici, degli obblighi relativamente all'uso di formati di file specifici ovvero di vincoli aggiuntivi su formati generici (quali, ad esempio, l'uso di particolari dialetti o specializzazioni per formati generici), le pubbliche amministrazioni, assolvendo tali obblighi, accettano i suddetti documenti elettronici solo se prodotti nei formati o con i vincoli aggiuntivi obbligatori.

È possibile utilizzare formati diversi da quelli elencati nell'Allegato 2 "Formati di file e riversamento", effettuando una valutazione di interoperabilità.

La valutazione di interoperabilità è effettuata in base alle indicazioni previste nell'Allegato 2 "Formati di file e riversamento". La valutazione di interoperabilità, in quanto parte della gestione informatica dei documenti, viene effettuata periodicamente e, comunque, ogni anno, allo scopo di individuare tempestivamente cambiamenti delle condizioni espresse dai punti sopra elencati.

Il manuale di gestione documentale contiene l'elenco dei formati utilizzati e la valutazione di interoperabilità.

3.7. Riversamento

A seguito della valutazione di interoperabilità, i soggetti di cui all'art. 2 comma 2 e comma 3 del CAD valutano l'esigenza o l'opportunità di effettuare o pianificare il riversamento dei file da un formato di file ad un altro formato, sempre tenendo in considerazione quanto previsto nel punto precedente. Il riversamento è effettuato in base alle indicazioni previste nell'Allegato 2 "Formati di file e riversamento".

3.8. Trasferimento al sistema di conservazione

I termini entro cui i documenti informatici e le aggregazioni documentali informatiche devono essere trasferiti in conservazione sono stabiliti in conformità alla normativa vigente e al piano di conservazione.

Coerentemente con quanto stabilito dal Codice dei beni culturali, il trasferimento a un sistema di conservazione di documenti e aggregazioni documentali informatiche, appartenenti ad archivi pubblici e privati dichiarati di interesse storico particolarmente importante, è assoggettato all'obbligo di cui all'art. 21 del Codice dei Beni Culturali[38] di comunicazione agli organi competenti in materia di tutela dei beni archivistici o, nel caso di affidamento esterno, alla loro autorizzazione.

[38] L'art. 21, comma 1, del Codice dei beni culturali prevede che: "Sono subordinati ad autorizzazione del Ministero: a) la rimozione o la demolizione, anche con successiva ricostituzione, dei beni culturali; b) lo spostamento, anche temporaneo, dei beni culturali mobili, salvo quanto previsto ai commi 2 e 3; c) lo smembramento di collezioni, serie e raccolte; d) lo scarto dei documenti degli archivi pubblici e degli archivi privati per i quali sia intervenuta la dichiarazione ai sensi

Firmato digitalmente da ROBERTO FRACCIA

I documenti informatici e le aggregazioni documentali informatiche possono essere oggetto di selezione e scarto nel sistema di gestione informatica dei documenti nel rispetto della normativa sui beni culturali.

3.9. Misure di sicurezza

Nell'attuazione delle presenti Linee Guida, le Pubbliche Amministrazioni sono tenute ad ottemperare alle misure minime di sicurezza ICT emanate dall'AgID con circolare del 18 aprile 2017, n. 2/2017. In tale ottica, il responsabile della gestione documentale ovvero, ove nominato, il coordinatore della gestione documentale, in accordo con il responsabile della conservazione di cui al paragrafo 4.6, con il responsabile per la transizione digitale e acquisito il parere del responsabile della protezione dei dati personali, predispone il piano della sicurezza del sistema di gestione informatica dei documenti, prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali, ai sensi dell'art. 32 del Regolamento UE 679/2016 (GDPR)[39], anche in funzione delle tipologie di dati trattati, quali quelli riferibili alle categorie particolari di cui agli artt. 9-10 del Regolamento stesso.

L'adozione delle predette misure è in capo al titolare o, in caso di trattamento effettuato per suo conto, al responsabile del trattamento, individuato sulla base dell'art. 28 "Responsabile del trattamento" del Regolamento.

Il piano conterrà altresì la descrizione della proceduta da adottarsi in caso di violazione dei dati personali ai sensi degli artt. 33-34 del Regolamento UE 679/2016[40], e sarà redatto nell'ambito del

---

dell'articolo 13, nonché lo scarto di materiale bibliografico delle biblioteche pubbliche, con l'eccezione prevista all'articolo 10, comma 2, lettera c), e delle biblioteche private per le quali sia intervenuta la dichiarazione ai sensi dell'articolo 13; e) il trasferimento ad altre persone giuridiche di complessi organici di documentazione di archivi pubblici, nonché di archivi privati per i quali sia intervenuta la dichiarazione ai sensi dell'articolo 13".
Il successivo comma 3 prevede che: "Lo spostamento degli archivi correnti dello Stato e degli enti ed istituti pubblici non è soggetto ad autorizzazione, ma comporta l'obbligo di comunicazione al Ministero per le finalità di cui all'articolo 18".

[39] L'art. 32 del Regolamento (UE) 2016/679 prevede che: "1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. 3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo. 4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri".

[40] Gli artt. 33 e 34 del Regolamento (UE) 2016/679 prevedono, rispettivamente, la procedura di notifica di una violazione dei dati personali all'autorità di controllo e quella di comunicazione di una violazione dei dati personali all'interessato.

Firmato digitalmente da ROBERTO FRACCIA

piano generale della sicurezza, in coerenza con quanto previsto dal Piano Triennale per l'Informatica nella Pubblica Amministrazione vigente.

In conformità all'art. 28 del Regolamento UE 679/2016, i soggetti esterni a cui è eventualmente delegata la tenuta del sistema di gestione informatica dei documenti sono individuati come Responsabili del trattamento dei dati e devono presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato.

I soggetti privati appartenenti ad organizzazioni che applicano particolari regole di settore per la sicurezza dei propri sistemi informatici possono adottare misure di sicurezza per garantire la tenuta del documento informatico. Le citate misure di sicurezza ICT emanate dall'AGID possono costituire, a tal fine, un modello di riferimento, fermo restando gli obblighi previsti dal citato Regolamento Reg. UE 679/2016.

I servizi devono sempre organizzati nel rispetto dei principi e dei requisiti previsti in materia di sicurezza dei dati e dei sistemi dagli artt.32 e 34 del Regolamento, avuto riguardo anche alla notifica delle violazioni dei dati personali di cui all'art.33 del Regolamento stesso.

Firmato digitalmente da ROBERTO FRACCIA

CAPITOLO 4 Conservazione

4.1. Sistema di conservazione

Nella Pubblica Amministrazione, il sistema di gestione informatica dei documenti trasferisce al sistema di conservazione, ai sensi dell'art. 44, comma 1-bis, del CAD[41],:

a) i fascicoli informatici chiusi e le serie informatiche chiuse, trasferendoli dall'archivio corrente o dall'archivio di deposito;
b) i fascicoli informatici e le serie non ancora chiuse trasferendo i documenti in essi contenuti sulla base di specifiche esigenze dell'ente, con particolare attenzione per i rischi di obsolescenza tecnologica.

Il sistema di conservazione assicura, dalla presa in carico fino all'eventuale scarto, la conservazione dei seguenti oggetti digitali in esso conservati, tramite l'adozione di regole, procedure e tecnologie, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità:

a) i documenti informatici e i documenti amministrativi informatici con i metadati ad essi associati;
b) le aggregazioni documentali informatiche (fascicoli e serie) con i metadati ad esse associati contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che costituiscono le aggregazioni medesime, nel rispetto di quanto indicato per le Pubbliche Amministrazioni nell'articolo 67, comma 2, del DPR 445/2000[42] e art. 44, comma 1-bis, CAD.

Il sistema di conservazione garantisce l'accesso all'oggetto conservato per il periodo previsto dal piano di conservazione del titolare dell'oggetto della conservazione e dalla normativa vigente, o per un tempo superiore eventualmente concordato tra le parti, indipendentemente dall'evoluzione del contesto tecnologico.

Il sistema di conservazione è almeno logicamente distinto dal sistema di gestione informatica dei documenti.

Gli elenchi degli standard, delle specifiche tecniche e dei formati utilizzabili quali riferimento per il

[41] L'art. 44, comma 1-bis, del CAD prevede che: "Il sistema di gestione dei documenti informatici delle pubbliche amministrazioni è gestito da un responsabile che opera d'intesa con il dirigente dell'ufficio di cui all'articolo 17 del presente Codice, il responsabile del trattamento dei dati personali di cui all'articolo 29 del decreto legislativo 30 giugno 2003, n. 196, ove nominato, e con il responsabile del sistema della conservazione dei documenti informatici delle pubbliche amministrazioni, nella definizione e gestione delle attività di rispettiva competenza. Almeno una volta all'anno il responsabile della gestione dei documenti informatici provvede a trasmettere al sistema di conservazione i fascicoli e le serie documentarie anche relative a procedimenti non conclusi".
[42] L'art. 67, comma 2, del TUDA prevede che: "Il trasferimento deve essere attuato rispettando l'organizzazione che i fascicoli e le serie avevano nell'archivio corrente".

Firmato digitalmente da ROBERTO FRACCIA

sistema di conservazione sono riportati negli allegati 2 "Formati di file e riversamento" e 4 "Standard e specifiche tecniche".

4.2. Pacchetti informativi

Gli oggetti della conservazione sono trattati dal sistema di conservazione in pacchetti informativi che si distinguono in:

a) pacchetti di versamento;
b) pacchetti di archiviazione;
c) pacchetti di distribuzione.

L'interoperabilità tra i sistemi di conservazione dei soggetti che svolgono attività di conservazione è garantita dall'applicazione delle specifiche tecniche del pacchetto di archiviazione definite dalla norma UNI 11386 - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.

Il Titolare dell'oggetto della conservazione utilizza, già al momento della formazione, le modalità e i formati individuati nel manuale di gestione e nel manuale di conservazione in conformità con le presenti Linee Guida.

4.3. Modelli organizzativi della conservazione

Le Pubbliche Amministrazioni realizzano il processo di conservazione ai sensi dall'art. 34, comma 1-bis, del CAD[43], fatte salve le competenze del Ministero per i beni e le attività culturali e del turismo ai sensi del decreto legislativo 22 gennaio 2004, n. 42.

Il processo di conservazione può essere pertanto svolto all'interno o all'esterno della struttura organizzativa dell'ente.

I requisiti del processo di conservazione, le responsabilità e i compiti del responsabile della conservazione e del responsabile del servizio di conservazione, e le loro modalità di interazione sono formalizzate nel manuale di conservazione del Titolare dell'oggetto della conservazione e nelle specifiche del contratto di servizio o dell'accordo. Tali modalità trovano riscontro anche nel manuale di conservazione del conservatore.

[43] L'art. 34, comma 1-bis, del CAD prevede che: "Le pubbliche amministrazioni possono procedere alla conservazione dei documenti informatici:
a) all'interno della propria struttura organizzativa;
b) affidandola, in modo totale o parziale, nel rispetto della disciplina vigente, ad altri soggetti, pubblici o privati che possiedono i requisiti di qualità, di sicurezza e organizzazione individuati, nel rispetto della disciplina europea, nelle Linee guida di cui all'art 71 relative alla formazione, gestione e conservazione dei documenti informatici nonché in un regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici emanato da AgID, avuto riguardo all'esigenza di assicurare la conformità dei documenti conservati agli originali nonché la qualità e la sicurezza del sistema di conservazione".

Firmato digitalmente da ROBERTO FRACCIA

Al fine di garantire l'autenticità, l'integrità, l'affidabilità, la leggibilità e la reperibilità dei documenti, i fornitori di servizi di conservazione devono possedere requisiti di elevato livello in termini di qualità e sicurezza in aderenza allo standard ISO/IEC 27001 (*Information security management systems - Requirements*) del sistema di gestione della sicurezza delle informazioni nel dominio logico, fisico e organizzativo nel quale viene realizzato il processo di conservazione e ISO 14721 OAIS (*Open Archival Information System - Sistema informativo aperto per l'archiviazione)*, e alle raccomandazioni ETSI TS 101 533-1 v. 1.2.1, *Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni*.

4.4. Ruoli e responsabilità

I ruoli individuati nel processo di conservazione sono:

a) titolare dell'oggetto della conservazione;
b) produttore dei PdV;
c) utente abilitato;
d) responsabile della conservazione
e) conservatore.

Nelle Pubbliche Amministrazioni, il ruolo di produttore del PdV è svolto da persona interna alla struttura organizzativa.

L'utente abilitato può richiedere al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge e nelle modalità previste dal manuale di conservazione.

Nelle Pubbliche Amministrazioni il responsabile della gestione documentale o il coordinatore della gestione documentale, ove nominato, svolge il ruolo di produttore di PdV e assicura la trasmissione del pacchetto di versamento al sistema di conservazione, secondo le modalità operative definite nel manuale di conservazione.

Nel caso di affidamento a terzi, il produttore di PdV provvede a generare e trasmettere al sistema di conservazione i pacchetti di versamento nelle modalità e con i formati concordati con il conservatore e descritti nel manuale di conservazione del sistema di conservazione. Provvede inoltre a verificare il buon esito della operazione di trasferimento al sistema di conservazione tramite la presa visione del rapporto di versamento prodotto dal sistema di conservazione stesso.

4.5. Responsabile della conservazione

Il responsabile della conservazione opera secondo quanto previsto dall'art. 44, comma 1-quater, del CAD[44].

[44] L'art. 44, comma 1-quater, del CAD prevede che: "Il responsabile della conservazione, che opera d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei sistemi informativi, può affidare, ai sensi dell'articolo 34, comma 1-bis, lettera b), la conservazione dei documenti informatici ad

Firmato digitalmente da ROBERTO FRACCIA

Nella Pubblica Amministrazione, il responsabile della conservazione:

a) è un ruolo previsto dall'organigramma del Titolare dell'oggetto di conservazione;
b) è un dirigente o un funzionario interno formalmente designato e in possesso di idonee competenze giuridiche, informatiche ed archivistiche;
c) può essere svolto dal responsabile della gestione documentale o dal coordinatore della gestione documentale, ove nominato.

Per i soggetti diversi dalla Pubblica Amministrazione, il ruolo del responsabile della conservazione può essere svolto da un soggetto esterno all'organizzazione, in possesso di idonee competenze giuridiche, informatiche ed archivistiche, purché terzo rispetto al Conservatore al fine di garantire la funzione del Titolare dell'oggetto di conservazione rispetto al sistema di conservazione.

Il responsabile della conservazione definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.

Il responsabile della conservazione, sotto la propria responsabilità, può delegare lo svolgimento delle proprie attività o parte di esse a uno o più soggetti, che all'interno della struttura organizzativa, abbiano specifiche competenze ed esperienze. Tale delega, riportata nel manuale di conservazione, deve individuare le specifiche funzioni e competenze delegate.

In particolare, il responsabile della conservazione:

a) definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;
b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
c) genera e sottoscrive il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
d) genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
f) effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;
g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;
h) provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
i) predispone le misure necessarie per la sicurezza fisica e logica del sistema di conservazione come previsto dal par. 4.11;
j) assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
l) provvede per le amministrazioni statali centrali e periferiche a versare i documenti

altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative, e tecnologiche e di protezione dei dati personali. Il responsabile della conservazione della pubblica amministrazione, che opera d'intesa, oltre che con i responsabili di cui al comma 1-bis, anche con il responsabile della gestione documentale, effettua la conservazione dei documenti informatici secondo quanto previsto all'articolo 34, comma 1-bis".

Firmato digitalmente da ROBERTO FRACCIA

informatici, le aggregazioni informatiche e gli archivi informatici, nonché gli strumenti che ne garantiscono la consultazione, rispettivamente all'Archivio centrale dello Stato e agli archivi di Stato territorialmente competenti, secondo le tempistiche fissate dall'art. 41, comma 1, del Codice dei beni culturali[45];

m) predispone il manuale di conservazione di cui al par. 4.7 e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Nel caso in cui il servizio di conservazione venga affidato ad un conservatore, le attività suddette o alcune di esse, ad esclusione della lettera m), potranno essere affidate al responsabile del servizio di conservazione, rimanendo in ogni caso inteso che la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile, rimane in capo al responsabile della conservazione, chiamato altresì a svolgere le necessarie attività di verifica e controllo in ossequio alle norme vigenti sul servizi affidati in outsourcing dalle PA.

Si precisa che il nominativo ed i riferimenti del responsabile della conservazione devono essere indicati nelle specifiche del contratto o della convenzione di servizio con il Conservatore nel quale sono anche riportate le attività affidate al responsabile del servizio di conservazione.

4.6. Manuale di conservazione

Il manuale di conservazione è un documento informatico che deve illustrare dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.

Il manuale di conservazione, inoltre, deve riportare:

a) i dati dei soggetti che nel tempo hanno assunto la responsabilità del sistema di conservazione, descrivendo in modo puntuale, in caso di delega, i soggetti, le funzioni e gli ambiti oggetto della delega stessa;
b) la struttura organizzativa comprensiva delle funzioni, delle responsabilità e degli obblighi dei diversi soggetti che intervengono nel processo di conservazione;
c) la descrizione delle tipologie degli oggetti digitali sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di oggetti e delle eventuali eccezioni;
d) la descrizione delle modalità di presa in carico di uno o più pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento;
e) la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione;
f) la modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;
g) la descrizione del sistema di conservazione, comprensivo di tutte le componenti tecnologiche, fisiche e logiche, opportunamente documentate e delle procedure di gestione

[45] L'art. 41, comma 1, del Codice dei beni culturali prevede che: "Gli organi giudiziari e amministrativi dello Stato versano all'archivio centrale dello Stato e agli archivi di Stato i documenti relativi agli affari esauriti da oltre trent'anni, unitamente agli strumenti che ne garantiscono la consultazione. Le liste di leva e di estrazione sono versate settant'anni dopo l'anno di nascita della classe cui si riferiscono. Gli archivi notarili versano gli atti notarili ricevuti dai notai che cessarono l'esercizio professionale anteriormente all'ultimo centennio".

Firmato digitalmente da ROBERTO FRACCIA

e di evoluzione delle medesime;
h) la descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie;
i) la descrizione delle procedure per la produzione di duplicati o copie;
j) i tempi entro i quali le diverse tipologie di oggetti digitali devono essere trasferite in conservazione ed eventualmente scartate, qualora, nel caso delle Pubbliche Amministrazioni, non siano già indicati nel piano di conservazione allegato al manuale di gestione documentale;
k) le modalità con cui viene richiesta la presenza di un pubblico ufficiale, indicando anche quali sono i casi per i quali è previsto il suo intervento;
l) le normative in vigore nei luoghi dove sono conservati gli oggetti digitali.

Le Pubbliche Amministrazioni sono tenute a redigere, adottare con provvedimento formale e pubblicare sul proprio sito istituzionale il Manuale di conservazione.

La pubblicazione è realizzata in una parte chiaramente identificabile dell'area "Amministrazione trasparente" prevista dall'art. 9 del d.lgs. 33/2013.

In caso di affidamento del servizio di conservazione ad un conservatore esterno, le Pubbliche Amministrazioni possono descrivere nel proprio manuale anche le attività del processo di conservazione affidate al conservatore, in conformità con il contenuto del manuale di conservazione predisposto da quest'ultimo, o rinviare, per le parti di competenza, al manuale del conservatore esterno.

Resta fermo l'obbligo in carico alla Pubblica Amministrazione di individuare e pubblicare i tempi di versamento, le tipologie documentali trattate, i metadati, le modalità di trasmissione dei PdV e le tempistiche di selezione e scarto dei propri documenti informatici.

Resta ferma inoltre la competenza del Ministero dei beni e delle attività culturali e del Turismo in materia di tutela dei sistemi di conservazione sugli archivi pubblici e privati che rivestono interesse storico particolarmente importante, così come disciplinato dalla normativa sui beni culturali.

4.7. Processo di conservazione

Il trasferimento dell'oggetto di conservazione nel sistema di conservazione avviene generando un PdV nelle modalità e con il formato previsti dal manuale di conservazione di cui al paragrafo 4.6.

Il processo di conservazione prevede:

a) l'acquisizione da parte del sistema di conservazione del PdV per la sua presa in carico;
b) la verifica che il PdV e gli oggetti digitali contenuti siano coerenti con le modalità previste dal manuale di conservazione e con quanto indicato nell' allegato 2 "Formati di file e riversamento" relativo ai formati;
c) il rifiuto del PdV, nel caso in cui le verifiche di cui alla lettera b) abbiano evidenziato delle anomalie. Il numero massimo di rifiuti è stabilito nell'ambito di un contratto o convenzione;
d) la generazione, anche in modo automatico, del rapporto di versamento relativo ad uno o più pacchetti di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo universale coordinato (UTC), e una o più impronte, calcolate sull'intero contenuto del pacchetto di versamento, secondo le modalità descritte nel manuale di conservazione;
e) la sottoscrizione del rapporto di versamento con la firma digitale o firma elettronica

Firmato digitalmente da ROBERTO FRACCIA

qualificata o avanzata apposta dal responsabile della conservazione o dal responsabile del servizio di conservazione, ove prevista nel manuale di conservazione;

f) la preparazione, la sottoscrizione con firma digitale o firma elettronica - qualificata o avanzata - del responsabile della conservazione o del responsabile del servizio di conservazione o con il sigillo elettronico - qualificato o avanzato – apposto dal conservatore esterno, nonché la gestione del pacchetto di archiviazione sulla base delle specifiche della struttura dati indicate dallo standard UNI 11386 e secondo le modalità riportate nel manuale di conservazione;
g) ai fini dell'esibizione richiesta dall'utente la preparazione e la sottoscrizione con firma digitale o firma elettronica qualificata o avanzata del responsabile della conservazione o del responsabile del servizio di conservazione, oppure l'apposizione del sigillo elettronico qualificato o avanzato, secondo le modalità indicate nel manuale di conservazione, di pacchetti di distribuzione che possono contenere parte, uno o più pacchetti di archiviazione;
h) ai soli fini della interoperabilità tra sistemi di conservazione, la produzione di pacchetti di distribuzione coincidenti con i pacchetti di archiviazione o comunque contenenti pacchetti di archiviazione generati sulla base delle specifiche della struttura dati indicate dallo standard UNI 11386 e secondo le modalità riportate nel manuale di conservazione;
i) la produzione di duplicati informatici o di copie informatiche effettuati su richiesta degli utenti in conformità a quanto previsto dalle presenti linee guida;
j) la produzione di copie informatiche tramite attività di riversamento al fine di adeguare il formato alle esigenze conservative di leggibilità nel tempo in base alle indicazioni previste dall'allegato 2 "Formati di file e riversamento";
k) l'eventuale scarto del pacchetto di archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dalla norma o secondo quanto indicato dal piano di conservazione del Titolare dell'oggetto di conservazione e le procedure descritte nel successivo paragrafo 4.12;
l) nel caso degli archivi pubblici o privati, che rivestono interesse storico particolarmente importante, l'eventuale scarto del pacchetto di archiviazione avviene previa autorizzazione del MIC rilasciata al Titolare dell'oggetto della conservazione secondo quanto previsto dalla normativa vigente in materia e al successivo paragrafo 4.12.

Nel caso di affidamento a terzi del servizio di conservazione le modalità sono indicate nei manuali del Titolare dell'oggetto di conservazione e del conservatore e concordate tra le parti.

4.8. Infrastrutture

Fatto salvo quanto previsto dal Codice dei beni culturali, nel rispetto del principio di libera circolazione dei dati all'interno dell'Unione europea[46], si sottolinea l'obbligo, in capo al fornitore del servizio di conservazione, di conservare e rendere disponibili le descrizioni del sistema di conservazione all'interno del territorio nazionale. I conservatori devono altresì garantire alle amministrazioni l'accesso elettronico effettivo e tempestivo ai dati conservati, indipendentemente dallo Stato membro nel cui territorio i dati sono conservati.

Le componenti tecnologiche hardware e software utilizzate dai sistemi di conservazione delle Pubbliche Amministrazioni e dei conservatori sono segregate logicamente. Qualora i servizi di conservazione siano erogati in modalità cloud, il servizio deve essere qualificato come previsto dalla Circolare Agid n. 3 del 9 aprile 2018 e, conseguentemente, essere presente nel "Catalogo dei servizi

[46] Reg. (UE) 2018/1807 all'articolo 4, paragrafo 1 recita:" Gli obblighi di localizzazione di dati sono vietati a meno che siano giustificati da motivi di sicurezza pubblica nel rispetto del principio di proporzionalità."

Firmato digitalmente da ROBERTO FRACCIA

Cloud per la PA qualificati" pubblicato sul sito di Agid.

I sistemi di conservazione devono essere realizzati nel rispetto del principio di integrità e riservatezza, nonché dei principi di protezione fin dalla progettazione e per impostazione predefinita, e dei conseguenti adempimenti previsti dagli artt. 25[47] e 32 del citato Regolamento UE 679/2016.

4.9. Modalità di esibizione

Fermi restando gli obblighi previsti in materia di esibizione dei documenti dalla normativa vigente, il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, agli oggetti digitali conservati, attraverso la produzione di pacchetti di distribuzione secondo le modalità descritte nel manuale di conservazione, prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio e modalità di accesso diverse, in funzione delle tipologie di dati personali trattati, nonché delle operazioni di trattamento consentite.

Nel caso di affidamento esterno del servizio di conservazione tali modalità sono concordate tra le parti e indicate nei rispettivi manuali.

4.10. Misure di sicurezza

Nell'attuazione delle presenti Linee Guida, le Pubbliche Amministrazioni sono tenute ad ottemperare alle misure minime di sicurezza ICT emanate dall'AgID con circolare del 18 aprile 2017, n. 2/2017. In tale ottica, il responsabile della conservazione, di concerto con il responsabile per la transizione digitale, con il responsabile della gestione documentale e acquisito il parere del responsabile della protezione dei dati personali, predispone il piano della sicurezza del sistema di gestione informatica dei documenti, prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali, ai sensi dell'art. 32 del Regolamento UE 679/2016[48], anche in funzione delle tipologie di dati trattati, quali quelli riferibili alle categorie particolari di cui agli artt. 9-10 del Regolamento stesso.

---

[47] L'art. 25 del Regolamento "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita**"**

[48] L'art. 32 del Regolamento (UE) 2016/679 prevede che: "1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. 3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere

Firmato digitalmente da ROBERTO FRACCIA

L'adozione delle predette misure è in capo al titolare o, in caso di trattamento effettuato per suo conto, al responsabile del trattamento, individuato sulla base dell'art.28 del Regolamento.

Il piano conterrà altresì la descrizione della proceduta da adottarsi in caso di violazione dei dati personali ai sensi degli artt. 33-34 del Regolamento UE 679/2016[49], e sarà redatto nell'ambito del piano generale della sicurezza, in coerenza con quanto previsto dal Piano Triennale per l'Informatica nella Pubblica Amministrazione vigente.
Le misure di sicurezza sono descritte nel manuale di conservazione di cui al par. 4.7.

Nel caso di affidamento esterno del servizio di conservazione le misure di sicurezza sono concordate tra le parti e indicate nei rispettivi manuali. In conformità all'art. 28 del Regolamento UE 679/2016, i soggetti esterni a cui è delegata la tenuta del sistema di conservazione sono individuati come Responsabili del trattamento dei dati e devono presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato.

I soggetti privati appartenenti ad organizzazioni che applicano particolari regole di settore per la sicurezza dei propri sistemi informatici adeguano il sistema di conservazione a tali regole. Le citate misure di sicurezza ICT emanate dall'AGID possono costituire, a tal fine, un modello di riferimento, fermo restando gli obblighi previsti dal citato Regolamento UE 679/2016.

I servizi devono sempre organizzati nel rispetto dei principi e dei requisiti previsti in materia di sicurezza dei dati e dei sistemi dagli artt.32 e 34 del Regolamento, avuto riguardo anche alla notifica delle violazioni dei dati personali di cui all'art.33 del Regolamento stesso.

4.11. Selezione e scarto dei documenti informatici

I documenti informatici e le aggregazioni documentali informatiche possono essere oggetto di selezione e scarto nel sistema di conservazione nel rispetto della normativa sui beni culturali.

Nel sistema di conservazione, la selezione e lo scarto dei pacchetti di archiviazione sono definiti dal Titolare dell'oggetto di conservazione e, nel caso delle Pubbliche Amministrazioni, secondo quanto indicato dal piano di conservazione. Nel caso di affidamento esterno del servizio di conservazione le modalità operative sono concordate dal Titolare dell'oggetto di conservazione e dal Conservatore.

Il responsabile della conservazione genera l'elenco dei pacchetti di archiviazione contenenti i documenti destinati allo scarto e, dopo aver verificato il rispetto dei termini temporali stabiliti dal piano di conservazione, lo comunica al responsabile della gestione documentale o del coordinatore della gestione documentale, ove nominato. In caso di affidamento esterno del servizio di conservazione l'elenco dei pacchetti di archiviazione contenenti i documenti destinati allo scarto è generato dal responsabile del servizio di conservazione e trasmesso al responsabile della conservazione che a sua volta, verificato il rispetto dei termini temporali stabiliti dal piano di

---

utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo. 4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri".

[49] Gli artt. 33 e 34 del Regolamento (UE) 2016/679 prevedono, rispettivamente, la procedura di notifica di una violazione dei dati personali all'autorità di controllo e quella di comunicazione di una violazione dei dati personali all'interessato.

Firmato digitalmente da ROBERTO FRACCIA

conservazione, lo comunica al responsabile della gestione documentale o al coordinatore della gestione documentale.

Nel caso degli archivi pubblici e degli archivi privati con il solo riferimento a quelli dichiarati di interesse storico particolarmente importante l'autorizzazione è rilasciata ai sensi della normativa vigente in materia di beni culturali.

Il Titolare dell'oggetto di conservazione, una volta ricevuta l'autorizzazione, che può essere concessa anche solo su una parte dell'elenco proposto, procede alla distruzione dei pacchetti di archiviazione.

Nel caso di affidamento esterno del servizio di conservazione, il Titolare dell'oggetto di conservazione, una volta ricevuta l'autorizzazione, che può essere concessa anche solo su una parte dell'elenco proposto, provvede a trasmetterlo al conservatore affinché provveda alla distruzione dei pacchetti di archiviazione.

L'operazione di scarto viene tracciata sul sistema mediante la produzione delle informazioni essenziali sullo scarto, inclusi gli estremi della richiesta di nulla osta allo scarto e il conseguente provvedimento autorizzatorio.

Al termine delle operazioni di distruzione dal sistema di conservazione dei pacchetti di archiviazione scartati, il Titolare dell'oggetto di conservazione notifica l'esito della procedura di scarto agli organi preposti alla tutela come già indicato in precedenza. Analoga comunicazione è inviata al Ministero dell'interno in caso di eliminazione di pacchetti di archiviazione contenenti documenti e/o dati di carattere riservato.

Tale operazione avrà completa efficacia solo al momento del completo aggiornamento delle copie di sicurezza del sistema.

I documenti e le aggregazioni documentali informatiche sottoposti a scarto nel sistema di conservazione devono essere distrutti anche in tutti i sistemi gestiti dal Titolare dell'oggetto di conservazione.

Firmato digitalmente da ROBERTO FRACCIA

Elenco dei formati ammessi alla ricezione

Salvo i casi in cui, in relazione a specifici flussi documentali, vi siano particolari previsioni normative, provvedimenti del Responsabile della gestione documentale o istruzioni operative per la fruizione di servizi telematici che dispongano diversamente, l'Istituto assicura l'accettazione dei documenti elettronici inviati ai suoi uffici tramite posta elettronica, posta elettronica certificata e altri canali telematici oppure consegnati direttamente su supporti informatici quando sono prodotti in uno dei seguenti formati:

- .pdf (compreso il formato PDF/A);
- .gif, .jpg, .tif;
- OOOXML - Office Open XML (principali estensioni: .docx, .xlsx, .pptx);
- OpenDocument – OpenOffice XML (principali estensioni: odt, ods, odp);
- .txt (codifica Unicode UTF 8);
- .zip (a condizione che i file contenuti all'interno del file compresso siano prodotti in uno dei formati previsti nel presente elenco);
- .p7m (documenti firmati digitalmente con sottoscrizione di tipo CADES e a condizione che i file originali oggetto di sottoscrizione digitale siano prodotti in uno dei formati previsti nel presente elenco).
- .eml, .msg – Messaggi di posta elettronica

In ogni caso i documenti elettronici inviati o consegnati all'Istituto dovranno essere privi di elementi attivi, tra cui macro e campi variabili.
L'Istituto si riserva comunque la facoltà di non accettare documenti informatici prodotti in formati che consentano la modifica dei contenuti.

Firmato digitalmente da ROBERTO FRACCIA

DOCUMENTI PER I QUALI SI STABILISCONO PARTICOLARI MODALITA' DI TRATTAMENTO

I documenti contenenti dati sanitari o giudiziari o comunque dati sensibili non sono scansionati.
Se in formato elettronico, devono essere previsti opportuni sistemi di crittazione per garantirne la riserva- tezza.

Firmato digitalmente da ROBERTO FRACCIA

NUVOLA– SEGRETERIA DIGITALE TIPOLOGIE

DI FASCICOLI ELETTRONICI

Allegato7

TIPOLOGIA	DESCRIZIONE	
FASCICOLO DI PROCEDIMENTO AMMINISTRATIVO	Conserva i documenti relativa ad una pluralità di atti tra loro autonomi, scanditi nel tempo e destinati allo stesso fine cioè all'emanazione di un provvedimento finale.	
FASCICOLO PERSONA FISICA: ALUNNO	Il fascicolo nominativo per alunno conserva tutta la documentazione, anche se appartenente a classifiche diverse, inerente uno specifico alunno.	
FASCICOLO PERSONA FISICA: PERSONALE	Il fascicolo nominativo per il personale conserva tutta la documentazione, anche se appartenente a classifiche diverse, inerente uno specifico dipendente.	
FASCICOLO DI PERSONA FISICA/GIURIDICA: FORNITORI/CREDITORI	Il fascicolo nominativo per la persona fisica/giuridica conserva tutta la documentazione, anche se appartenente a classifiche diverse, inerente uno specifico creditore/fornitore.	
FASCICOLO ALTRI	Il fascicolo conserva tutta la documentazione relativa a diverse tipologie di procedimenti amministrativi.	

Firmato digitalmente da ROBERTO FRACCIA

Allegato08
Accertamento visita fiscale
Approvazione Consuntivo
Approvazione Programma Annuale
Archivio Posta Elettronica
Bando di gara
Bando di gara
Bilancio web - Distinte di trasmissione
Bilancio web - Ricevuta distinte di trasmissione
Buono d'ordine
Calendario scolastico
Cessazione servizio Dipendente
Circolari
Circolari ATA
Circolari docenti
Circolari famiglie
Comunicazione assenza alunno
Concessione assemblea sindacale
Contrattazione integrativa-pubblicazione
Contratto fornitura beni e servizi
Contratto fornitura beni e servizi
Convocazione Collegio Docenti
Convocazione Consiglio classe/interclasse
Convocazione Consiglio di Istituto
Convocazione genitori
Convocazione Giunta esecutiva
Convocazione per nomina
CUD - CU Certificazione Unica
Decreto apettativa Dipendente
Decreto assenza L104 Dipendente
Decreto astensione facoltativa Dipendente
Decreto congedo maternità Dipendente

Firmato digitalmente da ROBERTO FRACCIA

Decreto congedo straordinario Dipendente
Decreto ferie Dipendente
Decreto permesso retribuito Dipendente
Decreto permesso sindacale Dipendente
Decreto Variazione
Denunce furti
Denunce infortuni alunni - personale
Denuncia INPS - UNIEMENS
Denuncia IRAP
Determina Dirigente Scolastico
Diploma-attestato richiesta
Diploma-attestato rilascio
Documenti con Timbro Digitale
Documenti generici
Documenti generici alunni
Documenti generici personale
Domande riscatto
DURC / Tracciabilità / Equitalia
Edilizia Scolastica
Emergenza e Evacuazione
Emissione ricostruzione carriera
Eventi - iniziative - celebrazioni
Fattura
Fonogramma assenza
Formazione/Aggiornamento
GDPR Web - Consenso trattamento dati per Firma grafometrica
GDPR Web - Informativa
GDPR Web - Nomina o incarico
Graduatorie
Inventario: nomine consegnatari
Inventario: passaggio di consegne
Inventario: ricognizione

Firmato digitalmente da ROBERTO FRACCIA

Inventario: scarico beni
Iscrizione/Revoca sindacale Dipendente
MAD
Mandato di pagamento
Messe a disposizione MAD
Modello 770
Modulistica
Monitoraggio INVALSI
Nomine/Incarichi/Autorizzazioni a Personale
Normative
Nulla Osta richiesta
Nulla Osta rilascio
Organico: invio dati
PA04 / TFR / Riscatti
Piano attività DOCENTI / ATA
POF - PTOF
Posta elettronica inviata protocollata
Pratiche ricostruzione carriera
Preventivo Fornitore
RAV Rapporto autovalutazione
Registro - Verbali scrutini
Registro Elettronico - Elaborati III Media
Registro Elettronico - Registri dei docenti
Registro Elettronico - Registri di classe
Registro Elettronico - Tabelloni
Registro Elettronico - Verbali
Relazione Consuntivo
Relazione Programma Annuale
Richiesta accesso agli atti
Richiesta apettativa Dipendente
Richiesta assemblea sindacale
Richiesta assenza L104 Dipendente
Richiesta assenza personale ATA

Firmato digitalmente da ROBERTO FRACCIA

Richiesta assenza personale docente
Richiesta astensione facoltativa Dipendente
Richiesta congedo maternità Dipendente
Richiesta congedo straordinario Dipendente
Richiesta di pubblicazione all’albo
Richiesta ferie Dipendente
Richiesta intervento Comune/Provincia
Richiesta permesso retribuito Dipendente
Richiesta permesso sindacale Dipendente
Richiesta preventivo
Richiesta visita fiscale
Richiesta/trasmissione fascicolo Personale
Richieste di sportello digitale
Richieste SERCOP
Risposta mezzo mail da procedimento
Servizi Web - Domanda di messa a disposizione ATA
Servizi Web - Domanda di messa a disposizione Docente
Servizi Web - Richiesta di accesso civico generalizzato
Servizi Web - Richiesta di accesso civico semplice
Statistiche assenteismo Dipendenti
Tempestività pagamenti
Uscite didattiche
Verbale Consiglio classe/interclasse
Verbale Consiglio di Istituto
Verbale Giunta esecutiva
Verbali Collegio Docenti

Firmato digitalmente da ROBERTO FRACCIA

Piano di conservazione e scarto per gli archivi delle Istituzioni scolastiche (massimario)

Premessa

Il presente massimario, è frutto del lavoro di revisione su un primo elaborato redatto dalla Provincia autonoma di Trento, condotto da un Gruppo di lavoro misto fra la Soprintendenza archivistica e l'Ufficio scolastico regionale del Piemonte e, successivamente, ulteriormente rivisto da un gruppo di lavoro istitutito presso la Direzione generale per gli archivi.

Esso fornisce indicazioni riguardo ai documenti da conservare illimitatamente o che possono essere proposti per lo scarto dopo un periodo di tempo stabilito.

Per favorire l'utilizzo da parte dei responsabili degli archivi scolastici, le tipologie documentarie non si trovano suddivise per periodi di conservazione, ma vengono presentate in base alle *due aree organizzative* tipiche degli istituti scolastici, quella *amministrativa* e quella *didattica*, a loro volta suddivise in *aree funzionali*. Si vuole in tal modo agevolare chi deve predisporre gli elenchi di scarto dei documenti che si presentano normalmente raggruppati secondo le funzioni o le attività che li hanno prodotti. Alle medesime necessità operative intende rispondere *l'indice alfabetico* che segue la tabella organizzata per funzioni. Naturalmente la singola tipologia documentaria è reperibile nell'indice sia in base alla prima parola della denominazione con cui compare nella tabella sia tramite le altre parole significative che compaiono nella medesima denominazione.

Per i documenti derivanti da attività avviate di recente, come ad esempio il sistema di valutazione delle scuole (INVALSI), si è preferito adottare criteri di conservazione relativamente più severi, in attesa di verificarne l'effettivo valore documentale.

Le indicazioni per la selezione e la conservazione si applicano anche a tutti i documenti prodotti per i *Corsi post-diploma (iFTS)* come pure a quelli relativi all'istituzione ed al funzionamento dei *Centri territoriali permanenti (CTP, ex 150 ore)*

Il massimario può costituire un valido strumento anche per gli *Istituti paritari*, i quali hanno gli stessi obblighi di conservazione degli Istituti pubblici per quanto concerne i documenti relativi al personale, agli alunni, alla didattica e alla sicurezza; invece per i documenti amministrativo-contabili e gestionali possono liberamente far riferimento al presente piano di conservazione nel rispetto della normativa civilistica e fiscale.

Nel caso in cui l'Istituto scolastico abbia adottato procedure informatiche per lo svolgimento di determinate funzioni occorrerà individuare la modalità più affidabile per la conservazione dei documenti di cui sia obbligatoria la conservazione illimitata. Ad esempio il registro di protocollo informatico potrà essere conservato stampando su carta e rilegando il relativo tabulato, firmandolo per dargli certezza giuridica, oppure conservandolo su supporti digitali che dovranno essere mano mano adeguati alle norme tecniche e amministrative in continua evoluzione.

Firmato digitalmente da ROBERTO FRACCIA

STRUTTURA DEL MASSIMARIO

A) Area amministrativa:

1. Norme, disposizioni organizzative, ispezioni
2. Organi Collegiali e Direttivi
3. Carteggio e atti
4. Contabilità
5. Edifici ed impianti
6. Inventari dei beni
7. Personale docente e non docente
8. Alunni

B) Area didattica:

1. Documentazione ufficiale dell'attività didattica
2. Attività didattiche specifiche

Abbreviazioni e sigle:

C.M.	=	Circolare Ministeriale
D.M.	=	Decreto Ministeriale
L.	=	Legge
M.P.I.	=	Ministero Pubblica Istruzione
OO.CC.	=	Organi Collegiali
R.D.	=	Regio Decreto
D.I.	=	Decreto Interministeriale
T.I.	=	Tempo indeterminato
T.D.	=	Tempo determinato

Indicazioni per la procedura di scarto

La procedura di scarto si svolge in quattro fasi:

A) Il dirigente dell'istituzione scolastica trasmette alla Soprintendenza Archivistica, con lettera protocollata, l'elenco in due copie, entrambe da lui firmate, delle tipologie archivistiche che si ritiene non abbiano più utilità amministrativa, chiedendo l'autorizzazione prevista dal D.lgs. 42/2004 art. 21.
In testa all'elenco di scarto, redatto conformemente al modello (all.2), è indicato il numero di pagine di cui si compone. L'elenco comprende:

- la descrizione delle tipologie dei documenti (es. elaborati delle prove in classe, richieste di certificati, ecc.);
- gli anni di riferimento;
- la quantità del materiale (in numero di faldoni, scatole, pacchi e in peso approssimativo);
- i motivi della proposta di eliminazione.

B) La Soprintendenza Archivistica restituisce una copia dell'elenco, vistato con approvazione totale o parziale.

C) L'Istituzione scolastica provvede a distruggere i documenti da scartare. Qualora ci si avvalga di soggetti esterni (come ditte o organizzazioni di volontariato, ex D.P.R.37/2001, art. 8, che operano nella raccolta della carta) occorre che questi diano attestazione scritta dell'effettiva distruzione (tramite triturazione, incenerimento, macerazione al fine di riciclare il materiale) della documentazione loro conferita.

D. l'Istituzione scolastica trasmette alla Soprintendenza Archivistica copia del verbale attestante le modalità dell'avvenuta distruzione.

Firmato digitalmente da ROBERTO FRACCIA

A -Area amministrativa

A1 – Norme, disposizioni organizzative e ispezioni

N.	*Tipologia Documentaria*	*Tempi di conservazione*	*Note e riferimenti normativi*
A1/1	Leggi, regolamenti e tutta la documentazione relativa a • istituzione della scuola • intitolazione • eventuali accorpamenti e trasformazioni (ad es. in istituto comprensivo)	ILLIMITATA	Compresi eventuali statuti e regolamenti per gli istituti paritari
A1/2	Norme e regolamenti interni (regolamento dell'istituto, carta dei servizi, regolamenti della biblioteca, dei laboratori e direttive varie ecc.)	ILIMITATA	
A1/3	Norme e disposizioni Economato	ILLIMITATA	
A1/4	Norme e disposizioni relative al personale e CCNL	50 anni dall'entrata in vigore	
A1/5	Registro verbali riunioni per contrattazione d'istituto	ILLIMITATA	
A1/6	Contrattazione d'istituto	ILLIMITATA	
A1/7	Privacy – Documento programmatico di sicurezza dati (DPS)	ILLIMITATA	
A1/8	Documento valutazione dei rischi (L.626/94) e relativi allegati (es. piani di evacuazione, controlli periodici, nomine, ecc.)	ILLIMITATA	Le relative prove di evacuazione possono essere scartate dopo 6 anni
A1/9	Certificazioni di qualità e accreditamenti (es. ministeriali e regionali, ecc.)	ILLIMITATA	
A1/10	Circolari e ordinanze interne esplicative e direttive	ILLIMITATA di almeno 1 esemplare per circolare/ordinanza	
A1/11	Convenzioni e accordi di rete (con scuole, con enti ecc.)	ILLIMITATA	
A1/12	Verbali di consegna ed elenchi di consistenza di archivi o altri beni inventariati	ILLIMITATA	In occasione di accorpamenti di scuole statali o di estinzione di scuole già parificate o paritarie
A1/13	Norme e disposizioni relative all'archivio	ILLIMITATA	
A1/14	Titolari di classificazione d'archivio (compresi quelli non più in uso)	ILLIMITATA	

Firmato digitalmente da ROBERTO FRACCIA

A1/15	Scarto di atti d'archivio (procedure, elenchi, autorizzazioni e verbali di distruzione…)	ILLIMITATA	

A2 - Organi collegiali e direttivi

N.	***Tipologia Documentaria***	***Tempi di conservazione***	***Note e riferimenti normativi***
A2/1	Verbali di riunioni collegiali (precedenti i Decreti Delegati del 1974)	ILLIMITATA	
A2/2	Verbali del Consiglio di Amministrazione	ILLIMITATA	Per le sole istituzioni scolastiche a gestione economica autonoma (L.15 giugno 1931, n.889; C.M..21 agosto 1945, n.28; C.M.28 maggio 1960, n.213)
A2/3	Registri dei verbali del Consiglio o Staff di Presidenza	ILLIMITATA	
A2/4	Verbali delle Commissioni Elettorali. Atti di nomina degli Organi collegiali a livello di circolo e di istituto	**ILLIMITATA**	
A2/5	Atti delle elezioni degli Organi collegiali: - verbale di consegna di materiale elettorale - liste candidati - elenchi elettori - certificati elettorali - scheda votazioni - prospetti per il calcolo dei voti - tabelle scrutinio	**Scartabili dopo 6 anni dalle elezioni** **Conservando 1 campione di scheda non utilizzata per ciascuna elezione e per ciascuna categoria di elettori**	**In caso di contenzioso i 6 anni decorrono dalla data di esaurimento del contenzioso**
A2/6	Registri dei verbali degli Organi collegiali (Consiglio di circolo o di istituto, Giunta esecutiva, Collegio docenti, Consigli di classe o di interclasse) e degli eventuali gruppi di lavoro derivati (es. dipartimenti, commissioni, ambiti disciplinari ecc)	ILLIMITATA .	
A2/7	Convocazioni riunioni Organi Collegiali	**Scartabili dopo 6 anni**	In caso di contenzioso i 6 anni decorrono dalla data di esaurimento del contenzioso.
A2/8	Registro delle deliberazioni	ILLIMITATA	
A2/9	Determinazioni dirigenziali (raccolte in serie cronologiche)	ILLIMITATA	

Firmato digitalmente da ROBERTO FRACCIA

A3 - Carteggio ed atti

N.	***Tipologia Documentaria***	***Tempi di conservazione***	***Note e riferimenti normativi***
A3/1	Registri di protocollo (generali e riservati)	ILLIMITATA	Altrimenti detti Protocolli della corrispondenza
A3/2	Repertori dei fascicoli d'archivio	ILLIMITATA	
A3/3	Rubriche alfabetiche del protocollo	ILLIMITATA	
A3/4	Registro della posta in partenza e/o documentazione attestante la spedizione o la ricezione (anche a mano o mediante affissione in bacheca)	10 anni dalla data dell'ultima registrazione (salvo contenziosi in corso)	
A3/5	**Corrispondenza** in arrivo e in partenza (compresa la riservata)	ILLIMITATA	Per la corrispondenza riservata v. R.D.30 aprile 1924, n.965, art.11; L.7 maggio 1948, n.1243, art.2; C.M.28 gennaio 1954, n.360.
A3/6	Richiesta di accesso ai documenti	Scartabili dopo 1 anno, conservando illimitatamente eventuali registri delle richieste (salvo contenziosi in corso)	
A3/7	Richieste di copie di atti e relativo rilascio	Scartabili dopo 1 anno, conservando illimitatamente eventuali registri delle copie rilasciate	
A3/8	Richieste di certificati e loro trasmissione	Scartabili dopo 6 anni	
A3/9	Autorizzazioni all'uso di locali scolastici e impianti sportivi	Scartabili dopo 6 anni, conservando eventuali atti riassuntivi	
A3/10	Inchieste, indagini ambientali e socio-economiche	ILLIMITATA	
A3/11	Documentazione relativa a cerimonie, inaugurazioni e relazioni esterne	ILLIMITATA	

Firmato digitalmente da ROBERTO FRACCIA

A4 – Contabilità

N.	***Tipologia Documentaria***	***Tempi di conservazione***	***Note e riferimenti normativi***
A4/1	Bilanci o programmi annuali e conti consuntivi (in originale o nell'unica copia esistente)	ILLIMITATA	
A4/2	Giornale di cassa Partitario delle Entrate Partitario delle Uscite	ILLIMITATA	
A4/3	Mandati di pagamento e reversali con la relativa documentazione giustificativa (ordinativi di acquisto, buoni d'ordine, fatture, corrispondenza varia)	Scartabili dopo 10 anni, (previa verifica della conservazione dei rispettivi giornali di cassa e partitari) conservando illimitatamente progetti, collaudi, perizie degli impianti e delle manutenzioni straordinarie delle attrezzature durevoli (macchinari tecnici, arredi di particolare interesse, ecc.)	La possibilità di scartare i mandati si applica a quelli emessi dopo il 1975
A4/4	Convenzione di cassa con Istituto Cassiere	ILLIMITATA	
A4/5	Rapporti con Istituto Cassiere (corrispondenza)	Scartabili dopo 10 anni	
A4/6	Distinte di trasmissione al Tesoriere di reversali e mandati	Scartabili dopo 10 anni	
A4/7	Estratti conto bancari e postali	Scartabili dopo 10 anni	
A4/8	Registro delle operazioni di conto corrente postale	Scartabile dopo 10 anni	
A4/9	Bollettini di conto corrente postale, ricevute di versamento	Scartabili dopo 10 anni	
A4/10	Registro delle spese su aperture di credito e rendiconto trimestrale	ILLIMITATA	Mod.26 C.G. previsto per la registrazione delle spese effettuate su ordini di accreditamento. Rappresentava il documento più importante di tutta la contabilità erariale. Vi si registravano tutti i fatti riferiti ad ogni singolo capitolo
A4/11	Registri dei contratti per fornitura di materiali, espletamento di	ILLIMITATA	Era prevista la tenuta di un registro

Firmato digitalmente da ROBERTO FRACCIA

	servizi , assunzione personale		nel quale venivano annotati tutti i contratti stipulati dall'istituto, in ordine cronologico (R.D. 18 novembre 1923, n.2440)
N.	***Tipologia Documentaria***	***Tempi di conservazione***	***Note e riferimenti normativi***
A4/12	Contratti per fornitura di materiali, per espletamento di servizi, assunzione personale	50 anni, conservando illimitatamente il relativo registro (vedi A4/11)	In caso di perdita del registro la documentazione va conservata illimitatamente.
A4/13	Registro cronologico dei contratti	ILLIMITATA	Art. 29 c.1 lett. g del D.I.n.44/2001
A4/14	Contratti di prestazione d'opera di varia natura	50 anni, conservando illimitatamente il relativo registro (vedi A4/13)	Art. 29 c.1 lett. g del D.I. n.44/2001
A4/15	Documentazione prodotta e acquisita nel corso di transazioni, conciliazioni e ricorsi amministrativi e giurisdizionali	ILLIMITATA	Nel caso di documentazione relativa a dipendenti conservare nel fascicolo personale dell'interessato.
A4/16	Registri dei verbali della cassa scolastica	ILLIMITATA	Tenuti in conformità alla normativa vigente fino alla sua soppressione
A4/17	- Elenchi dei buoni libro concessi e documentazione di supporto - Cedole librarie	Scartabili dopo 6 anni, conservando illimitatamente l'elenco dei percipienti ed eventuali relazioni o rendiconti speciali	
A4/18	Contributi per biblioteca scolastica (documentazione relativa)	Scartabili dopo 6 anni, conservando illimitatamente il registro cronologico di entrata (vedi A6/1)	
A4/19	Matrici di buoni d'acquisto, generi di refezione / di consumo	Scartabili dopo 6 anni	
A4/20	Abbonamenti e/o acquisti a giornali, riviste e pubblicazioni: corrispondenza relativa	Scartabile dopo 6 anni, conservando illimitatamente gli elenchi dei periodici in abbonamento e delle pubblicazioni acquistate	Si suggerisce di conservare la documentazione relativa ai periodici /quotidiani ricevuti in abbonamento gratuito
A4/21	Acquisto di attrezzature, materiale, interventi di manutenzione: corrispondenza relativa	Scartabile dopo 10 anni	

Firmato digitalmente da ROBERTO FRACCIA

A4/22	Acquisto di materiale di consumo: corrispondenza relativa	Scartabile dopo 6 anni, conservando i relativi Registri di materiale facile consumo (vedi A4/23)	
N.	***Tipologia Documentaria***	***Tempi di conservazione***	***Note e riferimenti normativi***
A4/23	Registri dei materiali di facile consumo	Scartabili dopo 10 anni	
A4/24	Verbali di collaudo di apparecchiature ed attrezzature	Scartabili dopo la dismissione del bene, salvo contenzioso in corso	
A4/25	Certificati di garanzia di apparecchiature ed attrezzature	Scartabili dopo la dismissione del bene, salvo contenzioso in corso	
A4/26	Dotazioni strumentali: richieste di intervento	Scartabili dopo 6 anni	
A4/27	"Libretto di macchina" degli autoveicoli in dotazione presso l'istituto	Scartabile dopo 6 anni	Usato per la registrazione dei consumi di carburante.
A4/28	Bollettario di richiesta degli stampati	Scartabile dopo 6 anni	Modulistica precedente all'autonomia scolastica
A4/29	Registro delle tasse scolastiche (iscrizione, diploma…)	Scartabile dopo 10 anni dall'ultima registrazione, conservando a campione una annata ogni dieci	Vi si annotano gli esoneri a fianco dei nominativi degli alunni dispensati dal pagamento
A4/30	Mensa: richieste di iscrizione al servizio mensa ed elenchi presenze	Scartabili dopo 6 anni, conservando illimitatamente contratti, relazioni sull'attività, diete e menu seguiti	
A4/31	Trasporto alunni: richieste di iscrizione al servizio ed attestazioni di pagamento	Scartabili dopo 6 anni	Certificati originali allegati alla richiesta non soggetti a scadenza sono a disposizione degli interessati.
A4/32	Trasporto alunni: richieste per trasporto gratuito	Scartabili dopo 6 anni, conservando elenchi riassuntivi	Certificati originali allegati alla richiesta non soggetti a scadenza sono a disposizione degli interessati
A4/33	Documentazione riguardante le utenze (telefono, elettricità…) e tassa raccolta rifiuti	Scartabile dopo 10 anni salvo contenziosi in atto	
A4/34	Tabelle stipendi (nominative) Tabulati mensili riepilogativi retribuzioni	Scartabili dopo 50 anni	

Firmato digitalmente da ROBERTO FRACCIA

A4/35	Compensi per lavoro straordinario, gruppi sportivi, funzioni strumentali e aggiuntive, incarichi specifici, funzioni miste, ore straordinarie per sostituzione colleghi assenti, ore di insegnamento aggiuntive, ore funzionali di non insegnamento, compensi da fondo istituto, o da fondi esterni, ecc.	Scartabili dopo 50 anni	
N.	***Tipologia Documentaria***	***Tempi di conservazione***	***Note e riferimenti normativi***
A4/36	Acconti e conguagli per il personale, riepiloghi	Scartabili dopo 50 anni	
A4/37	Liquidazioni consulenze	Scartabili dopo 50 anni	
A4/38	Copie di delibere e/o di determine di liquidazione	Scartabili dopo 10 anni	
A4/39	Contributi – modello DM/10- INPS tabulati riepilogativi imponibili, regolarizzazioni contributive – personale, rapporti con INPS MODELLI EMENS (Denunce Retributive Mensili)	Scartabili dopo 50 anni	
A4/40	Modello 01/M (copia del datore di lavoro)	Archiviato nel fascicolo personale	
A4/41	D.M.A Denuncia mensile analitica	Scartabile dopo 50 anni	Modello INPDAP che raccoglie i dati retributivi e le informazioni necessarie per l'aggiornamento delle posizioni assicurative individuali
A4/42	FONDO ESPERO	Scartabile dopo 50 anni	
A4/43	Modelli 101 – Modelli CUD	Archiviati nel Fascicolo personale	
A4/44	Modello 770	Scartabile dopo 50 anni	
A4/45	Denunce annuali IRAP	Scartabili dopo 50 anni	
A4/46	Atti costitutivi il Collegio dei Revisori	ILLIMITATA	
A4/47	Registro dei verbali del Collegio dei Revisori	ILLIMITATA	

Firmato digitalmente da ROBERTO FRACCIA

A5 – Edifici e impianti

N.	*Tipologia Documentaria*	*Tempi di conservazione*	*Note e riferimenti normativi*
A5/1	Immobili di proprietà - progetti tecnici, contratti di costruzione, ristrutturazione e manutenzione - verbali e perizie di collaudo, autorizzazioni e certificazioni relative alla sicurezza e alla messa a norma dei locali e degli impianti (L.626/94) - atti relativi a donazioni, acquisti e vendite di immobili di proprietà	ILLIMITATA	
A5/2	Immobili in uso (di proprietà di altri enti) - atti relativi a locazione e comodati degli immobili (sia di proprietà sia appartenenti ad altri enti) - progetti tecnici, planimetrie, verbali e perizie di collaudo, autorizzazioni e certificazioni relative alla sicurezza e alla messa a norma dei locali e degli impianti (L. 626/94)	ILLIMITATA	
A5/3	Impianti ed attrezzature durevoli: disegni tecnici, progetti	ILLIMITATA	
A5/4	Immobili in uso (di proprietà di altri enti) - documentazione pervenuta in copia dagli enti proprietari, non compresa in quella descritta al punto A5/2	Scartabile dopo 10 anni	

Firmato digitalmente da ROBERTO FRACCIA

A6 - Inventari dei beni

N.	***Tipologia Documentaria***	***Tempi di conservazione***	***Note e riferimenti normativi***
A6/1	Inventari patrimoniali (registri inventariali) dei beni mobili; registri di entrata della biblioteca; registri di entrata dei sussidi multimediali; inventari e repertori dell'archivio	ILLIMITATA	Ex mod. 94 PGS e mod. 98 PGS
A6/2	Bollettari di carico e scarico	Scartabili dopo 10 anni	mod.130 PGS
A6/3	Registro di magazzino	Scartabile dopo 6 anni	
A6/4	Registro licenze software	ILLIMITATA	
A6/5	Licenze software	Scartabili dopo 10 anni	
A6/6	Ricognizioni patrimoniali di scuole confluite	ILLIMITATA	
A6/7	Ricognizioni patrimoniali decennali	ILLIMITATA	
A6/8	Rivalutazioni patrimoniali quinquennali	ILLIMITATA	
A6/9	Verbali dei passaggi di consegna	ILLIMITATA	Redatti in occasione di mutamento del Capo d'Istituto e del Direttore dei Servizi Generali ed Amministrativi, riguardano la consegna di tutto il materiale e di tutti gli atti esistenti, quindi anche dell'archivio. (R.D.26 ago. 1927, n.1917; C.M.20 febb. 1940, n.23; D.I. 44/2001)

Firmato digitalmente da ROBERTO FRACCIA

A7 -Personale docente e non docente

N.B.: Ove non specificato, con il termine *Personale* si indica sia il personale docente sia il personale non docente.

N.	***Tipologia Documentaria***	***Tempi di conservazione***	***Note e riferimenti normativi***
A7/1	Fascicoli individuali del personale docente e non docente in servizio, in quiescenza, di ruolo e non di ruolo (ora T.I. e T.D.): • Decreti di nomina e contratti individuali • Presa di servizio • Decreti di trasferimento • Certificati di nascita e residenza del personale di ruolo • Stato di famiglia e relativa documentazione • Certificati di sana e robusta costituzione • Lettere di invito per l'assegnazione della sede • Ordini di servizio individuali • Decreti (per congedi maternità anticipata, ecc.) • Decreti congedi parentali • Decreti congedi straordinari • Permessi • Decreti aspettative • Titoli di studio, attestati di partecipazione a corsi di formazione, aggiornamento, ecc. • Posizioni previdenziali, stipendiali, tributarie • Riscatto periodi assicurativi • Cessione "quinto" dello stipendio • Modello 01/M • Modello 101 e CUD • Richieste accertamenti sanitari (visite fiscali e collegiali, referti) • Accertamenti individuali infortuni e malattie professionali (documentazione sanitaria e tecnica) • Azioni legali del singolo dipendente • ***Pensione e trattamento di quiescenza*** • Certificati di servizio • Domande di trasferimento • Permessi di studio • Domande scatti anticipati • Autorizzazioni varie (lezioni private, esercizio a libere professioni,	ILLIMITATA	

Firmato digitalmente da ROBERTO FRACCIA

	collaborazioni plurime, ecc.) • Rilascio della tessera ministeriale (ferroviaria)		
N.	***Tipologia Documentaria***	***Tempi di conservazione***	***Note e riferimenti normativi***
A7/2	Ruoli del personale: documenti istruttori e deliberativi, albi, elenchi, registri, ecc	ILLIMITATA	
A7/3	Domande di ferie (congedo ordinario), permessi brevi	Scartabili dopo 6 anni	
A7/4	Azioni legali collettive del personale	ILLIMITATA	
A7/5	Recupero retribuzione dipendenti assenti dal lavoro per responsabilità di terzi	Scartabile dopo 50 anni	
A7/6	**Documentazione relativa alla pianta organica**	ILLIMITATA	
A7/7	Ordini di servizio generali	ILLIMITATA	
A7/8	Registro delle tessere di riconoscimento (Mod. AT)	ILLIMITATA	
A7/9	Registri delle autorizzazioni ad impartire lezioni private	Scartabili dopo 6 anni dall'ultima registrazione	Registri per l'annotazione delle autorizzazioni ad impartire lezioni private (art.43 del R.D. 30 aprile 1924, n.965 e s.d.)
A7/10	Registri dello stato personale	ILLIMITATA	
A7/11	Registro degli stipendi ed altri assegni	ILLIMITATA	
A7/12	Pensione e trattamento di quiescenza: norme e disposizioni	Scartabile dopo 10 anni dalla decadenza	
A7/13	Verbali di Ispettori scolastici	ILLIMITATA	
A7/14	Accertamenti sanitari e tecnici: documentazione relativa a malattie professionali, ecc.	ILLIMITATA	

Firmato digitalmente da ROBERTO FRACCIA

A7/15	Registri degli infortuni	ILLIMITATA	Unico per docenti, ATA e alunni
A7/16	Registri dei certificati di servizio rilasciati dalla scuola	ILLIMITATA	
A7/17	Copie certificati di servizio	Scartabili dopo 6 anni, conservando una copia nel fascicolo personale	
A7/18	Fogli di presenza	Scartabili dopo 10 anni, salvo contenzioso	
A7/19	Recupero orario: relazioni, dichiarazioni e autocertificazioni	Scartabili dopo 10 anni	
A7/20	Registri assenze	Scartabili dopo 50 anni	
A7/21	Aggiornamento personale - programmi - relazioni finali - dispense	ILLIMITATA	
A7/22	- Rapporti con organizzazioni sindacali e rappresentanze interne - Scioperi	ILLIMITATA	
A7/23	Graduatorie interne del personale in servizio	Scartabili dopo 10 anni	
A7/24	Graduatorie d'Istituto per supplenze personale docente e non docente	Scartabili dopo 10 anni dalla decadenza di validità	
A7/25	Domande di inserimento in graduatoria d'Istituto, con relativa documentazione, inerenti graduatorie non più in vigore	Scartabili dopo 10 anni, dalla decadenza di validità della relativa graduatoria conservando a disposizione degli interessati eventuali titoli di studio allegati in originale	
A7/26	Domande di supplenza e relative graduatorie in calce	Scartabili dopo 1 anno	

Firmato digitalmente da ROBERTO FRACCIA

A8 –Alunni

N.	***Tipologia Documentaria***	***Tempi di conservazione***	***Note e riferimenti normativi***
A8/1	Registri di immatricolazione e/o di iscrizione degli alunni	ILLIMITATA	Registri previsti per la registrazione cronologica ed ininterrotta di tutti gli alunni e candidati
A8/2	Elenchi alunni per iscrizioni	Scartabili dopo 10 anni	Redatti nel periodo delle iscrizioni, con data di nascita degli alunni, firme dei genitori (non compresi nei registri), possono essere scartati, appurato che i dati presenti in questi elenchi siano riportati nei registri
A8/3	Schede individuali degli alunni (schedario)	ILLIMITATA	Strumento facoltativo di reperimento dati e documentazione sugli alunni talvolta corredato di fotografia
A8/4	Domande e documenti prodotti da alunni e candidati per l'iscrizione ai vari tipi di scuola e per l'ammissione agli esami	Scartabili dopo 6 anni dalla fine dell'appartenenza all'Istituto o dall'iscrizione all'esame	I titoli di studio in originale e i documenti relativi vanno conservati nel fascicolo personale a disposizione degli interessati. *Inoltre vanno conservati tutti i documenti relativi agli alunni stranieri.*
A8/5	Certificati di nascita e di vaccinazione	Scartabili dopo 6 anni dalla cessazione dell'appartenenza all'Istituto o dall'iscrizione agli esami, *con l'eccezione dei documenti degli allievi stranieri*	
A8/6	Campagne di vaccinazione e disinfestazione, atti e documenti relativi alla loro effettuazione	Scartabili dopo 6 anni, conservando illimitatamente la documentazione e i registri riassuntivi	

Firmato digitalmente da ROBERTO FRACCIA

N.	***Tipologia Documentaria***	***Tempi di conservazione***	***Note e riferimenti normativi***
A8/7	Certificazioni per richieste di abbonamenti ferroviari e diversi	Scartabili dopo 1 anno	
A8/8	Registri generali dei voti, delle valutazioni	ILLIMITATA	Contengono dati anagrafici, votazioni o giudizi; firma del capo istituto a fianco di ciascun nominativo, a convalida del risultato finale, redatti secondo le norme di volta in volta vigenti
A8/9	Relazioni inerenti le ripetenze degli alunni	ILLIMITATA nei rispettivi fascicoli personali	
A8/10	Fascicoli personali alunni	ILLIMITATA	Con l'eccezione dei documenti di cui al punto A8/4-A8/5
A8/11	Registri delle assenze degli alunni	Scartabili dopo 6 anni	
A8/12	Orari delle lezioni	ILLIMITATA di un esemplare dell'orario di ciascuna classe di tutte le sezioni, scartando dopo un anno eventuali copie d'uso e dopo 6 anni gli atti relativi alla definizione dell'orario	
A8/13	Registri dei certificati di studio rilasciati dalla scuola	ILLIMITATA	
A8/14	Documentazione riguardante assistenza scolastica e Patronato scolastico	ILLIMITATA	
A8/15	Documentazione riguardante il diritto allo studio	ILLIMITATA	
A8/16	Certificazioni per richieste ai fini della fruizione di assegni di studio	Scartabili dopo 10 anni	
A8/17	Pratiche per assistenza e soggiorni climatici /colonie	ILLIMITATA	
A8/18	Cooperative di alunni: atti costitutivi, documenti istruttori e deliberativi, corrispondenza	ILLIMITATA	

Firmato digitalmente da ROBERTO FRACCIA

A8/19	Borse di studio / stage: bandi, studi e relazioni	ILLIMITATA	
A8/20	Statistiche	ILLIMITATA	

B) Tipologie documentarie didattiche

B1- Documentazione ufficiale dell'attività didattica

N.	*Tipologia Documentaria*	*Tempi di conservazione*	*Note e riferimenti normativi*
B1/1	Registri dei profili degli alunni redatti dai Consigli di classe	ILLIMITATA	
B1/2	Registri di classe	ILLIMITATA	
B1/3	Registri personali dei docenti	ILLIMITATA fino all'anno scolastico 1969/70. Successivamente scartabili dopo 10 anni, conservando illimitatamente un anno ogni 5 .	
B1/4	Registri e verbali del debito formativo	Scartabili dopo 10 anni, conservando illimitatamente un anno a campione ogni 5	Si suggerisce di effettuare la campionatura adottando il medesimo criterio per i registri del debito formativo e per quelli dei docenti.
B1/5	Registro riunioni per materia	ILLIMITATA	
B1/6	Registro riunioni per dipartimento	ILLIMITATA	
B1/7	Verbali e relazioni riguardanti l'adozione dei libri di testo	ILLIMITATA	
B1/8	Piani di lavoro, Programmi, Relazioni finali di classe	ILLIMITATA	Redatti dai singoli docenti
B1/9	Relazioni finali di istituto	ILLIMITATA	Comprendono tutti gli elementi relativi all'andamento didattico e disciplinare dell'istituto in ogni anno scolastico (C.M.26 ott. 1961, n.311; C.M. 12 sett. 1964, n.334; C.M.31 mar. 1966, n.170 e succ.disposiz.)
B1/10	Piano Offerta Formativa (POF)	ILLIMITATA	
B1/11	Educazione alla salute: progetti, interventi e convenzioni	ILLIMITATA	

Firmato digitalmente da ROBERTO FRACCIA

N.	*Tipologia Documentaria*	*Tempi di conservazione*	*Note e riferimenti normativi*
B1/12	Progetti formativi (teatro,musica interventi di recupero, inserimento alunni stranieri, orientamento, sport, patentino, ecc)	ILLIMITATA	
B1/13	Progetti operativi nazionali (PON); Progetti operativi regionali (POR);	ILLIMITATA	
B1/14	Piano Educativo Individualizzato (PEI)	ILLIMITATA nel fascicolo personale dell'alunno	
B1/15	Convenzioni per attività formative e parascolastiche	ILLIMITATA	
B1/16	Relazioni su collaborazioni con (o consulenze da parte di): - istituzioni socio-assistenziali - enti locali - cooperative ed associazioni - Tribunale dei minori - servizio sanitario nazionale - esperti esterni	ILLIMITATA	
B1/17	Elaborati delle prove scritte, grafiche e pratiche degli alunni (esclusi quelli prodotti per l'esame di Stato)	Scartabili dopo un anno, conservando illimitatamente a campione una annata ogni 10	
B1/18	Elaborati delle prove scritte, grafiche per gli esami di Stato	ILLIMITATA nel plico dell'esame	Compresi gli esami di licenza elementare fino all'anno scolastico 2002/2003 (L.53 del 28/03/2003)
B1/19	Elaborati delle prove pratiche per gli esami di Stato	Scartabili dopo un anno; conservando nel plico dell'esame le fotografie dei manufatti	
B1/20	Questionari e monitoraggio	Scartabili dopo un anno, conservando illimitatamente una copia in bianco del questionario e i suoi risultati sintetici	
B1/21	Prospetti trimestrali o quadrimestrali	ILLIMITATA	
B1/22	Prospetti scrutinio finale	ILLIMITATA	
B1/23	Registri dei verbali degli scrutini	ILLIMITATA	
B1/24	Registri dei verbali degli esami e delle relative prove	ILLIMITATA	
B1/25	Programmi d'esame	ILLIMITATA	

Firmato digitalmente da ROBERTO FRACCIA

N.	*Tipologia Documentaria*	*Tempi di conservazione*	*Note e riferimenti normativi*
B1/26	Pagelle scolastiche Schede di valutazione Schede alunni	ILLIMITATA sino alla consegna all'interessato	Le pagelle eventualmente rimaste giacenti saranno inserite nei fascicoli personali degli interessati
B1/27	Libretti scolastici e altra documentazione relativa agli studi dell'alunno (es. Portfolio)	ILLIMITATA	Al termine del corso di studio vengono consegnati agli interessati, completati con i profili finali. Le eventuali giacenze vengono inserite nei fascicoli personali (L.31 dicembre 1962, n.1859; C.M. 26 giugno 1963, n.205).
B1/28	Registri di carico e scarico dei diplomi	ILLIMITATA	
B1/29	Registri di consegna dei diplomi	ILLIMITATA	
B1/30	Giornalini di classe o d'istituto	ILLIMITATA di almeno un esemplare	
B1/31	Commissioni, comitati e gruppi di lavoro: nomine, verbali, documenti istruttori e deliberativi	ILLIMITATA	
B1/32	Valutazioni, rilevazioni dati, e relazioni sull'attività della scuola , redatte sia da personale interno sia da esterni (INVALSI, OCSE-PISA, ecc)	ILLIMITATA	
B1/33	Registri attività del Gruppo sportivo	**Scartabili dopo 10 anni**	
B1/34	Annuari, rassegna stampa e pubblicazioni varie della scuola	ILLIMITATA di almeno un esemplare degli annuari e delle pubblicazioni e della rassegna stampa	
B1/35	Locandine e manifesti di qualsiasi tipo pubblicati o stampati dalla o per conto della scuola	ILLIMITATA di almeno un esemplare	
B1/36	Documentazione per programmazione ed attuazione di attività scolastiche anche esterne (manifestazioni teatrali, gite, visite di studio ecc.)	Scartabile dopo 6 anni, conservando illimitatamente a campione un'annata ogni 10	
B1/37	Richieste di consultazione dell'archivio della scuola per finalità storico-culturali	Scartabili dopo 6 anni, conservando illimitatamente il registro delle consultazioni	
B1/38	Cataloghi e regolamenti delle biblioteche dell'Istituto (dei docenti, degli alunni, ecc):	ILLIMITATA	

Firmato digitalmente da ROBERTO FRACCIA

B2 - Attività didattiche specifiche

N.	*Tipologia Documentaria*	*Tempi di conservazione*	*Note e riferimenti normativi*
B2/1	Documenti prodotti da docenti e studenti in preparazione e nel corso di attività didattiche (dispense, percorsi, sussidi, sperimentazioni multidisciplinari, testi teatrali, sceneggiature cinematografiche ecc.)	ILLIMITATA di almeno un esemplare	Compresi i documenti audiovisivi, fotografici, informatici, ecc.

N.B. : le indicazioni si applicano anche a tutti i documenti relativi all'istituzione e funzionamento dei Centri Territoriali Permanenti (CTP, ex 150 ORE) e dei Corsi post-diploma (IFTS)

Firmato digitalmente da ROBERTO FRACCIA

INDICE

Firmato digitalmente da ROBERTO FRACCIA

Biblioteca:	
- contributi	A4/18
- registri di entrata	A6/1
- regolamenti, norme e cataloghi	A1/2-B1/38
Bilanci annuali	A4/11
Bollettari di carico e scarico	A6/2
Bollettario di richiesta stampati	A4/28
Bollettini di c/c postale	A4/9
Borse di studio	A8/19
Buoni acquisto di generi di refezione e consumo	A4/19
Buoni d'ordine	A4/3
Buoni libro, elenco buoni concessi e documentazione di supporto	A4/17
Campagne di disinfestazione e vaccinazione	A8/6
Carta dei servizi	A1/2
Cassa scolastica, registri dei verbali	A4/16
Cassa, libro/giornale	A4/2
Cassiere, Istituto	A4/4-A4/5
Cataloghi biblioteca d'Istituto	B1/38
Cedole librarie	4/17
Cerimonie, documentazione relativa	A3/4
Certificati:	
- garanzie di apparecchiature ed attrezzature	A4/25
- nascita e vaccinazione alunni	A8/5
- nascita, residenza, sana e robusta costituzione, servizio del personale	A7/1
- richieste	A3/8
- servizio, registri e copie	A7/16
- studio, registri	A8/13
Certificazioni:	
- qualità e accreditamenti	A1/9
- sicurezza locali e impianti (L.626/94) per immobili di proprietà ed immobili in uso	A5/1-A5/2
Cessione del quinto dello stipendio	A7/1
Circolari interne esplicative e direttive	A1/10
Collaudo, apparecchiature ed attrezzature, verbali	A4/24
Collegio dei Revisori, atti costitutivi	A4/45
Colonie, pratiche per assistenza	A8/17
Comitati: nomine, verbali, documenti istruttori e deliberativi	B1/31
Commissioni:	
- elettorali, verbali	A2/4
- gruppi di lavoro	A2/6
- nomine, verbali, documenti istruttori e deliberativi	B1/31
Comodati immobili	A5/2
Compensi a vario titolo	A4/35
Compiti in classe	B1/17
Conciliazioni, documentazione prodotta e acquisita	A4/15
Congedi: maternità anticipata, parentali, straordinari, aspettative	A7/1
Conguagli per il personale	A4/36
Consiglio di Amministrazione e di Presidenza, verbali e registri dei verbali	A2/2-A2/3
Consulenza di istituzioni ed enti vari	B1/16
Consultazione archivio della scuola, richieste	B1/37
Conti consuntivi	A4/1
Conto corrente postale, registro delle operazioni	A4/8
Contrattazione d'Istituto, documentazione preparatoria e registri verbali riunioni	A1/5-A1/6
Contratti:	
- Collettivo Nazionale di Lavoro, norme e disposizioni	A1/4
- costruzione, immobili di proprietà	A5/1
- forniture di materiali, espletamento di servizi, assunzione di personale	A4/12
- individuali	A7/1
- prestazione d'opera di varia natura	A4/14
- registro	A4/11
- registro cronologico	A4/13
Contributi:	

Firmato digitalmente da ROBERTO FRACCIA

- INPS	A4/39
- biblioteca scolastica	A4/18
Convenzioni:	
- con Istituto Cassiere	A4/4-A4/5
- con scuole, enti ecc.	A1/11
- per attività formative e parascolastiche	B1/15
- per educazione alla salute	B1/11
Convocazioni riunioni Organi Collegiali	A2/7
Cooperative di alunni: atti costitutivi, documenti istruttori e deliberativi, corrispondenza	A8/18
Cooperative ed Associazioni, relazioni sul collaborazioni e consulenze	B1/16
Copie determine e delibere di liquidazione	A4/38
Corrispondenza:	
- in arrivo e in partenza	A3/5
- relativa agli acquisti	A4/3
D.M.A. - Denuncia mensile analitica	A4/41
Debito formativo, registri e verbali	B1/4
Decreti Delegati	A2/1
Decreti di nomina, di trasferimento e contratti individuali	A7/1
Decreti per aspettative, congedi di maternità anticipata, parentali, straordinari	A7/1
Deliberazioni, registri	A2/8
Determinazioni dirigenziali	A2/9
Dipartimenti, gruppi di lavoro	A2/6
Diplomi, registri di carico e scarico e di consegna	B1/28-B1/29
Diritto allo studio, documentazione	A8/15
Disegni, immobili di proprietà	A5/1
Disinfestazione, campagne	A8/6
Dispense:	
- aggiornamento personale	A7/21
- documenti prodotti da docenti e studenti in preparazione e nel corso di attività didattiche	B2/1
Distinte di trasmissione al tesoriere di reversali e mandati	A4/6
Documento programmatico di sicurezza dati-privacy	A1/7
Documento valutazione rischi (L. 626/94) e relativi allegati	A1/8
Domande:	
- di ferie	A7/3
- di supplenze	A7/24 –A7/25 – A7/26
- dei candidati per l'ammissione agli esami e per l'iscrizione alla scuola	A8/4
Donazioni, immobili di proprietà	A5/1
Dotazioni strumentali: richieste di intervento	A4/26
Economato, norme e disposizioni	A1/3
Educazione alla salute	B1/11
Elaborati:	
- prove pratiche per gli esami di Stato	B1/19
- prove scritte e grafiche per gli esami di Stato	B1/18
- prove scritte, grafiche e pratiche degli alunni (escluse quelle prodotte per gli esami di Stato)	B1/17
Elenchi di:	
- alunni per l'iscrizione	A8/2
- consistenza di archivi o altri beni inventariati	A1/12
- personale	A7/2
Elezioni degli Organi Collegiali, atti	A2/5
EMENS modelli denunce retributive mensili	A4/39
Enti locali, relazioni su collaborazioni e consulenze	B1/16
Entrate, partitario	A4/2
Esami:	
- di Stato, elaborati prove scritte, grafiche e pratiche	B1/18-B1/19
- domande d'ammissione	A8/4
- registro dei verbali	B1/24
Esperti esterni, relazioni su collaborazioni e consulenze	B1/16
Estratti conto bancari e postali	A4/7
Fascicoli:	

Firmato digitalmente da ROBERTO FRACCIA

- individuali del personale docente e non docente in servizio, in quiescenza, di ruolo e non di ruolo (ora T.D. e T.I.)	A7/1
- personali degli alunni	A8/10
Fatture	A4/3
Ferie, domande	A7/3
Foglie di presenza	A7/18
Fondo Espero	A4/42
Fornitura materiali, registro contratti	A4/11
Garanzia di apparecchiature ed attrezzature	A4/25
Giornali:	
- acquisto o abbonamento	A4/20
- di cassa	A4/2
Giornalini di classe o d'Istituto	B1/30
Gite scolastiche	B1/36
Graduatorie:	
- d'Istituto	A7/24
- in calce	A7/26
- interne	A7/23
- non più in vigore	A7/25
Gruppi di lavoro:	
- derivati dagli Organi Collegiali	A2/6
- nomine, verbali, documenti istruttori e deliberativi	B1/31
Gruppo sportivo, registri attività	B1/33
Immatricolazione alunni, registri	A8/1
Immobili:	
- di proprietà	A5/1
- in uso, compresa la documentazione pervenuta in copia	A5/2-A5/4
Impianti:	
- durevoli, disegni tecnici e progetti	A5/3
- sportivi, autorizzazioni all'uso	A3/
Inaugurazioni, documentazione relativa	A3/11
Inchieste e indagini ambientali e socio-economiche	A3/10
Infortuni, documentazione e registri	A7/1-A7/14-A7/15
INPS, contributi	A4/39
Inserimento alunni stranieri, progetti formativi	B1/12
Interventi:	
- educazione alla salute	B1/11
- manutenzione, corrispondenza relativa	A4/21
- recupero, progetti formativi	B1/12
Intitolazione della scuola	A1/1
INVALSI, progetto	B1/32
Inventari patrimoniali dei beni mobili e d'archivio	A6/1
IRAP - Denunce annuali	A4/44
Iscrizioni a scuola, domande e documenti prodotti	A8/4
Ispettori scolastici, verbali	A7/13
Istituti:	
- cassiere	A4/4-A4/5
- paritari, Statuti e regolamenti	A1/1
- regolamenti interni e norme	A1/2
Istituzione della scuola	A1/1
Istituzioni socio-assistenziali, relazione su collaborazione e consulenze	B1/16
Laboratori, regolamenti interni e norme	A1/2
Legge 626/94:	
- documento valutazione rischi e relativi allegati	A1/8
- sicurezza locali e impianti degli immobili di proprietà ed in uso	A5/1-A5/2
Lezioni private, registro	A7/9
Libretti scolastici	B1/27
Libretto degli autoveicoli in dotazione	A4/27
Libri di testo, verbali e relazioni per l'adozione	B1/7
Libri, acquisto	A4/20
Licenze software	A6/5
Liquidazioni:	

Firmato digitalmente da ROBERTO FRACCIA

- consulenze	A4/37
- copie delibere e determine	A4/38
Locali scolastici, autorizzazioni all'uso	A3/9
Locandine pubblicate o stampate dalla o per conto della scuola	B1/35
Locazione immobili, atti relativi	A5/2
Malattie professionali	A7/1-A7/14
Mandati di pagamento e relativa documentazione giustificativa	A4/3
Manifestazioni teatrali	B1/36
Manifesti pubblicati o stampati dalla o per conto della scuola	B1/35
Manutenzione:	
- interventi	A4/21
- immobili di proprietà	A5/1
Matrici di buoni acquisto per generi di refezione e consumo	A4/19
Mensa, elenco presenze e richiesta di iscrizione al servizio	A4/30
Modelli:	
- 26 C.G.	A4/10
- EMENS, denunce retributive mensili	A4/39
- 101, CUD	A4/43
- 770	A4/44
- 01/M, copia del datore di lavoro	A4/40
Monitoraggio	B1/20
Musica, progetti formativi	B1/12
Norme interne relative a biblioteca, laboratori, Istituto	A1/2
OCSEA-PISA, progetto	B1/32
Orari delle lezioni	A8/12
Ordinanze interne esplicative e direttive	A1/10
Ordinativi di acquisto	A4/3
Ordini di servizio generali	A7/7
Organi Collegiali, di Circolo e d'Istituto:	
- atti delle elezioni	A2/5
- atti di nomina	A2/4
- convocazioni riunioni	A2/7
- registri dei verbali	A2/6
Organizzazioni sindacali, rapporti con	A7/22
Orientamento, progetti formativi	B1/12
Pagelle scolastiche	B1/26
Partitario delle entrate e delle uscite	A4/2
Passaggi di consegna, verbali	A6/9
Patentino, progetti formativi	B1/12
Patronato Scolastico	A8/14
PEI (piano educativo individualizzato)	B1/14
Pensione e trattamento di quiescenza	A7/1-A7/12
Percorsi didattici, documenti prodotti da docenti e studenti	B2/1
Perizie su immobili di proprietà ed immobili in uso	A5/1-A5/2
Permessi del personale: brevi e di studio	A7/1-A7/3
Personale:	
- aggiornamento	A7/21
- norme e disposizioni	A1/4
Piani di lavoro	B1/8
Pianta organica	A7/6
Planimetrie di immobili di proprietà ed immobili in uso	A5/1-A5/2
POF (piano offerta formativa)	B1/10
PON e POR (Progetti Operativi Nazionali e Regionali)	B1/13
Portfolio	B1/27
Posizioni previdenziali, stipendiali, tributarie	A7/1
Posta in partenza e in arrivo, registro	A3/4
Presa di servizio	A7/1
Presenze, fogli	A7/18
Prestazioni d'opera, contratti	A4/14
Privacy - documento programmatico di sicurezza dati	A1/7
Profili degli alunni, registri	B1/1
Progetti:	

Firmato digitalmente da ROBERTO FRACCIA

- educazione alla salute	B1/11
- formativi	B1/12
- operativi	B1/13
- scrutinio finali	B1/22
- tecnici per immobili di proprietà ed in uso	A5/1-A5/2
- trimestrali o quadrimestrali	B1/21
Programmi:	
- aggiornamento del personale	A7/21
- contabili annuali	A4/1
- d'esame	B1/25
- dei singoli docenti	B1/8
Protocolli della corrispondenza generali e riservati	A3/1
Prove esami, registri verbali	B1/24
Pubblicazioni varie della scuola	B1/34
Questionari	B1/20
Quiescenza, trattamento	A7/1-A7/12
R.S.U.	A7/22
Rapporti con organizzazioni sindacali e rappresentanze interne	A7/22
Rappresentanze sindacali interne	A7/22
Rassegna stampa della scuola	B1/34
Recupero orario, documentazione relativa	A7/19
Recupero retribuzione dipendenti assenti dal lavoro per responsabilità di terzi	A7/5
Registri:	
- assenze degli alunni	A8/11
- assenze del personale	A7/20
- attività del Gruppo Sportivo	B1/33
- autorizzazioni ad impartire lezioni private	A7/9
- carico e scarico dei diplomi	B1/28
- certificati di servizio rilasciati	A7/16
- certificati di studio	A8/13
- classe	B1/2
- consegna dei diplomi	B1/29
- conto corrente postale, ricevute di versamento	A4/8
- contratti per fornitura di materiali, espletamento di servizi, assunzione di personale	A4/11
- cronologici dei contratti	A4/13
- debito formativo	B1/4
- deliberazioni	A2/8
- entrata dei sussidi multimediali	A6/1
- entrata della biblioteca	A6/1
- generali dei voti	A8/8
- generali delle valutazioni	A8/8
- immatricolazione alunni	A8/1
- infortuni	A7/15
- inventariali dei beni mobili	A6/1
- iscrizione alunni	A8/1
- licenze software	A6/4
- magazzino	A6/3
- materiali di facile consumo	A4/23
- personali dei docenti	B1/3
- posta in partenza	A3/4
- profili alunni redatti dai Consigli di classe	B1/1
- protocollo, generali e riservati	A3/1
- riunioni per dipartimento	B1/6
- riunioni per materia	B1/5
- spese per apertura di credito e rendiconto trimestrale	A4/10
- stato del personale	A7/10
- stipendi ed altri assegni	A7/11
- tasse scolastiche per iscrizione e diploma	A4/29
- tessere di riconoscimento (mod. AT)	A7/8
- verbali degli esami	B1/24

Firmato digitalmente da ROBERTO FRACCIA

- verbali degli Organi Collegiali	A2/6
- verbali degli scrutini	B1/23
- verbali del Collegio dei Revisori	A4/46
- verbali del Consiglio o Staff di Presidenza	A2/3
- verbali della cassa scolastica	A4/16
- verbali riunioni per contrattazione d'Istituto	A1/5
Regolamenti:	
- biblioteche d'Istituto	B1/38
- e Statuti, Istituti paritari	A1/1
- interni relativi a biblioteca, laboratori, Istituto	A1/2
Regolarizzazioni contributive personali	A4/39
Relazioni:	
- attività della scuola	B1/22
- collaborazioni con istituzioni ed enti	B1/16
- esterne	A3/11
- finali di classe e d'Istituto	B1/8-B1/9
- finali, aggiornamento personale	A7/21
- ripetenze alunni	A8/9
Rendiconto trimestrale	A4/10
Repertori:	
- archivio	A6/1
- fascicoli d'archivio	A3/2
Reti di scuole, convenzioni e accordi	A1/11
Retribuzione dipendenti, recupero	A7/5
Reversali di pagamento e relativa documentazione giustificativa	A4/3
Revisori	A4/46-A4/47
Richieste:	
- accesso ai documenti	A3/6
- certificati	A3/8
- consultazione archivio della scuola	B1/37
- copie di atti	A3/7
- intervento - risorse strumentali	A4/26
Ricognizioni patrimoniali:	
- decennali	A6/7
- di scuole confluite	A6/6
Ricorsi amministrativi e giurisdizionali	A4/15
Rilevazioni dati sull'attività della scuola	B1/32
Ripetenze alunni, relazioni	A8/9
Riscatto periodi assicurativi	A7/1
Ristrutturazione immobili di proprietà	A5/1
Riunioni Organi Collegiali e verbali degli stessi	A2/1-A2/7
Rivalutazioni patrimoniali quinquennali	A6/8
Riviste, abbonamento e acquisto	A4/20
Rubriche alfabetiche del protocollo	A3/3
Ruoli del personale	A7/2
Salute, progetti educativi	B1/11
Scarto di atti d'archivio	A1/15
Scatti anticipati, domande	A7/1
Sceneggiature cinematografiche, documenti prodotti da docenti e studenti	B2/1
Schedario degli alunni	A8/3
Schede alunni, individuali e di valutazione	A8/3-B1/26
Scioperi	A7/22
Scrutini, prospetti e registri verbali	B1/22-B1/23
Servizi, espletamento: registri contratti	A4/11
Servizio Sanitario Nazionale, relazione su collaborazioni e consulenze	B1/16
Sindacato, rappresentanze	A7/22
Soggiorni climatici	A8/17
Sperimentazioni multidisciplinari, documenti prodotti da docenti e studenti	B2/1
Spese, registro	A4/10
Sport, progetti formativi	B1/12
Staff di Presidenza, registri dei verbali	A2/3

Firmato digitalmente da ROBERTO FRACCIA

Stage	A8/19
Stampati, richiesta	A4/28
Statistiche	A8/20
Stato di famiglia e relativa documentazione	A7/1
Statuti e regolamenti, Istituti paritari	A1/1
Stipendi, registro	A7/11
Supplenze, domande	A7/25
Sussidi multimediali, registri di entrata	A6/1
Sussidi, documenti prodotti da docenti e studenti	B2/1
Tabelle stipendi	A4/34
Tabulati:	
- mensili riepilogativi retribuzioni	A4/34
- riepilogativi imponibili	A4/39
Tasse scolastiche per iscrizione e diploma	A4/29
Teatro, progetti formativi	B1/12
Tesoriere, distinte di trasmissione	A4/6
Tessere.	
- ministeriale	A7/1
- di riconoscimento (mod. AT), registro	A7/8
Testi teatrali, documenti prodotti da docenti e studenti	B2/1
Titolari di classificazione d'archivio	A1/14
Titoli di studio	A7/1
Transazioni, documentazione prodotta e acquista	A4/15
Trasferimento, domande	A7/1
Trasformazioni di scuole	A1/1
Trasporto alunni, richiesta:	
- iscrizione al servizio ed attestazioni di pagamento	A4/31
- trasporto gratuito	A4/32
Trattamento di quiescenza	A7/12
Tribunale dei minori, relazioni su collaborazioni e consulenze	B1/16
Uscite, partitario	A4/2
Utenze per telefono, elettricità, tassa rifiuti	A4/33
Vaccinazione, campagne	A8/6
Valutazioni:	
- alunni	B1/26
- attività della scuola	B1/32
- registri	A8/8
Vendite, immobili di proprietà	A5/1
Verbali:	
- collaudo di apparecchiature e attrezzature	A4/24
- collaudo di immobili di proprietà ed immobili in uso	A5/1
- commissioni elettorali	A2/4
- Consiglio d'Amministrazione	A2/2
- consegna ed elenchi consistenza di archivi od altri beni inventariati	A1/12
- debito formativo	B1/4
- ispettori scolastici	A7/13
- passaggi di consegna	A6/9
- riunioni collegiali	A2/1
Visite:	
- collegiali e fiscali e relativi referti	A7/1
- di studio	B1/36

Firmato digitalmente da ROBERTO FRACCIA

Allegato 2
ELENCO DEGLI ATTI CHE SI PROPONGONO PER L'ELIMINAZIONE

N. d'ordine	Classificazione (1)	Descrizione degli atti (2)	Estremi cronologici	N. pezzi (3)	Peso in Kg. (4)	Motivazioni dell'eliminazione (5)

Data _____ Firma (6)_____

NOTE
1) Si riporta la classificazione che le unità archivistiche possiedono
2) Descrizione sintetica di ogni voce, sufficiente a rendere riconoscibili i documenti
3) Oltre alla quantità, specificare anche la qualità dei contenitori (cartelle,faldoni,scatole, pacchi, sacchi…)
4) Il peso può anche essere indicato complessivamente per tutte le unità che si propongo per lo scarto
5) Indicare sinteticamente il motivo dello scarto e/o la documentazione alternativa che viene conservata
6) Indicare con chiarezza la qualifica e la responsabilità di chi firma, apponendo il timbro dell'Ente

Firmato digitalmente da ROBERTO FRACCIA

Firmato digitalmente da ROBERTO FRACCIA

ISTITUTO COMPRENSIVO STATALE
"ADA NEGRI"
Via Don Milani 4 - 20086 MOTTA VISCONTI (MILANO)
Tel./Fax02.90000266
E- mail : miic872009@istruzione.it - miic872009@pec.istruzione.it
www.icmottavisconti.edu.it
C.F. 90015610158 – C.M. MIIC872009

Allegato10

Piano di sicurezza informatica

1 Politiche accettabili di uso del sistema informativo

1.1 Premessa

L'incarico del Responsabile della Sicurezza (RS), o suo delegato, di pubblicare le politiche accettabili di uso, è quello di stabilire le regole per proteggere l'Amministrazione da azioni illegali o danneggiamenti effettuati da individui in modo consapevole o accidentale senza imporre restrizioni contrarie a quanto stabilito dall'Amministrazione in termini di apertura, fiducia e integrità del sistema informativo.
Sono di proprietà dell'Amministrazione i sistemi di accesso ad Internet, l'Intranet, la Extranet ed i sistemi correlati, includendo in ciò anche i sistemi di elaborazione, la rete e gli apparati di rete, il software applicativo, i sistemi operativi, i sistemi di memorizzazione/archiviazione delle informazioni, il servizio di posta elettronica, i sistemi di accesso e navigazione in Internet, etc. Questi sistemi e/o servizi devono essere usati nel corso delle normali attività di ufficio solo per scopi istituzionali e nell'interesse dell'Amministrazione e in rapporto con possibili interlocutori della medesima.
L'efficacia e l'efficienza della sicurezza è uno sforzo di squadra che coinvolge la partecipazione ed il supporto di tutto il personale (impiegati funzionari e dirigenti) dell'Amministrazione ed i loro interlocutori che vivono con l'informazione del sistema informativo. È responsabilità di tutti gli utilizzatori del sistema informatico conoscere queste linee guida e comportarsi in accordo con le medesime.

1.2 Scopo

Lo scopo di queste politiche è sottolineare l'uso accettabile del sistema informatico dell'Amministrazione. Le regole sono illustrate per proteggere gli impiegati e l'Amministrazione.
L'uso non appropriato delle risorse strumentali espone l'Amministrazione al rischio di non poter svolgere i compiti istituzionali assegnati, a seguito, ad esempio, di virus, della compromissione di componenti del sistema informatico, ovvero di eventi disastrosi.

1.3 Ambito di applicazione

Queste politiche si applicano a tutti gli impiegati dell'Amministrazione, al personale esterno (consulenti, personale a tempo determinato) e agli impiegati della/e ditta/e Axios Italia di Roma e suoi rappresentanti sul territorio nazionale, includendo tutto il personale affiliato con terze parti.
Queste politiche si applicano a tutti gli apparati che sono di proprietà dell'Amministrazione o "affittate" da questa.

1.4 Politiche – Uso generale e proprietà

1. Gli utenti del sistema informativo dovrebbero essere consapevoli che i dati da loro creati sui sistemi dell'Amministrazione e comunque trattati, rimangono di proprietà della medesima.
2. Gli impiegati sono responsabili dell'uso corretto delle postazioni di lavoro assegnate e dei dati ivi conservati anche perché la gestione della rete (Intranet) non può garantire la confidenzialità dell'informazione memorizzata su ciascun componente "personale" della rete dato che l'amministratore della rete ha solo il compito di fornire prestazioni elevate e un ragionevole livello di confidenzialità e integrità dei dati in transito.
3. Le singole aree o settori o Divisioni o Direzioni, sono responsabili della creazione di linee guida per l'uso personale di Internet/Intranet/Extranet. In caso di assenza di tali politiche gli impiegati

Firmato digitalmente da ROBERTO FRACCIA

dovrebbero essere guidati dalle politiche generali dell'Amministrazione e in caso di incertezza, dovrebbero consultare il loro Dirigente.

4. Per garantire la manutenzione della sicurezza e della rete, soggetti autorizzati dall'Amministrazione (di norma amministratori di rete) possono monitorare gli apparati, i sistemi ed il traffico in rete in ogni momento.
5. Per i motivi di cui sopra l'Amministrazione si riserva il diritto di controllare la rete ed i sistemi per un determinato periodo per assicurare la conformità con queste politiche.

1.5 Politiche - Sicurezza e proprietà dell'informazione

1. Il personale dell'Amministrazione dovrebbe porre particolare attenzione in tutti i momenti in cui ha luogo un trattamento delle informazioni per prevenire accessi non autorizzati alle informazioni.
2. Mantenere le credenziali di accesso (normalmente UserID e password) in modo sicuro e non condividerle con nessuno. Gli utenti autorizzati ad utilizzare il sistema informativo sono responsabili dell'uso delle proprie credenziali, componente pubblica (UserID) e privata (password). Le password devono essere cambiate con il primo accesso al sistema informativo e successivamente, al minimo ogni quattro mesi, ad eccezione di coloro che trattano dati personali sensibili o giudiziari per i quali il periodo si riduce a tre mesi. Le password devono rispondere ai requisiti di complessità così come previsto dal D.lgs 196/2003.
1. Al momento della redazione del presente documento non sono presenti sistemi che registrano in chiaro le password; tutti i servizi web sono dotati di protocollo HTTPS e tutti i sistemi locali utilizzano sistemi di archiviazione crittografata delle credenziali.
2. Tutte le postazioni di lavoro (PC da tavolo e portatili) dovrebbero essere rese inaccessibili a terzi quando non utilizzate dai titolari per un periodo massimo di dieci minuti attraverso l'attivazione automatica del salva schermo protetto da password o la messa in stand-by con un comando specifico.
3. Uso delle tecniche e della modalità di cifratura dei file coerentemente a quanto descritto in materia di confidenzialità dall'Amministrazione.
4. Poiché le informazioni archiviate nei PC portatili sono particolarmente vulnerabili su essi dovrebbero essere esercitate particolari attenzioni.
5. Eventuali attività di scambio di opinioni del personale dell'Amministrazione all'interno di "new group" che utilizzano il sistema di posta elettronica dell'Amministrazione dovrebbero contenere una dichiarazione che affermi che le opinioni sono strettamente personali e non dell'Amministrazione a meno che non si tratti di discussioni inerenti e di interesse dell'Amministrazione eseguite per conto della medesima.
6. Tutti i PC, i server ed i sistemi di elaborazione in genere, che sono connessi in rete interna dell'Amministrazione (Intranet) e/o esterna (Internet/Extranet) di proprietà dell'Amministrazione o del personale, devono essere dotati di un sistema antivirus approvato dal responsabile della sicurezza dell'Amministrazione ed aggiornato.
7. Il personale deve usare la massima attenzione nell'apertura dei file allegati alla posta elettronica ricevuta da sconosciuti perché possono contenere virus, bombe logiche e cavalli di Troia.
8. Non permettete ai colleghi, né tanto meno ad esterni, di operare sulla vostra postazione di lavoro con le vostre credenziali. Sempre voi risultate autori di qualunque azione.

2 Politiche accettabili di uso del sistema informativo

Firmato digitalmente da ROBERTO FRACCIA

2.1 Premessa

I virus informatici costituiscono ancora oggi la causa principale di disservizio e di danno delle Amministrazioni.
I danni causati dai virus all'Amministrazione, di tipo diretto o indiretto, tangibili o intangibili, secondo le ultime statistiche degli incidenti informatici, sono i più alti rispetto ai danni di ogni altra minaccia.
I virus, come noto, riproducendosi autonomamente, possono generare altri messaggi contagiati capaci di infettare, contro la volontà del mittente, altri sistemi con conseguenze negative per il mittente in termini di criminalità informatica e tutela dei dati personali.

2.2 Scopo

Stabilire i requisiti che devono essere soddisfatti per collegare le risorse elaborative ad Internet/Intranet/Extranet dell'Amministrazione al fine di assicurare efficaci ed efficienti azioni preventive e consuntive contro i virus informatici.

2.3 Ambito di applicazione

Queste politiche riguardano tutte le apparecchiature di rete, di sistema ed utente (PC) collegate ad Internet/Intranet/Extranet. Tutto il personale dell'Amministrazione è tenuto a rispettare le politiche di seguito richiamate.

2.4 Politiche per le azioni preventive

- Deve essere sempre attivo su ciascuna postazione di lavoro un prodotto antivirus aggiornabile da un sito disponibile sulla Intranet dell'Amministrazione.
- Su ciascuna postazione deve essere sempre attiva la versione corrente e aggiornata con la più recente versione resa disponibile sul sito centralizzato.
- Non aprire mai file o macro ricevuti con messaggi dal mittente sconosciuto, sospetto, ovvero palesemente non di fiducia. Cancellare immediatamente tali oggetti sia dalla posta che dal cestino.
- Non aprire mai messaggi ricevuti in risposta a messaggi "probabilmente" mai inviati.
- Cancellare immediatamente ogni messaggio che invita a continuare la catena di messaggi, o messaggi spazzatura.
- Non scaricare mai messaggi da siti o sorgenti sospette.
- Evitate lo scambio diretto ed il riuso di supporti rimovibili (floppy disk, CD, DVD, tape, pen drive, etc.) con accesso in lettura e scrittura a meno che non sia espressamente formulato in alcune procedure dell'amministrazione e, anche in questo caso, verificare prima la bontà del supporto con un antivirus.
- Evitare l'uso di software gratuito (freeware o shareware) o documenti di testo prelevati da siti Internet o copiato dai CD/DVD in allegato a riviste.
- Evitare l'utilizzo, non controllato, di uno stesso computer da parte di più persone.
- Evitare collegamenti diretti ad Internet via modem.
- Non utilizzare il proprio supporto di archiviazione rimovibile su di un altro computer se non in condizione di protezione in scrittura.
- Se si utilizza una postazione di lavoro che necessita di un "bootstrap" da supporti di archiviazione rimovibili, usare questo protetto in scrittura.
- Non utilizzare i server di rete come stazioni di lavoro.
- Non aggiungere mai dati o file ai supporti di archiviazione rimovibili contenenti programmi originali.
- Effettuare una scansione della postazione di lavoro con l'antivirus prima di ricollegarla, per qualsiasi motivo (es, riparazione, prestito a colleghi o impiego esterno), alla Intranet dell'Organizzazione.

Firmato digitalmente da ROBERTO FRACCIA

Di seguito vengono riportati ulteriori criteri da seguire per ridurre al minimo la possibilità di contrarre virus informatici e di prevenirne la diffusione, destinati a tutto il personale dell'Amministrazione ed, eventualmente, all'esterno.

- Tutti gli incaricati del trattamento dei dati devono assicurarsi che i computer di soggetti terzi, esterni, qualora interagiscano con il sistema informatico dell'Amministrazione, siano dotati di adeguate misure di protezione antivirus.
- Il personale delle ditte addette alla manutenzione dei supporti informatici deve usare solo supporti rimovibili preventivamente controllati e certificati singolarmente ogni volta.
- I supporti di archiviazione rimovibili provenienti dall'esterno devono essere sottoposti a verifica da attuare con una postazione di lavoro dedicata, non collegata in rete (macchina da quarantena).
- Il personale deve essere a conoscenza che la creazione e la diffusione, anche accidentale dei virus è punita dall'Articolo 615 quinquies del Codice penale concernente la "Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico… [omissis]…che prevede la reclusione sino a due anni e la multa sino a lire venti milioni".
- Il software acquisito deve essere sempre controllato contro i virus e verificato perché sia di uso sicuro prima che sia installato.
- È proibito l'uso di qualsiasi software diverso da quello fornito dall'Amministrazione.

In questo ambito, al fine di minimizzare i rischi di distruzione anche accidentale dei dati a causa dei virus informatici, il RSP stabilisce le protezioni software da adottare sulla base dell'evoluzione delle tecnologie disponibili sul mercato.

2.5 Politiche per le azioni consuntive

Nel caso in cui su una o più postazioni di lavoro dovesse verificarsi perdita di informazioni, integrità o confidenzialità delle stesse a causa di infezione o contagio da virus informatici, il titolare della postazione interessata deve immediatamente isolare il sistema e poi notificare l'evento al responsabile della sicurezza, o suo delegato, che deve procedere a:

- verificare se ci sono altri sistemi infettati con lo stesso Virus Informatico;
- verificare se il virus ha diffuso dati;
- identificare il virus;
- attivare l'antivirus adatto ad eliminare il virus rilevato e bonificare il sistema infetto;
- installare l'Antivirus adatto su tutti gli altri sistemi che ne sono sprovvisti;
- diffondere la notizia dell'evento, all'interno dell'Amministrazione, nelle forme opportune.

3 Politiche – uso non accettabile

Le seguenti attività sono in generale proibite. Il personale può essere esentato da queste restrizioni in funzione del ruolo ricoperto all'interno dell'Amministrazione (ad esempio, nessuno può disconnettere e/o disabilitare le risorse ad eccezione degli amministratori di sistema o di rete).
In nessun caso o circostanza il personale è autorizzato a compiere attività illegali utilizzando le risorse di proprietà dell'Amministrazione.
L'elenco seguente non vuole essere una lista esaustiva, ma un tentativo di fornire una struttura di riferimento per identificare attività illecite o comunque non accettabili.

3.1 Attività di rete e di sistema

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione.

1. Violazioni dei diritti di proprietà intellettuale di persone o società, o diritti analoghi includendo, ma non limitando, l'installazione o la distribuzione di copie pirata o altri software prodotti che non sono espressamente licenziati per essere usati dall'Amministrazione.

Firmato digitalmente da ROBERTO FRACCIA

2. Copie non autorizzate di materiale protetto da copyright (diritto d'autore) includendo, ma non limitando, digitalizzazione e distribuzione di foto e immagini di riviste, libri, musica e ogni altro software tutelato per il quale l'Amministrazione o l'utente finale non ha una licenza attiva.
3. È rigorosamente proibita l'esportazione di software, informazioni tecniche, tecnologia o software di cifratura, in violazione delle leggi nazionali ed internazionali.
4. Introduzione di programmi maliziosi nella rete o nei sistemi dell'Amministrazione.
5. Rivelazione delle credenziali personali ad altri o permettere ad altri l'uso delle credenziali personali, includendo in ciò i familiari o altri membri della famiglia quando il lavoro d'ufficio è fatto da casa o a casa.
6. Usare un sistema dell'Amministrazione (PC o server) per acquisire o trasmettere materiale pedo-pornografico o che offende la morale o che è ostile alle leggi e regolamenti locali, nazionali o internazionali.
7. Effettuare offerte fraudolente di prodotti, articoli o servizi originati da sistemi dell'Amministrazione con l'aggravante dell'uso di credenziali fornite dall'Amministrazione stessa.
8. Effettuare affermazioni di garanzie, implicite o esplicite, a favore di terzi ad eccezione di quelle stabilite nell'ambito dei compiti assegnati.
9. Realizzare brecce nelle difese periferiche della rete del sistema informativo dell'Amministrazione o distruzione della rete medesima, dove per brecce della sicurezza si intendono, in modo riduttivo:
    a. accessi illeciti ai dati per i quali non si è ricevuta regolare autorizzazione,
    b. attività di "sniffing";
    c. disturbo della trasmissione;
    d. spoofing dei pacchetti;
    e. negazione del servizio;
    f. le modifiche delle mappe di instradamento dei pacchetti per scopi illeciti;
    g. attività di scansione delle porte o del sistema di sicurezza è espressamente proibito salvo deroghe specifiche.
10. Eseguire qualsiasi forma di monitor di rete per intercettare i dati in transito.
11. Aggirare il sistema di autenticazione o di sicurezza della rete, dei server e delle applicazioni.
12. Interferire o negare l'accesso ai servizi di ogni altro utente abilitato.
13. Usare o scrivere qualunque programma o comando o messaggio che possa interferire o con i servizi dell'Amministrazione o disabilitare sessioni di lavoro avviate da altri utenti di Internet/Intranet/Extranet.
14. Fornire informazioni o liste di impiegati a terze parti esterne all'Amministrazione.

3.2 Attività di messaggistica e comunicazione

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione.

1. Inviare messaggi di posta elettronica non sollecitati, includendo "messaggi spazzatura", o altro materiale di avviso a persone che non hanno specificamente richiesto tale materiale (spamming).
2. Ogni forma di molestia via e-mail o telefonica o con altri mezzi, linguaggio, durata, frequenza o dimensione del messaggio.
3. Uso non autorizzato delle informazioni della testata delle e-mail,
4. Sollecitare messaggi di risposta a ciascun messaggio inviato con l'intento di disturbare o collezionare copie.
5. Uso di messaggi non sollecitati originati dalla Intranet per altri soggetti terzi per pubblicizzare servizi erogati dall'Amministrazione e fruibili via Intranet stessa.
6. Invio di messaggi non legati alla missione dell'Amministrazione ad un grande numero di destinatari utenti di news group (news group spam).

4 Linee telefoniche commutate (analogiche e digitali)

Firmato digitalmente da ROBERTO FRACCIA

4.1 Scopo
Di seguito vengono illustrate le linee guida per un uso corretto delle linee telefoniche commutate (analogiche convenzionali) e digitali (ISDN, ADSL).
Queste politiche coprono due diversi usi distinti: linee dedicate esclusivamente ai telefax e linee di collegamento alle risorse elaborative dell'Amministrazione.

4.2 Ambito di applicazione
Queste politiche sono relative solo a quelle linee che sono terminate all'interno della/e sede/i dell'Amministrazione. Sono pertanto escluse le eventuali linee collegate con le abitazioni degli impiegati che operano da casa e le linee usate per gestire situazioni di emergenza.

4.3 Politiche – Scenari di impatto sull'Amministrazione
Esistono due importanti scenari che caratterizzano un cattivo uso delle linee di comunicazione che tentiamo di tutelare attraverso queste politiche.
Il primo è quello di un attaccante esterno che chiama un gruppo di numeri telefonici nella speranza di accedere alle risorse elaborative che hanno un modem collegato. Se il modem è predisposto per la risposta automatica, allora ci sono buone probabilità di accesso illecito al sistema informativo attraverso un server non monitorato. In questo scenario, al minimo possono essere compromesse solo le informazioni contenute sul server.
Il secondo scenario è la minaccia di una persona esterna che può accedere fisicamente alle risorse dell'Amministrazione e utilizza illecitamente un PC da tavolo o portatile corredato di un modem connesso alla rete. In questo caso l'intruso potrebbe essere capace di connettersi, da un lato, alla rete sicura dell'Amministrazione attraverso la rete locale e, dall'altro, simultaneamente di collegarsi con il modem ad un sito esterno sconosciuto (ma precedentemente predisposto). Potenzialmente potrebbe essere possibile trafugare tutte le informazioni dell'Amministrazione, comprese quelle vitali.

4.4 Politiche – Telefax
Dovrebbero essere adottate le seguenti regole:
- le linee fax dovrebbero essere approvate solo per uso istituzionale;
- nessuna linea dei telefax dovrebbe essere usata per uso personale;

Le postazioni di lavoro che sono capaci di inviare e ricevere fax non devono essere utilizzate per svolgere questa funzione.
Eventuali deroghe a queste politiche possono essere valutate ed eventualmente concesse dal Responsabile della sicurezza caso per caso dopo una attenta valutazione delle necessità dell'Amministrazione rispetto ai livelli di sensitività dei dati.

4.5 Politiche – Collegamento di PC alle linee telefoniche analogiche
La politica generale è quella di non approvare i collegamenti diretti dei PC alle linee telefoniche commutate. Le linee commutate rappresentano una significativa minaccia per l'Amministrazione di attacchi esterni. Le eccezioni alle precedenti politiche dovrebbero essere valutate caso per caso dal responsabile della sicurezza.

4.6 Politiche – Richiesta di linee telefoniche analogiche

Firmato digitalmente da ROBERTO FRACCIA

Una volta approvata la richiesta individuale di linea commutata dal responsabile dell'incaricato all'uso della linea medesima, questa deve essere corredata dalle seguenti informazioni da indirizzare al responsabile della sicurezza di rete:

- una chiara e dettagliata relazione che illustri la necessità di una linea commutata dedicata in alternativa alla disponibilità di rete sicura dell'Amministrazione;
- lo scopo istituzionale per cui si rende necessaria la linea commutata;
- il software e l'hardware che deve essere collegato alla linea e utilizzato dall'incaricato;
- che cosa la connessione esterna richiede per essere acceduta.

5 Politiche per l'inoltro automatico di messaggi di posta elettronica

5.1 Scopo

Lo scopo di queste politiche è prevenire rivelazioni non autorizzare o involontarie di informazioni confidenziali o sensitive dell'Amministrazione

5.2 Ambito di applicazione

Queste politiche riguardano l'inoltro automatico di messaggi e quindi la possibile trasmissione involontaria di informazioni confidenziali o sensitive a tutti gli impiegati o soggetti terzi.

5.3 Politiche

1. Gli impiegati devono esercitare estrema attenzione quando inviano qualsiasi messaggio all'esterno dell'Amministrazione. A meno che non siano espressamente approvati dal Dirigente responsabile i messaggi non devono essere automaticamente inoltrati all'esterno dell'Amministrazione.
2. Informazioni confidenziali o sensitive non devono essere trasmesse per posta elettronica a meno che, non siano espressamente ammesse e precedentemente cifrate in accordo con il destinatario.

6 Politiche per le connessioni in ingresso su rete commutata

6.1 Scopo

Proteggere le informazioni elettroniche dell'Amministrazione contro compromissione involontaria da parte di personale autorizzato ad accedere dall'esterno su rete commutata.

6.2 Ambito di applicazione

Lo scopo di queste politiche è definire adeguate modalità di accesso da remoto ed il loro uso da parte di personale autorizzato.

6.3 Politiche

Il personale dell'Amministrazione e le persone terze autorizzate (clienti, venditori, altre amministrazioni, cittadini, etc.) possono utilizzare la linea commutata per guadagnare l'ingresso alla Intranet dell'Amministrazione. Tale accesso dovrebbe essere rigidamente controllato usando sistemi di autenticazione forte, quali: password da usare una sola volta (one time password), sistemi di firma digitale o tecniche di sfida/risposta (challenger/response).
È responsabilità del personale con i privilegi di accesso dall'esterno alla rete dell'Amministrazione garantire che personale non autorizzato possa accedere illecitamente alla Intranet dell'Amministrazione ed alle sue informazioni. Tutto il personale che può accedere al sistema informativo dell'Amministrazione dall'esterno deve essere consapevole che tale accesso costituisce "realmente" una estensione del sistema informativo che potenzialmente può trasferire informazioni sensitive.

Firmato digitalmente da ROBERTO FRACCIA

Il personale e le persone terze devono, di conseguenza, porre in essere tutte le ragionevoli misure di sicurezza in loro possesso per proteggere il patrimonio informativo ed i beni dell'Amministrazione.
Solo la linea commutata convenzionale può essere utilizzata per realizzare il collegamento.
Non sono ammessi cellulari per realizzare collegamenti dati facilmente intercettabili o che consentono un re instradamento della connessione.

7 Politiche per l'uso della posta istituzionale dell'amministrazione

7.1 Scopo
Evitare l'offuscamento dell'immagine dell'Amministrazione. Quando un messaggio di posta esce dall'Amministrazione il pubblico tenderà a vedere ed interpretare il messaggio come una affermazione ufficiale dell'Amministrazione.

7.2 Ambito di applicazione
La politica di seguito descritta intende illustrare l'uso appropriato della posta elettronica istituzionale in uscita che deve essere adottata da tutto il personale e dagli interlocutori dell'Amministrazione stessa.

7.3 Politiche – Usi proibiti
Il sistema di posta dell'Amministrazione non deve essere usato per la creazione o la distribuzione di ogni distruttivo od offensivo messaggio, includendo come offensivi i commenti su razza, genere, capelli, colore, disabilità, età, orientamenti sessuali, pornografia, opinioni e pratiche religiose o nazionalità. Gli impiegati che ricevono messaggi con questi contenuti da colleghi dovrebbero riportare questi eventi ai diretti superiori immediatamente.

7.4 Politiche – Uso personale
Non è ammesso l'uso della posta istituzionale per usi personali e, in ogni caso, non si deve dare seguito a catene di lettere o messaggi scherzosi, di disturbo o di altro genere.

8 Politiche per le comunicazioni wireless

8.1 Scopo
Queste politiche proibiscono l'accesso alla rete dell'Amministrazione via rete wireless insicura.
Solo i sistemi wireless che si adattano a queste politiche o hanno la garanzia di sicurezza certificata dal responsabile della sicurezza, possono essere utilizzati per realizzare i collegamenti all'Amministrazione.

8.2 Ambito di applicazione
La politica riguarda tutti i dispositivi di comunicazione dati senza fili collegati (PC e cellulari telefonici) alla Intranet dell'Amministrazione, ovvero qualunque dispositivo di comunicazione wireless capace di trasmettere "pacchetti" di dati.
Dispositivi wireless e/o reti senza connettività alla Intranet dell'Amministrazione, sono esclusi da queste politiche.

8.3 Politiche – Registrazione delle schede di accesso

Firmato digitalmente da ROBERTO FRACCIA

Tutti i "punti di accesso" o le "stazioni base" collegati alla Intranet devono essere registrati e approvati dal responsabile della sicurezza.
Questi dispositivi sono soggetti a periodiche "prove di penetrazione" e controlli (auditing).
Tutte le schede di PC da tavolo o portatili devono essere parimenti registrate tramite l'attribuzione di specifiche credenziali di accesso.

8.4 Politiche – Approvazione delle tecnologie

Tutti i dispositivi di accesso alle LAN dell'Amministrazione devono utilizzare prodotti di venditori accreditati dal responsabile della sicurezza e configurati in sicurezza.

9. Piano di sicurezza

Il presente capitolo riporta le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, anche in relazione alle norme sulla protezione dei dati personali.

9.1 Obiettivi del piano di sicurezza

Il piano di sicurezza garantisce che:

- i documenti e le informazioni trattati dall'amministrazione/AOO siano resi disponibili, integri e riservati;
- i dati personali comuni, sensibili e/o giudiziari vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

9.2 Generalità

Il RSP ha predisposto il piano di sicurezza (o lo ha fatto predisporre sotto la sua guida e responsabilità) in collaborazione con il responsabile del sistema informativo ed il responsabile del trattamento dei dati personali e/o altri esperti di sua fiducia.
Il piano di sicurezza, che si basa sui risultati dell'analisi dei rischi a cui sono esposti i dati (personali e non), e/o i documenti trattati e sulle direttive strategiche stabilite dal vertice dell'amministrazione, definisce:

- le politiche generali e particolari di sicurezza da adottare all'interno della AOO;
- le modalità di accesso al servizio di protocollo, di gestione documentale ed archivistico;
- gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, con particolare riferimento alle misure minime di sicurezza, di cui al disciplinare tecnico richiamato nell'allegato b) del decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali, in caso di trattamento di dati personali;
- i piani specifici di formazione degli addetti;
- le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Il piano in argomento è soggetto a revisione con cadenza almeno biennale. Esso può essere modificato anticipatamente a seguito di eventi gravi.

Firmato digitalmente da ROBERTO FRACCIA

Il RSP ha adottato le misure tecniche e organizzative di seguito specificate, al fine di assicurare la sicurezza dell'impianto tecnologico dell'AOO, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti interni ed esterni:

- protezione periferica della Intranet dell'Amministrazione/AOO;
- protezione dei sistemi di acceso e conservazione delle informazioni;
- assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;
- cambio delle password con frequenza almeno trimestrale durante la fase di esercizio;

Axios prevede il tempo massimo di validità della password impostabile dall'RSP. Il controllo quindi di tempo massimo per la validità della password può anche essere gestito in modalità automatica.
Questa Amministrazione ha deciso che è opportuno, al fine di evitare rallentamenti nel lavoro di tutti i giorni, che sia responsabilità di ogni UOP modificare la propria password di accesso secondo quanto stabilito dal presente manuale.

- piano di continuità del servizio con particolare riferimento, sia alla esecuzione e alla gestione delle copie di riserva dei dati e dei documenti da effettuarsi con frequenza giornaliera, sia alla capacità di ripristino del sistema informativo entro sette giorni in caso di disastro;

Il PdP Axios essendo completamente in cloud provvede in maniera autonoma ad effettuare copie di sicurezza giornaliere e garantire un ripristino delle funzionalità, in caso di malfunzionamento, entro le 24/48 ore.

- conservazione, a cura del RsP, delle copie di riserva dei dati e dei documenti, in locali diversi e se possibile lontani da quelli in cui è installato il sistema di elaborazione di esercizio che ospita il PdP;
- gestione delle situazioni di emergenza informatica attraverso la costituzione di un gruppo di risorse interne qualificate (o ricorrendo a strutture esterne qualificate);
- impiego e manutenzione di un adeguato sistema antivirus e di gestione dei "moduli" (patch e service pack) correttivi dei sistemi operativi;
- cifratura o uso di codici identificativi (o altre soluzioni ad es. separazione della parte anagrafica da quella "sensibile") dei dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, allo scopo di renderli temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettendo di identificare gli interessati solo in caso di necessità;
- impiego delle misure precedenti anche nel caso di supporti cartacei di banche dati idonee a rilevare lo stato di salute e la vita sessuale;
- archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo, dei file di log di sistema, di rete e applicativo contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l'arco della giornata, comprese le operazioni di backup e manutenzione del sistema.

I dati personali registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema di protocollazione e gestione dei documenti utilizzato saranno consultati solo in caso di necessità dal RSP e dal titolare dei dati e, ove previsto dalle forze dell'ordine.

9.3 Formazione dei documenti – aspetti di sicurezza

Le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici garantiscono:

- l'identificabilità del soggetto che ha formato il documento e l'amministrazione/AOO di riferimento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;

Firmato digitalmente da ROBERTO FRACCIA

- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti all'interno della stessa AOO e con AOO diverse.

I documenti dell'AOO sono prodotti con l'ausilio di applicativi di videoscrittura o text editor che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura. Si adottano preferibilmente i formati PDF, XML e TIFF.
I documenti informatici prodotti dall'AOO con altri prodotti di text editor sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard (PDF, XML e TIFF) come previsto dalle regole tecniche per la conservazione dei documenti, al fine di garantire la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento.
Per attribuire in modo certo la titolarità del documento, la sua integrità e, se del caso, la riservatezza, il documento è sottoscritto con firma digitale.
L'intero sistema gestionale in uso presso questa Amministrazione/AOO consente l'elaborazione e la produzione automatica di praticamente qualsiasi documento utile al corretto funzionamento della segreteria.
I documenti possono essere prodotti direttamente in formato PDF/A e firmati digitalmente nello stesso momento.
Sempre all'interno del sistema gestionale in uso è possibile anche effettuare la firma massiva di diversi documenti in un'unica soluzione.
Per attribuire una data certa a un documento informatico prodotto all'interno di una AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici di cui al decreto del Presidente del Consiglio dei Ministri del 13 gennaio 2004 (regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici).
L'esecuzione del processo di marcatura temporale avviene utilizzando le procedure previste dal certificatore accreditato, con le prescritte garanzie di sicurezza; i documenti così formati, prima di essere inviati a qualunque altra stazione di lavoro interna all'AOO, sono sottoposti ad un controllo antivirus onde eliminare qualunque forma di contagio che possa arrecare danno diretto o indiretto all'amministrazione/AOO.
L'amministrazione si è dotata di un sistema di marcatura temporale certificata e, sempre grazie al sistema gestionale adottato, può marcare temporalmente i documenti in modo automatico nel momento stesso in cui vengono prodotti dal sistema dando così alla marca temporale una valore di immediatezza rispetto alla produzione del documento stesso.
E' ovviamente anche possibile marcare temporalmente e massivamente una serie di documenti.

9.4 Gestione dei documenti informatici

Il sistema operativo del PdP utilizzato dall'amministrazione/AOO, è conforme alle specifiche previste dalla classe ITSEC F-C2/E2 o a quella C2 delle norme TCSEC e loro successive evoluzioni (scritture di sicurezza e controllo accessi).

- Il sistema operativo del server che ospita i file utilizzati come deposito dei documenti è configurato in modo tale da consentire:
- l'accesso esclusivamente al server del protocollo informatico in modo che qualsiasi altro utente non autorizzato non possa mai accedere ai documenti al di fuori del sistema di gestione documentale;

Firmato digitalmente da ROBERTO FRACCIA

- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Il PdP in uso presso questa Amministrazione ha un sistema di scrittura automatica del log delle operazioni eseguite.

Le informazioni che vengono memorizzate, sia nel log della parte client/server, sia che nelle applicazioni CLOUD sono le seguenti:

Area Indica l'area di competenza (protocollo, personale, ecc. ecc.)
Menu Sigla della maschera video utilizzata
Utente Nome utente che ha effettuato l'operazione
Data e ora operazione Data e ora (hh:mm:ss) dell'operazione
Percorso Percorso del menu seguito
Operazione Nome specifico dell'operazione
Nome del pc della rete internaNome del pc della rete interna dell'Amministrazione/AOO
Nome del logon Nome del logon Windows
SQL eseguito (dove possibile) Istruzione SQL eseguita
Versione dell'area Versione dell'area (vedi primo campo)
Utente cloud Eventuale nome dell'utente cloud

Il sistema di gestione informatica dei documenti:

- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;

L'accesso alla base dati locale è possibile solo tramite login e password inseriti nel gestionale.
In nessun caso è possibile accedere alla base dati fuori dalla procedura sopra indicata.
La base dati è protetta e non può essere in alcun modo modificato il suo contenuto.
Il server dove è custodito il DB locale è locato in ambiente sicuro non raggiungile e l'accesso è consentito solo tramite password.

- garantisce la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
- La procedura interna stabilita dall'Amministrazione/AOO prevede l'immediata registrazione del protocollo prima di qualsiasi altra operazione venga effettuata sul documento.
- fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;

Il PdP in uso presso questa Amministrazione/AOO consente la completa gestione del ciclo del documento ivi compresa, ovviamente, la sua collocazione logica in tutti i fascicoli ove necessaria.
Ad esempio un certificato di servizio sarà legato logicamente al fascicolo generico del personale/sottofascicolo certificati di servizio, al fascicolo personale della singola utenza, al fascicolo dei documenti emessi in un certa data e, perché no, anche al fascicolo legato alla UOP che ha emesso il documento.

- consente il reperimento delle informazioni riguardanti i documenti registrati;
- consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy" con particolare riferimento al trattamento dei dati sensibili e giudiziari;
- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

Firmato digitalmente da ROBERTO FRACCIA

9.4.1 Componente organizzativa della sicurezza

La componente organizzativa della sicurezza legata alla gestione del protocollo e della documentazione si riferisce principalmente alle attività svolte presso il sistema informatico dell'amministrazione/AOO.
Nella conduzione del sistema informativo Il piano di sicurezza garantisce che:
- i documenti e le informazioni trattati dall'Istituto siano resi disponibili, autentici e integri;
- i dati personali, i dati sensibili e quelli giudiziari vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento..

Nella conduzione del sistema di sicurezza, dal punto di vista organizzativo, sono state individuate le seguenti funzioni specifiche:

- Il piano di sicurezza, basato sui risultati dell'analisi dei rischi a cui sono esposti i dati (personali e non), e/o i documenti trattati e sulle direttive strategiche stabilite dal vertice dell'amministrazione, definisce:
  - le politiche generali e particolari di sicurezza da adottare all'interno dell'Istituto
  - le modalità di accesso al sistema di protocollo e gestione documentale
  - le misure di sicurezza operative adottate sotto il profilo organizzativo, procedurale e tecnico
  - le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza

Al fine di garantire la sicurezza dell'impianto tecnologico, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti interni ed esterni, l'Istituto ha adottato le misure tecniche e organizzative di seguito specificate:

- protezione periferica della Intranet dell'amministrazione;
- protezione dei sistemi di accesso e conservazione delle informazioni;
- assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;
- cambio delle password con frequenza almeno trimestrale durante la fase di esercizio
- piano di continuità del servizio con particolare riferimento, sia alla esecuzione e alla gestione delle copie di riserva dei dati e dei documenti da effettuarsi con frequenza giornaliera, sia alla capacità di ripristino del sistema informativo entro sette giorni in caso di disastro;
- conservazione delle copie di riserva dei dati e dei documenti, in locali diversi e lontani da quelli in cui è installato il sistema di elaborazione di esercizio;
- impiego e manutenzione di un adeguato sistema antivirus;
- archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo, dei file di log contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l'arco della giornata, comprese le operazioni di backup e manutenzione del sistema.

I dati personali registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema di protocollazione e gestione dei documenti utilizzato saranno consultabili in caso di necessità dalle forze dell'ordine.
In relazione alla componente fisica della sicurezza sono stati definiti i seguenti ruoli:
E' messo in atto ai sensi della normativa vigente6 il Piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici nel rispetto delle misure minime di sicurezza previste nel disciplinare tecnico pubblicato in

Firmato digitalmente da ROBERTO FRACCIA

allegato B del decreto legislativo del 30 giugno 2003, n. 196 e successive modificazioni, d'intesa con il responsabile della conservazione, il responsabile dei sistemi informativi.

9.4.2 Componente fisica della sicurezza

Il controllo degli accessi fisici ai luoghi in cui sono custodite le risorse del sistema informatico è regolato secondo i seguenti criteri:
Si garantisce la sicurezza fisica degli accessi fisici ai luoghi in cui sono custodite le risorse del sistema informatico attraverso locali dotati di:

- porte blindate
- impianti elettrici dedicati
- sistemi di raffreddamento delle apparecchiature
- la continuità elettrica è garantita dal Gruppo di continuità
- estintori
- un controllo dell'attuazione del piano di verifica periodica sull'efficacia dei sistemi di sorveglianza e degli estintori
- impianto antincendio

9.4.3 Componente logica della sicurezza

La componente logica della sicurezza garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi.
Tale componente, nell'ambito del PdP, è stata realizzata attraverso:

- Login specifico per ogni utenza con password a scadenza trimestrale.
- Profilazione dei diversi utenti con accessibilità ai dati in base a stringenti criteri di sicurezza e di necessità di utilizzo degli stessi
- Richiesta conferma di tutte le operazioni di aggiornamento/cancellazione
- In caso di operazioni particolarmente delicate, il messaggio di richiesta conferma di tale operazione, viene richiesto per 2 volte
- In altri casi la funzione non viene eseguita se le copie di sicurezza non sono aggiornate alla stessa data di richiesta dell'operazione

In base alle esigenze rilevate dall'analisi delle minacce e delle vulnerabilità, è stata implementata una infrastruttura tecnologica di sicurezza come di seguito descritto:
La componente logica della sicurezza garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi. Tale componente, nell'ambito del sistema di protocollo informatico e di gestione documentale Axios, è stata realizzata attraverso:

- identificazione e autenticazione utente
- profilazione degli accessi (ACL)
- politica antivirus
- firma digitale
- monitoraggio sessioni di lavoro
- disponibilità del software e dell'hardware

L'utilizzo delle PdL e della rete intranet è garantito ai soli utenti dotati di apposite credenziali d'accesso (user ID + password) al sistema informatico dell'Istituto.
L'operatore può accedere unicamente al livello "interfaccia utente" e solamente se dotato di specifiche credenziali e autorizzazioni al sistema Axios.
L'interfaccia viene generata in funzione delle autorizzazioni in possesso dell'utente connesso; funzioni e dati ai quali l'utente non è autorizzato ad accedere non vengono resi disponibili.
Agli utenti "generici" dell'Istituto non è quindi consentito:

Firmato digitalmente da ROBERTO FRACCIA

- interrogare direttamente il DBMS
- interagire direttamente con il repository dei file
- accedere direttamente ai server fisici e virtualizzati

Le precedenti operazioni sono possibili ai soli soggetti autorizzati ed appartenenti al Settore Servizi Informatici e Telematici per le sole attività sistemistiche di amministrazione, aggiornamento e manutenzione delle componenti di sistema.

9.4.4 Componente infrastrutturale della sicurezza

Il sistema informatico utilizza i seguenti impianti:

- scrittura su database in modalità sincrona (scrittura logica che coincide con scrittura fisica sul disco)
- copie di backup realizzate su dischi RAID in mirroring e/o RAID 5
- consegna di una copia di sicurezza dei back up in un locale diverso come previsto dalla normativa

Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo (ad es. dati o transazioni) - presenti o transitate sul PdP - che è opportuno mantenere poiché possono essere necessarie sia in caso di controversie legali che abbiano ad oggetto le operazioni effettuate sul sistema stesso, sia al fine di analizzare compiutamente le cause di eventuali incidenti di sicurezza.
Le registrazioni di sicurezza sono costituite:

- dai log di sistema generati dal sistema operativo;
- dai log dei dispositivi di protezione periferica del sistema informatico (Intrusion Detection System (IDS), sensori di rete e firewall);
- dalle registrazioni del PdP.

Le registrazioni di sicurezza sono soggette alle seguenti misure:

- Le registrazioni del log delle operazioni effettuate dal PdP sono memorizzate nella medesima base dati e la copia avviene quindi insieme alla normale copia di backup giornaliero.
- La struttura della tabella di log del PdP è stata precedentemente illustrata
- I log di sistema rimangono automaticamente residenti all'interno del sistema
- I log del firewall sono salvati all'interno del firewall stesso
- La scuola, per ora, non intende avvalersi di sistemi particolarmente sofisticati come, ad esempio, IDS.

In questa sede viene espressamente richiamato quanto indicato nell'ultimo capoverso del paragrafo 9.2 del presente Manuale.

9.5 Trasmissione ed interscambio dei documenti informatici

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni che, per loro natura o per espressa indicazione del mittente, sono destinate ad essere rese pubbliche.
Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.
Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all'interno della AOO o ad altre pubbliche amministrazioni, contengono soltanto le informazioni relative a stati, fatti e

Firmato digitalmente da ROBERTO FRACCIA

qualità personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.
Il server di posta certificata del fornitore esterno (provider) di cui si avvale l'amministrazione, (o, in alternativa, del servizio disponibile all'interno dell'amministrazione/AOO) oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni:

- accesso all'indice dei gestori di posta elettronica certificata allo scopo di verificare l'integrità del messaggio e del suo contenuto;
- tracciamento delle attività nel file di log della posta;
- gestione automatica delle ricevute di ritorno.

Lo scambio per via telematica di messaggi protocollati tra AOO di amministrazioni diverse presenta, in generale, esigenze specifiche in termini di sicurezza, quali quelle connesse con la protezione dei dati personali, sensibili e/o giudiziari come previsto dal decreto legislativo del 30 giugno 2003, n. 196.
Per garantire alla AOO ricevente la possibilità di verificare l'autenticità della provenienza, l'integrità del messaggio e la riservatezza del medesimo, dove possibile, viene utilizzata la tecnologia di firma digitale a disposizione delle amministrazioni coinvolte nello scambio dei messaggi.

9.5.1 All'esterno della AOO (Interoperabilità dei sistemi di protocollo informatico)

Per interoperabilità dei sistemi di protocollo informatico si intende la possibilità di trattamento automatico, da parte di un sistema di protocollo ricevente, delle informazioni trasmesse da un sistema di protocollo mittente, allo scopo di automatizzare anche le attività ed i processi amministrativi conseguenti (articolo 55, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e articolo 15 del decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000, pubblicato nella Gazzetta Ufficiale del 21 novembre 2000, n. 272).
Per realizzare l'interoperabilità dei sistemi di protocollo informatico gestiti dalle pubbliche amministrazioni è necessario, in primo luogo, stabilire una modalità di comunicazione comune, che consenta la trasmissione telematica dei documenti sulla rete.
Ai sensi del decreto del Presidente del Consiglio dei Ministri del 31 ottobre 2000, il mezzo di comunicazione telematica di base è la posta elettronica, con l'impiego del protocollo SMTP e del formato MIME per la codifica dei messaggi.
La trasmissione dei documenti informatici, firmati digitalmente e inviati attraverso l'utilizzo della posta elettronica è regolata dalla circolare AIPA 7 maggio 2001, n. 28.

9.5.2 All'interno della AOO (Interoperabilità dei sistemi di protocollo informatico)

Per i messaggi scambiati all'interno della AOO con la posta elettronica non sono previste ulteriori forme di protezione rispetto a quelle indicate nel piano di sicurezza relativo alle infrastrutture.
Gli Uffici dell'amministrazione (UOR) si scambiano documenti informatici attraverso l'utilizzo del sistema di posta interno completamente gestito dal software in possesso dell'Amministrazione/AOO.
L'intero scambio di informazioni all'interno del sistema viene completamente tracciato e memorizzato in una tabella di log non modificabile e non accessibile dall'esterno.
Il sistema consente anche lo scambio di informazioni all'interno dell'Amministrazione anche tramite l'utilizzo di normali caselle di posta elettronica (in attuazione di quanto previsto dalla direttiva 27 novembre 2003 del Ministro per l'innovazione le tecnologie concernente l'impiego della posta elettronica nelle pubbliche amministrazioni) o misto.

9.6 Accesso ai documenti informatici

Firmato digitalmente da ROBERTO FRACCIA

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso (pubblica e privata o PIN nel caso di un dispositivo rimovibile in uso esclusivo all'utente) ed un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva.
La profilazione preventiva consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate ad un utente del servizio di protocollo e gestione documentale.
Il software Axios adottato dall'Amministrazione consente di definire per ogni utente ed ogni funzione, anche in base alla funzione stessa, se l'utente ha i diritti necessari a:
Creazione
Lettura
Aggiornamento
Cancellazione
Stampa
Duplicazione
Download
Autorizzazione speciale

Composizione della password:
La password di accesso al sistema è generata in automatico la prima volta con una lunghezza, a scelta dell'Amministrazione da 8 a 16 caratteri, con caratteri alfabetici maiuscoli, minuscoli e numeri.

Blocco delle utenze:
Il sistema utilizzato dall'Amministrazione è completamente integrato e questo consente una gestione dinamica delle utenze ed il relativo blocco delle stesse.
Se ad esempio un dipendente viene sospeso o è in malattia per un periodo, registrando l'evento all'interno dell'area personale, automaticamente l'utenza viene sospesa per il periodo necessario.
Ovviamente è possibile sospendere un'utenza in qualsiasi momento tramite la gestione dell'archivio utenze.

Le relative politiche di composizione, di aggiornamento e, in generale, di sicurezza delle password, in parte riportate di seguito, sono configurate sui sistemi di accesso come obbligatorie tramite il sistema operativo.

Il PdP adottato dall'amministrazione/AOO:
• consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppi di utenti;
• assicura il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.
Il PdP in uso dall'Amministrazione/AOO consente la gestione dei gruppi di utenti e, per ogni tipo di documento è possibile associare il gruppo che lo deve lavorare e la fase del processo di cui si deve occupare. All'interno del gruppo sono presenti poi i diversi utenti ognuno con diversi livelli di accesso e di operatività sul documento.
Ciascun utente del PdP può accedere solamente ai documenti che sono stati assegnati al suo UOR, o agli Uffici Utente (UU) ad esso subordinati.
Il sistema consente altresì di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'amministrazione. I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio.

9.6.1 Utenti interni all'AOO

I livelli di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti sono attribuiti dal RSP dell'amministrazione/AOO. Tali livelli si distinguono in: abilitazione alla consultazione, abilitazione all'inserimento, abilitazione alla cancellazione e alla modifica delle informazioni.

Firmato digitalmente da ROBERTO FRACCIA

La gestione delle utenze rispetta i seguenti criteri operativi:
Vengono creati gruppi di utenti corrispondenti ai diversi UOR.
Vengono create le diverse tipologie di documento.
Vengono creati i flussi operativi per ogni tipologia di documento
Assegnazione dei documenti ai gruppi con specifiche funzioni in base al flusso operativo
Definizione dei livelli di accesso e competenza di ogni utente nell'ambito del singolo gruppo

9.6.2 Accesso al registro di protocollo per utenti interni alla AOO

L'autorizzazione all'accesso ai registri di protocollo è regolata tramite i seguenti strumenti:
L'accesso al registro di protocollo è regolamentato da una procedura di accesso tramite programma con login e password. In nessun altro modo è possibile accedere a tale registro.
La visibilità completa sul registro di protocollo è consentita solo al personale autorizzato secondo i criteri di sicurezza prima illustrati. In particolare ai soli utenti aventi un livello di sicurezza tale da poter avere la visibilità completa sul registro.
L'utente assegnatario dei documenti protocollati è invece abilitato sempre secondo i criteri di sicurezza sopra indicati, ad assegnare un numero di protocollo al documento e, se previsto, inviarlo in conservazione a norma. Può anche effettuare la scannerizzazione dello stesso se il documento giunge in forma cartacea.
A questo punto il documento continuerà il suo iter, completamente digitale ed automatizzato, secondo il flusso stabilito per la sua tipologia.
L'operatore che gestisce lo smistamento dei documenti può scannerizzare il documento se giunto in forma cartacea, scaricare la posta elettronica, marcare il documento secondo le regole tipologiche stabilite ed avviarlo al flusso al documento stesso assegnato. Può anche segnalare l'eventuale mancanza di una specifica tipologia di documento al RSP.
Nel caso in cui sia effettuata la registrazione di un documento sul protocollo particolare, la visibilità completa sul documento stesso è possibile solo all'utente abilitato alla gestione del registro particolare di protocollo, ad esempio il registro dei protocolli riservati.
Tutti gli altri utenti possono accedere solo ai dati di registrazione e visualizzazione del documento sempre in formato digitale, solo con determinate autorizzazioni l'utente può anche stampare o memorizzare il documento in oggetto.

9.6.3 Utenti esterni alla AOO – Altre AOO/Amministrazioni

L'accesso al sistema di gestione informatica dei documenti dell'amministrazione da parte di altre AOO avviene nel rispetto dei principi della cooperazione applicativa, secondo gli standard e il modello architetturale del Sistema Pubblico di Connettività (SPC) di cui al decreto legislativo 28 febbraio 2005, n. 49.
Le AOO che accedono ai sistemi di gestione informatica dei documenti attraverso il SPC utilizzano funzioni di accesso per ottenere le seguenti informazioni:
• numero e data di registrazione di protocollo del documento inviato/ricevuto, oggetto, dati di classificazione, data di spedizione/ricezione ed eventuali altre informazioni aggiuntive opzionali;
• identificazione dell'UU di appartenenza del RPA.

9.6.4 Utenti esterni alla AOO – Privati

Per l'esercizio del diritto di accesso ai documenti, sono possibili due alternative: l'accesso diretto per via telematica e l'accesso attraverso l'Ufficio Relazioni con il Pubblico (URP).
L'accesso per via telematica da parte di utenti esterni all'amministrazione è consentito solo con strumenti tecnologici che permettono di identificare in modo certo il soggetto richiedente, quali: firme elettroniche,

Firmato digitalmente da ROBERTO FRACCIA

firme digitali, Carta Nazionale dei Servizi (CNS), Carta d'Identità Elettronica (CIE), sistemi di autenticazione riconosciuti dall'AOO.
L'accesso attraverso l'URP prevede che questo ufficio sia direttamente collegato con il sistema di protocollo informatico e di gestione documentale sulla base di apposite abilitazioni di sola consultazione concesse al personale addetto.
Se la consultazione avviene allo sportello, di fronte all'interessato, a tutela della riservatezza delle registrazioni di protocollo, l'addetto posiziona il video in modo da evitare la diffusione di informazioni di carattere personale.
Nei luoghi in cui è previsto l'accesso al pubblico e durante l'orario di ricevimento devono essere resi visibili, di volta in volta, soltanto dati o notizie che riguardino il soggetto interessato.

9.7 Conservazione dei documenti informatici

La conservazione dei documenti informatici avviene con le modalità e con le tecniche specificate nella deliberazione CNIPA 19 febbraio 2004, n. 11.

9.7.1 Servizio archivistico

Il responsabile del sistema archivistico dell'AOO ha individuato nella sede centrale della scuola la sede dell'archivio dell'amministrazione.
Il responsabile del servizio in argomento ha effettuato la scelta a seguito della valutazione dei fattori di rischio che incombono sui documenti (ad es. rischi dovuti all'ambiente in cui si opera, rischi nelle attività di gestione, rischi dovuti a situazioni di emergenza) e del fatto che gli archivi fossero già presenti ed organizzati in tale sede.
Per contenere i danni conseguenti a situazioni di emergenza, il responsabile del servizio ha predisposto e reso noto, un piano individuando i soggetti incaricati di ciascuna fase.
Sono state pure regolamentate minutamente le modalità di consultazione, soprattutto interne, al fine di evitare accessi a personale non autorizzato.
Il responsabile del servizio di gestione archivistica è a conoscenza, in ogni momento, della collocazione del materiale archivistico e ha predisposto degli elenchi di consistenza del materiale che fa parte dell'archivio di deposito e un registro sul quale sono annotati i movimenti delle singole unità archivistiche.
Per il requisito di "accesso e consultazione", l'AOO garantisce la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti adottando i formati previsti dalle regole tecniche vigenti, (ovvero altri formati non proprietari eventualmente di seguito indicati).

9.7.2 Servizio di conservazione a norma

Il responsabile della conservazione a norma dei documenti fornisce le disposizioni, in sintonia con il piano generale di sicurezza e con le linee guida tracciate dal RSP, per una corretta esecuzione delle operazioni di salvataggio dei dati su supporto informatico rimovibile.
Per l'archiviazione ottica dei documenti sono utilizzati i supporti di memorizzazione digitale che consentono registrazioni non modificabili nel tempo Questa Amministrazione ha scelto di avvalersi dei servizi della società Axios Italia come software e dei servizi della società 2C Solution come tenutari dello spazio per l'archiviazione ottica a norma. Si fa inoltre presente che è stato verificato nell'elenco dell'AGID che la società 2C Solution è accreditata come CA.
Il responsabile della conservazione digitale:

- adotta le misure necessarie per garantire la sicurezza fisica e logica del sistema preposto al processo di conservazione digitale e delle copie di sicurezza dei supporti di

Firmato digitalmente da ROBERTO FRACCIA

memorizzazione, utilizzando gli strumenti tecnologici e le procedure descritte nelle precedenti sezioni;
- assicura il pieno recupero e la riutilizzazione delle informazioni acquisite con le versioni precedenti in caso di aggiornamento del sistema di conservazione;
- definisce i contenuti dei supporti di memorizzazione e delle copie di sicurezza;
- verifica periodicamente, con cadenza non superiore ai cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento del contenuto dei supporti.

9.7.3 Conservazione dei documenti informatici e delle registrazioni di protocollo

I luoghi di conservazione previsti per i supporti contenenti le registrazioni di protocollo e le registrazioni di sicurezza sono differenziati in base al livello di sicurezza loro attribuito: le registrazioni di protocollo cosi come le registrazioni del log di sicurezza sono entrambi presenti all'interno della base dati della scuola.
Il log delle operazioni effettuate viene esportato con cadenza mensile e conservato su supporti removibili da parte dell'RSP che provvede alla archiviazione di tali supporti in un luogo sicuro e distante dal server della scuola. Le registrazioni di protocollo invece, o meglio il registro delle stesse, viene conservato giornalmente in maniera a norma.

È compito dell'ufficio che si occupa del servizio di sicurezza del sistema informativo (Bassi Ferdinando, responsabile tecnico Easyteam.org SRL) l'espletamento delle seguenti procedure atte ad assicurare la corretta archiviazione, la disponibilità e la leggibilità dei supporti stessi.
L'archiviazione di ogni supporto viene registrata in un specifico file di cui è disponibile la consultazione per le seguenti informazioni:
- descrizione del contenuto;
- responsabile della conservazione;
- lista delle persone autorizzate all'accesso ai supporti, con l'indicazione dei compiti previsti;
- indicazione dell'ubicazione di eventuali copie di sicurezza;
- motivi e durata dell'archiviazione.

Tale tabella è stata creata come foglio Excel protetto da password a conoscenza solo dell'RSP e del responsabile AOO.
È stato implementato e viene mantenuto aggiornato un archivio dei prodotti software (nelle eventuali diverse versioni) necessari alla lettura dei supporti conservati con lo stesso sistema del precedente.
Presso il sistema informativo sono altresì mantenuti i sistemi con la configurazione hardware necessaria al corretto funzionamento del software.
Nell'archivio di cui al terzo capoverso del presente paragrafo, viene quindi indicato anche:
- il formato del supporto rimovibile;
- il prodotto software col quale è stato generato e la versione della release;
- la configurazione hardware e software necessaria per il suo riuso.

Deve essere inoltre indicata l'eventuale necessità di refresh periodico dei supporti, che questa AOO ha stabilito essere annuale. Annualmente quindi si farà una verifica di tali supporti decidendo, in base al loro stato, la necessità o meno di un refresh degli stessi.
Il personale addetto alla sicurezza del sistema informativo verifica la corretta funzionalità del sistema e dei programmi in gestione e l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento sostitutivo del contenuto su altri supporti.

9.7.4 Conservazione delle registrazioni di sicurezza

Firmato digitalmente da ROBERTO FRACCIA

Un operatore addetto alla sicurezza dell'amministrazione/AOO, con periodicità settimanale, provvede alla memorizzazione su supporto non riscrivibile dei seguenti file di sicurezza: LOG di sistema.
Viene salvato su tali supporti sia l'esportazione del file di log delle operazioni svolte sul sistema e gestito dall'applicazione sia il file di log gestito dal database.
I supporti così realizzati sono conservati in Come previsto dal Dlgs 192/2003, conservazione delle copie di riserva dei dati e dei documenti, in locali diversi e lontani da quelli in cui è installato il sistema di elaborazione di esercizio per un periodo minimo di cinque anni ove specifiche disposizioni di legge non ne prevedano la conservazione per un più lungo periodo.

9.7.5 Riutilizzo e dismissione dei supporti rimovibili

Non è previsto il riutilizzo dei supporti rimovibili. Al termine del previsto periodo di conservazione i supporti sono distrutti secondo una specifica procedura operativa.
Qualora però alcuni di questi, magari residui di vecchie procedure di salvataggio, debbano essere riutilizzati, questi vengono formattati a basso livello in modo tale da non consentire la lettura di vecchie informazioni prima memorizzate sui supporti stessi.

9.8 Politiche di sicurezza adottate dalla AOO

Le politiche di sicurezza, riportate nell'allegato 15.9 stabiliscono sia le misure preventive per la tutela e l'accesso al patrimonio informativo, sia le misure per la gestione degli incidenti informatici.
Le politiche illustrate sono corredate dalle procedure sanzionatorie che l'AOO intende adottare in caso di riscontrata violazione delle prescrizioni dettate in materia di sicurezza da parte di tutti gli utenti che, a qualunque titolo, interagiscono con il servizio di protocollo, gestione documentale ed archivistica.
È compito del RSP, assistito dal il DSGA Luciano Zamponi, procedere al perfezionamento, alla divulgazione e al riesame e alla verifica delle politiche di sicurezza.
Il riesame delle politiche di sicurezza è conseguente al verificarsi di incidenti di sicurezza, di variazioni tecnologiche significative, di modifiche all'architettura di sicurezza che potrebbero incidere sulla capacità di mantenere gli obiettivi di sicurezza o portare alla modifica del livello di sicurezza complessivo, ad aggiornamenti delle prescrizioni minime di sicurezza richieste dal CNIPA o a seguito dei risultati delle attività di audit.
In ogni caso, tale attività è svolta almeno con cadenza annuale.

Firmato digitalmente da ROBERTO FRACCIA

ISTITUTO COMPRENSIVO STATALE
"ADA NEGRI"
Via Don Milani 4 - 20086 MOTTA VISCONTI (MILANO)
Tel./Fax02.90000266
E- mail : miic872009@istruzione.it - miic872009@pec.istruzione.it
www.icmottavisconti.edu.it
C.F. 90015610158 – C.M. MIIC872009

REGOLAMENTO DI ISTITUTO PER L'ACCESSO AGLI ATTI AMMINISTRATIVI

Approvato dal Consiglio di Istituto con delibera N. 6 del 07/02/2022

Si riassumono qui di seguito le modalità di esercizio del diritto di accesso ai documenti amministrativi in conformità a quanto stabilito dal capo V della Legge 7 agosto 1990 n. 241 e successive modificazioni e integrazioni, in particolare la Legge 11 febbraio 2005 n. 15, e dal D.P.R.12 aprile 2006, n. 184.

Art. 1 – Ambito di applicazione

1. Il diritto di accesso è la facoltà per gli interessati di prendere visione e di estrarre copia di documenti amministrativi ed è esercitabile da chiunque abbia un interesse diretto, concreto e attuale, corrispondente a una situazione giuridicamente tutelata e collegata al documento al quale è richiesto l'accesso.
2. Il diritto di accesso si esercita con riferimento ai documenti amministrativi materialmente esistenti al momento della richiesta e detenuti alla stessa data dall'Istituzione scolastica.
3. L'Istituzione scolastica non è tenuta ad elaborare dati in suo possesso al fine di soddisfare le richieste di accesso.

Art. 2 – Definizione di documento amministrativo

1. L'art. 22 della L. 241/90, modificato dalla L. 15/2005, definisce documento amministrativo "ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti anche interni o non relativi ad uno specifico procedimento detenuti da una P. A. e concernenti attività di pubblico interesse indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale".

2. In ambito scolastico i documenti di cui sopra risultano essere, tra gli altri, i seguenti (elenco non esaustivo dei possibili casi):

- elaborati scritti e atti della Commissione giudicatrice degli esami di Stato;
- compiti scritti, documenti relativi a scrutini intermedi, finali e relativi verbali, con esclusione delle parti riguardanti altri alunni;
- registri personali dei docenti e verbali dei Consigli di classe, a favore di genitori di alunno non ammesso alla classe successiva e con esclusione delle parti che concernono altri alunni;
- atti formali, anche di natura endo procedimentale, emanati nel corso dell'istruttoria a favore del soggetto che produca istanza di trasferimento e di mobilità professionale;
- relazione ispettiva ed atti presupposti e connessi a favore di insegnante sottoposto a ispezione e/o procedimento disciplinare;

Firmato digitalmente da ROBERTO FRACCIA

- atti relativi alla formulazione delle graduatorie interne e di istituto;
- atti finalizzati alla stipula di contratti per l'aggiudicazione di forniture di beni e servizi.

Art. 3 – Atti esclusi dal diritto di accesso

1. Sono esclusi dal diritto di accesso, ai sensi del D.Lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) e del D.P.R. 12 aprile 2006, n. 184 (Regolamento recante disciplina in materia di accesso ai documenti amministrativi):

- rapporti informativi sul personale dipendente;
- documenti rappresentativi di accertamenti e dichiarazioni medico-legali relativi al personale anche in quiescenza;
- documenti attinenti al trattamento economico individuale o a rapporti informativi o valutativi;
- documenti rappresentativi di interventi dell'autorità giudiziaria o della Procura della Corte dei Conti, relativi a soggetti per i quali si delinea responsabilità civile, penale, amministrativa;
- documenti contenenti atti sensibili o giudiziari, se l'accesso non è strettamente indispensabile per la tutela dell'interessato o dei suoi diritti di pari rango (art. 60 del D.Lgs. 196/2003);
- gli atti dei privati detenuti occasionalmente dall'Istituzione scolastica in quanto non scorporabili da documenti direttamente utilizzati e, in ogni modo, gli atti che non abbiano avuto specifico rilievo nelle determinazioni amministrative;
- documenti attinenti a procedimenti penali (per i quali è prevista una tutela più ampia in ambito giudiziario), o utilizzabili a fini disciplinari o di dispensa dal servizio, monitori o cautelari, nonché concernenti procedure conciliative o arbitrali;
- annotazioni, appunti e bozze preliminari;
- documenti inerenti all'attività relativa all'informazione, alla consultazione e alla concertazione e alla contrattazione sindacale, fermi restando i diritti sindacali previsti anche dal protocollo sindacale.

2. Non sono ammissibili istanze di accesso preordinate ad un controllo generalizzato dell'operato dell'Istituzione scolastica. L'accesso ai documenti amministrativi non può essere negato ove sia sufficiente fare ricorso al potere di differimento.
3. Sarà garantito ai richiedenti l'accesso ai documenti amministrativi la cui conoscenza sia necessaria per curare o per difendere i propri interessi giuridici. Nel caso di documenti contenenti dati sensibili e giudiziari, l'accesso è consentito nei limiti in cui sia strettamente indispensabile e nei termini previsti dall'art. 60 del D.Lgs. 196/2003, in caso di dati idonei a rivelare lo stato di salute e la vita sessuale.

Firmato digitalmente da ROBERTO FRACCIA

Art. 4 – Interessati al diritto di accesso

1. Sono interessati al diritto di accesso tutti i soggetti privati, compresi quelli portatori di interessi pubblici o diffusi, di cui all'art. 1 del presente Regolamento.
2. Il diritto di accesso dei soggetti di cui al precedente comma è esercitato relativamente ai documenti amministrativi e alle informazioni dagli stessi desumibili il cui oggetto è correlato con l'interesse di cui il richiedente dimostri, con idonea e specifica motivazione, di essere il titolare.

Art. 5 – Controinteressati

1. Per controinteressati si intendono tutti i soggetti, individuati o facilmente individuabili in base alla natura del documento richiesto, che, dall'esercizio dell'accesso, vedrebbero compromesso il loro diritto alla riservatezza.

2. Qualora l'Istituzione scolastica dovesse individuare soggetti controinteressati, è tenuta a darne comunicazione agli stessi (con raccomandata con avviso di ricevimento) o mediante Posta Elettronica Certificata.
3. I controinteressati hanno dieci giorni di tempo dalla ricezione della comunicazione per presentare una motivata opposizione alla richiesta di accesso. Decorso tale termine, l'Istituzione scolastica, accertata la ricezione della comunicazione da parte dei controinteressati, provvede sulla valutazione della richiesta.

Art. 6 – Modalità di accesso

1. Si ha un accesso informale qualora non risulti l'esistenza di controinteressati; in tale caso il diritto di accesso può essere esercitato mediante richiesta, anche verbale, all'Ufficio di Segreteria.
2. Per poter ottenere l'accesso al documento, il richiedente deve:
3. indicare gli estremi del documento oggetto della richiesta, ovvero gli elementi che ne consentano l'individuazione;
4. specificare e, ove occorra, comprovare l'interesse connesso all'oggetto della richiesta;
5. dimostrare la propria identità e, ove occorra, i propri poteri di rappresentanza del soggetto interessato.
6. La richiesta viene esaminata immediatamente e senza formalità, nell'ambito dell'orario d'ufficio, presso la segreteria della scuola e, compatibilmente con gli altri obblighi di servizio del personale, è accolta, se possibile, mediante indicazione della pubblicazione contenente le notizie, esibizione del documento, estrazione di copie, ovvero altra modalità idonea.
7. La scuola, invece, invita l'interessato a presentare richiesta formale (non assoggettata all'imposta di bollo, ai sensi della C.M. 16 marzo1994, n. 94) nei seguenti casi:
8. quando, in base al contenuto del documento richiesto, riscontri l'esistenza di controinteressati;
9. quando non risulti possibile l'accoglimento immediato della richiesta in via informale;

Firmato digitalmente da ROBERTO FRACCIA

10. quando sorgano dubbi sulla legittimazione del richiedente, sulla sua identità, sui suoi poteri rappresentativi, sulla sussistenza dell'interesse alla stregua delle informazioni e delle documentazioni fornite, sull'accessibilità del documento o sull'esistenza di controinteressati.
11. Nei suddetti casi la scuola mette a disposizione dell'interessato un apposito modulo per la richiesta, allegato al presente Regolamento.
12. Il responsabile del procedimento di accesso è il Dirigente scolastico o il dipendente delegato, competente a formare il documento o a detenerlo stabilmente.

Art. 7 – Risposta dell'Amministrazione scolastica

1. Il procedimento di accesso deve concludersi nel termine di trenta giorni, decorrenti dalla presentazione della richiesta all'ufficio competente o dalla ricezione della medesima.
2. Il Dirigente scolastico, valutata la richiesta, decide:

- l'accoglimento della richiesta: la domanda viene ritenuta completa, e pertanto tutta la documentazione viene messa a disposizione del richiedente;
- la limitazione della richiesta: è possibile accedere solo a una parte della documentazione che viene messa a disposizione del richiedente;
- il differimento della richiesta: la domanda non può essere accolta immediatamente, ma solo in un secondo momento, indicato dall'Istituzione scolastica;
- il rifiuto della richiesta: la domanda non può essere accolta.

3. Ove la richiesta sia irregolare o incompleta, il Dirigente scolastico, entro dieci giorni, ne dà comunicazione al richiedente (con raccomandata con avviso di ricevimento o altro mezzo idoneo a comprovarne la ricezione). In tale caso, il termine del procedimento ricomincia a decorrere dalla presentazione della richiesta corretta.
4. Dell'accoglimento della richiesta formale, della limitazione, del differimento o del rifiuto (che devono essere motivati) va data comunicazione all'interessato a mezzo notifica, PEC o raccomandata A.R. entro dieci giorni dall'arrivo al protocollo; qualora sia necessario il coinvolgimento di soggetti controinteressati il termine viene posticipato di ulteriori dieci giorni.

   La comunicazione di accoglimento indica inoltre il giorno e l'ora fissato per l'accesso. In caso di impossibilità da parte del richiedente per tale giorno, possono essere concordati, con il Dirigente scolastico, un altro giorno e l'orario entro i 15 giorni successivi.

5. L'atto che dispone il differimento dell'accesso ne indica la durata.
6. L'inosservanza da parte dell'Amministrazione dei termini indicati nel presente Regolamento viene considerata, a tutti gli effetti, come silenzio-rifiuto.

Firmato digitalmente da ROBERTO FRACCIA

7. Il richiedente, in caso di diniego della domanda, può presentare ricorso nel termine di 30 giorni alla Commissione per l'accesso ai documenti amministrativi presso la Presidenza del Consiglio dei Ministri o al Tribunale Amministrativo Regionale.

Art. 8 – Accoglimento della richiesta

1. Il richiedente avrà accesso per l'esamina dei documenti presso l'Istituzione scolastica negli orari e nel periodo indicati nell'atto di accoglimento della richiesta e alla presenza del personale addetto.
2. I documenti per i quali è consentito l'accesso non possono essere asportati dal luogo presso cui sono presi in visione e non possono essere alterati in qualsiasi modo, per cui l'interessato può solo prendere appunti e trascrivere in tutto o in parte i documenti presi in visione.
3. I cittadini, a cui sia stato affidato un documento di pertinenza dell'Istituzione scolastica, rispondono ad ogni effetto di legge dei danni che eventualmente dovessero arrecare ai documenti: danneggiamento, distruzione o perdita.

   La sottoscrizione, la soppressione, la distruzione o il deterioramento di un documento è passibile anche di denuncia penale ai sensi dell'art. 351 del C. P.

4. Qualora un documento si riferisca contestualmente a più persone, l'accesso, mediante esame ed estrazione di copia, è consentito limitatamente alla parte del documento che si riferisce al soggetto richiedente, anche mediante copertura delle parti del documento concernenti persone diverse dal richiedente.
5. Su richiesta dell'interessato, le copie possono essere autenticate.
6. L'accesso ad eventuali informazioni contenute in strumenti informatici avviene mediante stampa dei documenti richiesti.
7. Qualora vi siano richieste di "prendere visione" per un numero di documenti ritenuto eccessivamente gravoso e incompatibile con le normali operazioni amministrative, potrà essere disposto l'accesso solo tramite rilascio di copie (con i necessari tempi procedurali e con gli oneri previsti dal presente Regolamento).

Art. 9 – Decadenza dell'autorizzazione

1. Il richiedente che – entro 30 giorni – non si è avvalso del diritto di esame degli atti a seguito di accoglimento della domanda, decade dal diritto stesso e per la durata di un anno non può presentare domanda di accesso agli stessi documenti.
2. L'inosservanza dei divieti previsti dall'art. 8, c. 3, comporta l'immediata decadenza del diritto di esame.

Firmato digitalmente da ROBERTO FRACCIA

Art. 10 – Rilascio di copie e costi di notifica

1. L'esame dei documenti è gratuito.
2. L'esercizio di accesso agli atti mediante rilascio di copia è subordinato soltanto al rimborso del costo di riproduzione fissato come segue:

   – € 0,25 a facciata A4, per documenti che non necessitano copertura di dati di altri soggetti;

   – € 0,50 a facciata A4, per documenti che necessitano copertura di dati di altri soggetti;

   – € 0,50 a facciata A3, per documenti che non necessitano copertura di dati di altri soggetti;

   – € 1,00 a facciata A3, per documenti che necessitano copertura di dati di altri soggetti.

3. Qualora la richiesta di accesso agli atti comporti la notifica a controinteressati, i costi necessari alla notifica sono quantificati in € 10,00 a controinteressato (ad esclusione delle notifiche indirizzate a personale in effettivo servizio presso l'Istituzione scolastica); tali importi, comprensivi delle spese postali e dei costi amministrativi, sono a carico del richiedente l'accesso e potranno essere richiesti in anticipo per l'avvio del procedimento.
4. Il pagamento verrà effettuato tramite versamento o bonifico bancario presso **IBAN** intestato all'Istituto **NOME SCUOLA** con causale: "Rimborso spese di riproduzione per l'accesso agli atti", prima del ritiro delle copie (per semplicità, non verrà richiesto pagamento per importi fino a € 3,00).
5. Qualora risulti prevedibile un importo superiore a € 20,00, potrà essere chiesto il versamento di un anticipo in base alle copie preventivabili prima di procedere alla predisposizione delle stesse.
6. Restano salve le disposizioni vigenti in materia di bollo.

Firmato digitalmente da ROBERTO FRACCIA

TITOLARIO UNICO DI CLASSIFICAZIONE PER LE ISTITUZIONI SCOLASTICHE

I	**AMMINISTRAZIONE**
I.1	Normativa e disposizioni attuative
I.2	Organigramma e funzionigramma
I.3	Statistica e sicurezza di dati e informazioni
I.4	Archivio, accesso, privacy, trasparenza e relazioni con il pubblico
I.5	Registri e repertori di carattere generale
I.6	Audit, qualità, carta dei servizi, valutazione e autovalutazione
I.7	Elezioni e nomine
I.8	Eventi, cerimoniale, patrocini, concorsi, editoria e stampa
II	**ORGANI E ORGANISMI**
II.1	Consiglio di istituto, Consiglio di circolo e Consiglio di Amministrazione
II.2	Consiglio di classe e di interclasse
II.3	Collegio dei docenti
II.4	Giunta esecutiva
II.5	Dirigente scolastico DS
II.6	Direttore dei servizi generali e amministrativi DSGA
II.7	Comitato di valutazione del servizio dei docenti
II.8	Comitato dei genitori, Comitato studentesco e rapporti scuola-famiglia
II.9	Reti scolastiche
II.10	Rapporti sindacali, contrattazione e Rappresentanza sindacale unitaria (RSU)
II.11	Commissioni e gruppi di lavoro
III	**ATTIVITÀ GIURIDICO-LEGALE**
III.1	Contenzioso
III.2	Violazioni amministrative e reati
III.3	Responsabilità civile, penale e amm.va
III.4	Pareri e consulenze
IV	**DIDATTICA**
IV.1	Piano triennale dell'offerta formativa PTOF
IV.2	Attività extracurricolari
IV.3	Registro di classe, dei docenti e dei profili
IV.4	Libri di testo
IV.5	Progetti e materiali didattici
IV.6	Viaggi di istruzione, scambi, stage e tirocini
IV.7	Biblioteca, emeroteca, videoteca e sussidi

Firmato digitalmente da ROBERTO FRACCIA

IV.8 Salute e prevenzione

IV.9 Attività sportivo-ricreative e rapporti con il Centro Scolastico Sportivo

IV.10 Elaborati e prospetti scrutini

V STUDENTI E DIPLOMATI

V.1 Orientamento e *placement*

V.2 Ammissioni e iscrizioni

V.3 Anagrafe studenti e formazione delle classi

V.4 *Cursus studiorum*

V.5 Procedimenti disciplinari

V.6 Diritto allo studio e servizi agli studenti (trasporti, mensa, buoni libro, etc.)

V.7 Tutela della salute e farmaci

V.8 Esoneri

V.9 Prescuola e attività parascolastiche

V.10 Disagio e diverse abilità – DSA

VI FINANZA E PATRIMONIO

VI.1 Entrate e finanziamenti del progetto

VI.2 Uscite e piani di spesa

VI.3 Bilancio, tesoreria, cassa, istituti di credito e verifiche contabili

VI.4 Imposte, tasse, ritenute previdenziali e assistenziali, denunce

VI.5 Assicurazioni

VI.6 Utilizzo beni terzi, comodato

VI.7 Inventario e rendiconto patrimoniale

VI.8 Infrastrutture e logistica (plessi, succursali)

VI.9 DVR e sicurezza

VI.10 Beni mobili e servizi

VI.11 Sistemi informatici, telematici e fonia

VII PERSONALE

VII.1 Organici, lavoratori socialmente utili, graduatorie

VII.2 Carriera

VII.3 Trattamento giuridico-economico

VII.4 Assenze

VII.5 Formazione, aggiornamento e sviluppo professionale

VII.6 Obiettivi, incarichi, valutazione e disciplina

VII.7 Sorveglianza sanitaria

VII.8 Collaboratori esterni

Firmato digitalmente da ROBERTO FRACCIA

Manuale della Conservazione

di InfoCert S.p.A.

Firmato digitalmente da: Danilo Cattaneo

Firmato digitalmente da ROBERTO FRACCIA

REGISTRO DELLE VERSIONI

N° versione	Data emissione	Modifiche apportate
01	Luglio 2014	Prima versione
02	Novembre 2015	Utilizzo dello schema proposto da AgID
03	Febbraio 2016	Correzioni formali e di layout
04	Marzo 2016	Correzioni formali e di layout
05	Settembre 2017	Glossario, Normativa, Mission, Comunità di riferimento, Riferimenti a policy aziendali interne
05.1	Novembre 2017	Specificità del contratto
06	Luglio 2018	Normativa GDPR, semplificazione glossario e nuovi Responsabili
07	Gennaio 2019	Nuovo logo aziendale
08	Maggio 2019	Nuovo Responsabile sistemi
09	Ottobre 2020	Glossario, nuovi Responsabili, aggiornamento procedure di monitoraggio, semplificazione delle Specificità del contratto
10	Novembre 2020	Ampliamento servizi di storage

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

INDICE DEL DOCUMENTO

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

1. SCOPO E AMBITO DEL DOCUMENTO

Il presente documento è il Manuale della Conservazione di InfoCert S.p.A. (Società soggetta a direzione e controllo di TecnoInvestimenti S.p.A.), ai sensi del Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'Amministrazione Digitale di cui al decreto legislativo n. 82 del 2005 pubblicato in GU Serie Generale n.59 del 12-3-2014 - Suppl. Ordinario n. 20.
Il Manuale della Conservazione illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.
In caso di ispezione da parte delle autorità di vigilanza preposte, il Manuale della Conservazione permette un agevole svolgimento di tutte le attività di controllo.

Torna al sommario

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

2. TERMINOLOGIA (GLOSSARIO, ACRONIMI)

TERMINE	DEFINIZIONE
ACCESSO	Operazione che consente di prendere visione dei documenti informatici.
AFFIDABILITÀ	Caratteristica che, con riferimento a un sistema di gestione documentale o conservazione, esprime il livello di fiducia che l'utente ripone nel sistema stesso, mentre con riferimento al documento informatico esprime la credibilità e l'accuratezza della rappresentazione di atti e fatti in esso contenuta.
AGGREGAZIONE DOCUMENTALE INFORMATICA	Insieme di documenti informatici o insieme di fascicoli informatici riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente.
ARCHIVIO	Complesso dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività.
ARCHIVIO INFORMATICO	Archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche.
AREA ORGANIZZATIVA OMOGENEA	Un insieme di funzioni e di uffici individuati dall'ente al fine di gestire i documenti in modo unitario e coordinato, secondo quanto disposto dall'art. 50 comma 4 del D.P.R. 28 dicembre 2000, n. 445. Essa rappresenta il canale ufficiale per l'invio di istanze e l'avvio di procedimenti amministrativi.
ATTESTAZIONE DI CONFORMITÀ DELLE COPIE PER IMMAGINE SU SUPPORTO INFORMATICO DI UN DOCUMENTO ANALOGICO	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.
AUTENTICITÀ	Caratteristica in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto un oggetto è autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze.
CERTIFICAZIONE	Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi.
CLASSIFICAZIONE	Attività di organizzazione di tutti i documenti secondo uno schema costituito da un insieme di voci articolate in modo gerarchico e che individuano, in astratto, le funzioni, competenze, attività e/o materie del soggetto produttore.
CLOUD DELLA PA	Ambiente virtuale che consente alle Pubbliche Amministrazioni di erogare servizi digitali ai cittadini e alle imprese nel rispetto di requisiti minimi di sicurezza e affidabilità.
CODEC	Algoritmo di codifica e decodifica che consente di generare flussi binari, eventualmente imbustarli in un file o in un *wrapper* (codifica), così come di estrarli da esso (decodifica).
CONSERVATORE	Soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici.
CONSERVAZIONE	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

CONVENZIONI DI DENOMINAZIONE DEL FILE	Insieme di regole sintattiche che definisce il nome dei file all'interno di un filesystem o pacchetto.
COORDINATORE DELLA GESTIONE DOCUMENTALE	Soggetto responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 nei casi di amministrazioni che abbiano istituito più AOO.
DESTINATARIO	Soggetto o sistema al quale il documento informatico è indirizzato.
DIGEST	Vedi Impronta crittografica.
DOCUMENTO AMMINISTRATIVO INFORMATICO	Ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa
DOCUMENTO ELETTRONICO	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva
DOCUMENTO INFORMATICO	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
DUPLICATO INFORMATICO	Vedi art. 1, comma 1, lett) i quinquies del CAD.
ESEAL	Vedi sigillo elettronico.
ESIBIZIONE	operazione che consente di visualizzare un documento conservato
ESIGNATURE	Vedi firma elettronica.
ESTRATTO DI DOCUMENTO INFORMATICO	Parte del documento tratto dal documento originale
ESTRATTO PER RIASSUNTO DI DOCUMENTO INFORMATICO	Documento nel quale si attestano in maniera sintetica fatti, stati o qualità desunti da documenti informatici.
ESTRAZIONE STATICA DEI DATI	Estrazione di informazioni utili da grandi quantità di dati (es. database, datawarehouse ecc…), attraverso metodi automatici o semi-automatici
EVIDENZA INFORMATICA	Sequenza finita di *bit* che può essere elaborata da una procedura informatica.
FASCICOLO INFORMATICO	Aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento.
FILE	Insieme di informazioni, dati o comandi logicamente correlati, raccolti sotto un unico nome e registrati, per mezzo di un programma di elaborazione o di scrittura, nella memoria di un computer.
FILE CONTAINER	Vedi Formato contenitore.
FILE WRAPPER	Vedi Formato contenitore.
FILE-MANIFESTO	File che contiene metadati riferiti ad un file o ad un pacchetto di file.
FILESYSTEM	Sistema di gestione dei file, strutturato mediante una o più gerarchie ad albero, che determina le modalità di assegnazione dei nomi, memorizzazione e organizzazione all'interno di uno storage.
FIRMA ELETTRONICA	Vedi articolo 3 del Regolamento eIDAS.
FIRMA ELETTRONICA AVANZATA	Vedi articoli 3 e 26 del Regolamento eIDAS.
FIRMA ELETTRONICA QUALIFICATA	Vedi articolo 3 del Regolamento eIDAS.
FLUSSO (BINARIO)	Sequenza di bit prodotta in un intervallo temporale finito e continuativo che ha un'origine precisa ma di cui potrebbe non essere predeterminato il suo istante di interruzione.

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

FORMATO CONTENITORE	Formato di file progettato per consentire l'inclusione ("imbustamento" o *wrapping*), in uno stesso file, di una o più evidenze informatiche soggette a differenti tipi di codifica e al quale possono essere associati specifici metadati.
FORMATO DEL DOCUMENTO INFORMATICO	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
FORMATO "DEPRECATO"	Formato in passato considerato ufficiale il cui uso è attualmente sconsigliato a favore di una versione più recente.
FUNZIONI AGGIUNTIVE DEL PROTOCOLLO INFORMATICO	Nel sistema di protocollo informatico, componenti supplementari rispetto a quelle minime, necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni.
FUNZIONI MINIME DEL PROTOCOLLO INFORMATICO	Componenti del sistema di protocollo informatico che rispettano i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445.
FUNZIONE DI *HASH* CRITTOGRAFICA	Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o *digest* (vedi) in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
GESTIONE DOCUMENTALE	Processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta, uso, selezione e conservazione dei documenti.
HASH	Termine inglese usato, impropriamente, come sinonimo d'uso di "impronta crittografica" o "*digest*" (vedi).
IDENTIFICATIVO UNIVOCO	Sequenza di numeri o caratteri alfanumerici associata in modo univoco e persistente ad un'entità all'interno di uno specifico ambito di applicazione.
IMPRONTA CRITTOGRAFICA	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di *hash* crittografica a un'evidenza informatica.
INTEGRITÀ	Caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità.
INTEROPERABILITÀ	Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi.
LEGGIBILITÀ	Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica.
MANUALE DI CONSERVAZIONE	Documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture.
MANUALE DI GESTIONE	Documento informatico che descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

METADATI	Dati associati a un o documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017.
NAMING CONVENTION	Vedi Convenzioni di denominazione
OGGETTO DI CONSERVAZIONE	Oggetto digitale versato in un sistema di conservazione.
OGGETTO DIGITALE	Oggetto informativo digitale, che può assumere varie forme tra le quali quelle di documento informatico, fascicolo informatico, aggregazione documentale informatica o archivio informatico.
PACCHETTO DI ARCHIVIAZIONE	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel manuale di conservazione.
PACCHETTO DI DISTRIBUZIONE	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione.
PACCHETTO DI FILE (*FILE PACKAGE*)	Insieme finito di più file (possibilmente organizzati in una struttura di sottoalbero all'interno di un filesystem) che costituiscono, collettivamente oltre che individualmente, un contenuto informativo unitario e auto-consistente.
PACCHETTO DI VERSAMENTO	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione.
PACCHETTO INFORMATIVO	Contenitore logico che racchiude uno o più oggetti di conservazione con i relativi metadati, oppure anche i soli metadati riferiti agli oggetti di conservazione.
PATH	Percorso (*vedi*).
PATHNAME	Concatenazione ordinata del percorso di un file e del suo nome.
PERCORSO	Informazioni relative alla localizzazione virtuale del file all'interno del filesystem espressa come concatenazione ordinata del nome dei nodi del percorso.
PIANO DELLA SICUREZZA DEL SISTEMA DI CONSERVAZIONE	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi.
PIANO DELLA SICUREZZA DEL SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi.
PIANO DI CLASSIFICAZIONE (TITOLARIO)	Struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata.
PIANO DI CONSERVAZIONE	Documento, allegato al manuale di gestione e integrato con il sistema di classificazione, in cui sono definiti i criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445.
PIANO DI ORGANIZZAZIONE DELLE AGGREGAZIONI DOCUMENTALI	Strumento integrato con il sistema di classificazione a partire dai livelli gerarchici inferiori di quest'ultimo e finalizzato a individuare le tipologie di aggregazioni documentali (tipologie di serie e tipologie di fascicoli) che devono essere prodotte e gestite in rapporto ai procedimenti e attività in cui si

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

	declinano le funzioni svolte dall'ente
PIANO GENERALE DELLA SICUREZZA	Documento che pianifica le attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza.
PRESA IN CARICO	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione e, in caso di affidamento del servizio all'esterno, dagli accordi stipulati tra il titolare dell'oggetto di conservazione e il responsabile del servizio di conservazione.
PROCESSO	Insieme di attività correlate o interagenti che trasformano elementi in ingresso in elementi in uscita.
PRODUTTORE DEI PDV	Persona fisica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con il responsabile della gestione documentale.
QSEAL	Sigillo elettronico qualificato, come da art. 35 del Regolamento eIDAS.
QSIGNATURE	Firma elettronica qualificata, come da art. 25 del Regolamento eIDAS.
RAPPORTO DI VERSAMENTO	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.
REGISTRO DI PROTOCOLLO	Registro informatico ove sono memorizzate le informazioni prescritte dalla normativa per tutti i documenti ricevuti e spediti da un ente e per tutti i documenti informatici dell'ente stesso.
REGISTRO PARTICOLARE	Registro informatico individuato da una pubblica amministrazione per la memorizzazione delle informazioni relative a documenti soggetti a registrazione particolare.
REGOLAMENTO EIDAS	electronic IDentification Authentication and Signature, Regolamento (UE) № 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
REPERTORIO	Registro su cui vengono annotati con un numero progressivo i fascicoli secondo l'ordine cronologico in cui si costituiscono all'interno delle suddivisioni del piano di classificazione.
RESPONSABILE DEI SISTEMI INFORMATIVI PER LA CONSERVAZIONE	Soggetto che coordina i sistemi informativi all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID.
RESPONSABILE DEL SERVIZIO DI CONSERVAZIONE	soggetto che coordina il processo di conservazione all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
RESPONSABILE DELLA CONSERVAZIONE	Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.
RESPONSABILE DELLA FUNZIONE ARCHIVISTICA DI CONSERVAZIONE	soggetto che coordina il processo di conservazione dal punto di vista archivistico all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

RESPONSABILE DELLA GESTIONE DOCUMENTALE	Soggetto responsabile della gestione del sistema documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445.
RESPONSABILE DELLA PROTEZIONE DEI DATI	Persona con conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, in grado di assolvere i compiti di cui all'articolo 39 del Regolamento (UE) 2016/679.
RESPONSABILE DELLA SICUREZZA DEI SISTEMI DI CONSERVAZIONE	soggetto che assicura il rispetto dei requisiti di sicurezza all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
RESPONSABILE DELLO SVILUPPO E DELLA MANUTENZIONE DEL SISTEMA DI CONSERVAZIONE	soggetto che assicura lo sviluppo e la manutenzione del sistema all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
RIFERIMENTO TEMPORALE	Insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC).
RIVERSAMENTO	Procedura mediante la quale uno o più documenti informatici sono convertiti da un formato di file (ovvero di busta, ovvero di pacchetto di file) ad un altro, lasciandone invariato il contenuto per quanto possibilmente permesso dalle caratteristiche tecniche del formato (ovvero dei formati) dei file e delle codifiche di destinazione.
SCARTO	Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico-culturale.
SERIE	Raggruppamento di documenti con caratteristiche omogenee (vedi anche aggregazione documentale informatica).
***SIDECAR* (FILE)**	File-manifesto (*vedi*).
SIGILLO ELETTRONICO	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi.
SISTEMA DI CONSERVAZIONE	Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, comma 1, del CAD.
SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI	Insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle organizzazioni per la gestione dei documenti. Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445
TIMELINE	Linea temporale virtuale su cui sono disposti degli eventi relativi ad un sistema informativo o a un documento informatico. Costituiscono esempi molto diversi di *timeline* un file di log di sistema, un flusso multimediale contenente essenze audio\video sincronizzate.
TITOLARE DELL'OGGETTO DI CONSERVAZIONE	Soggetto produttore degli oggetti di conservazione.
TRASFERIMENTO	Passaggio di custodia dei documenti da una persona o un ente ad un'altra persona o un altro ente.
TUDA	Testo Unico della Documentazione Amministrativa, Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni e integrazioni.

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

UFFICIO	Riferito ad un'area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico.
UTENTE ABILITATO	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.
VERSAMENTO	Passaggio di custodia, di proprietà e/o di responsabilità dei documenti. Nel caso di un organo giudiziario e amministrativo dello Stato operazione con la quale il responsabile della conservazione trasferisce agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali.

Torna al sommario

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

3. NORMATIVA E STANDARD DI RIFERIMENTO

3.1 Normativa di riferimento

Di seguito l'elenco dei principali riferimenti normativi italiani in materia, ordinati secondo il criterio della gerarchia delle fonti:

- Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- Legge 7 agosto 1990, n. 241 e ss.mm.ii. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e ss.mm.ii – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e ss.mm.ii. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e ss.mm.ii. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e ss.mm.ii. (D. Lgs. 26 agosto 2016, n.179) – Codice dell'amministrazione digitale (CAD);
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche per il protocollo informatico ai sensi degli articoli 40 -bis, 41, 47, 57 -bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Decreto del Ministero dell'Economia e delle Finanze 17 giugno 2014 - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82 del 2005;
- Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.
- eIDAS (electronic IDentification Authentication and Signature) EU Regulation 910/2014 of the European Parliament and of the Council, of 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market.
- GDPR (General Data Protection Regulation) EU Regulation 679/2016 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
- Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici del settembre 2020.

Torna al sommario

3.2 Standard di riferimento

Si riportano di seguito gli standard di riferimento elencati nell'allegato 3 delle citate Regole

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

Tecniche ai sensi del Codice:

- UNI EN ISO 9001:2015 Sistemi di gestione per la Qualità;
- ISO 14001:2015 Sistema di Gestione Ambientale;
- Norma ETSI 319 401 - Reg. UE 910/2014 – eIDAS (electronic IDentification Authentication and Signature);
- ISO 15489:2014 (cap. 5 Regulatory Environment; cap. 7 Records Management Requirements);
- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ISO/IEC 27017:2015 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud service;
- ISO/IEC 27018:2019 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors;
- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- ETSI TR 101 533-2 V1.3.1 (2012-04) Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- ISO/IEC 20000-1: 2018 Service Management System Requirements
- ISO 15836:2009 Information and documentation - The Dublin Core metadata element

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

set, Sistema di metadata del Dublin Core.

- UNI 11386:2020 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;

Torna al sommario

3.3 Procedure aziendali interne

Si riportano di seguito i riferimenti alle procedure aziendali interne e alle principali politiche aziendali applicate anche al sistema di conservazione:

- PR/225- Change Management InfoCert
- MG231 – Modello di Gestione e Organizzazione D.Lgs 231/01
- PR/235 Progettare e sviluppare un servizio informatico InfoCert
- MG294 Capacity Management
- MG/325 Gestire Verifiche Ispettive InfoCert
- MG445 – Gestione Documentale InfoCert
- PR456 Problem Management
- Procedura Service Management System – SMS
- Processo MG115/TB02_Processi e Responsabilità_Integrated Management System
- Procedura di hand-over tra conservatori e scarto archivistico in LegalDoc.

Torna al sommario

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

4. RUOLI E RESPONSABILITÀ

Si riportano di seguito i profili professionali di Responsabilità legate al servizio di conservazione e le rispettive attività di competenza.
Tutti i Responsabili sono assunti a tempo indeterminato.

RUOLI	NOMINATIVI	ATTIVITA'	PERIODI
Responsabile del servizio di Conservazione	Nicola Maccà	• Definizione e attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione. • Definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente. • Corretta erogazione del servizio di conservazione all'ente produttore. • Gestione delle convenzioni, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione. • Definizione delle condizioni generali del contratto di servizio in coordinamento con la funzione legale e la funzione commerciale e funzione	da luglio 2018

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

RUOLI	NOMINATIVI	ATTIVITA'	PERIODI
		marketing di InfoCert.	
Responsabile Sicurezza dei sistemi per la conservazione	Giovanni Belluzzo	• Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; • Segnalazione delle eventuali difformità al Responsabile del servizio di Conservazione e individuazione e pianificazione delle necessarie azioni correttive.	da luglio 2018
Responsabile funzione archivistica di conservazione	Marta Gaia Castellan	• Definizione e descrizione archivistica dei documenti e delle aggregazioni documentali per la fruizione del patrimonio documentario e informativo conservato. • Definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici. • Analisi archivistica per lo sviluppo di funzionalità del sistema di conservazione. • Collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza. • Definizione delle condizioni	da settembre 2015

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

RUOLI	NOMINATIVI	ATTIVITA'	PERIODI
		generali del contratto di servizio in coordinamento con la funzione legale e la funzione commerciale e funzione marketing di InfoCert. • Controlli periodici a campione sulla leggibilità dei documenti conservati.	
Responsabile trattamento dati personali	Ilenia Gentilezza	• Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali. • Garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.	da marzo 2020
Responsabile sistemi informativi per la conservazione	Francesco Griselda	• Presidio ed evoluzione dei sistemi informativi per la conservazione nel rispetto delle procedure ISO9001 ISO14000 ISO20000 ISO27000. • Gestione dell'esercizio delle componenti hardware e software di base del sistema di conservazione. • Monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore in collaborazione con Il Responsabile della	da ottobre 2020

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

RUOLI	NOMINATIVI	ATTIVITA'	PERIODI
		manutenzione del sistema di conservazione. • Segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di Conservazione e individuazione e pianificazione delle necessarie azioni correttive. • Pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione. • Controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di Conservazione. • Coordinamento dello sviluppo e manutenzione delle componenti hardware e software di base del sistema di conservazione.	
Responsabile sviluppo e manutenzione del sistema di conservazione	Lucia Bortoletto	• Sviluppo e manutenzione del sistema di conservazione nel rispetto delle procedure ISO9001 ISO14000 ISO20000 ISO27000. • Coordinamento dello sviluppo e manutenzione delle componenti software del sistema di conservazione. • Pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione.	da luglio 2018

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

RUOLI	NOMINATIVI	ATTIVITA'	PERIODI
		• Monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione. • Interfaccia con l'ente produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche in collaborazione con il Responsabile funzione archivistica di conservazione. • Gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.	

Di seguito sono storicizzate le figure professionali che hanno ricoperto ruoli di responsabilità precedentemente:

RUOLI	NOMINATIVI PRECEDENTI	PERIODI
Responsabile sistemi informativi per la conservazione	Stefano Mameli	da maggio 2019 a ottobre 2020
Responsabile trattamento dati personali	Valentina Zoppo	da luglio 2018 a marzo 2020

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

RUOLI	NOMINATIVI PRECEDENTI	PERIODI
Responsabile sistemi informativi per la conservazione	Nicolò Poniz	da luglio 2018 a maggio 2019
Responsabile sviluppo e manutenzione del sistema di conservazione	Nicola Maccà	da gennaio 2013 a luglio 2018
Responsabile sistemi informativi per la conservazione	Massimo Biagi	da marzo 2014 a luglio 2018
Responsabile funzione archivistica di conservazione precedente	Silvia Loffi	da dicembre 2014 ad agosto 2015
Responsabile trattamento dati personali	Alfredo Esposito	da gennaio 2011 a luglio 2018
Responsabile Sicurezza dei sistemi per la conservazione	Alfredo Esposito	da gennaio 2011 a luglio 2018
Responsabile del servizio di Conservazione	Antonio Dal Borgo	da luglio 2008 a luglio 2018
Responsabile del servizio di Conservazione	Pio Barban	da luglio 2007 a luglio 2008

Torna al sommario

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Profilo di InfoCert

Denominazione sociale	InfoCert S.p.A.
Sede Legale:	Piazza Sallustio, 9, 00187 Roma Tel.+39 06 836691
Sedi Operative:	• Piazza da Porto, 3, 35131 Padova • Via Via Carlo Bo, 11, 20143 Milano • Via Marco e Marcelliano, 45, 00147 Roma Tel: +39 06836691
Sito web	www.infocert.it
e-mail	info@infocert.it
PEC	infocert@legalmail.it
Codice Fiscale / Partita IVA	07945211006
Numero REA	RM – 1064345

InfoCert si pone sul mercato europeo come Trust Service Provider altamente specializzato, leader del mercato italiano nei servizi di digitalizzazione e dematerializzazione, nonché una delle principali Certification Authority a livello europeo, fornendo servizi di Posta Elettronica Certificata, Firma Avanzata e Digitale, Conservazione Digitale dei documenti e gestore accreditato AgID dell'identità digitale di cittadini e imprese, in conformità ai requisiti regolamentari e tecnici dello SPID (Sistema Pubblico per la gestione dell'Identità Digitale).

Da sempre la mission aziendale è credere nel futuro e nella trasformazione digitale, per questo dedichiamo la nostra esperienza, la nostra capacità di innovazione e la nostra passione per l'eccellenza, a tutti coloro che, in Italia e nel mondo, ricercano sicurezza e affidabilità nelle soluzioni digitali. Investiamo in ricerca e sviluppo per dare vita a nuove idee che supportino i nostri clienti nella costruzione di modelli e processi di business innovativi e conformi alle

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

normative, guidandoli verso una efficace trasformazione digitale e un futuro maggiormente sostenibile per le aziende, le persone e la realtà sociale.

La mission aziendale si declina anche nel servizio di Conservazione digitale: innovazione, sicurezza, affidabilità e conformità normativa, con lo scopo di assicurare la corretta gestione, archiviazione e conservazione dei documenti informatici di diversi soggetti produttori, assicurando l'esibizione a norma dei documenti conservati e la consulenza specialistica su progetti di paperless design.

InfoCert dal 2014 è tra le prime aziende italiane accreditate dall'Agenzia per l'Italia Digitale (AgID) come Conservatore, requisito normativo necessario per erogare servizi di Conservazione digitale per la Pubblica Amministrazione.

Inoltre, dal 2019, InfoCert ha ottenuto la qualifica AgID Cloud Marketplace (CSP Tipo B Infrastruttura e SaaS per LegalDoc).

La comunità di riferimento del servizio di Conservazione digitale di InfoCert è un gruppo identificato di clienti e di potenziali utenti in grado di comprendere un determinato set di informazioni: si tratta di un'unica comunità, ben definita, ma con alcune differenziazioni interne (multiple user communities), a seconda del mercato di riferimento (Pubblica Amministrazione centrale e locale, Sanità, Industry, Banking, Pharma, Utilities, Insurance, Ordini e Associazioni, PMI, liberi professionisti).

Il fine ultimo del servizio di Conservazione digitale è rendere i Pacchetti di Distribuzione ricercabili, esibibili, leggibili, integri, affidabili, autentici e fruibili dagli utenti della comunità di riferimento, attraverso la mediazione del soggetto produttore, in ottemperanza ai principali standard internazionali di records management (OAIS ISO14721 e ISO15489).

InfoCert è costantemente impegnata nel monitoraggio della propria comunità designata, al fine di acquisire nuove informazioni o esigenze o standard tecnologici, anche con lo scopo di combattere l'obsolescenza tecnologica. Per maggiori dettagli si rimanda al Service Management System.

InfoCert, inoltre, nello svolgimento delle proprie attività, ha conseguito le seguenti certificazioni:

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

- ISO 14001:2015 (Sistema di Gestione Ambientale)
- ISO/IEC 20000-1:2011 (Gestione dei Servizi Informatici)
- UNI EN ISO 9001:2015 (Sistemi di gestione per la qualità);
- ISO/IEC ISO 27001:2013 (Sistemi di gestione della sicurezza delle informazioni).
- ISO/IEC ISO 27017 e ISO/IEC ISO 27018 relativamente al Servizio di conservazione digitale a norma di documenti informatici erogato in modalità Cloud (SaaS) e relativi servizi di infrastruttura (IaaS privato).

InfoCert ha adottato il modello di organizzazione e controllo [MG231/01] di cui al D.lgs. del 08 giugno 2001 n.231 allo scopo di prevenire i reati per i quali la legge in questione prescrive la responsabilità amministrativa dell'impresa.

Il modello adottato da InfoCert rappresenta un'ulteriore garanzia dell'azienda in termini rigore, trasparenza e senso di responsabilità nella gestione dei processi interni e nei rapporti con il mondo esterno.

Il modello prevede l'istituzione di un Organismo di Vigilanza, la gestione di un processo formativo/informativo, la adozione di un Codice Etico e la definizione di un Sistema Sanzionatorio.

InfoCert si è dotata, inoltre, di un Integrated Management System per la gestione dei processi e delle responsabilità aziendali. Il documento MG115/TB02 descrive la mappatura dei processi aziendali in termini di ambiti di processo, procedure, ownership, modelli di gestione, pianificazioni, erogazioni, approvvigionamenti, controlli, governance e sicurezza.

Torna al sommario

5.2 Organigramma

L'organigramma di InfoCert è stato depositato presso AgID durante le procedure di accreditamento. Di seguito sono riportate le figure di responsabilità che intervengono nei processi e nelle attività di Conservazione.

Torna al sommario

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

5.3 Strutture organizzative

Nel processo di conservazione digitale intervengono numerosi soggetti, a differenti livelli e con diverse responsabilità, sintetizzate nella tabella seguente e dettagliate per singola attività.

Responsabilità Attività	Responsabile del servizio della Conservazione	Responsabile della funzione archivistica	Responsabile del trattamento dei dati personali	Responsabile della sicurezza dei sistemi per la conservazione	Responsabile dei sistemi informativi per la conservazione	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Soggetto Produttore
1. Condizioni Generali di Contratto	R						
2. Richiesta di attivazione	R	V	V	V	V	V-E	
3. Atto di affidamento	R						
4. Specifiche Tecniche di integrazione	V			A	A	R-E	
5. Impegno alla riservatezza	V		R	A			
6. Acquisizione del documento da conservare	R				E	V	
7. Metadatazione ed archiviazione	A	R			E	V	
8. Eventuale attestazione della conformità di quanto memorizzato nel documento d'origine da parte di un PU	R						

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

Responsabilità Attività	Responsabile del servizio della Conservazione	Responsabile della funzione archivistica	Responsabile del trattamento dei dati personali	Responsabile della sicurezza dei sistemi per la conservazione	Responsabile dei sistemi informativi per la conservazione	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Soggetto Produttore
9. Creazione del pacchetto di versamento							R
10. Invio al sistema di conservazione del pacchetto di versamento							R
11. Validazione Del pacchetto di versamento	R				E	V	
12. Generazione del pacchetto di archiviazione	R				E	V	
13. Memorizzazione e creazione “copia di sicurezza”	R			V	E	V	
14. Invio dell'IPdA al soggetto Produttore	R					E	
15. Scarto dei pacchetti di archiviazione	R	V			A	E	
16. Chiusura del servizio di conservazione al termine di un contratto	R	V			A	E	
17. Conduzione e manutenzione del	A				R	E	

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

Responsabilità Attività	Responsabile del servizio della Conservazione	Responsabile della funzione archivistica	Responsabile del trattamento dei dati personali	Responsabile della sicurezza dei sistemi per la conservazione	Responsabile dei sistemi informativi per la conservazione	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Soggetto Produttore
sistema di conservazione							
18. Monitoraggio del sistema di conservazione	**A**	**V**			**R**	**E**	
19. Change management		**V**		**V**	**A**	**R**	
20. Verifica periodica di conformità a normativa e standard di riferimento	**A**	**R**	**V**	**V**	**A**		

[**R**-responsabile; **E**-esegue; **V**- verifica; **A**-approva]

I Soggetti Produttori affidano in outsourcing il servizio di conservazione a InfoCert S.p.A., che assume le responsabilità della conservazione in accordo con quanto previsto dai documenti contrattuali descritti al capitolo 10 'Specificità del Contratto' e dagli articoli 5 e 6 del DPCM del 3 dicembre 2013.

Tutte le verifiche in carico al Responsabile del servizio della Conservazione sono garantite anche dal servizio di auditing interno. Il processo di conservazione è normalmente effettuato da procedure totalmente automatizzate, che non necessitano dell'intervento di altri soggetti o delegati. InfoCert si riserva, come specificato nelle Condizioni generali del Contratto, la possibilità di avvalersi di partner tecnologici per l'esecuzione di operazioni, singole attività, servizi relativi a funzioni o fasi del processo di conservazione, a terzi soggetti, fornitori esterni, che per conoscenza, esperienza, capacità e affidabilità forniscano idonee garanzie.

Torna al sommario

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

6. OGGETTI SOTTOPOSTI A CONSERVAZIONE

In generale si definisce 'pacchetto' un contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare.

I pacchetti (versamento/archiviazione/distribuzione) sono contrattualizzati con il Soggetto Produttore e si basano sui documenti che fanno parte delle 'Specificità del Contratto'.

Per "pacchetto di versamento" si intende l'insieme di documenti che il Soggetto Produttore invia al sistema di conservazione in un'unica sessione (login/logout).

Per "pacchetto di archiviazione" si intende un pacchetto informativo composto dalla trasformazione di pacchetti di versamento, depositato nei data center InfoCert descritto nelle 'Specificità del Contratto' SPT/NDOC- Specifiche tecniche per l'integrazione. Ad ogni documento il Sistema di conservazione associa un file XML, detto Indice del Pacchetto di Archiviazione (Indice di Conservazione UNI SInCRO). L'insieme degli Indici del Pacchetto di Archiviazione associati ai file componenti un pacchetto di versamento è detto Rapporto di Versamento.

Per "pacchetto di distribuzione" si intende un pacchetto informativo inviato dal sistema di conservazione all'utente in risposta a una sua richiesta, ovvero è la risposta alla ricerca effettuata dal Soggetto Produttore tramite interfaccia disponibile, che porta all'esibizione del documento conservato. Il documento da esibire è accompagnato sempre dall'IPdA.

Nel sistema, ad oggi, il "pacchetto di distribuzione" coincide con il "pacchetto di archiviazione".

Eventuali specificità sono concordate con il Soggetto Produttore e descritte nelle 'Specificità del Contratto' SPT/NDOC- Specifiche tecniche per l'integrazione e AL/NDOC – Allegato Tecnico al Contratto LegalDoc.

Torna al sommario

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

6.1 Oggetti conservati

Tipologie documentali, metadati e formati sono sempre concordati con il Soggetto Produttore, e vengono elencati nelle 'Specificità del Contratto' - 'Dati Tecnici di attivazione'.

I visualizzatori dei formati standard, previsti nell'allegato 2 del DPCM 3 dicembre 2013, sono automaticamente assegnati all'atto dell'attivazione del proprio ambiente di conservazione e sono forniti da InfoCert al Soggetto Produttore all'atto di attivazione del servizio. Tutti i documenti inviati in conservazione saranno associati al visualizzatore configurato per il particolare formato.

Formato	Estensione	MIME-Type	Standard
PDF o PDF/A	.pdf	application/pdf;NA	ISO 32000-1 (PDF), ISO 19005-1:2005 (vers. PDF 1.4), ISO 19005-2:2011 (vers. PDF 1.7)
TIFF	.tif	image/tiff;NA	ISO 12639(TIFF/IT); ISO 12234 (TIFF/EP)
XML	.xml	text/xml;1.0	
TXT	.txt	text/plain;NA	

Conservare documenti in altri formati (jpeg, Open Document Format, eml, DICOM, ecc..) è sempre possibile.

Qualora un Soggetto Produttore necessiti di formati aggiuntivi rispetto a quelli standard, dovrà segnalarlo nei 'Dati Tecnici di attivazione' (compresi nelle 'Specificità del Contratto') ed eventualmente conservare gli appositi visualizzatori in una sezione predefinita dell'ambiente assegnato.

I formati aggiuntivi devono essere concordati, dunque, tra il Soggetto Produttore e InfoCert in fase contrattuale e non è possibile caricare visualizzatori per formati non preventivamente concordati e configurati nel sistema.

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

I visualizzatori di formati aggiuntivi ai predefiniti devono essere inviati dal Soggetto Produttore prima di iniziare la conservazione dei documenti (il sistema accetta i documenti in conservazione anche se il visualizzatore non è caricato, ma finché non viene caricato non è possibile effettuare l'esibizione dei documenti). Il caricamento di un visualizzatore per un particolare mime/type va effettuato una sola volta, ulteriori caricamenti per lo stesso mime/type verranno identificati come aggiornamenti di versione del visualizzatore.

Di seguito è riportata la tabella di sintesi del processo di caricamento dei visualizzatori, inoltre per ognuna delle attività elencate saranno descritte le attività di dettaglio, seguendo lo schema: input\dettaglio delle attività\output.

Responsabilità **Attività**	Responsabile del servizio della Conservazione	Responsabile della funzione archivistica	Responsabile del trattamento dei dati personali	Responsabile della sicurezza dei sistemi per la conservazione	Responsabile dei sistemi informativi per la conservazione	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Soggetto Produttore
1. Creazione del file dei parametri di upload, del file della scheda tecnica e predisposizione dei file del visualizzatore.							**R**
2. Invio della richiesta al sistema di conservazione.							**R**
3. Validazione delle informazioni presenti nei file della richiesta	**R**				**E**	**V**	
4. Caricamento del visualizzatore, creazione del file IPdA, marcatura temporale e firma digitale	**R**				**E**	**V**	

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

Responsabilità Attività	Responsabile del servizio della Conservazione	Responsabile della funzione archivistica	Responsabile del trattamento dei dati personali	Responsabile della sicurezza dei sistemi per la conservazione	Responsabile dei sistemi informativi per la conservazione	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Soggetto Produttore
dello stesso ed invio al soggetto Produttore.							

[**R**-responsabile; **E**-esegue; **V**- verifica; **A**-approva]

Torna al sommario

6.2 Pacchetto di versamento

Di seguito è riportata la tabella di sintesi del processo di versamento del pacchetto, inoltre per ognuna delle attività elencate saranno descritte le attività di dettaglio, seguendo lo schema input\dettaglio delle attività\output.

Responsabilità Attività	Responsabile del servizio della Conservazione	Responsabile della funzione archivistica	Responsabile del trattamento dei dati personali	Responsabile della sicurezza dei sistemi per la conservazione	Responsabile dei sistemi informativi per la conservazione	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Soggetto Produttore
1. Invio al sistema di conservazione del pacchetto di versamento.							**R**
2. Validazione del pacchetto di	**R**				**E**	**V**	**R**

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

Responsabilità / Attività	Responsabile del servizio della Conservazione	Responsabile della funzione archivistica	Responsabile del trattamento dei dati personali	Responsabile della sicurezza dei sistemi per la conservazione	Responsabile dei sistemi informativi per la conservazione	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Soggetto Produttore
versamento.							
3. Generazione del pacchetto di archiviazione.	**R**				**E**	**V**	
4. Memorizzazione e creazione "copia di sicurezza".	**R**			V	**E**	**V**	
5. Invio dell'IPdA al Soggetto Produttore.	**R**						

L'art. 7 comma c) del DPCM del 3 dicembre 2013 introduce, inoltre, l'obbligo di generare il Rapporto di Versamento.

L'insieme degli Indici del Pacchetto di Archiviazione associati ai file componenti un pacchetto di versamento è detto Rapporto di Versamento.

Il Rapporto di Versamento attesta l'avvenuta presa in carico da parte del sistema di conservazione del pacchetto di versamento inviato dal Produttore ed è l'insieme degli Indici dei Pacchetti di Archiviazione prodotti per ogni singolo documento oggetto di versamento (per i dettagli tecnici si rimanda a 'Specificità del Contratto' SPT/NDOC- Specifiche tecniche per l'integrazione).

Il rifiuto dei pacchetti di versamento avviene nella modalità descritta nelle 'Specificità del Contratto' SPT/NDOC- Specifiche tecniche per l'integrazione e con le casistiche definite SPT/NDOCERR – Descrizione dei codici di errore di LegalDoc.

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

Le eventuali personalizzazioni specifiche di un contratto sono descritte nei documenti elencati e descritti nel capitolo 10 - 'Specificità del Contratto'.

Torna al sommario

6.3 Pacchetto di archiviazione

Per "pacchetto di archiviazione" si intende un pacchetto informativo composto dalla trasformazione di pacchetti di versamento, depositato nei data center InfoCert descritto nelle 'Specificità del Contratto' SPT/NDOC- Specifiche tecniche per l'integrazione. Ad ogni documento il Sistema di conservazione associa un file XML, detto Indice del Pacchetto di Archiviazione. L'insieme degli Indici del Pacchetto di Archiviazione associati ai file componenti un pacchetto di versamento è detto Rapporto di Versamento.

L'Indice del Pacchetto di Archiviazione è un file in formato XML, marcato temporalmente e firmato digitalmente dal Responsabile del servizio della Conservazione, generato dal sistema, che contiene i metadati in formato UNI SInCRO e le informazioni di conservazione del documento e viene con esso conservato.

In particolare, nel file sono riportati:

- informazioni sull'applicazione che ha generato l'IPdA
- il token del documento (ovvero il suo identificativo univoco)
- l'operazione eseguita (conservazione, rettifica, scarto e cancellazione)
- il bucket (ovvero l'area di conservazione) associato al Soggetto Produttore e la policy utilizzata
- il nome dei file che compongono il pacchetto, incluso il file dei parametri di conservazione ed il file di indici, e le rispettive impronte
- eventuali informazioni relative al documento rettificante e rettificato
- il tempo di creazione (timestamp) del file IPdA
- l'impronta di Hash del documento.

L'insieme degli IPdA di un pacchetto di versamento formano il Rapporto di versamento di cui all'art. 9, comma d) del DPCM del 3 dicembre 2013.

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

Il file IPdA è reso disponibile con il documento di riferimento ad ogni operazione di conservazione e richiesta di esibizione.

Torna al sommario

6.4 Pacchetto di distribuzione

Il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, al documento informatico conservato, attraverso la produzione di un pacchetto di distribuzione.

Le procedure di esibizione permettono di estrarre dal sistema un pacchetto di distribuzione per cui sia stata completata correttamente la procedura di conservazione, utilizzando il relativo token (ovvero l'identificativo univoco del documento da esibire) o utilizzando uno o più metadati versati.

Insieme ai file costituenti il pacchetto di distribuzione, sono rese disponibili anche le informazioni che qualificano il processo di conservazione, ossia il file IPdA e un'Attestazione di corretta conservazione e datacertazione firmata dal Responsabile del servizio di Conservazione.

Non è possibile esibire parti singole di documento.

L'esibizione può restituire i pacchetti in tre modalità differenti: in un pacchetto di distribuzione in formato zip contenente al suo interno tanti pacchetti quanti sono i documenti da esibire, in un unico pacchetto di distribuzione in formato zip, oppure un file alla volta (quest'ultima modalità deve essere compatibile con il client di esibizione dell'utente).

Le procedure del sistema mantengono e aggiornano ad ogni nuovo invio il database di tutti i token; il database viene interrogato ad ogni richiesta di rettifica, scarto e cancellazione, ricerca ed esibizione confrontando il token inviato con quelli memorizzati. La procedura assicura di agire solamente sul documento richiesto, e solamente se in possesso dei dovuti profili di autorizzazione.

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

L'esibizione del pacchetto di distribuzione ottenuto tramite interrogazione al sistema di conservazione rappresenta un'esibizione completa, legalmente valida ai sensi del secondo comma dell'articolo 10 del DPCM del 03 dicembre 2013 e dell'articolo 5 del DMEF del 17 giugno 2014.

Un apposito strumento di esibizione e verifica, anche detto “Esibitore a Norma”, permette di richiamare agevolmente un documento conservato e consente di ottenere in modo automatico sia la verifica delle firme digitali e delle marche temporali apposte che le verifiche di integrità dei documenti conservati e di tutti gli altri elementi conservati.

Si rimanda al ‘MU/ESIB Manuale Utente Esibitore LegalDoc’ – ‘Specificità del Contratto’ per il dettaglio delle funzionalità di verifica del sistema.

Torna al sommario

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

7. IL PROCESSO DI CONSERVAZIONE

Il sistema di conservazione è erogato in modalità SaaS (Software as a Service) secondo uno schema di Business Process Outsourcing (BPO) e permette di mantenere e garantire nel tempo l'integrità, la leggibilità e la validità legale di un documento informatico, nel rispetto della normativa vigente.

Il sistema consente le funzionalità di:

- **accettazione del pacchetto di versamento**, formato dal documento da conservare e dai metadati ad esso associati;
- **conservazione del pacchetto di archiviazione**: il documento, ricevuto nei Data Center di InfoCert in formato digitale statico non modificabile, viene conservato a norma di legge per tutta la durata prevista ed è contenuto in un pacchetto di archiviazione;
- **rettifica del pacchetto di archiviazione**: un documento inviato in conservazione può essere rettificato dall'invio di un documento successivo. La rettifica è una modifica logica, nel pieno rispetto del principio di tracciabilità e la rettifica si applica al pacchetto di archiviazione;
- **scarto/cancellazione del pacchetto di archiviazione:** in caso un documento sia stato versato per errore. La cancellazione è una modifica logica, nel pieno rispetto del principio di tracciabilità e si applica al pacchetto di archiviazione; per la cancellazione fisica di pacchetti di archiviazione ritenuti privi di valore amministrativo e di interesse storico-culturale dal Produttore, occorre formulare apposita richiesta a InfoCert (scarto archivistico);
- **ricerca dei documenti conservati**: l'utente autorizzato può eseguire una ricerca tra i documenti conservati trasversalmente sulle classi documentali, utilizzando uno o più metadati popolati in fase di caricamento;
- **esibizione del pacchetto di distribuzione:** il documento richiesto via web viene richiamato direttamente dal sistema di conservazione digitale ed esibito, con garanzia della sua opponibilità a terzi; attraverso l'Esibitore di LegalDoc è possibile visualizzare e scaricare sia il documento conservato che gli altri documenti a corredo della corretta conservazione (file di indici, file di parametri, Indice del Pacchetto di Archiviazione);
- **visualizzazione delle statistiche di conservazione**;
- **caricamento dei visualizzatori**: è previsto il deposito dei visualizzatori da parte del Soggetto Produttore qualora la tipologia dei file conservati non sia quella standard, definita in fase di attivazione del sistema.

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

Il sistema di conservazione, quindi, integra il sistema di gestione del Soggetto Produttore, sia esso un'azienda o un ente locale, e ne estende i servizi con funzionalità di stoccaggio digitale (archivio di deposito).

Le fasi di creazione, utilizzo e archiviazione dei documenti sono organizzate liberamente, in quanto il servizio interviene solamente nella fase di conservazione e solamente per i documenti che il Soggetto Produttore sceglie di conservare.

Torna al sommario

7.1 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico

Di seguito è riportata la tabella che descrive l'acquisizione dei pacchetti, seguendo lo schema: input\dettaglio delle attività\output.

ATT.1 Invio al sistema di conservazione del pacchetto di versamento

INPUT	*Documento da inviare al sistema di conservazione tramite il pacchetto di versamento*	
Sistema di gestione documentale del Soggetto Produttore		Invocazione del sistema di conservazione da parte del sistema di gestione, secondo lo standard descritto nelle SPT/NDOC – Specifiche tecniche per l'integrazione di LegalDoc.
		Autenticazione al sistema LegalDoc mediante credenziali (username/password) e ottenimento dell'identificativo di sessione (IdSessionId)
		Trasmissione del pacchetto di versamento costituente il documento (file di dati, il file di indici del documento e il file dei parametri di conservazione) secondo le modalità di trasmissione descritte nelle SPT/NDOC – Specifiche tecniche per l'integrazione di LegalDoc.
OUTPUT	*pacchetto di versamento inviato*	

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

Per maggiori dettagli si rimanda al documento “SPT/NDOC – Specifiche tecniche per l'integrazione di LegalDoc” – ‘Specificità del Contratto’.

Torna al sommario

7.2 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti

ATT.1 Validazione del pacchetto di versamento

INPUT	*Pacchetto di versamento*	
Sistema di conservazione		Generazione dell'impronta di ogni file costituente il documento e confronto con la corrispondente impronta inviata dal Soggetto Produttore, a garanzia dell'integrità del documento ricevuto. In caso di esito negativo delle verifiche, rigetto del documento con invio al sistema di gestione del Soggetto Produttore dell'errore intercorso. In questo caso, termine del flusso.
		Controllo dei valori indicati dal Soggetto Produttore nel file dei parametri di conservazione: verifica della policy dichiarata, verifica della congruenza dei tipi di file inviati (mimetype), verifica dell'univocità del file all'interno del path (cartella) indicato.
		Controllo dei valori indicati dal Soggetto Produttore nel file di indici del documento: validazione dei tracciati dei file di indice, verifica della correttezza della classe documentale, verifica della compatibilità fra policy dichiarate e policy configurate, verifica degli indici obbligatori (esistenza, valorizzazione, non duplicazione, correttezza del tipo di file, controllo numerico). I valori espressi nel file di indici vengono confrontati con la configurazione presente nelle apposite tabelle presenti nel database LegalDoc.
		Aggiornamento dei database del sistema con i dati relativi al documento e ai file che lo compongono per il mantenimento della tracciabilità delle operazioni.

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

OUTPUT	*pacchetto di versamento verificato*

Torna al sommario

7.3 Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico

Le fasi previste sono la memorizzazione, la creazione del file IPDA e la marcatura temporale dello stesso.

ATT.1 Generazione del pacchetto di archiviazione

INPUT	*Pacchetto di archiviazione*
Sistema di conservazione	Eventuale apposizione della firma digitale sul file di dati, cioè sul documento da conservare (se prevista da accordi contrattuali appositi esplicitati nei 'Dati Tecnici di attivazione', che fanno parte delle 'Specificità del contratto')
	Creazione del file XML IPdA (Indice del Pacchetto di Archiviazione) contenente: le informazioni sul processo di conservazione (in particolare sul software LegalDoc), le policy ed il bucket (area di conservazione) utilizzati, il nome e le impronte dei file costituenti il documento e l'identificativo (token) assegnato al documento,
	Marcatura e firma da parte del Responsabile del servizio della Conservazione del file IPdA. Copia del file sul supporto primario.
	Indicizzazione del documento conservato al fine di poter reperire lo stesso in seguito.
	Aggiornamento del database del sistema interessato alle modifiche di cui sopra.

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

OUTPUT	*pacchetto di archiviazione*

ATT.2 Memorizzazione e creazione copia di sicurezza

INPUT	*Pacchetto di archiviazione*
	Memorizzazione del pacchetto di archiviazione su supporto magnetico, mediante un sistema di archiviazione permanente dei contenuti digitali
	Inserimento nelle tabelle di interfaccia del sistema di archiviazione permanente delle informazioni di puntamento dei file, al fine di poter reperire gli stessi in seguito.
	La procedura di creazione della copia di sicurezza avviene in maniera automatica e gestita dal sistema di Storage.
OUTPUT	*Documenti conservati*

ATT.3 Invio dell'IPdA al soggetto Produttore

INPUT	*File IPdA*
	Invio dell'esito e del file IPdA al soggetto Produttore.
OUTPUT	*Esito conservazione inviato*

Torna al sommario

7.4 Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie

All'interno delle 'Specificità del Contratto' SPT/NDOCERR – Descrizione dei codici di errore di LegalDoc è presente la griglia riassuntiva dei codici errore che il servizio LegalDoc restituisce

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

in seguito a situazioni che impediscono la corretta e completa esecuzione del servizio richiesto. La griglia riporta le seguenti informazioni:

- Codice di errore - codifica abbreviata dell'errore avvenuto
- Messaggio di errore - breve descrizione dell'errore avvenuto

I campi codice e descrizione vengono inseriti nel corpo della risposta HTTP.

L'assistenza LegalDoc è contattabile mediante ticket https://help.infocert.it/

Torna al sommario

7.5 Preparazione e gestione del pacchetto di archiviazione

Di seguito è riportata la tabella che descrive la gestione dei pacchetti di archiviazione, seguendo lo schema: input\dettaglio delle attività\output.

ATT.1 Verifica del pacchetto di versamento

INPUT	*Pacchetto di versamento*	
Sistema di conservazione	1	Generazione dell'impronta di ogni file costituente il documento e confronto con la corrispondente impronta inviata dal soggetto Produttore, a garanzia dell'integrità del documento ricevuto. In caso di esito negativo delle verifiche, rigetto del documento con invio al sistema di gestione del soggetto Produttore dell'errore intercorso. In questo caso, termine del flusso.
	2	Controllo dei valori indicati dal soggetto Produttore nel file dei parametri di conservazione: verifica della policy dichiarata, verifica della congruenza dei tipi di file inviati (mimetype), verifica dell'univocità del file all'interno del path (cartella) indicato.
	3	Controllo dei valori indicati dal soggetto Produttore nel file di indici del documento: validazione dei tracciati dei file di indice, verifica della correttezza della classe documentale, verifica della compatibilità fra policy dichiarate e policy configurate, verifica degli indici obbligatori (esistenza, valorizzazione,

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

		non duplicazione, correttezza del tipo di file, controllo numerico). I valori espressi nel file di indici vengono confrontati con la configurazione presente nelle apposite tabelle presenti nel database LegalDoc.
	4	Aggiornamento dei database del sistema con i dati relativi al documento e ai file che lo compongono per il mantenimento della tracciabilità delle operazioni.
OUTPUT	*pacchetto di versamento verificato*	

ATT.2 Formazione del pacchetto di archiviazione

INPUT	*Pacchetto di archiviazione*	
Sistema di conservazione	1	Eventuale apposizione della firma digitale sul file di dati (se prevista da accordi contrattuali)
	2	Creazione del file XML IPdA (Indice del Pacchetto di Archiviazione) contenente: le informazioni sul processo di conservazione (in particolare sul software LegalDoc), le policy ed il bucket (area di conservazione) utilizzati, il nome e le impronte dei file costituenti il documento e l'identificativo assegnato al documento,
	2	Marcatura e firma da parte del Responsabile del servizio di Conservazione del file IPdA. Copia del file sul supporto primario.
	3	Indicizzazione del documento conservato al fine di poter reperire lo stesso in seguito.
	4	Aggiornamento del database del sistema interessato alle modifiche di cui sopra.
OUTPUT	*pacchetto di archiviazione*	

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

ATT.3 Memorizzazione del pacchetto di archiviazione

INPUT	*Pacchetto di archiviazione*	
Sistema di conservazione	1	Memorizzazione del pacchetto di archiviazione su supporto magnetico, mediante un sistema di archiviazione permanente dei contenuti digitali
	2	Inserimento nelle tabelle di interfaccia del sistema di archiviazione permanente delle informazioni di puntamento dei file, al fine di poter reperire gli stessi in seguito.
	3	La procedura di creazione della copia di sicurezza avviene in maniera automatica e gestita dal sistema di Storage.
OUTPUT	*Documenti conservati*	

Torna al sommario

7.6 Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione

ATT1. Ricerca del documento da esibire

INPUT	*Lista di token archiviati dal sistema*	
Sistema di Gestione documentale del Soggetto Produttore		Ricerca negli archivi del sistema del token relativo al documento da esibire attraverso le procedure previste dai sistemi di gestione.
		Restituzione del token corretto.
OUTPUT	*Token relativo al documento da esibire*	

ATT2. Richiesta di esibizione del documento conservato

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

INPUT	*Richiesta di esibizione da eseguire*
Sistema di Gestione documentale del Soggetto Produttore	Autenticazione al sistema LegalDoc mediante credenziali (username/password) e ottenimento dell'identificativo di session (ldSessionId).
	Invocazione del servizio di esibizione del sistema di conservazione secondo le modalità descritte nelle 'Specificità del Contratto' SPT/NDOC – Specifiche tecniche per l'integrazione di LegalDoc. In questa chiamata viene utilizzato il token ricavato in precedenza.
OUTPUT	*Richiesta di esibizione eseguita*

ATT.3 Accettazione della richiesta da parte del sistema di conservazione

INPUT	*Richiesta di esibizione*
Sistema di conservazione	Ricezione della richiesta di esibizione del documento.
	Controllo di corrispondenza tra il token inviato dal Soggetto Produttore e quelli dei documenti conservati.
OUTPUT	*Richiesta di esibizione presa in carico*

ATT.4 Risposta del sistema di conservazione ed esibizione del documento

INPUT	*Richiesta di esibizione acquisita*
	Ricerca dei file costituenti il documento e dei file attestanti il processo di conservazione corrispondenti al token inviato e preparazione del pacchetto di distribuzione.
	Invio della risposta al sistema del Soggetto Produttore.

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

OUTPUT	*Documento esibito*

Torna al sommario

7.7 Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti

Per duplicato si intende il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario.

Per copia si intende il documento informatico avente contenuto identico al documento da cui è tratto, ma con forma diversa.

La conservazione avviene su supporto primario e su supporto secondario, quindi con duplicazione automatica. Come descritto in seguito, tali supporti sono magnetici ad alte capacità e performance, che garantiscono la ridondanza interna del dato. È inoltre eseguito un backup periodico su tape magnetico.

La creazione di copie informatiche, invece, in caso di adeguamento del formato rispetto all'evoluzione tecnologica sarà presa in carico dal Responsabile del servizio della Conservazione e dalle figure professionali coinvolte nel processo di conservazione in base alle specifiche del formato in questione e al know-how tecnologico a disposizione. A fronte di questa analisi sarà progettata una soluzione di concerto con il Soggetto Produttore del formato più idoneo per permettere la leggibilità del documento conservato.

Possono essere generati anche duplicati o copie attraverso l'Esibitore o su supporto ottico, su specifica richiesta del Soggetto Produttore. Nel primo caso il Produttore/Utente agisce autonomamente con apposite credenziali attraverso l'Esibitore di LegalDoc. Nel secondo caso il Soggetto Produttore inoltra la richiesta ai suoi riferimenti abituali (help desk o account) che poi provvedono alla veicolazione verso gli operatori interni.

L'intervento di un Pubblico Ufficiale per attestare la conformità di una copia all'originale avviene secondo quanto previsto dagli articoli 22 e 23 del Codice e dalle Regole Tecniche del DPCM del 13 novembre 2014 - Regole tecniche in materia di formazione, trasmissione, copia,

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

Torna al sommario

7.8 Scarto dei pacchetti di archiviazione

In LegalDoc esistono due diverse metodologie di 'cancellazione':

1. Cancellazione logica: eliminazione di un documento versato in conservazione per errore materiale, gestita in autonomia solo dal Soggetto Produttore (attraverso apposite chiamate WS), per cui il documento cancellato è ancora consultabile dall'Utente (compare con lo 'stato': 'cancellato'), in ossequio al principio di tracciabilità informatica.

2. Cancellazione fisica o scarto archivistico: eliminazione vera e propria di un documento o di un pacchetto di archiviazione e di qualsiasi duplicato prodotto durante le attività di conservazione, sia dal punto di vista logico che dal punto di vista fisico, per cessata rilevanza ai fini amministrativi, legali o di ricerca storica, ai sensi del Codice Privacy, del GDPR e del Codice dei beni culturali. Questa attività è espressamente richiesta a InfoCert dal Soggetto Produttore, mediante apposita lista debitamente firmata (anche attraverso apposite chiamate WS).

Per gli enti pubblici e per gli archivi privati dichiarati di notevole interesse storico, le proposte di scarto sono sottoposte a nulla osta delle soprintendenze archivistiche o delle commissioni di sorveglianza di competenza. La stesura di 'Piani di Conservazione' (detti anche 'Massimari di selezione e scarto'), la selezione dei documenti da scartare e la procedura di sdemanializzazione e approvazione ministeriale sono in capo al Soggetto Produttore, che può avvalersi del supporto della Digital Consulting di InfoCert.

La distruzione degli eventuali supporti ottici rimovibili di back-up è effettuata mediante strumentazione adeguata e seguendo le procedure definite per lo smaltimento dei rifiuti prodotti.

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

Il Responsabile del servizio della Conservazione mantiene traccia delle richieste di scarto ricevute e correttamente eseguite, e vengono redatti Attestati di scarto firmati digitalmente dal Responsabile del servizio.

Per ulteriori dettagli si rimanda all'apposito documento interno 'Procedura di hand-over tra conservatori e scarto archivistico in LegalDoc'.

Torna al sommario

7.9 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori

Nel caso il Soggetto Produttore decida di rescindere o interrompere il contratto di affidamento del servizio di conservazione, il Responsabile del servizio della Conservazione provvede a comunicare al Soggetto Produttore la lista dei pacchetti di archiviazione conservati.

Il soggetto produttore può effettuare il download dei propri Pacchetti di Distribuzione in autonomia, attraverso la procedura di esibizione, o richiedendo il servizio di restituzione al proprio commerciale di riferimento (su supporto da concordare in base a volume ed esigenze).

Se i supporti sono removibili, i documenti contenuti sono criptati e compressi con password apposita e non devono contenere nel dorso o nella custodia nessun riferimento al soggetto produttore o al contenuto.

Il soggetto produttore provvederà a inviare anche copia della liberatoria denominata 'MODULO DI RESTITUZIONE DATI – SERVIZIO LEGALDOC' sottoscritta digitalmente dal Responsabile della Conservazione interno. Al termine della procedura di hand over verso il nuovo Conservatore per rescissione o risoluzione del contratto di servizio, i pacchetti conservati verranno cancellati da LegalDoc.

Insieme ai veri e propri documenti conservati, sono rese disponibili anche le informazioni e i documenti a corredo della corretta conservazione.

Gli archivi di conservazione generati dal sistema InfoCert sono conformi allo standard di interoperabilità UNI SInCRO: l'interrogazione di tali archivi restituisce le informazioni secondo il suddetto standard.

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

L’adozione di tale standard permette l’interoperabilità e la trasferibilità dei dati in modo semplificato.

Per ulteriori dettagli si rimanda all’apposito documento interno ‘Procedura di hand-over tra conservatori e scarto archivistico in LegalDoc’.

Torna al sommario

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

8. IL SISTEMA DI CONSERVAZIONE

La descrizione dell'architettura generale del sistema di conservazione è stata depositata in AgID in fase di accreditamento.

Il sistema è organizzato su più siti (Padova, Modena, Milano).

Il sistema di conservazione è implementato da un'applicazione software appositamente sviluppata a tale scopo (applicazione Java in architettura distribuita, ossia costituita da molteplici componenti) e da una serie di servizi di interesse generalizzato condivisi con altre applicazioni (marca temporale, HSM, supporti di conservazione, PEC).

Il sistema è reso in modalità SaaS (Softwareas a Service) e consente al Soggetto Produttore di accedere ai sistemi di conservazione dei documenti informatici su un elaboratore elettronico, gestito da InfoCert e fisicamente posto nei locali di quest'ultima, in conformità a quanto descritto nei documenti delle 'Specificità del Contratto'.

Il sistema è accessibile dalla apposita URL di rete e il Soggetto Produttore richiama il sistema di conservazione secondo le modalità concordate.

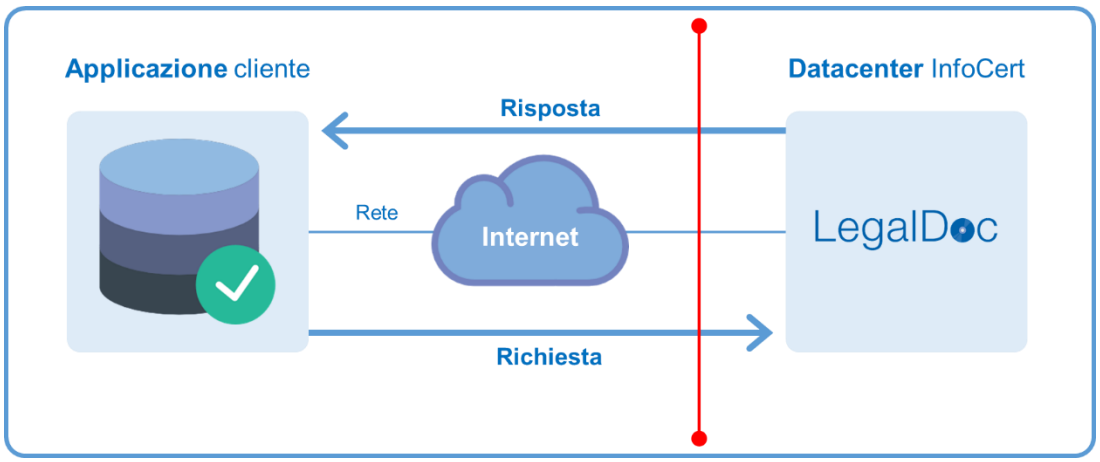


Figura 1 Rappresentazione del servizio attraverso la rete

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

Dal punto di vista architetturale LegalDoc è realizzato utilizzando la tecnologia dei Web Services.

I Web Services di LegalDoc sono implementati secondo architettura REST su protocollo HTTPS.

LegalDoc è dotato anche di un'interfaccia (LegalDoc WEB) utilizzata sia per il versamento manuale di alcune tipologie documentali, sia per la ricerca e l'esibizione a norma di documenti conservati.

L'esibitore è un'applicazione in tecnologia web, che permette ad un utente, precedentemente definito e in possesso delle debite autorizzazioni e credenziali, di accedere al sistema di conservazione LegalDoc da un qualsiasi computer, purché collegata in rete.

Attraverso l'esibizione a norma diventa possibile:

- estrarre un documento e visualizzarlo a video;
- produrre copia cartacea o su altro supporto informatico del documento;
- estrarre i visualizzatori memorizzati nel sistema di conservazione permettendone l'installazione sulla stazione dove si sta svolgendo l'esibizione;
- prendere visione dei file a corredo che formano il pacchetto di distribuzione e che qualificano il processo di conservazione attestandone il corretto svolgimento (Indice di Conservazione UNI SINCRO, altrimenti detto Indice del Pacchetto di Archiviazione, File di parametri, File di indici, File di dati, Attestato di conservazione);
- verificare la validità delle firme digitali e delle marche temporali apposte nel processo di conservazione;
- verificare l'integrità del documento.

Il sistema è protetto da firewall ed implementa un sistema di back-up dei dati memorizzati.

Torna al sommario

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

8.1 Componenti Logiche

Il servizio LegalDoc è basato su tecnologia REST e svolge le operazioni di conservazione, esibizione, rettifica, cancellazione e ricerca.

Torna al sommario

8.2 Componenti Tecnologiche

8.2.1 Firewall

I firewall assicurano la difesa del perimetro di sicurezza tra il sistema e il mondo esterno, nonché tra i sistemi dedicati all'erogazione del sistema e i sistemi che interfacciano i dispositivi sicuri per la generazione della firma digitale.

I firewall sono configurati in alta affidabilità e costantemente aggiornati per assicurare i massimi livelli di protezione possibile.

Torna al sommario

8.2.2 Back-up

L'intero sistema di conservazione viene interessato periodicamente da processi di back-up completo dei documenti, delle evidenze qualificanti il processo, dei database di gestione del sistema e di ogni altra informazione necessaria per la sicurezza.

Torna al sommario

8.2.1 Dispositivo HSM di firma digitale dei pacchetti

Al buon esito del processo di conservazione, il Responsabile del servizio della Conservazione di InfoCert appone la propria firma digitale su ogni pacchetto di archiviazione, mediante un sistema di firma digitale automatica erogato dalla Certification Authority InfoCert, che si avvale di un dispositivo crittografico ad altre prestazioni Hardware Security Module e di un certificato qualificato di firma appositamente generato e su cui ha pieno controllo.

Torna al sommario

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

8.2.2 Servizio di marcatura temporale dei pacchetti

Per l'emissione delle marche temporali il sistema si avvale del servizio di marcatura di InfoCert, Certification Authority accreditata, compliant eIDAS. La marca temporale viene richiesta al TSS (Time Stamping Service) che la restituisce firmata con un certificato emesso dalla TSA (Time Stamping Authority) di InfoCert. Il root-certificate della TSA è depositato presso AgID. Il TSS è sincronizzato via radio con l'I.N.RI.M di Torino (Istituto Nazionale di Ricerca Metrologica, già Istituto Elettrotecnico Nazionale "Galileo Ferraris") ed è protetto contro la manomissione della sincronizzazione mediante misure fisiche e logiche, nel pieno rispetto delle norme di legge.

Torna al sommario

8.3 Componenti Fisiche

InfoCert, in accordo con i Soggetti Produttori e come previsto dalle Condizioni Generali del Contratto si avvale di partner tecnologici per le componenti fisiche del data center.

Torna al sommario

8.3.1 Sistema Storage

Il sistema di conservazione di InfoCert e dei suoi partner tecnologici supporta la memorizzazione dei file sia su storage magnetici ad alte performance che su sistema *Object Storage S3*. Tali storage, scelti tra i primari fornitori di tecnologie presenti sul mercato, garantiscono adeguati requisiti di affidabilità e di ridondanza interna del dato e rispondono all'esigenza di memorizzazione a lungo termine dei *fixed content*, ossia dei file che devono essere conservati con garanzia nel tempo di integrità e disponibilità del contenuto.

Per garantire la riservatezza vengono applicate appropriate politiche sulle autorizzazioni che prevedano la cifratura dei documenti che contengono dati sensibili ed eventualmente anche degli altri.

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

I sistemi di storage sono stati valutati da InfoCert e dai suoi partner tecnologici sotto molteplici profili e, in virtù delle loro caratteristiche fisiche e architetturali, sono ritenuti idonei ad essere utilizzati nel sistema di conservazione.

Nell'ambito del sistema di conservazione, lo storage magnetico ad alte performance rappresenta sia il supporto primario di conservazione posto fisicamente presso la sede InfoCert di Padova, sia il supporto secondario posto nel sito di *disaster recovery* di Modena.

I due sistemi sono interconnessi mediante collegamenti ad alta velocità dedicati, completamente ridondati e protetti da misure di sicurezza. I collegamenti consentono la replicazione dei dati conservati eliminando il rischio di distruzione di tutte le copie delle informazioni in caso di danno irreparabile a livello di sito.

Questo secondo sistema funge anche da copia di sicurezza.

L'allineamento tra il sito primario e il sito secondario avviene coerentemente con le politiche generali di *Disaster Recovery* definite in InfoCert che garantiscono RTO e RPO inferiori alle 48 ore.

Per il sistema di *Object Storage S3* InfoCert si avvale dei servizi cloud computing *Amazon Web Services (AWS)* che garantisce la ridondanza e il rispetto delle misure di sicurezza.

Torna al sommario

8.3.2 Sincronizzazione dei sistemi

Tutti i server di InfoCert, attraverso il protocollo NTP (Network Time Protocol), sono sincronizzati sul “tempo campione” fornito dall’Istituto di Ricerca Metrologica – INRIM (già Istituto Elettrotecnico Nazionale “Galileo Ferraris”), abilitato a fornire il “tempo campione” ai sensi dell’articolo 2, comma 2, lettera b) del D.M. 30 novembre 1993, n. 591 “Regolamento concernente la determinazione dei campioni nazionali di talune unità di misura del Sistema internazionale (SI) in attuazione dell’art. 3 della L. 11 agosto 1991, n.273. La sincronizzazione è protetta da misure di sicurezza fisiche e logiche documentate per impedirne la manomissione.

Il meccanismo di allineamento temporale tra i sistemi fornisce la certezza della successione temporale degli avvenimenti nel sistema. La sincronizzazione delle macchine

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

infatti, genera dei file di log temporalmente omogenei tra loro, che permettono di ricostruire con certezza l'ordine di accadimento degli eventi intervenuti a tutti i livelli del sistema, e di individuare la sequenza di svolgimento delle varie operazioni.

Torna al sommario

8.4 Procedure di gestione e di evoluzione

Il sistema di conservazione di InfoCert e il processo da questi implementato rispondono interamente alle norme di legge che regolano la materia.

La progettazione e il continuo miglioramento del sistema di conservazione sono il frutto di una intensa opera di confronto tra le professionalità e le competenze delle diverse funzioni aziendali, al fine di giungere all'erogazione di un sistema pienamente conforme alle norme, architetturalmente stabile, affidabile, e che garantisca elevati livelli di servizio all'utente in condizioni di assoluta sicurezza, certezza degli accessi e tracciabilità delle operazioni.

Punto fondante del processo di progettazione è l'attenta disamina delle norme, al fine di definire puntualmente i requisiti legali che il sistema deve possedere per assicurare la corretta implementazione della conservazione.

Il rispetto dei requisiti di legge è la condizione imprescindibile per l'erogazione del servizio. Oltre a questi sono definiti ulteriori requisiti funzionali, di architettura e di connettività e interoperabilità. I requisiti funzionali, individuati dal gruppo di competenza, rispondono all'obiettivo di offrire al Soggetto Produttore le funzionalità da questi richieste, mentre i requisiti di architettura e di interoperabilità rispondono alla necessità di sviluppare e mantenere un sistema stabile, in linea con le evoluzioni tecnologiche e capace di interfacciarsi con gli altri sistemi sviluppati dall'azienda, sfruttando le economie di scala e di conoscenza.

I Responsabili InfoCert, infatti, sono costantemente impegnati nell'attività di 'technology watch' attraverso la partecipazione a gruppi di lavoro nazionali e internazionali, forum e associazioni di settore con lo scopo di monitorare e prevenire l'obsolescenza tecnologica sia logica che fisica.

Torna al sommario

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

8.4.1 Criteri di organizzazione del contenuto

Gli oggetti della conservazione sono trattati dal sistema di conservazione in pacchetti informativi in cui i documenti sono corredati da tutta una serie di metadati. I documenti inviati al sistema di conservazione, infatti, vengono aggregati secondo criteri di omogeneità secondo le informazioni di configurazione definite in fase contrattuale. In particolare, vengono concordati i parametri fondamentali (bucket, policy, classi documentali) con i quali sono organizzati i documenti presi in carico, per consentire la maggiore interoperabilità possibile tra i sistemi di conservazione.

Se le tipologie documentali conservate sono di tipo sanitario (es. referti, immagini diagnostiche, ecc..) si provvede alla conservazione in ambienti separati e cripatati, in ottemperanza della normativa sulla privacy e sulla data protection.

Torna al sommario

8.4.2 Organizzazione dei supporti

Come atto conclusivo della procedura di conservazione, i documenti vengono memorizzati nel sistema di storage, contenenti tutti i documenti inviati in conservazione e i relativi file IPdA in conformità alle Regole AgID, OAIS e UNI SInCRO.

Torna al sommario

8.4.3 Archivio dei viewer consegnati dal Soggetto Produttore

InfoCert ha stabilito dei formati standard per i documenti da inviare in conservazione, dettagliati nei 'Dati Tecnici di attivazione' a disposizione del Soggetto Produttore e nel DPCM del 3 dicembre 2013, per i quali l'azienda definisce e mette a disposizione dei Soggetti Produttori i relativi viewer, mantenendoli aggiornati. Al momento dell'attivazione del servizio, il Soggetto Produttore verifica che i documenti inviati siano nel formato standard e siano leggibili con il software definito da InfoCert.

Se un Soggetto Produttore ha l'esigenza di inviare in conservazione documenti in formati differenti da quelli definiti standard, provvede a fornire ad InfoCert, tramite apposita funzionalità dell'applicativo dell'interfaccia di LegalDoc, il relativo software di visualizzazione.

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

Se il Soggetto Produttore invia documenti in formato non standard senza depositare il relativo visualizzatore, oppure nel caso di invio di documenti in modalità cifrata, è sua cura la conservazione degli strumenti necessari per la decifratura e/o la visualizzazione di quanto conservato.

Il Responsabile del servizio della Conservazione mantiene i programmi consegnati in un apposito database sottoposto a un periodico processo di back-up; in questo processo, il Responsabile è supportato dalle apposite procedure automatiche del sistema.

Torna al sommario

8.4.4 Archivio dell'hardware e del software obsoleto

La tenuta di un archivio dell'hardware e dei sistemi operativi ormai obsoleti ma necessari alla visualizzazione dei documenti conservati non è esplicitamente prevista dalla norma, ma è un'attività che si desume dall'obbligo di tenuta dell'archivio dei software nelle eventuali diverse versioni, e a questo direttamente correlata e fa parte delle misure per combattere l'obsolescenza dei formati, citate all'art. 7 comma 1 lettera g) dal Decreto 2013.

Il progresso tecnologico dei sistemi, tuttavia, può portare all'impossibilità di utilizzare i viewer definiti dal Soggetto Produttore, se divenuti obsoleti, sulle macchine di ultima generazione, rendendo di fatto impossibile la presa di conoscenza del contenuto del documento e inficiandone così la validità legale nel tempo. Per far fronte a questo rischio, il Responsabile del servizio della Conservazione mantiene un archivio di tutte le componenti hardware e software non più compatibili con i programmi di visualizzazione garantiti e/o depositati dal Soggetto Produttore, nel caso questi siano i soli strumenti che consentono di rendere leggibile i documenti conservati associati a tale viewer.

Torna al sommario

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

9. MONITORAGGIO E CONTROLLI

InfoCert possiede un sistema di gestione integrato che risponde attualmente ai requisiti delle norme ISO 9001, 27001, 20000 e 14001.

È inoltre un Qualified Trust Service Provider (ETSI EN 319 401) per i servizi di certificazione qualificata di: firme elettroniche, sigilli elettronici, validazione temporale e autenticazione siti web.

Particolare attenzione viene quindi posta nel mantenimento di livelli di servizio. attraverso l'dozione di un modello di Service Management System conforme alla citata norma ISO/IEC 20000 ha permesso infatti di:

- mappare ed integrare i Livelli di Servizio (SLA) garantiti ai clienti in relazione ai Livelli di servizio operativi garantiti internamente e quelli contrattuali garantiti dai fornitori;
- strutturare e governare la catena di composizione del valore dei servizi;
- ottimizzare la gestione dei processi aziendali integrando processi produttivi con processi di business fornendo un modello per la gestione sui servizi erogati;
- facilitare l'allineamento tra i requisiti del cliente e l'offerta InfoCert impostando/definendo accordi di servizio formalizzati e misurabili (SLA) e garantiti;
- garantire un controllo dei fornitori che concorrono alla erogazione dei nostri servizi;
- migliorare la qualità dei servizi di business erogati.

Di seguito lo schema rappresentativo del Modello adottato da InfoCert:

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

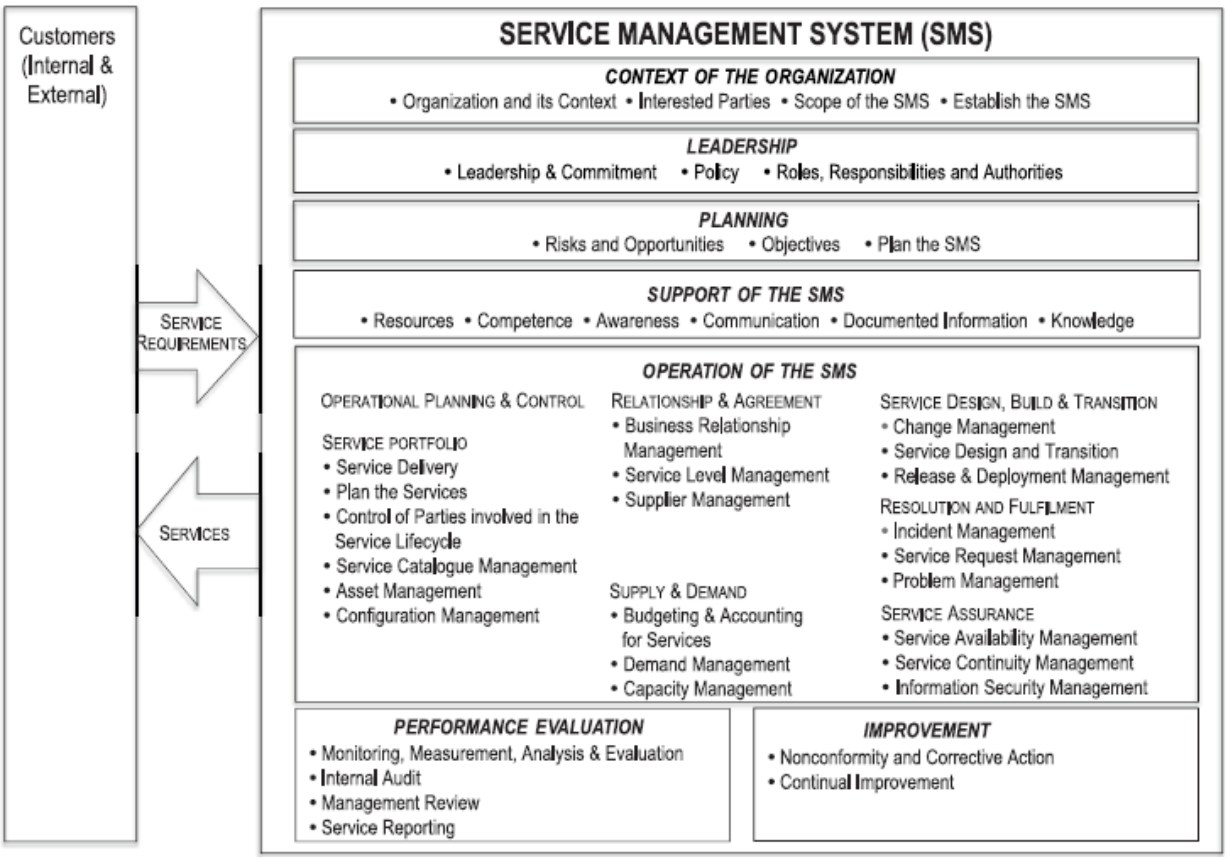


Figura 2 Rappresentazione grafica processi della norma ISO/IEC 20000:11

Le attività di istituzione, attuazione, monitoraggio e sviluppo del Service Management System-SMS seguono il modello ciclico PDCA che si sviluppa nelle seguenti fasi:

- istituzione del sistema - SMS (Plan) in cui si definiscono e si pianificano le politiche e i requisiti per la gestione dei servizi inerenti il campo di applicazione; si stabiliscono gli obiettivi di gestione del servizio a tutti i livelli pertinenti.
- implementazione ed attuazione del sistema-SMS (Do) e dei processi di design, transition, delivery e improvement continuo dei servizi sulla base di quanto definito nel

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

service management plan, con particolare attenzione al controllo delle modifiche al SMS valutando e limitando I rischi.

- azioni di monitoraggio e revisione del sistema-SMS (Check);
- attuazione di misure a miglioramento del sistema-SMS (Act) ove sono pianificate e attuate idonee azioni correttive sulla base dei risultati della fase precedente.

Il processo di gestione dei Livelli di Servizio [Service Level Management] è considerato un processo cardine del Service Management System in quanto ha effetto sui tre obiettivi principali quali:

- allineare i servizi di business con i bisogni correnti e futuri del cliente
- coordinare i requisiti del mercato sui servizi offerti con gli obbiettivi aziendali
- migliorare la qualità dei servizi di business erogati
- fornire attraverso gli SLA una base per la determinazione del valore del servizio.

Nello specifico InfoCert ha definito degli SLA baseline di riferimento in relazione ai seguenti KPI (Key Performance Indicator):

- Orario di servizio
- Disponibilità di servizio.

Torna al sommario

9.1 Procedure di monitoraggio

La soluzione di monitoraggio, nel seguito denominata TMS, è fornita dal Gruppo Sintesi che si occupa della completa gestione di tutta la piattaforma.

TMS si occupa di monitorare e misurare tutto lo stack tecnologico usato per erogare i servizi InfoCert, infatti non è solo in grado di dire se un servizio o un particolare componente hardware stanno funzionando correttamente, ma è anche in grado di misurarne le risorse utilizzate e le performance.

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

La piattaforma è costruita a partire da una versione customizzata del noto software open source Nagios e per rilevare i dati dai diversi componenti utilizza diverse tecnologie (SNMP, NRPE, Sahi, ecc.), inoltre, è stata sviluppata l'integrazione con la piattaforma di controllo *Cloudwatch*, tool nativo di AWS consente di avere il pieno controllo e la gestione delle metriche di tutte le componenti presenti in cloud I monitoraggi possono essere eseguiti in modalità attiva (quindi la piattaforma interroga puntualmente le diverse componenti) oppure in modalità passiva (ovvero sono le singole componenti che inviano dati alla piattaforma, senza il bisogno di venire interrogate da essa).

L'infrastruttura di monitoraggio, ad oggi, è composta da:

- due apparati fisici (denominati probe) posizionati all'interno del Data Center,
- una probe posizionata all'interno dei locali della CA,
- un'altra probe posizionata nel sito di DR.

Alle quattro probe fisiche si aggiunge un pool di macchine virtuali posizionate nella server farm di *Clouditalia* e la piattaforma *Cloudwatch* posizionata in AWS Le probe fisiche si occupano di effettuare i monitoraggi sull'infrastruttura ed i servizi ospitati nei locali nei quali sono installate mentre le macchine virtuali si occupano di effettuare le navigazioni dei servizi sia da rete interna che tramite internet, *Cloudwatch* invece gestisce i monitoraggi di tutte le metriche infrastrutturali presenti in AWS. Tutti i dati raccolti vengono infine centralizzati su una piattaforma resa disponibile online per una veloce e facile consultazione degli stessi.

Oltre alle misurazioni effettuate sull'infrastruttura e la verifica del traffico dati tra il cloud e il DC, il sistema di monitoraggio è in grado di misurare anche le performance dei servizi, infatti tramite le navigazioni effettuate dalle macchine virtuali si riesce a capire se un servizio è disponibile e anche quanto tempo impiega per effettuare una certa elaborazione.

Con tutti i dati raccolti si popola una base di dati in ottica di Business Intelligence che risulta di fondamentale importanza per la redazione della reportistica riguardante gli SLA dei vari servizi ma anche, e soprattutto, per supportare i processi di decisione aziendale.

La soluzione di monitoraggio fin qui descritta risulta indispensabile per individuare tempestivamente eventuali anomalie sui servizi erogati da InfoCert, ma soprattutto è in grado di segnalarci su quale dei molti componenti che compongono un servizio andare a concentrare l'azione correttiva per una rapida risoluzione degli incident.

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

Torna al sommario

9.1.1 Processi di monitoraggio del sistema di conservazione

Il monitoraggio del sistema di conservazione si esplica su due diversi livelli operativi:

- sistema di monitoring della disponibilità del sistema
- sistema di monitoring dell'integrità degli archivi.

Torna al sommario

9.1.2 Monitoring della disponibilità del sistema

Tale operazione viene svolta coerentemente con le procedure di monitoring generali di InfoCert. In particolare, tutte le componenti costituenti il sistema di conservazione, ovvero i servizi applicativi, i processi di elaborazione batch e le interfacce per l'utente finale sono monitorate con i tool definiti nella piattaforma di monitoraggio TMS precedentemente descritta.

A fronte di anomalie rilevate lo strumento invia delle segnalazioni al Service Desk InfoCert che le gestisce in conformità ai processi di Incident Management e, se necessario, Problem Management. Tali processi sono descritti nelle procedure che definiscono il Sistema di gestione integrato InfoCert.

Torna al sommario

9.2 Verifica dell'integrità degli archivi

Il sistema di memorizzazione utilizzato, grazie alle caratteristiche intrinseche dei supporti, alla configurazione architetturale e alle procedure di memorizzazione permanente dei dati, garantisce l'immodificabilità, l'integrità, la leggibilità e la reperibilità nel sistema di quanto conservato, ai fini della corretta esibizione.

Il sistema mantiene traccia di tutte le operazioni effettuate sui documenti in appositi file di log.

© InfoCert S.p.A. – All right reserved

Firmato digitalmente da ROBERTO FRACCIA

Inoltre, è garantita la tracciatura di tutti i documenti richiamati dal Soggetto Produttore mediante interrogazione al sistema e conseguentemente esibiti, che rappresenta un'ulteriore prova di leggibilità, effettuata direttamente dal Soggetto Produttore.

In aggiunta, come descritto dall'art. 7 comma 1 lettera g) del DPCM del 3 dicembre 2013, "al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati", InfoCert, per rispondere a tali richieste, ha attivato sottosistemi di controllo automatico dedicati alla simulazione della navigazione nel sistema e delle operazioni che effettua l'utente, svolgendo controlli di coerenza dei dati e attività di ripristino da situazioni di errore.

In ogni occasione in cui il file viene copiato o spostato di posizione, funzionalità automatiche verificano che le sue dimensioni non siano mutate durante lo spostamento e che non siano intervenute alterazioni, che possano inficiarne la visualizzazione.

Il Responsabile del servizio della Conservazione, come descritto nell'art. 7 comma 1 lettera f) "assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità" dei documenti conservati con procedure automatiche e manuali, al fine di prevenire il rischio che i documenti non possano essere visualizzabili, inficiando il mantenimento della loro validità legale nel tempo.

L'apposita procedura, detta verificatore, esegue il test di leggibilità binaria mediante il continuo calcolo delle impronte dei documenti conservati, con successivo confronto con l'hash del documento contenuto nel file delle direttive della conservazione inviato dal Soggetto Produttore. Se la procedura non registra differenze tra i due hash, il documento è inalterato rispetto a quanto trasmesso dal Produttore.

Vengono eseguiti i seguenti passi operativi:

- verifica della validità della firma digitale e della marcatura temporale apposte all'atto della conservazione dal Responsabile del servizio della Conservazione sul file IPdA e, se presenti, verifica della firma digitale e della marcatura temporale del documento;
- calcolo dell'impronta del documento e confronto con quella contenuta all'interno del file IPdA;

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

- generazione di un report che viene automaticamente sottoposto alla conservazione nell'area dedicata al Responsabile del servizio della Conservazione (quindi a sua volta firmato e marcato temporalmente dal Responsabile del servizio della Conservazione stesso).

La procedura appena descritta viene applicata sia sul supporto primario sia su quello secondario.

In caso di anomalie, se il documento risulta corrotto in uno dei due repository, il sistema tenta il ripristino automatico con il dato presente nel repository integro. Se invece ambedue le copie sono alterate, viene inviato un alert al Responsabile del servizio della Conservazione, che tenterà il ripristino manuale partendo da un'altra sorgente (per esempio le copie di backup). Se nessuna sorgente è disponibile viene redatto un verbale di incidente, sottoscritto e conservato dal Responsabile del servizio della Conservazione per attestare la situazione rilevata. Analoga procedura viene applicata in caso di perdita di tutte le copie del dato.

Periodicamente, il sistema produce dei report di sintesi dell'attività di verifica svolta.

In aggiunta alla verifica automatica dell'integrità binaria, il Responsabile del servizio della Conservazione e i suoi Responsabili incaricati sono dotati di apposita strumentazione (detta CORE, Console del Responsabile), con credenziali dedicate, con la quale procedono manualmente e periodicamente ad una verifica campionaria di leggibilità dell'archivio documentale conservato, scegliendo ed esibendo casualmente un campione di documenti presenti nel sistema di conservazione.

Viene poi redatto automaticamente un verbale che attesta l'elenco dei documenti visualizzati, successivamente sottoscritto e conservato dal Responsabile del servizio della Conservazione nell'area appositamente creata nel sistema di conservazione.

9.3 Controlli

Oltre ai monitoraggi appena descritti, il sistema di conservazione implementa numerosi sotto-processi dediti al controllo del corretto svolgimento dei processi, segnalando eventuali errori o anomalie al Soggetto Produttore o al personale incaricato dell'amministratore del sistema.

I controlli effettuati si distinguono nelle tre tipologie: controlli di versamento, controlli di

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

processo e controlli periodici.

Torna al sommario

9.3.1 Controlli di versamento

In fase di versamento dei pacchetti in LegalDoc vengono automaticamente eseguiti dei controlli, preventivamente concordati con il soggetto Produttore nelle 'Specificità del contratto' all'attivazione del servizio e che riguardano:

- abilitazione utenza al versamento;
- validità sessione in uso (di default della durata di un'ora tra login e logout);
- struttura del file di Parametri (contenente le informazioni per la leggibilità nel tempo del documento da conservare);
- struttura del file di Indici (contente i metadati del documento da conservare, alcuni dei quali obbligatori, in coerenza con i 'Dati Tecnici di attivazione');
- mime type dichiarato in coerenza con i 'Dati Tecnici di attivazione';
- dimensione massima del documento da conservare (di default 256 megabyte, variabile su richiesta);
- presenza nello stesso path dello stesso nome-file (su richiesta);
- validità del certificato qualificato di firma digitale con cui è sottoscritto il documento da conservare (su richiesta).

InfoCert non effettua controlli sull'eventuale presenza di virus nei pacchetti di versamento, che sono conservati in LegalDoc alla stregua di tutti gli altri file.

Torna al sommario

9.3.2 Controlli di processo di progettazione e sviluppo dei servizi

L'organizzazione garantisce che non vengano rilasciati prodotti/servizi per i quali non siano state completate le attività di controllo della qualità citate nelle relative procedure di rilascio.

Per maggiori dettagli si rimanda a "PR/235 Progettare e sviluppare un servizio informatico InfoCert", "PR/225- Change Management InfoCert", "Service Management System-SMS".

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

Torna al sommario

9.3.3 Monitoraggio e registrazioni durante il ciclo produttivo

Lungo l'intero ciclo produttivo si effettuano i controlli al fine di verificare la conformità del prodotto e del processo a quanto previsto dalle procedure applicabili.

Nelle procedure “PR/235 Progettare e sviluppare un servizio informatico InfoCert” e “PR/225- Change Management InfoCert” sono indicate le fasi specifiche per i controlli, i test e le misurazioni del prodotto/servizio in termini di ciclo di vita, tecniche, metriche del SW, gestione dei controlli, dello “sforzo/effort”, tenuta in controllo dei costi e dei tempi di realizzazione, la definizione dei mezzi e delle risorse necessarie.

Il prodotto/servizio è oggetto di un processo progressivo di accettazione: le registrazioni documentano la conformità del prodotto ai criteri di accettazione e indicano la persona che autorizza il rilascio.

Il prodotto/servizio è predisposto per la consegna al cliente ad esito positivo delle prove, controlli e collaudi. I prodotti che non superano le prove, i controlli e i collaudi sono sottoposti alla procedura per il trattamento dei prodotti non conformi.

Torna al sommario

9.3.4 Monitoraggio e registrazioni per collaudo finale

Il prodotto/servizio corrispondente ai requisiti contrattuali è oggetto di un processo progressivo di accettazione che viene attivato in occasione di ogni consegna ufficiale al Produttore, o di una accettazione globale fatta alla fine del processo produttivo secondo quanto previsto dalla procedura.

Torna al sommario

9.3.5 Controlli periodici

In InfoCert è attiva una struttura appositamente preposta alla supervisione e controllo della gestione dei problemi e del rispetto dei livelli del sistema per tutte le applicazioni.

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

La struttura si avvale di un gruppo di lavoro trasversale all'azienda ed effettua la raccolta dei dati relativi al funzionamento dei servizi.

Il gruppo si riunisce con una periodicità mensile al fine di individuare le cause dei malfunzionamenti registrati nel periodo, analizzare le soluzioni contingenti adottate per il superamento del problema e sviluppare eventuali proposte per rimedi strutturali.

Torna al sommario

9.4 Soluzioni adottate in caso di anomalie

Ad ogni semestre il Responsabile del servizio della Conservazione effettua un riesame generale del sistema insieme ai soggetti incaricati, al fine di accertare la conformità del sistema al livello atteso, analizzare le cause di eventuali incidenti o disservizi e promuovere attività di prevenzione o miglioramento.

Qualora necessario, una riunione di riesame può essere indetta a fronte di particolari eventi (ad esempio, a titolo non esaustivo, cambi tecnologici, normativi o di requisiti funzionali, stagionalità di carico elaborativo, arrivo consistente e non pianificato di nuova clientela, ecc.).

Torna al sommario

9.4.1 Auditing generale del sistema

Il Programma di AUDIT aziendale è attuato secondo le procedure del Sistema Integrato di Gestione.

Gli Audit sono condotti, sempre secondo le citate procedure, con il fine di determinare se i processi aziendali:

- sono in accordo con quanto previsto nei documenti di riferimento
- sono compliant alla normativa di riferimento
- sono compliant agli standard adottati dal sistema di conservazione
- sono attuati efficacemente
- sono idonei al conseguimento degli obiettivi della Qualità e miglioramento servizi

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

In ogni processo aziendale, le modalità di audit sono improntate alle indicazioni dello standard UNI EN ISO 19011 ed hanno per oggetto:

- strutture organizzative
- risorse utilizzate
- procedure
- processi
- prodotti e i risultati dell'attività
- documentazione
- addestramento
- segnalazioni dei clienti e terze parti.

Le attività di audit sono in capo all'Area Management System che le esegue direttamente o le delega a personale esterno qualificato.

Oltre alle verifiche ispettive sopra descritte indirizzate al Sistema Gestione Qualità, sono pianificati e condotti audit su tutti gli altri componenti del Sistema di Gestione Integrato (SGSI-ISO 27001, SMS-ISO 20000, SGA-ISO14001, Verifiche di interoperabilità condotte da AgID, Privacy, Sicurezza Fisica, M231/01 ecc.).

Relativamente al SGA-ISO14001 l'attività di audit comprende anche la verifica di conformità legislativa.

Relativamente al SGA-ISO14001 l'attività di audit comprende anche la verifica di conformità legislativa.

Il processo prevede inoltre la gestione controllata di tutti gli Audit esterni svolti dagli Enti istituzionali, relativi ai Sistemi di Gestione ed ai Prodotti/Servizi certificati.

A fronte di non conformità rilevate in sede di verifica ispettiva, il Responsabile della Struttura Organizzativa valutata definisce un piano di attuazione delle azioni correttive o migliorative richieste.

Il Responsabile delle verifiche e ispezioni (auditing) pianifica e implementa processi di audit che coinvolgono aspetti di processo, organizzazione, tecnologici e logistici. L'obiettivo è accertare la conformità del sistema alle leggi, ai regolamenti, al contratto, alla

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

documentazione generale del sistema, ai principi che ispirano il sistema qualità e al presente Manuale della Conservazione.

L'audit è un processo fondamentale per lo screening del sistema, in quanto consente l'individuazione delle aree critiche d'intervento e la pianificazione dei necessari interventi sul sistema, ragion per cui è svolto periodicamente.

Torna al sommario

9.4.2 Incident management

L'ambito completo del processo si applica alla gestione degli incidenti informatici che possono interessare uno o più servizi tecnologici eventualmente interconnessi ed è formalmente descritto dalla procedura 'PR455-Incident Management InfoCert'. La procedura definisce anche la metodologia di assegnazione della gravità di un incidente e della relativa priorità di gestione in base alla matrice di analisi di impatto/urgenza effettuata utilizzando le informazioni sul servizio di riferimento e sui relativi SLA del servizio o nelle istruzioni /policy specifiche relative alla sicurezza informatica.

Urgenza ⇨ Impatto⇩	ALTA	MEDIA	BASSA
ALTO	Critica	Alta	Media
MEDIO	Alta	Media	Bassa
BASSO	Media	Bassa	Molto bassa

L'impatto è definito in base alla BIA [Business Impact Analisys] del servizio.

L'urgenza è dettata dallo SLA di disponibilità del servizio.

Il processo di gestione degli incidenti, condotto secondo le raccomandazioni delle Best Practice ITIL e in conformità alle norme ISO 27001, si focalizza sulle modalità di gestione e di ripristino tempestivo degli incidenti informatici.

Il modello organizzativo prevede che il supporto specialistico sistemistico sia gestito dall'area di Product Factory che gestisce il ciclo di vita dell'incidente con gli strumenti per la rilevazione e tracciamento degli eventi.

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

Il processo d'Incident Management, che ha lo scopo di minimizzare impatti e tempi di disservizio, alimenta il processo di Problem Management (PR456), che a sua volta ha lo scopo di prevenire il verificarsi e il ripetersi di tali errori.

A tale scopo il Problem Management cerca di individuare la causa principale degli incidenti e ne attua le opportune azioni preventive, correttive e/o migliorative.

I processi di Incident Management e Problem Management sono soggetti a un miglioramento continuativo.

Il Responsabile del servizio della Conservazione mantiene il verbale degli incidenti e delle contromisure attuate sono inviate al sistema di conservazione.

Torna al sommario

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

10. SPECIFICITÀ DEL CONTRATTO

I servizi sono regolati dai seguenti documenti contrattuali, che contengono e descrivono tutte le esigenze richieste dai Soggetti Produttori.

La documentazione contrattuale e tecnica elencata è resa disponibile all'atto del perfezionamento dell'accordo di servizio al Produttore.

1. ***Condizioni Generali di Contratto*** che regola la vendita del servizio di conservazione nelle diverse modalità di erogazione;
2. ***Richiesta di attivazione*** che comporta l'adesione al servizio e disciplina le condizioni economiche;
3. ***Dati tecnici per l'attivazione*** con cui il Soggetto Produttore fornisce tutte le informazioni necessarie su tipologie documentali, metadati e credenziali di accesso di cui necessita;
4. ***File di configurazione*** redatto da InfoCert all'attivazione del servizio, contiene i dati di configurazione del soggetto produttore, delle user d'accesso, delle policy associate e delle tipologie documentali, comprensivi di metadati e formati configurati;
5. ***Atto di affidamento*** che rappresenta la formalizzazione dell'affidamento ad InfoCert del processo di conservazione, la nomina del Responsabile del trattamento dei dati personali ai sensi del Regolamento UE n. 679/2016 GDPR, e stabilisce espressamente quali attività di fatto vengano assunte da InfoCert e quali, al contrario, rimangano a carico dell'affidatario, Soggetto Produttore, come stabilito dagli articoli 5 e 6 del DPCM del 3 dicembre 2013;
6. ***Specifiche Tecniche di integrazione (sia per i web services che per LegalDoc Connector)*** che fornisce tutte le informazioni tecniche necessarie ad operare l'integrazione tra i Sistemi di Gestione documentali del Produttore e il sistema di conservazione di InfoCert;
7. ***Impegno alla riservatezza***;
8. ***Allegato Tecnico*** che descrive le modalità di fornitura del servizio e l'infrastruttura tecnico-tecnologica utilizzata per la sua erogazione;

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

9. ***Manuale Utente*** che risponde alla necessità di documentare operativamente il processo dal punto di vista del Produttore/Utente;
10. ***Descrizione dei codici di errore*** per fornire una casistica esaustiva dei possibili messaggi di errore del servizio di conservazione e delle azioni che è necessario intraprendere per porvi rimedio.

La documentazione relativa alle procedure e/o ai processi interni di InfoCert, invece, è resa disponibile solo su esplicita richiesta del Soggetto Produttore e all'atto del perfezionamento di una specifica NDA (non-disclosure agreement).

Per i Soggetti Produttori con una infrastruttura tecnologica complessa viene redatto un '**Manuale dei processi per la conservazione**', che rimanda al presente Manuale per quanto riguarda le sezioni standard (es. Struttura organizzativa e Ruoli di responsabilità del Conservatore, Dettaglio tecnico del sistema di conservazione e trattazione dei pacchetti di archiviazione, Monitoraggio e controlli del Conservatore), e dettaglia le specificità del singolo Produttore (es. modalità di versamento o esibizione, tipologie documentali, metadati scelti, infrastrutture tecnologiche particolari).

Torna al sommario

Firmato digitalmente da ROBERTO FRACCIA

© InfoCert S.p.A. – All right reserved

AGID | Agenzia per l'Italia Digitale

Formati di file e riversamento

Allegato 2 al documento *"Linee Guida sulla formazione, gestione e conservazione dei documenti informatici".*

Firmato digitalmente da ROBERTO FRACCIA

Sommario

Firmato digitalmente da ROBERTO FRACCIA

1 Introduzione

1. Il presente documento fornisce indicazioni iniziali sui formati dei file con cui vengono rappresentati i documenti informatici oggetto delle presenti linee guida. I termini indicati in azzurro, alla prima occorrenza all'interno di questo testo, sono definiti nel Glossario delle presenti Linee guida.
2. I formati descritti sono stati scelti tra quelli che possono maggiormente garantire il principio dell'interoperabilità tra i sistemi di gestione documentale e conservazione e in base alla normativa vigente riguardante specifiche tipologie di documenti. Va tuttavia segnalato che non tutti i formati di file nel presente documento sono leggibili da qualsivoglia elaboratore, a seconda della configurazione degli applicativi installati. Questo perché, nel caso di finalità specifiche e settoriali (come avviene ad esempio per i file multimediali), alcuni formati di file sono utilizzabili solo dopo l'installazione di software applicativi specifici per l'attuazione delle suddette finalità.
3. È bene precisare che, rispettando il principio di interoperabilità e cercando di mitigare il rischio di "obsolescenza tecnologica", i formati consigliati tra quelli elencati elencati –inclusi quelli per finalità specifiche, cfr. §1.2.3– sono quanto più possibile "aperti", liberamente utilizzabili e non coperti da brevetto. Sono inoltre reperibili online diversi software applicativi open-source in grado di leggere tali file. Tra i formati elencati
4. Tra i formati elencati nel presente Allegato, vi sono anche quelli non consigliati per finalità di interoperabilità, archiviazione o conservazione; essi sono presenti nell'elenco perché formati già ampiamente diffusi nella pubblica amministrazione e quindi non ignorabili per quanto riguarda il loro trattamento e il riversamento da questi formati verso formati più interoperabili.
5. Il presente Allegato, per la natura stessa dell'argomento trattato, viene periodicamente aggiornato sulla base dell'evoluzione tecnologica e dell'obsolescenza dei formati e potrà essere pubblicato online sotto forma di Avvisi, ovvero di un registro dei formati sul sito istituzionale dell'Agenzia per l'Italia Digitale[1].

1.1 Definizioni fondamentali

Si faccia riferimento al Glossario delle presenti linee guida per la definizione dei termini non ulteriormente introdotti in questa sezione.

[1] Qui di seguito indicata anche, per brevità, come Agenzia, ovvero come AGID.

Firmato digitalmente da ROBERTO FRACCIA

1.1.1 File, flussi digitali e buste-contenitori

1. Dal punto di vista tecnologico un documento informatico è rappresentato da un file, ovvero da un flusso binario (*stream*); in linea di principio un flusso binario di dimensione finita può essere contenuto in un file. Il parametro progettuale più importante associato a un file è la sua dimensione (espressa in byte o suoi multipli). Per un flusso binario, che invece può non avere una dimensione predeterminata, si parla invece del suo *data-rate* (ovvero *bit-rate*, quando espresso in bit o suoi multipli), cioè la media temporale dei bit contenuti dal flusso nell'arco di un secondo.
2. La capacità di poter produrre, elaborare o trasmettere flussi entro un data-rate massimo attraverso un canale di comunicazione digitale costituisce la banda dell'elaboratore ovvero del canale — in inglese *bandwidth*. In questo capitolo ci interessiamo prevalentemente ai documenti informatici rappresentati mediante file, mentre sarà presa in considerazione la rappresentazione mediante flussi binari nel caso di alcuni file multimediali (cfr. §§2.9–2.12).
3. In alcuni casi il documento informatico è rappresentato da un insieme di file distinti, organizzati in un pacchetto di file, in inglese (*file*) *package*.
4. L'algoritmo che permette di rappresentare un documento informatico mediante un'evidenza quale un file tramite un'operazione di codifica, o *encoding*, definisce dunque il formato del file; l'operazione inversa, per estrapolare dai dati binari di un file –codificato in un dato formato– nel contenuto informativo del documento, è chiamata decodifica (*decoding*). Formati diversi necessitano di codificatori e decodificatori specifici, che in una parola (soprattutto quando entrambi, per un formato specifico, sono implementati da una singola componente applicativa) sono abbreviati in codec.
5. Esistono una moltitudine di formati di file per rappresentare i documenti informatici ma, a seconda del contenuto del documento e delle esigenze specifiche di gestione e conservazione dello stesso, alcuni formati sono più adatti di altri. Alcuni formati possono essere utilizzati per codificare documenti di una sola tipologia (ad es. formati di file per immagini, generalmente, non possono codificare documenti audio); altri formati, invece, vengono usati per una o più finalità di codifica tra le seguenti:

- codificare documenti di tipologie diverse (ad es. sia testi, che immagini, che audio);
- codificare più documenti insieme nel medesimo file (ad es. scopo principale dei formati di archiviazione);
- codificare documenti di una medesima tipologia (ad es. video) usando però algoritmi di codifica diversa.

Firmato digitalmente da ROBERTO FRACCIA

I formati di file che assolvono ad una o più delle suddette funzioni sono chiamati (formati) busta, o (formati) contenitori — in inglese, rispettivamente, (*file*) *wrappers* o *containers*. Le due tipologie di documento si utilizzano prevalentemente formati contenitori sono i documenti che richiedono funzioni crittografiche avanzate (cfr. §2.16) e i file multimediali (immagini, suono, video, cfr. §§2.6–2.12).
6. Alcuni formati contenitori, infine, imbustano al loro interno, in un unico file-busta, pacchetti di più file precostituiti secondo un determinato formato di pacchetto di file. È questo il caso, ad esempio, dei formati OpenDocument e Microsoft® OOXML (cfr. §2.1 e §2.5), ovvero delle immagini virtuali di filesystem (cfr. §2.13).

1.1.2 Filesystem e metadati

1. I file sono solitamente archiviati una base di dati chiamata filesystem, ove i file con maggiore parentela fra loro (altrimenti detta *locality of reference*, ovvero "affinità per referenza") sono collocati nel medesimo nodo dell'albero: la cartella (ovvero *folder* o *directory* in inglese).
2. All'interno di un filesystem, ai file possono essere associate altre informazioni che ne completano l'esistenza all'interno dello stesso, anche se tali informazioni non fanno parte del contenuto binario del file propriamente detto; tali informazioni sono chiamate per questo motivo metadati (in inglese *metadata*) "esterni" del file.
3. Esistono molteplici formati di filesystem, che variano a seconda delle tecnologie di stoccaggio, di specifiche finalità. Alcuni di questi formati sono open-source; altri sono codificati in standard; altri ancora sono protetti da brevetti e/o copyright.
4. I metadati esterni rappresentabili in un dato filesystem possono differire anch'essi –per qualità, numero, sintassi e funzionalità– a seconda del formato di filesystem, ma di solito comprendono almeno:

- il nome del file, cioè una stringa di caratteri (di lunghezza variabile entro un limite massimo finito) che identifica univocamente il file all'interno della medesima cartella. Sussistono limitazioni differenti circa i caratteri ammessi nel nome e la sua lunghezza massima, a seconda dei diversi formati di filesystem considerati;
- la posizione virtuale del file all'interno del filesystem, chiamato "percorso del file" (path) — "locale" in quanto relativo al filesystem che lo ospita;
- la dimensione del file sopra definita, espressa da un numero intero di byte (o suoi multipli);

Firmato digitalmente da ROBERTO FRACCIA

- la data e l'ora relativa all'ultimo istante in cui il sistema informatico che gestisce il filesystem ha rilevato una modifica del file — chiamata "data di modifica" del file.

5. La concatenazione ordinata del percorso di un file e del suo nome prende il nome di percorso completo del file (*pathname*). Invece la parte, opzionale, del nome del file costituita, scorrendo i caratteri del nome da sinistra a destra, a partire dall'ultima occorrenza del carattere punto '.' in poi (codice ASCII $2E_{16}$ in esadecimale) è chiamata –quando esiste– "estensione" del file.
6. A titolo esemplificativo, fanno parte dei metadati esterni di un file anche i seguenti:

- la data e l'ora creazione del file (che, a seconda della tipologia di filesystem può, con diversi gradi di ambiguità, coincidere con il momento di prima comparsa del file sul filesystem specifico, ovvero il momento della creazione del file sul suo filesystem di origine, o altro);
- la data e l'ora relativa al più recente accesso in lettura sul file avvenuto nel filesystem specifico;
- un identificativo più o meno univoco dell'utente informatico che è il proprietario virtuale del file (rispetto agli altri utenti virtuali del sistema) — chiamato l'*owner* del file;
- una serie di attributi che istruiscono i sistemi informativi che gestiscono l'intero filesystem di appartenenza circa la possibilità di autorizzare determinate operazioni sullo specifico file, a seconda sia dell'operazione da compiere che dell'utenza informatica che presenta tale richiesta; per ogni file, tali metadati costituiscono o sono una parte del cosiddetto insieme dei suoi permessi (*permission*s), ovvero una vera e propria lista dei controlli d'accesso (*ACL*);
- un'etichetta che stabilisce il tipo di formato file (o container) impiegato per la codifica del documento; una cui codifica universalmente riconosciuta *MIME type* – cfr. RFC-2046 e RFC-3023).

7. È importante esplicitare che le "date" sopra descritte, pur non assolvono a requisiti di integrità, precisione e immutabilità nel tempo solo per il fatto di rappresentare una data e un'ora in un filesystem, non producendo dunque, a priori, la stessa validità giuridica di marcature temporali elettroniche qualificate ai sensi del Regolamento (UE) Nº 910/2014.
8. Come anticipato in §1.1.1, il documento informatico può essere rappresentato da un insieme di file distinti, organizzati in un pacchetto di file –in inglese (*file*) *package*– ove l'affinità per referenza tra di essi è realizzata, a seconda del formato del pacchetto, mediante *una o più* delle seguenti tecniche:

Firmato digitalmente da ROBERTO FRACCIA

- Parentela stretta dei file all'interno del filesystem realizzata definendo un sottoalbero riservano a contenente l'intero pacchetto. I file del pacchetto sono tutti contenuti nella cartella-radice del pacchetto ovvero in sue sottocartelle e, tipicamente, è escluso da tale sottoalbero qualunque file non appartenente al pacchetto. Esempi di formati che utilizzano questa tecnica sono le firme elettroniche avanzate nel formato ASiC (§2.16), il formato di master interoperabile (IMF), i pacchetti per il cinema digitale (DCP), e i pacchetti XDCAM (per tutti, §2.12).
- Sintassi dei nomi –rigida o parziale– per file ed eventuali sottocartelle costituenti il pacchetto. Formati che utilizzano esclusivamente questa tecnica sono le impronte crittografiche *detached* (§2.16) e i pacchetti video organizzati in sequenze di fotogrammi (quali ad esempio i master per la distribuzione del cinema digitale, DCDM, §2.12).
- Presenza di un "indice di pacchetto", generalmente rappresentato da un file che ha sia un nome che una posizione controllate e che contiene i *pathname* degli altri file costituenti il pacchetto. Tale indice assolve spesso a scopi aggiuntivi, come ad esempio consolidare in un unico punto i metadati esterni del pacchetto o dei singoli file (§1.1.3), che altrimenti potrebbero essere accidentalmente alterati (o persi) spostando il pacchetto da un filesystem ad un altro. In questi casi il file indice prende anche il nome di file-manifesto, ovvero *sidecar file*. Formati che utilizzano esclusivamente questo metodo sono i pacchetti di siti web (indice con nome *non* obbligatorio index.html, §2.2), alcuni tipi di firme elettroniche avanzate ASiC (tramite la cartella-indice META-INF, §2.16), i già menzionati pacchetti IMF e DCP (che utilizzano più di un file con funzioni di indice, §2.12).
- Riferimento mediante identificativi unici (UID) assegnati a ciascun file del pacchetto, quali ad esempio le loro impronte crittografiche. Esempi di formati che utilizzano questo metodo sono le firme elettroniche avanzate CAdES e XAdES *detached* (§2.16), le marche temporali *detached* e i già menzionati pacchetti IMF e DCP.
- Consolidamento di tutti e soli i file del pacchetto in un file-archivio (§2.13). Esempi che utilizzano questo metodo sono i documenti nei formati OpenDocument e Microsoft® OOXML (cfr. §2.1 e §2.5), gli applet Java e i pacchetti applicativi per dispositivi mobili con sistemi operativi Android e iOS® (§2.15), le firme elettroniche ASiC (§2.16) e, in senso lato, i file PDF (versione 1.7 e successive) quando imbustano altri documenti al loro interno sotto forma di "allegati PDF" (§2.1).

9. La tipologia di regole sintattiche che stabilisce come implementare i primi due metodi sopra elencati costituisce la *naming convention* del formato di pacchetto. La sua efficacia è ridotta quando non coadiuvata da ulteriori controlli di integrità del

Firmato digitalmente da ROBERTO FRACCIA

pacchetto, in quanto l'affinità per referenza è generalmente difficile da far rispettare tecnicamente (a meno di usare uno stretto controllo dei permessi di "sola-lettura", ovvero archiviare su dispositivi logicamente immodificabili). Per questo motivo la *naming convention* si affianca spesso ad altri metodi quali quelli ai punti dal 3 al 5 del sopracitato elenco.

1.1.3 Metadati e identificazione del formato

1. Abbiamo già parlato in §1.1.2 dei metadati esterni, che servono a descrivere meglio un file ma sono fortemente dipendenti dal filesystem ove il file è archiviato in un dato momento. Inoltre, tali metadati possono essere soggetti a modifiche che non pregiudicano l'integrità del file stesso.
2. Più importanti ancora sono perciò i cosiddetti metadati "interni" di un file, cioè informazioni descrittive del file che sono codificate nel suo formato stesso. A seconda del formato impiegato, la presenza di questi metadati interni può essere obbligatoria o facoltativa. Facendo parte del contenuto binario di un file, la modifica di tali metadati compromette l'integrità del documento informatico.
3. Il riconoscimento (in modalità automatica o manuale) del formato di file impiegato per rappresentare un documento informatico può avvenire attraverso alcune modalità, tra cui le più diffuse sono tramite metadati interni ovvero esterni:

a) L'estensione nel nome del file, anche se tale associazione:
   - non è resiliente — è solitamente banale rinominare un file cambiandone l'estensione [ovvero crearne direttamente il nome] con un'estensione non corrispondente al formato utilizzato (es. un file di testo semplice con codifica ASCII denominato con estensione .doc, che invece è prerogativa dei documenti di Microsoft® *Word*);
   - non è biunivoca — una medesima estensione può essere usata nel nome di file codificati in formati diversi (es. l'estensione .log, usata per rappresentare file di registro codificati in maniera diversa), ovvero un dato formato viene associato a file con una molteplicità di estensionI (es. i certificati elettronici in formato X.509 con codifica DER, rappresentati con diverse estensioni tra cui .crt ovvero .cer).

b) La "tipologia MIME" (*MIME type*) del formato di file, anche se tale associazione gode di svantaggi simili all'estensione, in quanto:
   - soprattutto se espressa come metadato esterno (si veda §1.1.2), non è resiliente a variazioni o rimozioni del medesimo in maniera non controllata;

Firmato digitalmente da ROBERTO FRACCIA

- sia nel caso in cui sia espressa come metadato interno che come metadato esterno del file, potrebbe descrivere il formato in modo comunque ambiguo.

c) La presenza di metadati interni al file, espressi in "campi" che si trovano in posizioni specifiche (prefissate ovvero ricalcolabili) all'interno del file[2]. La lettura di tali campi permette di dedurre il formato del file in maniera più diretta e affidabile. Molti formati impiegano, specificatamente a questo scopo, una stringa prefissata di pochi caratteri (generalmente dai 2 ai 6), posta all'inizio del file, chiamata *magic number* e che ne identifica univocamente[3] il tipo di file.

1. 2 Tassonomia

1.2.1 Tipologie di formati

1. L'evolversi delle tecnologie e la crescente disponibilità e complessità dell'informazione digitale ha indotto la necessità di gestire sempre maggiori forme di informazione digitale (testo, immagini, filmati, ecc.) e di disporre di funzionalità specializzate per renderne più facile la creazione e la modifica.
2. Questo fenomeno porta all'aumento del numero di formati disponibili e dei corrispondenti programmi necessari per codificarli, decodificarli e gestirli in ogni modo.
3. Segue una sommaria e non esaustiva catalogazione dei più diffusi formati di file e pacchetti, secondo il loro specifico utilizzo ("tipologia"). A fianco di ogni tipologia di formati sono indicati i formati pertinenti oggetto del presente Allegato; qualora l'estensione di file associata al formato sia diversa –a meno di maiuscole/minuscole– dall'eventuale acronimo del nome del formato stesso, essa sarà indicata affiancata al nome tra parentesi (e.g., il formato PDF non avrà un'estensione indicata tra parentesi in quanto la sua estensione predefinita è già .pdf).

- Documenti impaginati (§2.1) — PDF, Microsoft® OOXML (.docx) e *Word* (.doc), OpenDocument Text (.odt), Rich-Text Format (.rtf), EPUB, PostScript™ (.ps), Adobe® *InDesign*® Markup Language (.idml);

[2] La parte iniziale ovvero quella terminale di un file contengono spesso gran parte dei campi utili a contenere i metadati interni (e quindi anche a identificare il formato) del file; quando presenti, queste parti sono chiamate, rispettivamente, *header* (impropriamente tradotto come "intestazione") e *footer* del file.
[3] Il magic number può anche identificare l'allineamento delle word, che le architetture dei microprocessori e i sistemi operativi implementano diversamente per varie ragioni. Alcuni magic number notevoli sono indicati, per i rispettivi formati, nel §2.

Firmato digitalmente da ROBERTO FRACCIA

- Ipertesti (§2.2) — XML, dialetti e schemi XML (.xsd, .xsl), HTML (.html, .htm), fogli di stile per XML/HTML (.xsl, .xslt, .css), Markdown (.md);
- Dati strutturati (§2.3) — SQL, CSV, Microsoft® OOXML (.accdb) e *Access* (.mdb), OpenDocument Database (.odb), JSON, Linked OpenData (.json-ld), JWT[4];
- Posta elettronica (§2.4) — .eml, .mbox;
- Fogli di calcolo (§2.5) — Microsoft® OOXML (.xlsx) e *Excel* (.xls), OpenDocument Spreadsheet (.ods);
- Presentazioni multimediali (§2.5) — Microsoft® OOXML (.pptx) e *PowerPoint* (.ppt), OpenDocument Presentation (.odp);
- Immagini raster (§2.6) — JPEG (.jpg, .jpeg), TIFF (.tif, .tiff), PNG, GIF, OpenEXR (.exr), JPEG2000 (.jp2k, .jp2c, .jp2), DICOM, Adobe® DNG, Adobe® *Photoshop*® (.psd), DPX, ARRIRAW (.ari);
- Immagini vettoriali e modellazione digitale (§2.7) — SVG, Adobe® *Illustrator*® (.ai), Encapsulated PostScript™ (.eps);
- Modelli digitali (§2.7) — StereoLithography (.stl); Autodesk® DWG™, DXF™, DWF™, FBX™.
- Caratteri tipografici (§2.8) — OpenType (.otf), TrueType (.ttf), Web Open Font (.woff, .woff2);
- Suono (§2.9) — Waveform RIFF / Broadcast Wave (.wav, .bwf), MP3, audio RAW (.pcm, .raw, .snd), AIFF (.aiff, .aifc, .aif), FLAC, MusicXML™ (.music.xml), MIDI (.mid); molteplici codec audio;
- Video (§2.10) — formati video delle famiglie MPEG2 e MPEG4; molteplici codec video;
- Sottotitoli (§2.11) — TTML/IMSC/EBU-TT (.ttml, .dfxp, .xml), EBU STL;
- Contenitori multimediali (§2.12) — MP4, MXF, MPEG2 Transport/Program Stream (.vob, .ts, .ps), AVI RIFF (.avi), Matroska (.mkv), QuickTime (.mov, .qt), WebM;
- Pacchetti multimediali (§2.12) — pacchetto di master interoperabile (IMF, IMP); pacchetto per il cinema digitale (DCP); master per la distribuzione cinematografica (DCDM); pacchetti Digital Intermediate basati su sequenze di fotogrammi (.exr/.dpx; .wav), ACES metadata file (.amf); pacchetto XDCAM;
- Archivi compressi (§2.13) — TAR, ZIP, GZIP, 7-Zip (.7z), RAR, TAR compresso (.tgz, .t7z, …), ISO9660 (.iso), VMware® Disk (.vmdk), Apple Disk Image (.dmg);
- Documenti amministrativi (§2.14) — fattura elettronica, fascicolo sanitario elettronico, *response* SAML SPID, segnatura di protocollo;

[4] Il *Java Web Token* (*JWT*) è in realtà un formato di flusso digitale, che può essere banalmente contenuto in un file, cfr. §2.3.

Firmato digitalmente da ROBERTO FRACCIA

- Applicazioni e codice sorgente (§2.15) — eseguibili Microsoft® (.exe, .com), *applet* Java (.jar); pacchetti applicativi *Windows*® (.msi), Android (.apk), macOS® (.pkg), iOS® (.ipa); librerie statiche (.a, .lib) e dinamiche (.so, .dll, .dylib); script interpretabili (.sh, .*?*sh, .bat, .cmd, .py, .perl, .js, .go, .r, …); codice sorgente in vari linguaggi di programmazione (.c, .cpp, .h, .java, .asm, …).
- Applicazioni crittografiche (§2.16) — certificati elettronici (.cer, .crt, .pem), chiavi crittografiche (.pkix, .pem), marcature temporali elettroniche (.tsr, .tsd, .tst), impronte crittografiche (.sha1, .sha2, .md5, …); per le firme e i sigilli elettronici avanzati: buste crittografiche XAdES (.xml), CAdES (.p7m, .p7s), PAdES (.pdf), contenitori ASiC (.zip); KDM (.kdm.xml).

1.2.2 Classificazione di formati

1. L'evolversi delle tecnologie e la crescente disponibilità e complessità dell'informazione digitale ha indotto la necessità di gestire sempre maggiori forme di informazione digitale (testo, immagini, filmati, ecc.) e di disporre di funzionalità specializzate per renderne più facile la creazione e la modifica.
2. Gli *standard* tecnologici vengono incontro a tali esigenze, permettendo di definite regole di codifica e decodifica di un documento informatico, affinché sia rappresentato tramite un file, un flusso digitale, ovvero un pacchetto di file (tutti oggetti del presente allegato). Gli standard tendono a stabilizzare le specifiche tecniche dei formati di file –sia nel tempo che rispetto alle tecnologie di produzione, trasmissione e archiviazione– ma la loro importanza nel cristallizzare tali specifiche in una forma precisa serve ad impedire la nascita di varianti "esotiche" o dialetti non controllati del medesimo formato che, alla lunga, ne riducano l'interoperabilità (cfr. più avanti).
3. Un esempio su tutti: la mancata standardizzazione dei codec usati nei formati-busta multimediali (§2.12), specialmente dei file video, che spesso conduce all'impossibilità di riprodurre un filmato ritenuto compatibile con il sistema informativo a causa del riconoscimento della sola estensione del file da parte di svariate applicazioni (che al massimo può servire a identificare il formato contenitore), senza invece un'adeguata verifica del possesso dei codec adatti a riprodurne le essenze.
4. Gli standard migliori sono quelli che possono essere facilmente estesi, rivisti o aggiornati nel tempo per adattarsi all'immanente obsolescenza tecnologica. Tra questi inoltre, eccellono gli standard che sono *ab initio* disegnati con il preciso scopo di evolvere a lungo termine; per questo motivo essi sono detti formati "compatibili in avanti" o anche "*future-proof*".

Firmato digitalmente da ROBERTO FRACCIA

5. Esempi di questi standard "virtuosi", sono l'XML e il JSON; il PDF e l'OpenDocument per i documenti impaginati; il TIFF (e il DNG), il PNG e il DPX per le immagini *raster*; l'SVG e il DXF per i modelli vettoriali; il TTML per i dialoghi; l'MXF e l'MP4 come contenitori multimediale; l'IMF come pacchetto di file multimediali.
6. I formati di file sono soggetti a revisioni allo scopo di includere caratteristiche evolutive; a questo scopo gli standard corrispondenti vengono "versionati" con diverse tassonomie, cioè incrementandone progressivamente i numeri delle revisioni (possibilmente in gerarchie di non più di 2-4 componenti numeriche– ovvero utilizzando l'anno o una data più precisa di riferimento, ovvero mediante sia numeri progressivi che date).
7. Quando non sono più fatti evolvere in favore di un formato differente (e quindi vengono progressivamente abbandonati), il formato diventa quiescente ed eventualmente viene "deprecato" in favore di un altro standard.
8. Sebbene sia tecnicamente possibile continuare a produrre e riprodurre file in un formato deprecato, il progresso tecnologico, o per meglio dire l'*obsolescenza tecnologica*, condannerà tali file a non essere più definitamente leggibili, a causa della mancanza di applicativi che ne implementino la decodifica (a meno di non coinvolgere risorse economiche solitamente sproporzionate al bisogno di accesso ai dati contenuti). Quando ciò accade ed è riconosciuto in maniera manifesta, si parla di formati "obsoleti".
9. Esistono varie classificazioni per le tipologie di formati, le quali sono spesso determinanti –ancor più delle loro peculiarità tecniche– per la scelta d'uso di un formato in favore di altri, ovvero per prendere decisioni ragionate circa il riversamento da un formato verso un altro (cfr. §3.3).
10. Tali classificazioni, elencate brevemente qui sotto, sono per lo più dicotomiche (cioè del tipo presenza o assenza di una determinata caratteristica) e indipendenti fra loro. Accanto ad ogni classificazione è riportato un modificatore in grassetto, il cui significato è riferito all'indice di interoperabilità introdotto nel §3.2. Un formato più essere:

a) uno standard *de facto* (**+2**) quando questioni contingenti (anche fa loro correlate), quali l'efficienza in casi d'uso reali, l'autoregolazione dei mercati di riferimento, l'efficacia tecnica, ne hanno determinano una larghissima e non trascurabile diffusione, per lo meno in settori di riferimento. Un formato può essere invece uno standard *de iure* (**+3**), quando esistono normative che ne obblighino, o per lo meno ne raccomandino, l'uso in determinati contesti amministrativo-legali e settori di riferimento. Rappresentano esempi di tali normative le Linee guida di cui il presente Allegato è parte integrante (in quanto già Regole Tecniche) ovvero, a livello comunitario, alcune Decisioni di Esecuzione (UE). Sono standard *de iure*, inoltre, tutti i formati codificati come tali dalle organizzazioni nazionali, comunitarie e internazionali che hanno il compito di definire standard e linee guida nei settori di riferimento

Firmato digitalmente da ROBERTO FRACCIA

dei formati stessi (come, ad esempio, ISO, ITU, UNI, CEN, SMPTE, ecc.). Infine, un formato può anche non rappresentare alcuno standard (**0**), ma tale caratteristica tendenzialmente lo esclude dall'elenco dei formati virtuali contenuti nel presente Allegato.

b) aperto (**+3**) ovvero chiuso (**0**) a seconda che esista o meno, e sia resa pubblicamente disponibile, una "specifica tecnica" del medesimo: la documentazione che descrive dettagliatamente, come minimo, la procedura di formazione e di lettura di file in quel formato e, possibilmente, l'elaborazione e i suoi possibili scenari di utilizzo, spesso descritti organicamente mediante *operational patterns* (in italiano: schemi operativi).

c) proprietario (variabile) o non proprietario (**+4**), a seconda che sia stato creato da un'organizzazione privata –che dunque ne detenga la proprietà intellettuale– ovvero quando la gestione delle sue specifiche non è controllata in tale ambito (quindi possibilmente rilasciata al pubblico dominio, o comunque gestita da un organismo di standardizzazione). In particolare, i formati proprietari possono essere liberi (**+3**) ovvero limitati; in quest'ultimo caso la limitazione potrebbe permettere soltanto l'utilizzo libero di file già codificati in tale formato ma non la produzione di nuovi file (**+2**), ovvero limitare anche la lettura dei file formattati secondo tale formato (**0**); potrebbero essere possibili anche altri tipi di vincoli (pagamento di *royalty*, sottoscrizione di contratti di riservatezza o contratti vincolanti relativamente a particolari utilizzi quali lo sfruttamento commerciale, ecc.).

d) estendibile (**+2**) o non estendibile (**0**) qualora esso sia stato concepito *ab initio* per ammettere revisioni che ne aumentino progressivamente le funzionalità. I formati *non* estendibili, quindi, possono comunque essere soggetti a revisioni, che però potrebbero, per tali formati, richiedere una re-ingegnerizzazione o un adattamento più difficoltoso rispetto a formati estendibili, probabilmente anche a scapito delle compatibilità di cui al punto precedente.

e) livello del modello per i metadati (da **0** a **+3**) che segue l'analoga classificazione emanata nelle *Linee guida nazionali per la valorizzazione del patrimonio informativo pubblico*, emanate dall'Agenzia per l'Italia Digitale, ove al livello 1 vengono attribuiti 0 punti e così via via fino al livello 4 cui sono attribuiti 3 punti. Tale valore è indicato, per i formati descritti al §1.2.3, nelle loro tabelle riassuntive.

f) non robusto (**0**) ovvero parzialmente robusto (**+1**) a seconda che il file comprenda meccanismi per verificare l'eventuale perdita di *integrità* di un file (o pacchetto di file); completamente robusto (**+2**), invece, qualora tale meccanismo sia presente e consenta, inoltre, di leggere correttamente le parti integre del file.

Firmato digitalmente da ROBERTO FRACCIA

g) dipendente (**0**) ovvero indipendente dal dispositivo (**+4**) a seconda che esso richieda o meno specifici componenti hardware, firmware o software per essere creato o letto.
h) i formati il cui standard prevede *by design* che un applicativo in grado di interpretare una data revisione possa anche leggere file formattati con revisioni precedenti (eventualmente entro un limite massimo) si dicono retro-compatibili. Quelli per cui gli applicativi disegnati al momento in cui una data revisione sia corrente possano leggere anche file formattati in base a revisioni successive del medesimo standard si dicono invece "compatibili in avanti"[5] (**0**).
i) testuale (**0**) se, rappresentando ogni word di un file come caratteri testuali, sia possibile estrapolarne il contenuto informativo tramite lettura manuale e non automatizzata di tali caratteri — a seguito di uno sforzo di interpretazione di entità variabile, ma comunque proporzionato alle capacità intellettive di un tecnico di settore. Si parla, in alternativa, di formato binario (*binary*) (**0**) quando il processo è generalmente possibile solo mediante interpretazione automatizzata, "bit a bit", del contenuto digitale del file da parte di un algoritmo di parsing.

1.2.3 Formati generici e specifici

1. In ottica di interoperabilità è necessario, per le PP.AA., individuare un elenco di formati di file (e, *mutatis mutandis*, di formati di contenitori, pacchetti di file, flussi digitali e codec) per i quali vi siano obblighi o raccomandazioni in merito al riconoscimento o alla produzione in tali formati. Tale elenco non può presentare un unico tipo di obblighi e raccomandazioni, in quanto le organizzazioni di categoria, avendo necessità amministrative e operative differenti, utilizzano tecnologie digitali –e di conseguenza formati di file e applicazioni che li elaborano– estremamente variegate.
2. È auspicabile che i formati raccomandati nel presente Allegato siano adottati con modalità analoghe anche dagli enti privati –quando non già obbligatori per effetto di altre leggi– allo scopo di incrementare l'interoperabilità nello scambio di documenti informatici tra settore pubblico e privato. Per questo motivo queste Linee guida individuano, dall'insieme di formati di cui al §2:

[5] A titolo di esempio, un formato potrebbe essere progettato affinché, in uno schema di versionamento del tipo "*m.n*" (ove *m* sia il numero 'maggiore' della versione e *n* il numero 'minore') vi sia retrocompatibilità totale in scrittura di almeno *k* versioni precedenti, nonché estendibilità (in lettura) per tutte le revisioni minori della stessa versione. Ad esempio, per $k=2$, questo significa che un file codificato nella versione 3.12 di un dato formato, ad esempio, potrà essere prodotto anche da applicativi che producano file codificati con le versioni 4 e 5; inoltre ad un applicativo in grado di leggere la versione 3.12 sarà richiesto di poter leggere file di qualunque versione 3 (anche se eventuali funzionalità aggiuntive introdotte in revisioni minori successive alla 3.12, pur non "onorabili" dall'applicativo, non dovranno pregiudicarne la possibilità di aprire il file).

Firmato digitalmente da ROBERTO FRACCIA

a) una categoria generale di formati, rispetto ai quali *tutte* le PP.AA. e le organizzazioni sul territorio nazionale,
    a. sono in grado di leggere file prodotti in questi formati,
    b. seguono le indicazioni riportate nella tabella riassuntiva del formato per quanto concerne la produzione di nuovi documenti in questi formati;
b) diverse categorie specifiche o speciali, diversificate in base al settore merceologico o alla natura del documento informatico rappresentabile, verso le quali sono identificati ulteriori obblighi e raccomandazioni solo verso le PP.AA. che, in quanto utenti professionali,[6] trattano documenti di quella tipologia nell'ambito ristretto, o comunque delimitato, di quella categoria specifica. Tali categorie possono essere di riferimento anche per soggetti privati che trattano professionalmente i medesimi documenti informatici.

3. L'appartenenza di un formato di file alla categoria generale piuttosto che a una o più categorie speciali è indicata nelle tabelle riassuntive dei formati contenute nel §2, possibilmente differenziata per la lettura ovvero la scrittura (cioè la formazione) di documenti in tali formati.
4. Come indicato nelle Linee guida di cui il presente Allegato è parte integrante, qualora un formato di file sia indicato come generico, ma una sua particolare applicazione in un determinato settore specialistico fornisca anche un formato di file specifico, ovvero una variazione strutturale del medesimo formato generico (ad es. dialetti, specializzazioni, varianti, schemi operativi, profili, specifiche tecniche particolari o aggiuntive), la specializzazione del formato prevale su quella generale.
5. Ad esempio, nel caso di un documento informatico contenente informazioni fiscali relative a una prestazione, cessazione di beni o servizi, le organizzazioni non devono produrlo in un qualsiasi tipo di file XML (che è altresì un formato generico per dati strutturati, anche di codesto tipo, cfr. §2.3); ne è garantita, invece la produzione sotto forma di fattura elettronica nello specifico formato FatturaPA (cfr. §2.14), individuato dal legislatore come il dialetto XML per quell'utilizzo specifico.
6. Si precisa che, sempre in analogia con l'indice di interoperabilità introdotto nel §3.2, il caso di pacchetti e contenitori di file va sempre considerato congiuntamente con tutte le sue parti costituenti: cioè, per i pacchetti di file, il formato del pacchetto in se, insieme ai formati di tutti i file costituenti il pacchetto stesso; per i contenitori di file, il formato della busta in se, insieme ai formati di tutti i flussi e i codec di tutte le essenze imbustate nel contenitore.

[6] Il termine "utente professionale" va inteso ai sensi del Regolamento (UE) № 1807/2018 (regolamento "FFnpD") del Parlamento europeo e del Consiglio relativa a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione Europea.

Firmato digitalmente da ROBERTO FRACCIA

7. Ad esempio, si consideri un contenitore multimediale[7] i cui formati della busta (e.g. MP4, §2.12) e quello delle essenze audio e sottotitoli (e.g., rispettivamente, WAVE e EBU STL, §2.9) sono contenute nella categoria generale, mentre il codec usato nell'essenza video (e.g. XDCAM EX) non è presente in nessun elenco, trattandosi di un codec chiuso e proprietario. In effetti un documento elettronico così formato non è riproducibile integralmente, a meno di non avere a disposizione nell'applicativo d'utilizzo (riproduttore multimediale) il codec proprietario XDCAM, la cui disponibilità pubblica è, ad oggi, limitata e potrebbe ridursi sensibilmente in futuro, a causa dell'obsolescenza del codec rispetto alle tecnologie degli applicativi, della scadenza di licenze d'uso e brevetti, nonché delle sorti dell'organizzazione che li detiene. In questo esempio, dunque, il documento elettronico non può considerarsi un file codificato, nella sua interezza, in un formato interoperabile: lo sono le tracce audio, sottotitoli e il contenitore che le imbusta, ma non lo è la traccia video e, quindi, non lo è il documento informatico nella sua interezza.

2. Tipi di file

1. Si faccia riferimento al Glossario delle presenti linee guida per la definizione dei termini non ulteriormente introdotti in questa sezione.
La sezione mantiene la medesima suddivisione per tipologie di formato delineata in §1.2.1. Per ciascun formato di file, pacchetto di file, busta o codec, ne vengono ricapitolate le caratteristiche principali in una tabella sinottica, recante:

- **nome abbreviato**, **acronimo** ovvero **pseudonimo** del formato (in alto a sinistra).
- TIPOLOGIA DI FORMATO (in alto a destra) — in particolare se si tratti di un formato di file, di busta/contenitore, di pacchetto di file, di flusso, ovvero un codec per essenze multimediali.
- icona del formato (in alto a destra) — riferimento visivo, a scopo di mera indicazione o suggestione, della riproduzione grafica di un'icona specifica per

[7] Questi file sono, comunemente ma in maniera inesatta, chiamati «file video», perché l'essenza più importante contenuta al loro interno è quella video, ovvero in questo caso «file 'MP4'» in quanto si esplicita il solo formato della busta, ignorando i codec delle essenze al suo interno, perché la busta è spesso –impropriamente– il solo oggetto cui venga una visibilità tecnica, verso l'utente, da parte del sistema operativo e di archiviazione che conserva e processa il file. Tuttavia, tali contenitori possono avere più tracce video, audio, sottotitoli — talvolta persino file di altri formati in allegato. L'integrità di tali file, che ne consente un utilizzo pieno sotto ogni aspetto tecnico, amministrativo e giuridico, è legata perciò alla possibilità di aprire e decodificare non solo la busta e una traccia video, ma tutte le essenze ivi contenute. Per questo motivo è importante sottolineare la presenza di essenze di più tipologie diverse al suo interno, ciascuna potenzialmente codificata con un codec diverso, da cui l'esigenza di nominare correttamente questi file come «contenitori multimediali».

Firmato digitalmente da ROBERTO FRACCIA

la tipologia in oggetto (così come implementata nelle GUI dei principali sistemi operativi o software applicativi, per la riproduzione di detto formato).

- nome completo del formato.
- estensione di file — se più di una, la prima è da considerarsi raccomandata per la generazione dei file, mentre le altre sono estensioni meno comunemente usate, per le quali si raccomanda la capacità di lettura in tale formato. Nel caso dei pacchetti di file, sono invece indicate le estensioni dei formati di file che compongono obbligatoriamente il pacchetto (escludendo tutte le tipologie di formati ammessi dal pacchetto ma che non devono essere obbligatoriamente presenti all'interno).
- Tipologia MIME (*per i formati di file e busta*) — per i formati di file vengono indicati i possibili tipi MIME, come definiti in RFC-6838, per l'identificazione del formato a prescindere dall'estensione; qualora presenti più di un tipo MIME, il primo è sempre da intendersi quale preferenziale (e dunque raccomandato per la creazione di file in questo formato). Nel caso di pacchetti di file, sono invece indicati i tipi MIME usati dai file che compongono il pacchetto. Una lista aggiornata di tipi MIME registrati si può trovare al seguente indirizzo internet: www.digipres.org/formats/mime-types.
- Derivato da (*opzionale*) — eventuali formati di file, buste, pacchetti o codec di cui il formato è un'evoluzione ovvero, come nel caso di XML, ne rappresenti un dialetto. Possono essere indicati qui, per contenitori e pacchetti di file multimediali, l'applicabilità a uno o più schemi operativi.
- *Magic number* (*per i formati di file e busta*) — L'eventuale codice, definito nel Glossario e in §1.1.3, viene indicato nella sua codifica ASCII così; qualora i caratteri del *magic number* contengano caratteri speciali non alfanumerici e non diacritici, essi potranno essere indicati, *in toto* o in parte, in notazione esadecimale, come ad esempio 0x1A3F (2 byte).
- Profili (*per i soli codec*) — Molti codec posseggono parametri di compressione che sono usati per "tarare" l'algoritmo a diverse esigenze. Alcuni di questi parametri possono essere impostati –in maniera più o meno rigida– su valori determinati *a priori*, andando a costituire delle pre-selezioni che prendono il nomi di "profili", "livelli" o altro (a seconda del tipo di codec). Se rilevante o vincolante a livello di codec, può essere indicata qui la compatibilità di un codec con uno più schemi operativi (anche se uno schema operativo viene tecnicamente rafforzato al livello di contenitore o di pacchetto di file). Quando utile per distinguere ulteriormente i tipi di profilo fra loro, da un punto di vista puramente grafico, possono essere usati anche alcuni colori.
- Codice FourCC (*per i soli codec*) — definito in RFC-2361 (oltre che in www.fourcc.org) e nel Glossario, è usato per indicare una stringa identificativa di al più 4 caratteri alfanumerici minuscoli, indicata così, per distinguere i

Firmato digitalmente da ROBERTO FRACCIA

codec audio e video usati nelle essenze per alcuni tipi di formati di busta multimediale (§2.12).

- Sviluppato da — Nome dell'organizzazione di standardizzazione, azienda, dicasterio governativo di competenza, società o comunità che ne detiene la proprietà intellettuale (formati proprietari), ovvero che ne mantiene lo sviluppo (formati non proprietari).
- Tipologia di standard — viene brevemente elencato se il formato sia codificato in qualche tipo di standard, se sia o meno aperto, proprietario (con eventuali licenze d'uso), testuale/binario, retrocompatibile, estendibile, robusto e dipendente dal dispositivo. Qualora non espressamente indicato in tale casella (rispetto alla classificazione delle tipologie di formato di cui al §1.2.1), viene implicitamente assunto che il formato sia:
    a) non codificato in alcuno standard, né *de iure* né *de facto*,
    b) chiuso,
    c) proprietario con licenza d'uso vincolante sia in lettura che in scrittura,
    d) non estendibile,
    e) possegga modello per i metadati di livello 1,
    f) non robusto,
    g) *indipendente* dal dispositivo.
- Livello metadati — Il "livello del modello per i metadati", come introdotto nelle *Linee guida nazionali per la valorizzazione del patrimonio informativo pubblico* emesse dall'Agenzia per l'Italia Digitale, che si riferisce alla classificazione dei metadati supportati nativamente dal formato. Si precisa che la classificazione di ciascun formato in un dato livello si riferisce all'opportunità di valorizzare *tutti* i metadati, obbligatori e facoltativi, come previsti dalle specifiche tecniche del formato stesso riportate nella tabella, alla sezione Riferimenti). Qualora non vengano valorizzati tutti i metadati facoltativi, la classificazione può attestarsi a un livello inferiore. Altresì, non viene considerata, ai fini di tale classificazione, la valorizzazione *custom* di eventuali metadati "riservati" a casi d'uso non riportati dalle specifiche (quali, ad esempio, campi riempiti da singoli fornitori con metadati di loro propria rilevanza e sintassi). Nel caso di pacchetti di file, la classificazione si riferisce ai metadati complessivamente presenti nell'insieme di file minimi costituenti il pacchetto.
- Revisione — viene indicata qui la versione dello standard di riferimento per le PP.AA.; la "versione di riferimento" va intesa, salvo indicazione contraria in Revisione, come la versione più recente tra quelle supportate, nel senso che:

Firmato digitalmente da ROBERTO FRACCIA

- per le organizzazioni che *leggono* file in questo formato, è obbligatoria la leggibilità di file creati con questa versione e, con tutte le precedenti con cui tale versione è descritta come retrocompatibile (cfr. §1.2.2);[8]
- per le organizzazioni che *producono* documenti in tale formato, è obbligatoria la produzione di nuovi documenti in tale versione *ovvero* – qualora non tecnicamente praticabile– con una qualunque versione precedente rispetto alla quale la versione indicata in Revisione sia descritta come retrocompatibile (cfr. §1.2.2[9]), *ovvero* –qualora non tecnicamente praticabile neanche ciò– con una qualunque versione successiva rispetto alla quale, però, la quella indicata in Revisione sia descritta come compatibile in avanti.

- Riferimenti — sono qui elencate tutte le normative di riferimento (sotto forma di leggi, regolamenti tecnici, linee guida o standard) nonché –in mancanza o a complemento di altro– *best pratices* e indirizzi di siti web ove sia resa disponibile altra utile documentazione ufficiale;
- Conservazione — Sono date indicazioni in merito all'utilizzo del formato per la conservazione di cui alle presenti Linee guida. In alcuni casi, il formato può essere adottato per la conservazione dei documenti informatici purché siano adottate specifiche configurazioni, eventualmente indicate qui. Infine, è indicato in questo campo (con la dicitura "cfr. §2.8"), l'eventuale attenzione all'uso di caratteri tipografici non interoperabili.
- Racc. per la lettura — raccomandazioni per le PP.AA. relativamente alla capacità di leggere documenti informatici nel dato formato, oltre che eventuali obblighi normati dalle Linee guida di cui questo Allegato è parte integrante;
- Racc. per la scrittura — raccomandazioni per le PP.AA. relativamente alla capacità di formare documenti informatici nel dato formato, oltre che eventuali obblighi previsti dalle Linee guida di cui questo Allegato è parte integrante. In tale sezione sono collocate anche indicazioni in merito all'uso di tale formato per la conservazione, così come trattata nelle presenti Linee guida.

Ciascun formato può essere ulteriormente descritto, particolarmente riguardo alle raccomandazioni e agli eventuali obblighi, in una parte discorsiva successiva alla tabella sinottica.

[8] Se, ad esempio, è raccomandata la versione 3.0 di un dato formato di file, che è definito come una variante della versione 2.0 tale che qualunque lettore in grado di leggere la 3.0 leggerà anche la 2.0, l'obbligo in lettura si applica anche alla versione 2.0.

[9] Se, utilizzando il precedente esempio, è raccomandata la versione 3.5 di un dato formato di file ma qualunque applicazione in grado

Firmato digitalmente da ROBERTO FRACCIA

2. Si rimanda al Regolamento (UE) Nº 679/2016 ("GDPR") del Parlamento europeo e del Consiglio in materia di trattamento dei dati personali che, rappresentati in un documento informatico, possono essere soggetti a *pseudonimìa*, come metodologia atta a proteggerli, aggiornarli, cancellarli. La scelta dei formati di file da utilizzare può discendere anche dall'implementazione di tecnologie e procedure allo scopo di ottemperare agli obblighi imposti in capo al GDPR.
3. Si rimanda al Regolamento (UE) Nº 1807/2018 (regolamento "FFnpD") del Parlamento europeo e del Consiglio relativa a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione Europea, per quanto riguarda ulteriori considerazioni in merito sia alla localizzazione geografica dei documenti informatici, alla loro portabilità e alle distinzioni tra utilizzo e utenti professionali di dati non personali.
4. Si rimanda alle *Linee guida sull'accessibilità* e alle *Linee guida di design* per le considerazioni sulla rappresentazione di elementi testuali e grafici nei documenti elettronici, cui le PP.AA. si attengono per la produzione di documenti informatici. Come mero esempio, tali considerazioni possono riguardare i criteri di scelta:

- delle famiglie di caratteri tipografici (§2.8) e del loro corpo;
- dell'inclusione di un elemento grafico come immagine vettoriale (§2.6) ovvero *raster* (§2.7).

5. Il primo criterio di scelta è di particolare pertinenza con la formazione dei documenti informatici, in quanto in moltissime tipologie elencate nel §2 (non solo i documenti impaginati, bensì anche le pagine web, i fogli di calcolo, le presentazioni multimediali, le immagini vettoriali e la modellazione digitale, nonché i sottotitoli) il tipo di carattere è parte integrante del documento perciò, qualora il carattere tipografico non sia presente o non sia interpretabile dal sistema informativo che visualizza il documento, ciò può comportare una difformità o addirittura l'impossibilità di leggere lo stesso.
6. Nel caso di documenti la cui rappresentazione o utilizzo (si pensi, ad esempio, non soltanto a documenti impaginati, bensì a documenti multimediali) dipendano dalle caratteristiche tecniche del formato scelto e delle modalità con cui il documento viene specificatamente formato, le considerazioni di cui alle sopracitate Linee guida saranno valutate allo scopo di incrementare l'interoperabilità e l'accessibilità dei documenti.
7. Proprio in considerazione dei precedenti 2, 4, 5 e 6, le PP.AA. possono includere nella valutazione di interoperabilità (cfr. §3.1) le considerazioni relative alla scelta dei formati dei file, delle modalità con cui i documenti vengono formati usando determinati formati (profili, impostazioni o configurazione del sistema di formazione del file, ecc.).
8. Nel caso di formati di file che permettano di scegliere i caratteri tipografici da utilizzare salvando tali scelte come parte del documento informatico stesso, qualora

Firmato digitalmente da ROBERTO FRACCIA

i caratteri tipografici non facciano anch'essi parte del documento informatico, le PP.AA. adotteranno tutte le misure necessarie per la scelta di caratteri tipografici di uso comune, affinché la visualizzazione del documento sia il più possibile indipendente dai caratteri tipografici.
9. La raccomandazione di cui al punto 8 viene richiamata, nelle successive schede tecniche dei formati di file, mediante l'indicazione del capitolo sui caratteri tipografici, cioè con la semplice dicitura "cfr. §2.8", alla voce "Livello metadati".

2.1 Documenti impaginati

1. I formati "orientati alla pagina", o "impaginati", suddividono un documento informatico in unità separate chiamate *fogli*, in quanto il loro utilizzo primario è la carta stampata, come mezzo di origine (tramite scansione di documento cartaceo) ovvero di destinazione (tramite stampa). Non tutti i documenti impaginati sono però concepiti per la stampa, esibendo anzi caratteristiche tipiche del mondo digitale, quale la possibilità di allegare contenuti multimediali o anche di altro genere, così come di collegamenti di tipo URL a altre posizioni nella rete internet, intranet o in altro sistema di gestione dei documenti, in modo che l'utente possa accedervi tipicamente dopo aver attivato il collegamento di riferimento.
2. La pagina va inoltre considerata come un'entità virtuale — dunque non legata alla bidimensionalità e staticità di una superficie fisica di stampa. Con l'eccezione di alcuni formati nati ed evoluti esclusivamente nell'ambito della stampa tradizionale, e.g. il formato PostScript®, che dunque sono tecnicamente vincolati a rappresentare esclusivamente elementi direttamente stampabili (quali testi, disegni, immagini statiche), i formati più evoluti quali il PDF possono rappresentare dati multimediali, elementi interattivi o persino includere altri file all'interno di un documento impaginato (si legga la sezione corrispondente).
3. In formati di questo tipo viene descritta anche la "presentazione" (cioè la rappresentazione visuale) dei contenuti informativi all'interno delle pagine, utilizzando stili di visualizzazione di ipertesti (cfr. §2.2), immagini (raster o vettoriali, cfr. §2.6 e §2.7) e altre tecniche tipografiche, quali i caratteri tipografici (§0), che possono essere riferiti sia internamente nel medesimo file e che contiene dunque, al suo interno, un insieme completo o parziale di glifi.

PDF	FORMATO DI FILE
Nome completo	Portable Document Format
Estensione/i	.pdf
Magic number	%PDF
Tipo MIME	application/pdf
Sviluppato da	Adobe Systems

Firmato digitalmente da ROBERTO FRACCIA

Tipologia di standard	aperto (2.0)/proprietario (libero 1.7), estendibile, *de jure*
Livello metadati	4
Derivato da	Adobe® PostScript®
Revisione	2.0 (2017)
Riferimenti	Famiglie di standard **32000** e **19005** della ISO/IEC: • 32000-2:2017, *PDF v2.0* • 32000-1:2008, *PDF v1.7* • 19005-1:2005, *PDF/A-1* (v1.4) • 19005-2:2011, *PDF/A-2* (v1.7) • 19005-3:2012, *PDF/A-3* (v1.7) • Adobe, *Supplement to PDF v1.7 Extension 3*, ©2008 • Adobe, *Document management – PDF 1.7*, ©2008 • ISO 24517-1:2008, *PDF/E-1* (v1.6) • ISO 15930-1:2001, *PDF/X-1 e PDF/X-1a* (v1.4) • ISO 15930-8:2010, *PDF/X-5* (v1.6) • ISO 14289-1:2014, *PDF/UA-1* (v1.4) • ISO/CD 14289-2, *PDF/UA-2* (v2.0) • ISO 16612-2:2010, *PDF/VT-1 e PDF/VT-2* (PDF/X-4 e /X-5) • ISO/CD 16612-3, *PDF/VT-3* (PDF/X-6) (v2.0)
Conservazione	Sì, solo profili PDF/A e PDF/B; altrimenti, cfr. §2.8
Racc. per la lettura	Generico con riconoscimento obbligatorio (v1.*x*).
Racc. per la scrittura	Raccomandata: v1.7+. Obbligatoria: v1.4+. Profili raccomandati (leggere raccomandazioni più sotto): PDF/A-2a, PDF/A-2u, PDF/A-2b, PDF/A-1a, PDF/A-1b. Profili PDF/A e PDF/B adatti alla conservazione.

4. Il formato PDF è il "principe" dei formati per documenti impaginati. Nato come formato proprietario (sviluppato da Adobe Corporation), è stato rapidamente adottato come standard *de facto* per la produzione digitale del cartaceo; nel 2008 è diventato uno standard *de iure*, con il nome di ISO 32000-1 (PDF versione 1.7); successivamente rivisto nel 2017, con il nome di ISO 32000-2 (PDF versione 2.0). Il formato PDF è estremamente versatile in quanto è stato continuamente aggiornato nel tempo aggiungendo nuove funzionalità. Allo stato attuale (PDF versione 2.0) è possibile includere nel documento evidenze di vario tipo (incluse immagini, audio, video, modelli tridimensionali animati), imbustare all'interno del file di qualsivoglia formato sotto forma di "allegati", sovraimprimere graficamente alle pagine moduli interattivi che permettono all'utente compilazione libera o vincolata (per poi salvarne un'istanza con i campi riempiti). È anche possibile proteggere un documento PDF con password o firme elettroniche e usare la crittografia per

Firmato digitalmente da ROBERTO FRACCIA

limitarne la lettura o la modifica, anche se tale protezione è aggirabile con appositi strumenti software.
5. L'apposizione di firme e sigilli elettronici su documenti in formato PDF è effettuata mediante la busta crittografica PAdES (cfr. §2.16), mentre il servizio fiduciario elettronico costituto dalla convalida di documenti in formato PAdES è sancito dalla normativa comunitaria.
6. Il PDF è uno standard "modulare", nel senso che sono stati definiti profili diversi che introducono insiemi aggiuntivi di nuove funzionalità (quali quelle sopra elencate), ovvero vincolano alcune di esse allo scopo di migliorare l'interoperabilità del documento PDF in specifici ambiti. I profili possono prevedere sotto-profili con ulteriori specifiche (additive o vincolanti), chiamati livelli di conformità. Si noti inoltre che un file PDF può essere conforme a più livelli (profili o sotto-profili) contemporaneamente. I profili e sotto-profili ufficialmente riconosciuti sono i seguenti:

- **PDF/A** (*archival*) — Profilo particolarmente adatto alla creazione di documenti di cui deve essere garantita la leggibilità in caso di archiviazione a lungo termine e conservazione. Si divide in due sotto-profili:
  - **PDF/A-1** — Basato su PDF versione 1.4, impedisce al file di contenere (graficamente o come allegati) niente altro che testi, ipertesti, immagini *raster* o vettoriali; sono in particolar modo vietati i moduli con contenuti variabili (e.g. codice Java eseguibili), Infine, il formato contenere al suo interno tutti i caratteri tipografici utilizzati.
    - **PDF/A-1a** (*accessible*) — Specifica "forte" del sotto-profilo PDF/A-1, ove ad ogni contenuto non testuale del file è garantita piena coerenza semantica e accessibilità (p.es. ogni immagine deve avere un commento, ed ogni glifo un codice UNICODE); questo consente non solo una visualizzazione del file a lungo termine, ma anche un suo utilizzo da parte di *parser* e di lettori del documento per persone diversamente abili.
    - **PDF/A-1b** (*basic*) — Specifica "debole" del sotto-profilo PDF/A-1, ove non è richiesta la presenza di dati semantici come in PDF/A-1a.
  - **PDF/A-2** — Basato su PDF versione 1.7, è dotato di tre livelli di conformità:
    - **PDF/A-2a** — analogo a PDF/A-1a.
    - **PDF/A-2b** — analogo a PDF/A-1b.
    - **PDF/A-2u** — analogo a PDF/A-2b, ma con il vincolo aggiuntivo che tutti i caratteri impiegati devono essere codificati in base alla mappatura UNICODE.

Firmato digitalmente da ROBERTO FRACCIA

    - **PDF/A-3** — Sotto-profilo poco usato che aggiunge, rispetto a PDF/A-2, la possibilità di allegare file di qualsiasi tipo.
- **PDF/E** (*engineering*) — Profilo dedicato all'inclusione di disegni e altri dati tecnici nel PDF (versione 1.6), quali informazioni geografiche, e modelli grafici tridimensionali interattivi.
- **PDF/H** (*health*) — Inclusione di dati sanitari (sotto forma di XML) quali referti, sondaggi, testi di laboratorio o altri sistemi diagnostici.
- **PDF/X** (*graphics exchange*) — Interscambio professionale di contenuti grafici (sia *raster* che vettoriali, cfr. §2.6 e §2.7 rispettivamente)
    - **PDF/X-1** — Sotto-profilo basato su PDF versione 1.3.
        - **PDF/X-1a** — Variante in cui devono essere incluse tutte le fonti tipografiche, mentre i colori sono codificati in spazio-colore CMYK o come colori *spot*[10].
    - **PDF/X-3** — Sotto-profilo (basato su PDF versione 1.3) che include capacità colorimetriche avanzate, come ad esempio ammettere, oltre a colori *spot*, spazi-colore CMYK, CIELAB, RGB (calibrati o meno), profili ICC.
    - **PDF/X-4** — Ulteriore evoluzione del sotto-profilo PDF/X-3 (basato su PDF versione 1.4) che include anche le trasparenze.
    - **PDF/X-5** — Ulteriore evoluzione del sotto-profilo PDF/X-5 (basato su PDF versione 1.6), con una ulteriore distinzione: **PDF/X-5g**, **PDF/X-5pg** e **PDF/X-5n**.
- **PDF/UA** (*universal accessibility*) — Profilo dedicato all'accessibilità universale, che comprende ad esempio l'ordine con cui devono comparire commenti e note, le didascalie per i contenuti extra meno accessibili (ad es. foto o video), i requisiti per permettere a tecnologie di accessibilità di gestire tutte le parti del documento (incluse quelle criptate).
- **PDF/VT** (*variable and transactional printing*) — Profilo dedicato a PDF che andranno stampati con parti variabili da tiratura a tiratura (ad es. il numero seriale progressivo in ogni esemplare a tiratura limitata).
    - **PDF/VT-1** — Variante in cui tutte le parti sono auto-contenute in un singolo file PDF (compatibile con PDF/X-4).
    - **PDF/VT-2** — Variante in cui è contemplato l'uso di elementi grafici contenuti in file esterni (compatibile con PDF/X-5)

[10] Un colore *spot* è indicato digitalmente da un semplice codice corrispondente, nei plotter e stampanti professionali, ad un particolare inchiostro che viene inserito appositamente. I colori spot possono prevedere qualità colorimetriche non visibili digitalmente (p.es. colori lucidi, opachi, metallizzati, perlati, ruvidi), così come essere associati, in particolari processi di stampa, a lavorazioni completamente diverse nella zona dell'impaginato digitalmente indicata come da stampare con un dato color *spot*.

Firmato digitalmente da ROBERTO FRACCIA

- **PDF/VT-2s** — Ulteriore variante in cui sono ammessi contenuti presi da flussi digitali esterni al PDF stesso (p.es. dati provenienti da un sensore).

7. Come riportato nella scheda tecnica del formato PDF, a prescindere dalla tipologia di contenuto (e quindi dall'eventuale conformità con altri profili), la produzione di file in formato PDF privilegia, ove disponibile, la più recente versione conforme allo ISO 32000-2, adottando preferenzialmente i suoi i profili di accessibilità, con il seguente ordine di preferenza: PDF/A-2a, PDF/A-2u, PDF/A-2b. Qualora non siano disponibili strumenti per la produzione di documenti PDF conformi alla versione 2.0, si utilizza la versione più recente disponibile, preferendo le versioni conformi allo ISO 32000-1 (PDF versione 1.7 e successive), in nessun caso inferiori al PDF versione 1.4, adottando i profili di accessibilità con il seguente ordine di preferenza: PDF/A-1a, PDF/A-1b. La ragione principale di tale ordine di preferenza risiede nella maggiore versatilità del PDF versione 1.7 e successive nel:

- includere documenti (anche non in formato PDF), come *allegati* al PDF stesso;
- permettere l'utilizzo di campi modulo senza incidere sulla validità di firme o sigilli elettronici senza invalidare l'integrità del documento stesso, né tantomeno delle firme o sigilli elettronici PAdES eventualmente apposti;

8. L'obbligo di cui al precedente capoverso può essere disatteso per i documenti PDF prodotti per essere specificatamente modificati ovvero "compilabili" in un momento successivo alla loro produzione, come ad "modelli" o *template* per procedimenti amministrativi di varia natura. Tuttavia, le PP.AA. producono il documento compilabile e modificabile in formato PDF, usando versioni e profili adeguati, tenendo conto che una volta compilati o redatti in forma definitiva, tali file costituiranno documenti informatici (nel senso della rilevanza degli atti, fatti o dati giuridicamente rilevanti contenuti nella versione modificata o compilata). Si raccomanda, ad esempio, di utilizzare per file PDF compilabili o modificabili, solamente caratteri tipografici tra quelli interoperabili "standard" definiti nel §2.8.
9. I documenti che sono immodificabili salvo per la compilazione di campi vuoti o l'apposizione di firme o sigilli elettronici devono essere prodotti in formato PDF versione almeno pari a 1.7, sfruttando i campi modulo e la loro robustezza, come già esposto al punto 7.

WORD® 2007		FORMATO DI FILE
Nome completo	WordProcessingML OOXML Extension	
Estensione/i	.docx, .dotx	
Specializzazione di	XML imbustato dentro ZIP	
Tipo MIME	application/vnd.openxmlformats-officedocument.wordprocessingml.document application/vnd.openxmlformats-officedocument.wordprocessingml.template	

Firmato digitalmente da ROBERTO FRACCIA

Sviluppato da	Microsoft Corporation; ISO; ECMA
Tipologia di standard	proprietario (libero), estendibile, *de facto*, *testuale*
Livello metadati	3
Derivato da	Office Open XML; Microsoft® *Word* ®
Revisione	11.1 (2018)
Riferimenti	• Microsoft, *Word extensions to OOXML (.docx) file format* v11.1 (2018) • officeopenxml.com, *Anatomy of a WordProcessingML file*
Conservazione	Sì, solo profilo Strict; cfr. §2.8
Racc. per la lettura	Generico con riconoscimento obbligatorio
Racc. per la scrittura	Vedasi capoversi 10 e 11 per la conservazione.

9. La suite di applicativi Microsoft® *Office*®, dalla versione 2007 in poi, utilizza un formato di file unico per i suoi applicativi principali, chiamato Open Office XML (OOML, descritto più genericamente in §2.5). Il formato consiste in un pacchetto di file, suddiviso in più cartelle, imbustato e compresso con un algoritmo ZIP e presentato come un unico file. I file all'interno del pacchetto compresso sono prevalentemente in formato XML e utilizzano il dialetto WordprocessingML, riservato ai documenti di videoscrittura elaborati dall'applicativo *Word*® per definire l'intera struttura e il contenuto del documento. Eventuali documenti allegati (p.es. immagini, video, audio o altri file) sono inseriti, all'interno di opportune cartelle, nel loro formato nativo. L'estensione del documento compresso per gli impaginati normali (*senza macro* attive) è .docx, mentre altri tipi di documenti (p.es. modelli di documento, impaginati con *macro* attive) sono indicati semplicemente con estensioni diverse.
10. Come per altri formati basati su OOXML, si consiglia la produzione di documenti con il profilo Strict, che è più restrittivo ma consente di eliminare alcune estensioni "proprietarie" che possono ridurre l'interoperabilità del formato stesso.
11. Il documento è adatto alla conservazione solo se:

- sono utilizzati esclusivamente caratteri tipografici "standard" (cfr. §2.8 capoverso 2),
- è privo di contenuti dinamici ad eccezione di campi compilabili o campi-firma,
- è privo di contenuti audiovisivi (suoni, video),
- eventuali immagini o altri contenuti multimediali sono contenute direttamente nel documento e non mediante collegamenti a file esterni al documento.

Si consiglia inoltre di effettuare un controllo sull'intera accessibilità del documento.

Firmato digitalmente da ROBERTO FRACCIA

MS-DOC	FORMATO DI FILE
Nome completo	Microsoft® *Word* ® Binary File Format
Estensione/i	.doc, .dot
Magic number	0xD0CF11E0A1B11AE1
Tipo MIME	application/msword
Sviluppato da	Microsoft Corporation
Tipologia di standard	proprietario (libero), estendibile, *de facto*, binario, deprecato
Livello metadati	3
Derivato da	Microsoft® Compound File Binary format; Corel® *WordPerfect*™
Revisione	8.1 (2018)
Riferimenti	• Microsoft, *[MS-DOC]: Word (.doc) binary file format* v8.1 (2018)
Conservazione	No; cfr. §2.8
Racc. per la lettura	Obbligatorio con riversamento raccomandato
Racc. per la scrittura	Sconsigliato

12. Il formato binario *Word*,® utilizzato come formato principale fino alle versione 2003 da codesto applicativo di videoscrittura, è una variante specializzata del formato Compound File Binary, proprietario di Microsoft Corporation (cfr. §2.5); utilizza l'estensione .doc per il documenti impaginati normale, e la cambia in caso di varianti, quali ad esempio i modelli di documento (estensione .dot). Il formato contiene in un unico file i metadati, i contenuti testuali, ipertestuali e gli allegati dell'impaginato, senza offrire efficaci meccanismi di controllo dell'integrità. Inoltre, le revisioni al documento vengono in generale salvate come modifiche differenziali in coda al file, contribuendo ad ingrandire la dimensione del file e, al tempo stesso, renderne più complessa l'apertura e l'interpretazione da parte degli applicativi di videoscrittura. Per questa mancanza di robustezza (soprattutto in caso di documenti di dimensioni molto grandi a causa di contenuti multimediali allegati), l'azienda proprietaria del formato decide di cambiare strategia, adottando un nuovo formato per tutti i documenti della suite applicativa *Office*,® a partire dalla versione 2007, anche se il "formato .doc" è pienamente supportato dalle nuove versioni. In caso di produzione di nuovi documenti impaginati tramite *Word*® si raccomanda l'uso del nuovo, sopra descritto formato basato su Open Office XML.

ODT	FORMATO CONTENITORE
Nome completo	Open Document Text
Estensione/i	.odt
Specializzazione di	XML imbustato dentro ZIP
Tipo MIME	application/vnd.oasis.opendocument.text
Sviluppato da	Organization for the Advancement of Structured Information Standards

Firmato digitalmente da ROBERTO FRACCIA

Tipologia di standard	aperto, estendibile, *de iure*, binario
Livello metadati	3
Derivato da	—
Revisione	1.2 (2015)
Riferimenti	Famiglia di standard **26300** della ISO/IEC: • ISO/IEC 26300-1:2015, *ODF for Office Applications v1.2 – Part 1: OpenDocument Schema* • ISO/IEC 26300-3:2015, *ODF for Office Applications v1.2 – Part 3: Packages* • OASIS, *Open Document Format for Office Applications (OpenDocument)*, v1.2 (2015)
Conservazione	Sì; cfr. §2.8
Racc. per la lettura	Generico con riconoscimento obbligatorio
Racc. per la scrittura	Fortemente raccomandato

13. Il formato OpenDocument Text (ODT) è una particolare implementazione del più generale formato OpenDocument (cfr. §2.5). Esso è il formato di default usato dall'applicazione di videoscrittura *Writer* della suite open source *LibreOffice*, ma è ampiamente supportato da molti altri applicativi di videoscrittura. Come per l'Open Office XML, anche tale formato è costituito da una busta compressa ZIP contenente un pacchetto di file che descrive la composizione del documento, cui componenti principali sono in formato XML.

RICHTEXT	FORMATO DI FILE
Nome completo	Rich Text Format
Estensione/i	.rtf
Magic number	{\rtf1
Tipo MIME	text/rtf, application/rtf
Sviluppato da	Microsoft
Tipologia di standard	proprietario (libero), *de facto*, binario, deprecato
Livello metadati	1
Derivato da	Rich-Text; Enriched Text
Revisione	1.9.1 (2008)
Riferimenti	• Microsoft, *Word 2007: Rich Text Format (RTF) Specification* v1.9.1 (2008) • RFC-1521
Conservazione	No; cfr. §2.8
Racc. per la lettura	Generico con riconoscimento consigliato
Racc. per la scrittura	Non raccomandato

Firmato digitalmente da ROBERTO FRACCIA

14. Rich Text Format (RTF) è un formato di proprietà di Microsoft utilizzato come formati interoperabile di documenti impaginati. Il formato supporta un numero molto ridotto di caratteristiche grafiche e tipografiche, e una possibilità limitata relativamente a ipertesti e allegati multimediali, a fronte di una semplicità strutturale conforme con lo scopo della sua introduzione. Nonostante sia ancora supportato dai principali applicativi di videoscrittura (inclusi quelli installati di default nei principali sistemi operativi), ma seguito della standardizzazione e apertura di formati ben più evoluti e completi (cfr. quelli basati su OOXML e OpenDocument) e, se ne sconsiglia l'uso per la produzione di nuovi documenti.

ePub	Formato di file
Nome completo	EPUB
Estensione/i	.epub
Specializzazione di	HTML, CSS, XML, SVG, … imbustati dentro ZIP
Tipo MIME	application/epub+zip
Sviluppato da	International Digital Publishing Forum
Tipologia di standard	aperto, estendibile, *de facto*
Livello metadati	3; cfr. §2.8
Derivato da	Open eBook publication structure; XHTML; CSS
Revisione	3.1 (2017)
Riferimenti	Famiglia di standard **30135** della ISO/IEC: • ISO/IEC 30135-1:2014, *EPUB Part 1: EPUB3 overview* • ISO/IEC 30135-3:2014, *EPUB Part 3:content documents* • ISO/IEC 30135-5:2014, *EPUB Part 5: media overlay* • www.idpf.org/epub
Conservazione	No; cfr. §2.8
Racc. per la lettura	Generico con riconoscimento consigliato
Racc. per la scrittura	Raccomandato nell'editoria digitale

15. Il formato EPUB è costituito da un pacchetto di file che descrivono, complessivamente, una documento paginato comprensivo dei suoi allegati multimediali, compressi con compressione ZIP in un unico file con estensione .epub. I documenti prediletti da questo formato si chiamano anche eBook, in quanto si prestano ad una visualizzazione prevalentemente elettroica su dispositivi con diverse

Firmato digitalmente da ROBERTO FRACCIA

capacità di visualizzazione grafica, anche notevolmente ridotta, come ad esempio *smartphone* e *tablet* (inclusi gli '*eBook reader*' specializzati).[11]
All'interno di questo pacchetto, i metadati interni del documento sono contenuti in file XML, il contenuto testuale in uno o più file HTML, le sue impostazioni tipografiche in uno o più file CSS, e gli eventuali elementi grafici in file immagini di vari formati aperti (PNG, SVG, ecc.). La versatilità grafica dell'*eBook* è ottentuta da questo formato sfruttando le caratteristiche di adattamento ed "elasticità" dei contenuti HTML dotati di opportuni "stili" CSS (cfr. §2.2) basati su profili di dispositivo apposito.

InDesignML	Formato di file
Nome completo	Adobe® *InDesign*® Markup Language
Estensione/i	.idml
Specializzazione di	XML imbustato dentro ZIP
Tipo MIME	application/x-indesign+xml
Sviluppato da	Adobe Systems
Tipologia di standard	proprietario (libero), *de facto*, testuale
Livello metadati	4
Derivato da	Adobe® *InDesign*® file format (.indd)
Revisione	8.0 (2012)
Riferimenti	• Adobe, *IDML File Format Specification*, v8.0 (2012) • Adobe, *InDesign*® Developer Documentation
Conservazione	No; cfr. §2.8
Racc. per la lettura	Specifico; non raccomandato se non in editoria digitale
Racc. per la scrittura	Specifico; raccomandato (al posto di .indd) nel settore dell'editoria digitale *InDesign*

16. Adobe® *InDesign*® è uno degli applicativi più diffusi per l'editing grafico, ma è un applicativo commerciale non aperto, come il formato nativo e binario per i suoi impaginati (estensione .indd). Tale formato è inoltre altamente instabile in quanto Adobe, che lo mantiene, lo cambia in continuazione da una variante all'altra del software. Per ridurre i rischi di interoperabilità dovuti all'estrema variabilità del formato nativo ".indd", Adobe ha introdotto una variante del formato basato su XML e chiamato *InDesign*® Markup Language (estensione .idml). Tale versione, oltre ad essere testuale ed estendibile, è anche parzialmente pubblicata sul sito Adobe, ed

[11] Ad esempio lo stesso *eBook* visualizzato su due dispositivi elettronici con display tecnicamente diversi (un '*e-paper*' monocromatico da 800×600 punti a 167dpi, rispetto a un LCD a colori da 1920×1080 — cfr. §2.6) potrebbe essere visualizzato con caratteri tipografici simili (magari di dimensioni diverse) e con una diversa distribuzione di caratteri su ogni linea allo scopo di rendere l'esperienza di lettura più agevole e la fruibilità più simile a quella di un libro su carta stampata.

Firmato digitalmente da ROBERTO FRACCIA

è perciò consigliato come il formato d'elezione –al posto del formato nativo– per tutte le organizzazioni che archivino impaginati creati con *InDesign*®.

POSTSCRIPT™	FORMATO DI FILE
Nome completo	PostScript®
Estensione/i	.ps
Magic number	%!PS
Tipo MIME	application/postscript
Sviluppato da	Adobe Systems
Tipologia di standard	proprietario (libero), *de facto*, binario, deprecato
Livello metadati	1
Derivato da	Lisp
Revisione	3 (1997)
Riferimenti	• Adobe, *PostScript® Language reference*, 3rd ed. (1999) • Adobe, *PostScript® Language reference supplement: Adobe® PostScript® 3™ version 3010 and 3011 Product Supplement*, 30 August 1999
Conservazione	No
Racc. per la lettura	Raccomandato per l'editoria digitale
Racc. per la scrittura	Sconsigliato

17. Il formato PostScript™ deve il suo nome all'omonimo linguaggio di descrizione di pagine professionale. Come per i formati contenenti codici scritti in un linguaggio di programmazione, questo formato di file contiene un elenco ordinato di istruzioni in tale linguaggio PostScript™ (linguaggio di tipo pseudo-binario) che, eseguite una dopo l'altra da una stampante o altro dispositivo capace di interpretarle, hanno come effetto la stampa di un documento esattamente identico. Il PostScript™ è stato per anni uno dei linguaggi di riferimento per il trasporto e la conservazione di documenti finalizzati alla stampa digitale, sia di tipo testuale che grafico. La versatilità del formato è anche parte del motivo per cui lo standard PDF è basato su PostScript™. Ai formati per la produzione di documenti impaginati o altri tipi di stampa digitale, è tuttavia richiesto di supportare anche ipertesti e contenuti non strettamente stampabili (suono, video ,ecc.), per i quali tale formato, risultando dunque inadeguato, diviene obsoleto. Nonostante la grande varietà di documenti attualmente presenti salvati in questo formato (per il quale la capacità di lettura è ancora fortemente raccomanda alle organizzazioni di settore tecnico-editoriale), si sconsiglia di produrne degli altri, preferendovi formati più moderni. Gli applicativi dedicati alla formazione del documenti in tali formati al posto del PostScript™, così come gli applicativi di riversamento dal PostScript™ in questi formati devono tuttavia essere adeguatamente configurati affinché i documenti mantengano le caratteristiche di riproducibilità e qualità che il formato PostScript™ garantisce per

Firmato digitalmente da ROBERTO FRACCIA

sua natura, permettendo al contempo di includere funzionalità moderne nel documento, quali contenuti ipertestuali e multimediali. Esempi di tali funzionalità sono la rappresentazione delle immagini in modalità vettoriale o, qualora le immagini siano di tipo raster, garantire qualità equivalente (ad esempio mediante algoritmi di compressione senza perdita); cfr. §2.6 e §2.7.

LaTeX	FORMATO DI FILE
Nome completo	LaTeX
Estensione/i	.tex
Specializzazione di	TeX
Tipo MIME	application/x-tex
Sviluppato da	comunità open source
Tipologia di standard	aperto (licenza LPPL), estendibile, *de facto*, testuale
Livello metadati	1
Derivato da	TeX
Revisione	2ε
Riferimenti	• www.latex-project.org • github.com/latex3 • ctan.org (Comprehensive TeX Archive Network)
Conservazione	No; cfr. §2.8
Racc. per la lettura	Specifico; raccomandato per testi tecnico-scientifici
Racc. per la scrittura	Specifico; nessuna raccomandazione

18. LaTeX è la specializzazione più comunemente più usata del linguaggio di impaginazione testi denominato TeX, inventato nel 1979 da Donald Knuth. La versione attualmente in uso è la 2ε (denominata LaTeX2ε). In realtà, l'albero "glottologico" del TeX comprende dialetti derivati direttamente dal linguaggio-madre TeX, così come dal LaTeX stesso, come ad esempio *AMS*-LaTeX.

Come suggerisce il nome stesso, LaTeX è particolarmente efficace per la produzione di pubblicazioni tecnico-scientifiche pronte per la stampa e conformi a norme redazionali e tipografiche professionali. Ciò che ne ha determinato particolare diffusione nella comunità scientifica internazionale (nonostante la sua obsolescenza rispetto sia a linguaggi per ipertesti più evoluti come l'XML e a formati di documenti impaginati "WYSIWYG",[12] che permettono una visualizzazione diretta dei contenuti) sta, in prima istanza, nella capacità –innata nel TeX e contemporaneamente potenziata e semplificata nel LaTeX– di descrivere complesse formule matematiche, la cui tipografia è rigorosamente rappresentata con leggibilità superiore ad applicativi di videoscrittura da "ufficio". Il linguaggio, di per sé, si limita

[12] Acronimo dall'inglese «*what you see is what you get*» (parafrasabile in «esattamente così come lo vedi»).

Firmato digitalmente da ROBERTO FRACCIA

a descrivere la distribuzione di testi e ipertesti (immagini, tabelle, formule/equazioni, bibliografia, note, così come i loro riferimenti) all'interno del documento, contornati da *tag* che si riferiscono a *template* esterni contenenti le regole stilistiche e tipografiche da rispettare (come ad esempio le fonti, cfr. §2.8). Il documento LaTeX è, in questo senso, analogo al codice sorgente di un linguaggio di programmazione o scripting (cfr. §2.15): ha bisogno di essere *compilato* per produrre un documento informatico consultabile e completamente impaginato, che si raccomanda sia prodotto sempre nel formato PDF o comunque –ove ciò non sia possibile– in uno dei formati raccomandati in questo paragrafo per la produzione di documenti impaginati.
È attualmente in sviluppo una revisione maggiore delle specifiche, denominata LaTeX3, che modifica diversi aspetti (sia dal punto di vista lessicale che grafico), allo scopo di attualizzare questo linguaggio e integrarlo con le tecnologie allo stato dell'arte nel campo della tipografia, dell'editoria e della multimedialità che, semplicemente, non esistevano negli anni '80 e la cui integrazione nel TeX e nei dialetti derivati è solo parzialmente avvenuta, non senza numerose difficoltà tecniche.

2.1.1 Raccomandazioni per la produzione di documenti

1. Il formato raccomandato per la produzione di documenti informatici in senso stretto (quindi, tra le altre cose, non più modificabili) il formato raccomandato è il PDF/A-1 per via della maggiore "superficie di interoperabilità"; il PDF in generale è comunque il formato più raccomandato per i documenti impaginati, inclusi quelli che devono rimanere parzialmente compilabili o commentabili (come i moduli delle procedure amministrative).
2. Le caratteristiche avanzate quali l'apposizione di firme e sigilli elettronici anche multipli (si veda il formato PAdES, §2.16), l'inclusione di documenti (anche in formati diversi) come *allegati* di un unico file PDF, l'inclusione di essenze multimediali e modelli bi- o tri-dimensionali manipolabili in tempo reale all'interno del documento, lo rendono particolarmente versatile in molteplici occasioni.
3. Per quanto riguarda i formati di documenti impaginati che possono essere revisionati e modificati, o dai quali si possono derivare altri documenti, si raccomanda siano prodotti in formato OpenDocument (.odt), interoperabilmente utilizzabile dai principali applicativi di videoscrittura e, laddove non sia possibile, nel formato OOXML (.docx), ma con profilo Strict. Nel caso di documenti semilavorati a carattere temporaneo e non definitivo è consigliabile anche l'utilizzo di formati

Firmato digitalmente da ROBERTO FRACCIA

puramente "virtuali" quali quelli delle suite collaborative di fornitori di servizi in Cloud qualificati.
4. Per applicazioni specifiche, come l'editoria, la grafica o le pubblicazioni tecnico-scientifiche, possono essere raccomandabili anche altri formati definiti in questa sezione purché, in fase di conservazione, si valuti sempre l'interoperabilità del documento finito (a scopo di distribuzione attraverso vari mezzi di comunicazione) e della sua sorgente così (come generata da applicativi di videoscrittura o altro), in quanto tali requisiti potrebbero portare a differenti raccomandazioni di formato.

2.2 Ipertesti

1. Rientrano in questa categoria tutti i documenti, prevalentemente testuali, che contengono ipertesti, quali ad esempio riferimenti ad oggetti esterni (di tipo URI, URL o altro), ovvero codici di *markup* per rappresentare digitalmente insieme astratti di dati e loro ontologie.

XML	FORMATO DI FILE
Nome completo	Extensible Markup Language
Estensione/i	.xml
Magic number	<?xml 0x20
Tipo MIME	application/xml, text/xml
Sviluppato da	World Wide Web Consortium
Tipologia di standard	aperto, estendibile, retrocompatibile, *de iure*, testuale
Livello metadati	4
Derivato da	SGML
Revisione	1.0, 5ª edizione
Riferimenti	• W3C Recommendation *XML 1.0 (5th Ed.)*, 2013 • www.w3.org/standards/xml • validator.w3.org
Conservazione	Sì, se conservato insieme a un *XML Schema*
Racc. per la lettura	Generico; subordinato ad eventuali, ulteriori obblighi o raccomandazioni di conformità con schemi/dialetti.
Racc. per la scrittura	Generico; subordinato ad eventuali, ulteriori obblighi o raccomandazioni di conformità con schemi/dialetti.

2. Il principale tipo di sintassi è costituito dall'*Extensible Markup Language* (XML), la cui caratteristica aggiuntiva è di essere facilmente *human readable*. L'XML è estendibile in quanto:

- possono essere definite in continuazione nuove etichette;

Firmato digitalmente da ROBERTO FRACCIA

- più dizionari di etichette possono essere usati con un approccio modulare all'interno del medesimo file XML mediante l'utilizzo dei *namespace* ("spazi di nomi") sui nomi delle etichette;
- è possibile definire, in XML stesso, sintassi specializzate mediante schemi (.xsd) o dialetti (.dtd);
- un medesimo documento XML (come file unico ovvero pacchetto costituito da più file XML) può essere logicamente composto da parti distinte, ciascuna delle quali utilizza etichette e regole sintattiche definite da diversi *namespace* o schemi, mentre le diverse parti possono referenziarsi l'un l'altra sfruttando diversi meccanismi sintattici (p.es. *XQuery* e *XPath*).

3. Numerosi formati di file oggetto del presente Allegato che utilizzano il linguaggio XML impiegano un dialetto specializzato al loro contenuto; essi sono:

- OpenDocument e Microsoft® OOXML (cfr. § 2.1 e §2.5),
- XHTML, XSD, XSL, XSLT, MathML (§2.2),
- SVG (§2.7),
- tutti i formati descritti in §2.14 (FatturaPA, CDA2, asserzione SPID, …),
- MusicXML (§2.9),
- IMSC1, TTML, e EBU-TT (§ 2.11)
- alcuni file obbligatori nei pacchetti IMF e DCP, nonché ACESclip (§2.12),
- KDM e firme elettroniche XAdES (§2.16).

4. ***Nota Bene***: Alcuni dei formati basati su XML sopraelencati mantengono l'estensione .xml del linguaggio madre, altri usano le proprie (e.g. .html/.htm, .svg, .ttml, .kdm). Si raccomanda che le Pubbliche Amministrazioni che producano documenti informatici in qualunque formato basato su XML non descritto dal presente Allegato ma che utilizzasse (in base alle proprie linee guida, specifiche tecniche, raccomandazioni o *best practices*) un'estensione "propria" diversa da .xml, laddove fosse consentito dall'uso applicativo delle applicazioni che elaborano file in tali formati, di "appendere" l'estensione .xml alla propria. Questo accorgimento manterrà ed esporrà l'estensione propria del formato a livello di UI, consentendo ai sistemi operativi privi di applicazioni specifiche per interpretare tali formati di aprire e visualizzare tali file come fossero normali file XML.
Esistono moltissime altre estensioni di XML che, pur non descritte qui, possono essere utilizzate e integrate in documenti XML per mezzo dell'estendibilità del *namespace*.

HTML	FORMATO DI FILE
Nome completo	Hypertext Markup Language
Estensione/i	.html, .htm
Magic number	<!DOCTYPE 0x20; <head>
Tipo MIME	text/html

Firmato digitalmente da ROBERTO FRACCIA

Sviluppato da	World Wide Web Consortium
Tipologia di standard	aperto, estendibile, *de iure*, testuale
Livello metadati	2
Derivato da	XML
Revisione	5.2
Riferimenti	• W3C Recommendation *HTML 5.2*, 2017 • validator.w3.org • W3C Recommendation *XML 1.0 (5th Ed.)*, 2013
Conservazione	Sì, se conservato insieme al/i CSS; cfr. §2.8
Racc. per la lettura	Generico con riconoscimento obbligatorio
Racc. per la scrittura	Specifico; raccomandato HTML5 per contenuti web

5. Un particolare dialetto di XML è HTML (ufficialmente codificato come XML puro a partire dalle sue versioni "XHTML" e "HTML5"), che serve a rappresentare il contenuto di pagine web. In questo caso HTML (.htm, .html) è affiancato dal CSS, linguaggio specifico per descrivere i fogli di stile che trasformano i componenti logici di una pagina in elementi grafici (la cosiddetta "presentazione" della pagina).
6. Il CSS può essere iniettato direttamente all'interno dell'HTML, oppure venire referenziato da esso in dei file esterni (estensione .css).
7. Sia XML, che HTML, che CSS sono tutti standard del W3C. Più in generale, una pagina web è un esempio di pacchetto di file (cfr. §1.1.2) costituito, come minimo, da un solo indice HTML, più eventualmente altri file in vari formati (anche non inclusi in questo Allegato), quali ad esempio HTML, CSS, WOFF, JavaScript, ecc.

XHTML	FORMATO DI FILE
Nome completo	Extensible Hypertext Markup Language
Estensione/i	.xhtml, .html
Specializzazione di	XML
Tipo MIME	application/xhtml+xml
Sviluppato da	World Wide Web Consortium
Tipologia di standard	aperto, estendibile, *de iure*, testuale
Livello metadati	2
Derivato da	HTML
Revisione	1.1
Riferimenti	• W3C Recommendation *XHTML™ Basic 1.1 (2nd Ed.)*, 2010 • W3C Recommendation *XHTML™ 1.0 (2nd Ed.)*, 2018 • validator.w3.org • W3C Recommendation *XML 1.0 (5th Ed.)*, 2013

Firmato digitalmente da ROBERTO FRACCIA

Conservazione	Solo se conservato insieme al/i CSS
Racc. per la lettura	Generico con obbligo di riconoscimento
Racc. per la scrittura	Specifico; raccomandato HTML5 per contenuti web

8. L'HTML, originariamente (e fino a HTML 4.01), non era una specializzazione di XML; prima di introdurre la versione 5, è stato fatto dal W3C un tentativo di standardizzazione intermedio che ha portato ad un'altra versione di HTML, chiamato XHTML (a sua volta ramificato in due dialetti distinti –*Strict* e *Transitional*– sono i più diffusi, e in diverse versioni). Data la sua diffusione tale linguaggio (che condivide le estensioni di file con le versioni ufficiali di HTML) è stato incluso in questo elenco.

XSD	FORMATO DI FILE
Nome completo	XML Schema Definition
Estensione/i	.xsd
Specializzazione di	XML
Tipo MIME	application/xml
Sviluppato da	World Wide Web Consortium
Tipologia di standard	aperto, estendibile, *de iure*, testuale
Livello metadati	4
Derivato da	XML
Revisione	2.0
Riferimenti	• W3C Recommendation *XSL Schema Part 0: Primer, 2nd Ed.*, 2004 • W3C Recommendation *XSL Schema Part 1: Structures, 2nd Ed.*, 2004 • W3C Recommendation *XSL Schema Part 1: Datatypes, 2nd Ed.*, 2004
Conservazione	Sì
Racc. per la lettura	Speciale; per la convalida di documenti in XML
Racc. per la scrittura	Speciale; per la condivisione di sintassi e dialetti XML

9. Questo formato è in grado di descrivere, sempre in linguaggio XML la sintassi e la grammatica associata ad un particolare schema, che esso stesso definisce. Un documento XML può perciò essere convalidato in maniera automatica rispetto ad un dato schema, per verificare se ne rispetta tutti i criteri sintattici. Analogamente, un file XSD può essere usato per produrre in XML una struttura di dati o, più in generale, una procedura. In entrambe i casi (convalida o produzione di un documento XML rispetto ad uno schema), questa architettura consente di riutilizzare lo stesso algoritmo o applicativo, ma con la flessibilità aggiuntiva di poter

Firmato digitalmente da ROBERTO FRACCIA

cambiare le regole sintattiche e grammaticali in automatico non appena viene cambiato lo schema di riferimento su file XSD.

XSL	FORMATO DI FILE
Nome completo	Extensible Stylesheet Language
Estensione/i	.xsl
Specializzazione di	XML (*namespace* xsl)
Tipo MIME	text/xsl
Sviluppato da	World Wide Web Consortium
Tipologia di standard	aperto, estendibile, *de iure*, testuale
Livello metadati	4
Derivato da	XML
Revisione	2.0
Riferimenti	• W3C Working Draft *XSL Requirements*, v2.0, 2008 • W3C Recommendation *XSL Requirements*, v1.1, 2006 • www.w3.org/Style/XSL/
Conservazione	Sì
Racc. per la lettura	Generale; raccomandato per la visualizzazione di XML
Racc. per la scrittura	Speciale; raccomandato per la costruzione di presentazioni grafiche di documenti in formato XML

10. Un documento esistente in formato XML può essere trasformato in un altro documento, sia esso in XML o in qualunque altro formato, specificando le regole di traduzione mediante trasformazioni descritte –sempre in linguaggio XML– e raccolte in:

- File per la descrizione del linguaggio di stile (in caso si tratti di un linguaggio diverso da XML) o del dialetto (in caso si tratti di una specializzazione di XML) — in XSL (.xsl).

XSLT	FORMATO DI FILE
Nome completo	Extensible Stylesheet Language Transformations
Estensione/i	.xslt
Specializzazione di	XML (*namespace* xsl)
Tipo MIME	application/xslt+xml, text/xml
Sviluppato da	World Wide Web Consortium
Tipologia di standard	aperto, estendibile, *de iure*, testuale
Livello metadati	3
Derivato da	DSSSL
Revisione	2.0

Firmato digitalmente da ROBERTO FRACCIA

Riferimenti	• W3C Recommendation *XSL Transformations (XSLT) v2.0*, 2007
Conservazione	Sì
Racc. per la lettura	Generale; raccomandato per la visualizzazione di XML
Racc. per la scrittura	Speciale; raccomandato per la costruzione di presentazioni grafiche di documenti in formato XML

- File per la descrizione delle trasformazioni del linguaggio di stile, che permette regole più complesse che, ad esempio, possono includere il traversamento della struttura XML del documento di partenza (tramite i sopracitati metodi *xQuery* e *xPath*) —XSLT (.xslt).

CSS	FORMATO DI FILE
Nome completo	Cascaded Style Sheet
Estensione/i	.css
Magic number	—
Tipo MIME	text/css
Sviluppato da	World Wide Web Consortium
Tipologia di standard	aperto, estendibile, *de iure*, testuale
Livello metadati	2
Derivato da	—
Revisione	3
Riferimenti	• W3C Recommendation *CSS 2.1 Specification*, 2011 • W3C Recommendation *CSS Basic User Interface module Level 3 (CSS3 UI)*, 2018 • W3C Recommendation *CSS Color module Level 3*, 2018 • W3C Recommendation *CSS Media Queries*, 2012 • validator.w3.org
Conservazione	Sì; cfr. §2.8
Racc. per la lettura	Generale; raccomandato per visualizzare pagine web
Racc. per la scrittura	Generale; raccomandato per la presentazione di documenti sotto format di pagine web

11. Il formato CSS effettua trasformazioni stilistiche di un documento HTML per permettere al suo contenuto di essere visualizzato graficamente, tramite un *web browser*, inclusi gli adattamenti "dinamici" del contenuto stesso. Una pagina web viene così rappresentata da vari file, tra i quali spiccano quelli delle seguenti due tipologie:

- il contenuto vero e proprio della pagina (testi, ipertesti e altri tipi di riferimenti ad altre pagine o contenuti), formato in HTML;

Firmato digitalmente da ROBERTO FRACCIA

- la "presentazione" dei suddetti contenuti, formata in CSS.

12. Possono esistere più documenti CSS che adattano il medesimo contenuto a dispositivi di visualizzazione (p.es. stampa, monitor a bassa risoluzione, monitor ad alta risoluzione, dispositivi touch-screen, dispositivi per contenuti accessibili di vario tipo, …), ovvero adattano più contenuti diversi uniformandone lo stile. La versione di linguaggio CSS da usare dipende dalla versione HTML del contenuto: si raccomanda CSS3 per HTML5, ovvero CSS2 per XHTML.

MARKDOWN	FORMATO DI FILE
Nome completo	Markdown
Estensione/i	.md
Magic number	–
Tipo MIME	text/markdown
Sviluppato da	John Gruber, Aaron Swarz
Tipologia di standard	aperto, estendibile, *de iure*, testuale
Livello metadati	2
Derivato da	–
Revisione	0.28 (2017)
Riferimenti	• RFC-7763, RFC-7764 • spec.commonmark.org
Conservazione	Sì, se conservato insieme agli oggetti da esso riferiti
Racc. per la lettura	Generale; raccomandato per produzione di testi e ipertesti pubblicati online
Racc. per la scrittura	Generale; raccomandato per produzione di testi e ipertesti pubblicati online

13. *Markdown* ("md") è un linguaggio di markup pensato per scrivere contenuti testuali insieme ad una limitata quantità di ipertesti e di capacità "presentazionali". La sintassi semplificata del markdown è pensata per rendere il contenuto di un ipertesto accessibile e traducibile, in automatico, in linguaggi e sintassi che ne permettono un'adeguata presentazione e trasmissione, come ad esempio HTML, EPUB, OOXML, PDF o altro. Nella previsione che sempre più servizi delle PP.AA. saranno prodotti e accessibili online, il markdown si configura dunque come il linguaggio d'elezione per l'archiviazione a breve e lungo termine di questi contenuti, che sono perciò resi indipendenti dalla pagina web o dal file ove possano temporaneamente essere rappresentati. Gli ipertesti in markdown si prestano ad essere conservati, nella loro sintassi originale, sia all'interno di basi di dati generiche (cfr. §2.3) che in documenti informatici indipendenti, sottoforma di file con estensione .md.

Firmato digitalmente da ROBERTO FRACCIA

MATHML	FORMATO DI FILE
Nome completo	MathML
Estensione/i	.mml, .xml
Specializzazione di	XML
Tipo MIME	text/mathml, text/mathml-renderer[*]
Sviluppato da	World Wide Web Consortium
Tipologia di standard	aperto, estendibile, *de iure*, testuale
Livello metadati	4
Derivato da	XML
Revisione	3.0 (2014)
Riferimenti	• ISO/IEC 40314:2016, *MathML version 3.0, 2nd Ed.* • W3C Recommendation *MathML version 3.0, 2nd Ed.*, 2014 • W3C *Math Home*
Conservazione	Sì; cfr. §2.8
Racc. per la lettura	Speciale; obbligatorio per testi tecnico-scientifici basati su XML
Racc. per la scrittura	Speciale; fortemente raccomandato per testi tecnico-scientifici; obbligatorio per quelli basati su XML

14. MathML è un dialetto di XML adatto alla rappresentazione di formule matematiche generiche; tale estensione di XML viene dunque utilizzata per testi scientifici in qualsivoglia documento informatico basato su XML, suoi dialetti (e.g. XHTML) o linguaggi "imparentati" (e.g. HTML).

2.2.1 Raccomandazioni per la produzione di documenti

1. Si raccomanda di usare per gli ipertesti i formati più aperti, interoperabili e indipendenti dall'applicativo utilizzato, come ad esempio l'XML (con i suoi dialetti) e il markdown. Nel caso specifico di documenti destinati ad uso tramite internet o intranet, la scelta ricadrebbe naturalmente sulle versioni più recenti di HTML (HTML5) e XHTML, anche se tali linguaggi da un lato mantengono una dipendenza dal formato del documento ("pagina web"), dall'altro sono largamente dipendenti –per la loro visualizzazione– da altri file che ne descrivono la rappresentazione grafica (e.g. stili XSLT/XSLT e fogli di sitel CSS). Si invita dunque ad una scelta adeguata alle finalità del documento.
2. I documenti in formato XML sono adatti alla conservazione soltanto se accompagnati dal loro schema XML (XSD). Le pagine web possono essere mandate

Firmato digitalmente da ROBERTO FRACCIA

in conservazione soltanto quando completamente statiche, combinando il "contenuto vero e proprio" in formato HTML (incluso XHTML), con la parte "presentazionale" in formato CSS. Le pagine web con contenuto dinamico (ad esempio codice JavaScript lato client) non sono adatte alla conservazione a meno di non conservare l'intero contenuto JavaScript (incluse le librerie eventualmente richiamate – cfr. §2.15) che, a sua volta, non deve riferirsi esternamente ad alcun altro documento.

2.3 Dati strutturati

1. In questa sezione si descrivono brevemente alcuni formati dedicati al trasporto di dati strutturati, intendendo con questa accezione riferirsi a formati ove la tipologica di contenuto non è predeterminata a propri. Esempi di applicazioni che fanno uso di dati strutturati sono le basi di dati (per le quali rappresentno qui i formati SQL e quelli relativi all'applicativo Microsoft® *Access*®). Si sottolinea che l'adeguatezza di una base di dati alla normativa vigente in materia di protezione dei dati personali (p.es. pseudonimìa) e privacy può essere indipendente dal formato di file adottato, mentre è fortemente caratterizzata dai criteri architetturali adottati durante la fase progettuale.

SQL	FORMATO DI FILE
Nome completo	Structured Query Language
Estensione/i	.sql
Specializzazione di	Datalog query language
Tipo MIME	application/sql
Sviluppato da	International Organization for Standardization
Tipologia di standard	aperto, estendibile, *de iure*, testuale
Livello metadati	4
Derivato da	Datalog
Revisione	SQL:2016
Riferimenti	• RFC-6922 Famiglia di standard **9075** della ISO/IEC: • ISO/IEC 9075-1:2016, *SQL Part 1 – framework*
Conservazione	Sì
Racc. per la lettura	Speciale; raccomandato per basi di dati relazionali
Racc. per la scrittura	Speciale; raccomandato per basi di dati relazionali

Firmato digitalmente da ROBERTO FRACCIA

2. I file SQL servono a contenere configurazioni e tabelle per basi di dati relazionali, complete o parziali, sotto forma del loro linguaggio di programmazione comune. Ogni file SQL descrive la formazione della base di dati, "da zero" o a partire da una base supposta già esistente: fornendo un tale file ad un gestore di basi di dati vengono perciò costituite le sue tabelle. Vice versa, una o più tabelle possono essere archiviate effettuandone uno "scarico" (*dump* in inglese) in un file SQL che descrive come il contenuto dello scarico può essere formato, da zero, in un nuovo gestore di basi di dati che interpreti il medesimo linguaggio. A tale scopo bisogna dunque specificare che SQL è in realtà un ceppo linguistico, da cui sono derivati molteplici dialetti di SQL, differenziati a seconda dell'applicativo –commerciale o meno– che funge da gestore di basi di dati. Si raccomanda quindi, per l'archiviazione a lungo termine e l'interscambio, di utilizzare sempre il formato SQL standardizzato dalla ISO (e riportato in tabella).
3. Ove non possibile, va sempre indicata la versione esatta del linguaggio SQL adottato, incluso preferenzialmente il nome e la versione completa dell'applicativo di gestione (MySQL, Microsoft® SQL™, ecc.).

Access® 2007	Formato di file
Nome completo	Microsoft® *Access* ® Connectivity Engine
Estensione/i	.accdb
Magic number	0x00010000 Standard ACE DB
Tipo MIME	application/msaccess
Sviluppato da	Microsoft Corporation
Tipologia di standard	proprietario (chiuso), *de facto*, binario
Livello metadati	3
Derivato da	MS-MDB
Revisione	2017
Riferimenti	• Microsoft, *Which* Access® *file format should I use?* – the .accdb file format (2019)
Conservazione	No
Racc. per la lettura	Speciale; raccomandato per piccole basi di dati
Racc. per la scrittura	Speciale; sconsigliato

4. Il formato proprietario usato da Microsoft per il suo gestore di basi di dati *Access*®, a partire dalla versione 2007, permette di archiviare non soltanto tabelle, ma anche righe di codice SQL e dati nonstrutturati. Tuttavia, esseno il formato proprietario e a sorgente chiusa, viene elencato qui in caso vi siano organizzazioni con basi di dati basati sugli applicativi Microsoft, affinché migrino i dati un un formato non proprietario ovvero, qualora non altrimenti possibile, dal vecchio formato .mdb (si legga più avanti) a quello attuale .accdb.

Firmato digitalmente da ROBERTO FRACCIA

MS-MDB	FORMATO DI FILE
Nome completo	Microsoft® *Access*® Binary file format
Estensione/i	.mdb
Magic number	0x00010000 Standard Jet DB
Tipo MIME	application/msaccess
Sviluppato da	Microsoft Corporation
Tipologia di standard	proprietario (chiuso), *de facto*, deprecato, binario
Livello metadati	3
Derivato da	–
Revisione	2017
Riferimenti	• Microsoft, *Which* Access® *file format should I use?* – the .mdb file format (2019)
Conservazione	No
Racc. per la lettura	Generico; valutare riversamento in formato aperto
Racc. per la scrittura	Sconsigliato; valutare un riversamento in altro formato

5. Il formato proprietario MDB è stato usato in precedenza da Microsoft per il suo gestore di basi di dati *Access*,® fino alla versione 2003. È ora un formato deprecato.

ODB	FORMATO CONTENITORE
Nome completo	Open Document Format for Database
Estensione/i	.odb
Specializzazione di	XML imbustato dentro ZIP
Tipo MIME	application/vnd.oasis.opendocument.[data]base
Sviluppato da	Organization for the Advancement of Structured Information Standards
Tipologia di standard	aperto, estendibile, *de iure*, binario, deprecato
Livello metadati	3
Derivato da	–
Revisione	1.2 (2015)
Riferimenti	Famiglia di standard **26300** della ISO/IEC. • OASIS, *Open Document Format for Office Applications (OpenDocument)*, v1.2 (2015)
Conservazione	No
Racc. per la lettura	Generico; raccomandato solo a scopo di riversamento
Racc. per la scrittura	Sconsigliato; valutare riversamento in altro formato

6. Specializzazione del formato OpenDocument per la rappresentazione di basi di dati, ODP è un formato deprecato e va perciò evitata la produzione di nuovi file;

Firmato digitalmente da ROBERTO FRACCIA

inoltre, si consiglia di valutare il riversamento di basi di dati preesistenti in questo formato.

JSON	FORMATO DI FILE
Nome completo	JavaScript Object Notation
Estensione/i	.json
Specializzazione di	JavaScript
Tipo MIME	application/json
Sviluppato da	dominio pubblico
Tipologia di standard	aperto, estendibile, *de iure*, testuale
Livello metadati	4
Derivato da	JavaScript
Revisione	2018
Riferimenti	• RFC-8259 • ECMA-404 • json.org • ISO/IEC 8825-8:2018, *ASN.1 encoding rules, part 8: JSON*
Conservazione	Sì, se adottato insieme a uno schema JSON
Racc. per la lettura	Generico; obbligatorio; eventualmente subordinato a ulteriori obblighi di conformità con determinati schemi.
Racc. per la scrittura	Fortemente raccomandato per documenti contenenti dati sia strutturati che non strutturati; eventualmente subordinato a ulteriori obblighi di conformità con determinati schemi.

7. Il formato *JavaScript Object Notation* (JSON) è un altro formato estremamente versatile ed estendibile che, come XML, è usato in moltissimi ambiti informatici e viene dunque impiegato per svariate applicazioni. Come definito nello standard RFC-8259 del 2018, in un file JSON le evidenze informatiche sono rappresentate gerarchicamente in più livelli:

- Ogni livello (compresa la "radice") è delimitato da parentesi graffe '{' e '}'.
- In ogni livello, ogni elemento (tranne l'ultimo) è separato dal successivo da una virgola ','.
- Ogni elemento è costituito da una coppia nome–valore, separati fra loro da due punti ':', ove il nome è sempre una stringa (delimitata da virgolette '"') e il valore può essere:
  - anch'esso una stringa (delimitata da virgolette '"');
  - un numero intero o in virgola mobile[13];

[13] Sono ammessi segni '+' e '-', punto decimale '.' e un numero arbitrario di cifre, ma non notazioni scientifiche (e.g. quella esponenziale).

Firmato digitalmente da ROBERTO FRACCIA

- un booleano rappresentato dalle parole chiavi ‘true’ ovvero ‘false’;
- un *array* di valori, delimitato da parentesi quadre ‘[’ e ‘]’, separati (tranne l’ultimo) da virgole ‘,’ e con ciascun valore essendo di un qualsiasi tipo in questo elenco,
- un oggetto JSON (cioè sottolivello di questa medesima struttura);
- un tipo di dato che non indica nulla, rappresentato dalla parola chiave ‘null’.

- Tra i caratteri di delimitazione[14] sopra elencati, possono essere aggiunti un qualsivoglia numero di caratteri di spaziatura e interruzione di linea (soprattutto nella rappresentazione di tale struttura dati in un file), ottenendo un’equivalenza del medesimo contenuto.
- L’ordine degli elementi al medesimo livello di un *array* o di una struttura JSON è indifferente.

8. Un esempio di documento informatico rappresentato in formato JSON è dato dal seguente elenco di attributi di identificazione elettronica:

```
{
    "id":"cae8877c-e533-4d8a-9f38-d7f219392b1f",
    "firstName":"Mario",
    "lastName":"Rossi",
    "fiscalCode":"RSSMRA75L01H501A",
    "phoneNum":["+393201234567","+393398901234"],
    "children":[
        "id":"cae8877c-e533-4d8a-9f38-d7f219392b1f",
        "firstName":"Luigi",
        "lastName":"Bianchi",
        "fiscalCode":"RSSMRA75L01H501A",
        "phoneNum":["+393332468013"],
        "children":[
            .....
        ],
        "alive?":true
    ],
    "alive?":no
}
```

9. Un vantaggio di JSON rispetto a XML è la semplicità della sintassi che, pur non offrendo capacità avanzate quali i *namespace* o la possibilità di “attraversare” la struttura ad albero (offerte da XML), dispone di una struttura più semplice da interpretare –soprattutto da parte di processi automatici– senza perdere la caratteristica fondamentale della leggibilità da parte dell’uomo. Un impiego particolare di JSON è in alcuni tipi di basi di dati che necessitano uno scambio di tabelle potenzialmente grandi e complesse ma non necessariamente relazionate fra

[14] Indicati, in questo elenco e come al solito nell’Allegato, mediante caratteri a spaziatura fissa.

Firmato digitalmente da ROBERTO FRACCIA

loro: in tali casi viene solitamente considerata una rappresentazione di interscambio mediante JSON piuttosto che i formati nativi dei altri tipi di basi di dati (p.es. SQL). Un'ulteriore caratteristica del JSON nel rappresentare basi di dati è che ogni dato può avere una struttura completamente diversa dagli altri; per questo motivo tale formato è ideale per l'archiviazione l'elaborazione, in automatico, di dati cosiddetti "non strutturati".

JSON-LD	FORMATO DI FILE
Nome completo	JavaScript Object Notation for Linked Data
Estensione/i	.jsonld
Specializzazione di	JSON
Tipo MIME	application/ld+json
Sviluppato da	dominio pubblico
Tipologia di standard	aperto, estendibile, *de iure*, testuale
Livello metadati	2
Derivato da	JavaScript
Revisione	2014
Riferimenti	• W3C Recommendation *JSON-LD 1.0*, 2014 • W3C Recommendation *JSON-LD 1.0 Processing Algorithms and API*, 2014
Conservazione	Sì
Racc. per la lettura	Generico; obbligatorio; eventualmente subordinato ad obblighi di conformità a schemi.
Racc. per la scrittura	Fortemente raccomandato per documenti contenenti Open Data generati con procedure automatizzate

10. Un particolare dialetto di JSON è costituito da JSON-LD, che segue una sintassi più rigida organizzata per poter gestire dati strutturati e collegati fra loro da relazioni astratte il più generiche possibili. Nell'ambito delle PP.AA., ad esempio, l'utilizzo di questo formato è –al pari di altri contenuti in questo Allegato– fortemente consigliato per la generazione di Open Data, particolarmente attraverso procedure automatizzate.

CSV	FORMATO DI FILE
Nome completo	Comma-Separated Value
Estensione/i	.csv
Magic number	–
Tipo MIME	text/csv
Sviluppato da	dominio pubblico
Tipologia di standard	aperto, estendibile, *de iure*, testuale
Livello metadati	1
Derivato da	tabelle preformattate in FORTRAN77

Firmato digitalmente da ROBERTO FRACCIA

Revisione	2005
Riferimenti	• RFC-4180 • RFC-7111 • W3C Recommendation *Model for tabular data and metadata on the Web*, 2015 • dati.gov.it
Conservazione	Sì
Racc. per la lettura	Generale; obbligatorio
Racc. per la scrittura	Raccomandato per documenti contenenti dati strutturati leggibili dall'uomo (inclusi gli Open Data)

11. Uno dei formati più semplici per la rappresentazione di dati *fortemente* strutturati è il CSV che è un file testuale ove i dati sono rappresentati in una tabella:

- Ogni riga della tabella è una linea del file, delimitata da un'opportuna evidenza di fine linea.
- Le colonne, all'interno di ogni linea, si distinguono perché delimitate da caratteri specifici (ad esempio la virgola ',' che da il nome al formato, ma sono possibili anche altre combinazioni di caratteri di interpunzione o di spaziatura).
- Opzionalmente, la prima linea del file (indicata con un carattere iniziale particolare e con la medesima distinzione in colonne del resto delle linee) costituisce una legenda circa il significato dei valori delle colonne.

12. Il formato CSV è uno dei formati d'elezione per la rappresentazione degli Open Data, il cui archivio nazionale per i dati aperti pubblici è dati.gov.it.

JWT	CODEC
Nome completo	JSON Web Token
Estensione/i	–
Specializzazione di	JSON
Tipo MIME	application/jwt
Sviluppato da	pubblico dominio
Tipologia di standard	aperto, estendibile, *de iure*, binario
Derivato da	JSON
Revisione	2016
Riferimenti	• RFC-7797 • jwt.io • ISO/IEC 29500-6:2017 • RFC-7515 • RFC-7516
Conservazione	Sì, se da JSON-LD o conservato insieme a schema
Racc. per la lettura	Speciale; consigliato per flussi digitali in richieste POST

Firmato digitalmente da ROBERTO FRACCIA

Racc. per la scrittura	Speciale; consigliato per flussi digitali in richieste POST

13. Il *JSON Web Token* (JWT), definito dall'RFC-7797, è un codec[15] utilizzato per documenti informatici già organizzati in una struttura JSON; tale codifica ottimizza la dimensione dell'evidenza informatica e consente di trasferirla come un flusso digitale (cfr. §1.1.1) in tempo reale o attraverso un canale che permette un insieme limitato di caratteri — ad esempio inserendo l'evidenza in richieste HTTP di tipo POST. Il JWT (analogamente al JSON-LD) richiede che nella struttura JSON testuale possano essere presenti alcuni elementi, facoltativi ma dal significato predefinito, che semplificano il trasporto e la decodifica dell'evidenza JWT stessa.
Lo standard JWT include un sistema di controllo della propria integrità e può, facoltativamente, essere accompagnato da cifratura (per la confidenzialità), da apposizione di firma o sigillo elettronico nel pacchetto, o da entrambe. Le evidenze informatiche JWT firmate sono, impropriamente, chiamate *JSON Web Signature* (JWS) e definite nell'RFC-7515; le evidenze informatiche JWT cifrate sono, impropriamente, chiamate *JSON Web Encryption* (JWE) e definite nell'RFC-7516.

OOXML	Formato contenitore
Nome completo	Office Open XML
Estensione/i	.docx, .xlsx, .pptx, …
Specializzazione di	XML imbustato dentro ZIP
Tipo MIME	–
Sviluppato da	Microsoft Corporation
Tipologia di standard	aperto, estendibile, *de iure*, testuale
Livello metadati	4; cfr. §2.8
Derivato da	OpenXML; Microsoft® COM Structured Storage
Revisione	12.0 (2019)
Riferimenti	• ISO/IEC 29500-1:2016, *fundamentals and markup language reference* • ISO/IEC 29500-2:2012, *open packaging conventions* • ISO/IEC 29500-3:2015, *markup compatibility and extensibility* • ISO/IEC 29500-4:2016, *transitional migration features* • ECMA-376: *Office Open XML File Formats*, 5th ed., 2016 • officeopenxml.com
Conservazione	Sì, solo profilo Strict; cfr. §2.8
Racc. per la lettura	–

[15] Per la precisione, la codifica binaria è ottenuta mediante algoritmo *Base64*, specificato in RFC-4648.

Firmato digitalmente da ROBERTO FRACCIA

Racc. per la scrittura	–

14. Vengono elencati due formati contenitore utilizzati dalle principali suite di applicativi per ufficio: Microsoft® *Office*® e *LibreOffice*. Tali buste contengono in realtà un pacchetto di file che rappresenta, complessivamente, un documento informatico (testo impaginato, foglio di calcolo, presentazione, basi di dati, contenuto multimediale, o altro) mediante più file strutturati in un filesystem virtuale, con gerarchie di cartelle predeterminate. Il pacchetto, una volta formato in memoria, viene poi compresso in un unico file mediate algoritmi noti (tra quelli elencati in §2.13), o loro varianti. I file contenuti nel pacchetto descrivono sia i metadati interni del documento, che parte del documento informatico stesso: ad esempio testi, collegamenti ipertestuale e la loro rappresentazione grafica (impaginazione, colore, tipografia, ecc.) e sono tipicamente in formato XML. Eventuali contenuti ipertestuali (pagine web, immagini, suono, video, contenitori crittografici ecc.) sono rappresentati da file in altri formati –tipicamente aperti o proprietari ma liberi– (HTML, PNG, WAV, PEM, ecc.) a seconda della necessità. Il pacchetto di file viene di solito formato e archiviato nello storage soltanto previa compressione in un unico file, mentre al caricamento da parte di un applicativo viene scompattato in memoria. La strutturazione in un pacchetto di file consente una migliore gestione del documento particolarmente nei casi di dimensioni elevate del file: una lieve modifica parziale di un documento informatico molto grande comporta la modifica di un sottoinsieme di file costituenti il pacchetto, non di tutti, perciò lo sforzo computazionale si riduce, così come i rischi di corruzione dell'intero file in caso di problemi durante la scrittura di file così grandi.

15. *Office Open XML*[16] (*OOXML*) è il contenitore generico utilizzato prevalentemente dalle versioni più recenti (dalla 2007 in poi) della suite applicativa Microsoft® *Office*® che si specializza a seconda della tipologia di documento da contenere (e di applicativo della suite). Un documento in formato OOXML è in realtà costituito da un pacchetto di file che sono poi compressi in un'unica busta ZIP (cfr. §2.13), rinominata con estensione differente a seconda della specializzazione.
16. In questo Allegato sono descritte tre specializzazioni di OOXML ai documenti impaginati (.docx, §2.1), ai fogli di calcolo e alle presentazioni multimediali (rispettivamente .xlsx e .pptx, §2.5)

[16] Da non confondersi con *OpenOffice.org XML* — formato simile utilizzato da versioni obsolete dell'omonima suite applicativa.

Firmato digitalmente da ROBERTO FRACCIA

OPENDOCUMENT	FORMATO CONTENITORE
Nome completo	Open Document Format for Office Applications
Estensione/i	.odt, .ods, .odp, .odg, .odi, .odf
Specializzazione di	XML imbustato dentro ZIP
Tipo MIME	–
Sviluppato da	Organization for the Advancement of Structured Information Standards
Tipologia di standard	aperto, estendibile, *de iure*, binario
Livello metadati	4
Derivato da	–
Revisione	1.2 (2015)
Riferimenti	Famiglia di standard **26300** della ISO/IEC: • ISO/IEC 26300-1:2015, *ODF for Office Applications v1.2 – Part 1: OpenDocument Schema* • ISO/IEC 26300-3:2015, *ODF for Office Applications v1.2 – Part 3: Packages* • OASIS, *Open Document Format for Office Applications (OpenDocument)*, v1.2 (2015)
Conservazione	Sì; cfr. §2.8
Racc. per la lettura	–
Racc. per la scrittura	–

17. OOXML è dotato di vari "profili", che possono essere più o meno interoperabili. Per tutti i documenti della P.A., si consiglia perciò il profilo Strict, che è più restrittivo, ma consente di eliminare alcune estensioni "proprietarie" che possono ridurre l'interoperabilità dei formati.

18. Come per OOXML, anche OpenDocument è un contenitore generico di quelli sopraelencati, per archiviare documenti prodotti da suite applicative open source — prima fra tutte *LibreOffice*.

In questo allegato sono descritte alcune specializzazioni di OpenDocument ai documenti impaginati (.odt, §2.1), ai fogli di calcolo e alle presentazioni multimediali (rispettivamente .ods e .odp, §2.5), ai

CFB	FORMATO CONTENITORE
Nome completo	Compound File Binary file format
Estensione/i	.doc, .xls, .ppt, .pst; .aaf, …
Magic number	0xD0CF11E0A1B11AE1
Tipo MIME	–
Sviluppato da	Microsoft Corporation
Tipologia di standard	proprietario, estendibile, *de facto*, binario, deprecato

Firmato digitalmente da ROBERTO FRACCIA

Livello metadati	–
Derivato da	Microsoft® COM Structured Storage
Revisione	9.0 (2018)
Riferimenti	• Microsoft, *[MSD-CFB]: Compound File Binary file format* v9.0 (2018)
Conservazione	No; cfr. §2.8
Racc. per la lettura	–
Racc. per la scrittura	–

19. CFB è invece il contenitore di file su cui Microsoft® si è basata per le versioni obsolete della suite *Office*® (cfr. § 2.1 e §2.5). È anche il formato contenitore da cui deriva AAF (cfr. §2.12). Il formato CFB rappresenta all'interno un pacchetto di file organizzati in un filesystem virtuale vagamento ispirato al FAT[17] (anziché in un archivio compresso come fanno altri formati). Una delle principali problematiche del CFB, soprattutto nel caso di documenti informatici di grandi dimensioni, è ereditata proprio dal FAT, essendo caratterizzato dall'estrema facilità con file contenuti del pacchetto soffrono di frammentazione interna. Ad un livello più superficiale, ogni applicativo della suite Microsoft® *Office*® versione '2003' o antecedenti utilizza una propria serie ti tipi di file, dotati di estensioni differenti (p.es. .doc, .xls, .ppt, …, cfr. §1.1.2), ma tutti basati su CFB;[18] a partire dalla versione '2007' la suite ha abbandonato i formati basati su CFB in favore di quelli basati su OOXML (Office Open XML), producendo nuovi formati, stavolta strutturalmente differenti ma gemellati ai precedenti per via delle estensioni di file, ottenute quasi sempre aggiungendo una semplice 'x': .docx, .xlsx, .pptx, ….

2.3.1 Raccomandazioni per la produzione di documenti

1. La scelta dei formati di file per conservare dati strutturati quali grandi e piccole basi di dati è soggetta non soltanto alla tipologia dei dati "a riposo", ma anche agli

[17] Acronimo di *File Allocation Table*, dal nome dell'evidenza informatica, contenuta (o replicata più volte) in dispositivo di storage a blocchi inizializzato con tale filesystem, per indicizzarne tutti i file contenuti e i loro metadati esterni (cfr. §1.1.2). Esistono diversi filesystem basati su FAT — alcuni aperti (FAT16, FAT32), altri coperti da licenze d'uso di proprietà di Microsoft Corporation (exFAT). Per ulteriori dettagli consultare it.wikipedia.org/wiki/File_Allocation_Table e i collegamenti ipertestuali ivi contenuti.

[18] A ciascuno di tali formati si affiancano delle varianti, strutturalmente identiche, per rappresentare specializzazioni dei medesimi documenti, quali ad esempio i "modelli di documento" (*template*, in inglese), per i quali cambia solo l'estensione del file (tipicamente una 't' in sostituzione dell'ultimo carattere: p.es. .dot e .xlt).

Firmato digitalmente da ROBERTO FRACCIA

aspetti "dinamici" legati alla loro generazione e riutilizzo. Sono perciò coinvolti aspetti fortemente quantitativi sui dati, quali:

- dimensione informatica delle evidenze "a riposo",
- capacità dei flussi informatici "in transito" (banda richiesta e sue variazioni statistiche in base alla distribuzione geografica e cronologica, valutata su più scale di grandezza e indici statistici);
- previsioni sul ciclo di vita (generazione, modifiche, trasporto, archiviazione, distruzione);
- considerazioni in merito a conservazione e interoperabilità in generale (a livello europeo e nazionale);
- considerazioni in merito alla protezione dei dati, con particolare riferimento a:
  - dati personali e privacy: cfr. Regolamento (UE) Nº 679/2016 ("GDPR") del Parlamento europeo e del Consiglio e il D.Lgs. 101/2018;
  - trattamento da parte di infrastrutture critiche e fornitori di servizi essenziali: cfr. il D.Lgs. 65/2018 e la Direttiva (UE) Nº 1148/2016 ("NIS") da esso recepita.

2. Si raccomanda perciò alle PP.AA. di effettuare un'adeguata valutazione di interoperabilità, che tenga in considerazione anche dei sopracitati aspetti.

2.4 Posta elettronica

EML	FORMATO DI FILE
Nome completo	Electronic Mail Format
Estensione/i	.eml
Magic number	–
Tipo MIME	application/email
Sviluppato da	comunità open source
Tipologia di standard	aperto, estendibile, *de facto*, testuale
Livello metadati	1
Derivato da	RFC-822
Revisione	2008
Riferimenti	• RFC-5322 • RFC-2822 • US Library of Congress, *Email (EMF)* (2014)
Conservazione	Sì; cfr. §2.8

Firmato digitalmente da ROBERTO FRACCIA

Racc. per la lettura	Generico; obbligatorio per singoli messaggi email
Racc. per la scrittura	Generico; obbligato per singoli messaggi email

1. Il formato EML rappresenta interamente l'evidenza informatica costituente un singolo messaggio di posta elettronica MIME, così come definito negli standard RFC-5322 e RFC-2822.

MBOX	FORMATO CONTENITORE
Nome completo	"default" *mbox* database format
Estensione/i	.mbox
Specializzazione di	EML
Tipo MIME	application/mbox
Sviluppato da	comunità open source
Tipologia di standard	aperto, estendibile, *de facto*, testuale
Livello metadati	3
Derivato da	sistema operativo UNIX
Revisione	2005
Riferimenti	• RFC-4155 • RFC-2822 • en.wikipedia.org/wiki/Mbox
Conservazione	Sì; cfr. §2.8
Racc. per la lettura	Generico; raccomandato per caselle di messaggi email
Racc. per la scrittura	Generico; raccomandato per caselle di messaggi email

2. Così come EML rappresenta, integralmente un singolo messaggio di posta elettronica, il formato MBOX può usarsi per contenervi diversi messaggi di posta elettronica, organizzati su più livelli.

MS-PST	FORMATO DI FILE
Nome completo	Microsoft® *Outlook*® Personal Folder file
Estensione/i	.pst
Magic number	0xD0CF11E0A1B11AE1
Tipo MIME	application/vnd.ms-outlook
Sviluppato da	Microsoft Corporation
Tipologia di standard	proprietario (libero), estendibile, *de facto*, binario
Livello metadati	3
Derivato da	Microsoft® Compound File binary format
Revisione	7.0 (2018)
Riferimenti	• Microsoft, *[MS-PST]: Outlook Personal Folders (.pst) file format* v7.0 (2018)
Conservazione	No; cfr. §2.8

Firmato digitalmente da ROBERTO FRACCIA

Racc. per la lettura	Generico; raccomandato per importare rubriche, ecc.
Racc. per la scrittura	Specifico; raccomandata migrazione dell'applicativo e, successivamente, dell'intero formato

3. Il formato proprietario usato in Microsoft® *Outlook*® (applicativo di rubrica messaggi e contatti) è un'alternativa al formato MBOX per memorizzare non soltanto intere caselle di posta (a loro volta strutturabili in sottocartelle), ma anche per memorizzare altre tipologie di dati utilizzabili in *Outlook*®, quali ad esempio schedari dei contatti, note personali, ecc. Il formato PST è anch'esso costituito da un pacchetto di file compressi in un unico file.

2.4.1 Raccomandazioni per la produzione di documenti

1. Si raccomanda di utilizzare il formato EML per archiviare un singolo messaggio di posta elettronica, ovvero il formato MBOX per l'archiviazione di più messaggi ovvero di un'intera casella di posta elettronica.

2.5 Fogli di calcolo e presentazioni multimediali

1. Per formati di file maggiormente utilizzati per gli applicativi integrativi "da ufficio" si rimanda alle considerazioni già fatte in § 2.1 relativamente agli applicativi di videoscrittura ad essi affini, in particolare quelle al capoverso 10 del paragrafo in merito all'utilizzo delle fonti tipografiche.

EXCEL® 2007	FORMATO DI FILE
Nome completo	SpreadsheetML OOXML Extension
Estensione/i	.xlsx, .xltx
Specializzazione di	XML imbustato dentro ZIP
Tipo MIME	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
Sviluppato da	Microsoft Corporation
Tipologia di standard	proprietario (libero), estendibile, *de facto*
Livello metadati	3
Derivato da	Office Open XML; Microsoft® *Excel* ®
Revisione	16.0 (2018)

Firmato digitalmente da ROBERTO FRACCIA

Riferimenti	• Microsoft, *Excel (.xlsx) extensions to SpreadsheetML file format* v16.0 (2018) • officeopenxml.com, *Anatomy of a SpreadsheetML file*
Conservazione	Sì, solo profilo Strict; cfr. §2.8
Racc. per la lettura	Generico con riconoscimento obbligatorio
Racc. per la scrittura	Raccomandato nel profilo Strict

2. SpreadsheetML è il dialetto XML usato nei file di metadati all'interno di un pacchetto compresso in formato OOXML (§2.3), specializzato per la rappresentazione di fogli di calcolo (estensione .xlsx). È stato introdotto con la versione 2007 di Microsoft® *Office*®, ma è compatibile con moltissimi altri applicativi. L'unico profilo raccomandato di OOXML per SpreadsheetML è Strict.
3. Si segnala che Microsoft® *Excel*® presenta un *glitch* (i.e. un *bug* volutamente introdotto) considerando erroneamente l'anno 1900 d.C. come bisestile; il formato SpreadsheetML (profilo Transitional), di per sé, non corregge questo comportamento, permettendo il salvataggio, nelle celle di un foglio di calcolo, della data inesistente del 29 febbraio 1900. Tale inesattezza è però imputabile ad *Excel*® e non inficia la capacità di altri applicativi che fanno uso di codesto formato di file (p.es. Google *Documents*) di adeguarsi ad un corretto calcolo degli anni bisestili (correggendo automaticamente le date inesatte nei fogli di calcolo).

PowerPoint® 2007	Formato di file
Nome completo	PresentationML OOXML Extension
Estensione/i	.pptx, .ppsx, .potx
Specializzazione di	XML imbustato dentro ZIP
Tipo MIME	application/vnd.openxmlformats-officedocument.presentationml.presentation
Sviluppato da	Microsoft Corporation
Tipologia di standard	proprietario (libero), estendibile, *de facto*
Livello metadati	3
Derivato da	Office Open XML; Microsoft® *PowerPoint*®
Revisione	15.0 (2018)
Riferimenti	• Microsoft, *PowerPoint (.pptx) extensions to OOXML file format* v15.0 (2018) • officeopenxml.com, *Anatomy of a PresentationML file*
Conservazione	Sì, solo profilo Strict; cfr. §2.8
Racc. per la lettura	Generico con riconoscimento obbligatorio
Racc. per la scrittura	Raccomandato nel profilo Strict

Firmato digitalmente da ROBERTO FRACCIA

3. PresentationML è il dialetto XML usato nei file di metadati all'interno di un pacchetto compresso in formato OOXML (§2.3), specializzato per la rappresentazione di presentazioni multimediali (estensione .pptx). È stato introdotto con la versione 2007 di Microsoft® *Office*®, ma è compatibile con moltissimi altri applicativi. L'unico profilo raccomandato di OOXML per PresentationML è Strict.

MS-XLS	FORMATO DI FILE
Nome completo	Microsoft® *Excel* ® Binary file format
Estensione/i	.xls
Magic number	0xD0CF11E0A1B11AE1
Tipo MIME	application/vnd.ms-excel
Sviluppato da	Microsoft Corporation
Tipologia di standard	proprietario (libero), estendibile, *de facto*, deprecato, binario
Livello metadati	3
Derivato da	Microsoft® Compound File binary format
Revisione	8.0 (2018)
Riferimenti	• Microsoft, *[MS-XLS]: Excel Binary file format (.xls) structure* v8.0 (2018)
Conservazione	No; cfr. §2.8
Racc. per la lettura	Obbligatorio con riversamento raccomandato
Racc. per la scrittura	Sconsigliato

5. Il foramto XLS è una specializzazione usata nei file di metadati all'interno di un pacchetto compresso in formato CFB (§2.3), specializzato per la rappresentazione di fogli di calcolo (estensione .xls). È stato utilizzato, come formato principale per tali documenti fino alla versione 2003 di Microsoft® *Office*®, ma è compatibile con moltissimi altri applicativi. Nonostante l'obbligo per le PP.AA. di accettare e aprire documenti in questo formato, si raccomanda di non formarne altri esemplari e di valutare il riversamento di fogli di calcolo preesistenti in altro formato della stessa tipologia: in quest'ordine, OpenDocument Spreadsheet (.ods) ovvero SpreadsheetML (.xlsx).

MS-PPT	FORMATO DI FILE
Nome completo	Microsoft® *PowerPoint* ® Binary format
Estensione/i	.ppt
Magic number	0xD0CF11E0A1B11AE1
Tipo MIME	application/vnd.ms-powerpoint

Firmato digitalmente da ROBERTO FRACCIA

Sviluppato da	Microsoft Corporation
Tipologia di standard	proprietario (libero), estendibile, *de facto*, deprecato, binario
Livello metadati	3
Derivato da	Microsoft® Compound File binary format
Revisione	6.0 (2018)
Riferimenti	• Microsoft, *[MS-PPT]: PowerPoint (.ppt) Binary file format* v6.0 (2018)
Conservazione	No; cfr. §2.8
Racc. per la lettura	Obbligatorio con riversamento raccomandato
Racc. per la scrittura	Sconsigliato

6. Il foramto PPT è una specializzazione usata nei file di metadati all'interno di un pacchetto compresso in formato CFB (§2.3), specializzato per la rappresentazione di presentazioni multimediali (estensione .ppt). È stato utilizzato, come formato principale per tali documenti fino alla versione 2003 di Microsoft® *Office*®, ma è compatibile con moltissimi altri applicativi. Nonostante l'obbligo per le PP.AA. di accettare e aprire documenti in questo formato, si raccomanda di non formarne altri esemplari e di valutare il riversamento di presentazioni preesistenti in altro formato della stessa tipologia: in quest'ordine, OpenDocument Presentation (.odp) ovvero PresentationML (.pptx).

ODS	FORMATO CONTENITORE
Nome completo	Open Document Format for Office Spreadsheets
Estensione/i	.ods
Specializzazione di	XML imbustato dentro ZIP
Tipo MIME	–
Sviluppato da	Organization for the Advancement of Structured Information Standards
Tipologia di standard	aperto, estendibile, *de iure*, binario
Livello metadati	3
Derivato da	–
Revisione	1.2 (2015)
Riferimenti	Famiglia di standard **26300** della ISO/IEC. • OASIS, *Open Document Format for Office Applications (OpenDocument)*, v1.2 (2015)
Conservazione	Sì; cfr. §2.8
Racc. per la lettura	Generico con riconoscimento obbligatorio
Racc. per la scrittura	Fortemente raccomandato

7. Il formato OpenDocument Spreadsheet è una specializzazione dell'omonimo formato (§2.3) per rappresentare fogli di calcolo (estensione .ods). È attualmente

Firmato digitalmente da ROBERTO FRACCIA

utilizzato dalla suite open source di applicativi da ufficio *LibreOffice*, anche se è pienamente utilizzabile in Microsoft® *Office*®, in OpenOffice.org e in altri applicativi che elaborano documenti di questo tipo.

ODP	FORMATO CONTENITORE
Nome completo	Open Document Format for Presentations
Estensione/i	.odp
Specializzazione di	XML imbustato dentro ZIP
Tipo MIME	–
Sviluppato da	Organization for the Advancement of Structured Information Standards
Tipologia di standard	aperto, estendibile, *de iure*, binario
Livello metadati	3
Derivato da	–
Revisione	1.2 (2015)
Riferimenti	Famiglia di standard **26300** della ISO/IEC. • OASIS, *Open Document Format for Office Applications (OpenDocument)*, v1.2 (2015)
Conservazione	Sì; cfr. §2.8
Racc. per la lettura	Generico con riconoscimento obbligatorio
Racc. per la scrittura	Fortemente raccomandato

8. Il foramto OpenDocument Presentation è una specializzazione dell'omonimo formato (§2.3) per rappresentare fogli di calcolo (estensione .odp). È attualmente utilizzato dalla suite open source di applicativi da ufficio *LibreOffice*, anche se è pienamente utilizzabile in Microsoft® *Office*® in OpenOffice.org e in altri applicativi che elaborano documenti di questo tipo.

2.5.1 Raccomandazioni per la produzione di documenti

1. Si raccomanda alle PP.AA. la produzione di fogli di calcolo e presentazioni multimediali in formati aperti e consistenti con gli applicativi "da ufficio" più diffusi sul territorio nazionale e comunitario: in particolare, si individua nei formati derivati da OOXML (profilo Strict) e da OpenDocument le alternative più valide.
2. Nel caso di documenti semilavorati a carattere temporaneo e non definitivo è consigliabile anche l'utilizzo di formati puramente "virtuali" quali quelli delle suite collaborative di fornitori di servizi in Cloud qualificati,[19] purché tali formati siano

[19] Si veda a tale proposito le Circolari AGID N°2/2018 e N°3/2018.

Firmato digitalmente da ROBERTO FRACCIA

interoperabili e disponibili su sistemi informativi senza vincoli o particolari requisiti tecnologi (ad esempio, totalmente fruibili attraverso browser web).

2.6 Immagini raster

1. Si dicono *raster* tutte le immagini che sono descritte come un insieme finito di punti (*pixel*) virtuali disposti regolarmente su una griglia rettangolare. Il numero di punti lungo i due lati del rettangolo (lunghezza e larghezza) costituiscono le dimensioni dell'immagine, mentre il numero di bit necessari a rappresentare le caratteristiche di ciascun pixel (espresso in bit/pixel) è chiamata profondità o (*bit-*)*depth* dell'immagine. Tali caratteristiche sono tipicamente le coordinate-colore (*code-values*) di ciascun pixel secondo un tipo di codifica matematica ove ogni possibile colore rappresentabile dalle immagini (*gamut*) è definito dalle coordinate di uno spazio-colore astratto, all'interno del quale la gamut dell'immagine rappresenta una varietà discreta.
2. A seconda delle esigenze di conservazione possono essere utili o necessari riferimenti che permettono di correlare la distribuzione spaziale dei pixel di un'immagine raster con dimensioni fisiche. Alcuni formati di file descrivono tali informazioni mediante metadati interni, che possono essere facoltativi o meno. La scelta del formato di file per usi professionali dipende spesso dalla possibilità di creare e, successivamente, fruire di tali metadati, rilevanti sia per raster che provengono da oggetti reali (come nel caso di fotografie, scansioni digitali e diagnostica medica), che per immagini di sintesi usate per la produzione oggetti reali (p.es. stampe o modelli di altro tipo).
3. In alcuni casi sono indicati le dimensioni equivalenti dell'immagine in unità di misura fisiche (lunghezza, larghezza, profondità; ovvero aree, volumi); in altri casi è indicata la risoluzione espressa come densità di punti per unità di misura lineare, quali punti/pollice ("dpi", cioè *dots per inch*) ovvero pixel/cm (nel caso dei raster i termini "punto" e "pixel" sono spesso intercambiabili).
4. Il numero di bit usati per rappresentare il colore dei pixel è chiamata profondità di colore (*colour-depth*) e coincide con l'intera profondità dell'immagine raster qualora la sola caratteristica rappresentata sia il colore dei pixel.
5. Altre volte sono rappresentate una o più di altre caratteristiche del pixel (in alternativa o in aggiunta al colore), quali:

- trasparenza (chiamata anche "alfa", *alpha* in inglese),
- densità ottica,
- riflettanza,
- intensità radiante,

Firmato digitalmente da ROBERTO FRACCIA

- velocità angolare o lineare,

ciascuna di queste caratteristiche del pixel (inclusa ciascuna coordinata dello spazio-colore) sono chiamate, individualmente, "canali" dell'immagine; il numero di bit usati per rappresentare ciascun canale (qualora sia uguale per tutti i canali) permette di specificare la profondità dell'immagine, alternativamente, in bit/canale.

6. Ad esempio, un'immagine raster a colori che usa il tipico modello colorimetrico rosso-verde-blu e un canale alfa, tutti a 16 bit/canale (4 canali in tutto: RGBα) ha dunque una profondità complessiva di 64bit/pixel e una profondità-colore di 48 bit/pixel.

7. Molti formati di immagini raster possono –opzionalmente o obbligatoriamente– implementare algoritmi di compressione dati per ottenere una minore occupazione di spazio. Tali algoritmi sono *lossless* ovvero *lossy*, a seconda che la compressione sia reversibile (cioè sia possibile, decomprimendo, ritornare punto per punto all'immagine originale) o meno.

8. Un'altra possibilità per le immagini raster è una rappresentazione mediante sotto-campionamento, cioè utilizzando una codifica con un modello di spazio-colore a 3 componenti (anziché un modello RGB), ove il primo canale (luminanza) ha una risoluzione spaziale piena (cioè è codificato per ogni punto dell'immagine), mentre gli altri due canali, detti complessivamente di crominanza,[20] sono codificati con una minore risoluzione.

9. I formati di immagini raster maggiormente diffusi per usi non professionali, quali ad esempio web e fotografia amatoriale, sono: PNG, JPEG (.jpg, .jpeg), TIFF (.tif, .tiff), GIF.

10. I formati di immagini raster diffusi per vari usi professionali quali grafica, stampa industriale, fotografia e cinematografia, si differenziano dai precedenti per un ampio supporto –ed effettivo utilizzo– di metadati interni, prevalentemente di tipo colorimetrico. Tra questi formati si annoverano: OpenEXR (.exr), Adobe® DNG (.dng), JPEG2000 (.jp2k, .jp2c), DPX, Adobe® *Photoshop*® (.psd), ARRIRAW (.ari).

PNG	FORMATO DI FILE
Nome completo	Portable Network Graphics
Estensione/i	.png
Magic number	0x89 PNG 0x0D0A1A0A
Tipo MIME	image/png
Sviluppato da	ACME
Tipologia di standard	aperto, *de iure*, binario, muto
Livello metadati	3

[20] Tali canali codificano le differenze cromatiche da un colore neutro –di solito qualche tipo di verde– la cui intensità è rappresentata dalla sola luminanza. Gli spazi-colore di questo tipo (p.es. *Y'*c_Bc_R e *Y'uv*) sono nati per permettere la retrocompatibilità del segnale televisivo analogico a colori con quello in bianco e nero, affiancati da altre tecnologie indipendenti, quali il sotto-campionamento.

Firmato digitalmente da ROBERTO FRACCIA

Derivato da	–
Revisione	1.2, 2ª edizione
Riferimenti	• ISO/IEC 15948:2004 • W3C Recommendation *PNG Specification (2nd Ed.)*, 2003 • RFC-2083 • www.libpng.org
Conservazione	Sì
Racc. per la lettura	Generico; con riconoscimento obbligatorio della v1.0
Racc. per la scrittura	Generico; fortemente raccomandato per immagini a 16 ovvero 48 bit/pixel (più eventuale trasparenza) senza particolari obblighi relativi ad altri metadati

11. Il formato PNG è particolarmente raccomandato per la rappresentazione di immagini raster che non hanno bisogno di essere accompagnate da metadati particolarmente complessi (come quelli colorimetrici, geometrico-fisico o ottici). La versione 1.0 di questo formato (cfr. RFC-2083) –ancora largamente utilizzata e, per questo motivo, ammessa parimenti per la produzione di nuovi documenti raster– supporta un insieme ristrettissimo di metadati, per la cui mancanza il formato di questa versione è poco usato in ambiti professionali. Sono invece supportate nativamente le profondità di 24 e 48 bit/pixel in tricromia, la trasparenza sotto forma di un ulteriore canale "alfa", nonché uno dei pochi formati non professionali ad ammettere la compressione dell'immagine mediante algoritmo *lossless*. La versione 1.2 del formato introduce alcuni metadati più professionali che permettono, ad esempio, di specificare autori e brevi descrizioni, orari di modifica, così come metadati colorimetrici (quali le coordinate di cromaticità delle primarie RGB e del punto di bianco, profili ICC integrati, dimensioni fisiche dell'immagine, ecc.).

JPEG	FORMATO DI FILE
Nome completo	JPEG File Interchange Format (JFIF)
Estensione/i	.jpg, .jpeg
Magic number	0xFFD8, 0xFFD8FFE00010 JFIF 0x0001
Tipo MIME	image/jpg, image/jpeg
Sviluppato da	Joint Photographic Experts Group
Tipologia di standard	aperto, estendibile, *de iure*, binario
Livello metadati	4
Derivato da	–
Revisione	2012
Riferimenti	• ITU-T Recommendation T.81, 1992 • ITU-T Recommendation T.871, 2011 • www.jpeg.org/jpeg • www.exif.org/Exif2-2.PDF

Firmato digitalmente da ROBERTO FRACCIA

Conservazione	Sì, solo per immagini formate nativamente in JPEG
Racc. per la lettura	Generico con riconoscimento obbligatorio
Racc. per la scrittura	Generico; fortemente raccomandato per immagini fotografiche senza particolari vincoli qualitativi

12. Il formato JPEG è un altro "pilastro" storico per le immagini raster, permettendo una loro rappresentazione generica e, soprattutto, estremamente compatta per via dell'uso di un algoritmo di compressione *lossy*, in cui alcuni parametri algoritmici sono selezionabili in fase di formazione del file, permettendo così un bilanciamento tra "qualità" dell'immagine[21] e dimensione del file. Le immagini sono inoltre codificate sempre in uno spazio-colore del tipo *Y'uv* e sotto-campionate; non sono supportate le trasparenze. Nonostante queste carenze lo standard *EXIF* estende il formato per la sola rappresentazione di metadati interni, tra i quali possono essere presenti:

- informazioni sull'hardware o software usato per creare o modificare l'immagine (p.es. modello di fotocamera, ottiche, flash e altra apparecchiatura, con i loro parametri di scatto);
- data, ora ed eventuale posizione geografica della creazione;
- nome o altre caratteristiche dell'autore;
- eventuali licenze d'uso dell'immagine (Copyright©, Creative Commons, ecc.);
- informazioni colorimetriche (spazio-colore, punto di bianco, profilo ICC, ecc.);
- eventuale proiezione piana di uno spazio curvo (p.es. equi-rettangolare, altrimenti detta 'latitudine/longitudine' o, più impropriamente, "*360°*").

13. Qualora si disponga delle medesime immagini in un formato di maggiore qualità (in termini di risoluzione, di assenza di compressione *lossy*, o altro), si consiglia di non riversare mai in JPEG il medesimo contenuto (a meno che non si tratti di una seconda copia per altri scopi).

TIFF	FORMATO DI FILE
Nome completo	Tagged Image File Format
Estensione/i	.tiff, .tif
Magic number	II 0x2A00; MM 0x002A
Tipo MIME	image/tiff
Sviluppato da	Adobe Systems
Tipologia di standard	proprietario (libero), estendibile, *de iure*, binario

[21] Da intendersi qui come fedeltà dell'immagine compressa (con perdite dovute alla compressione) rispetto all'immagine originale non compressa. Tale quantità è misurata con opportune metriche, tra cui quelle basate sul rapporto segnale-rumore percepito, o pSNR.

Firmato digitalmente da ROBERTO FRACCIA

Livello metadati	4
Derivato da	—
Revisione	2004
Riferimenti	• Adobe, *TIFF™ Revision 6.0*, 1992 • www.adobe.io/open/standards/TIFF Famiglia di standard **12234** della ISO: • ISO 12234-2:2001, TIFF/*EP* • ISO 12234-3:2016, *XMP* • ISO 12639:2004, TIFF/*IT* • RFC-2306, TIFF-*F* • RFC-3949, TIFF-*FX* • www.exif.org/Exif2-2.PDF
Compressione	Sì, senza compressione
Racc. per la lettura	Generico con riconoscimento obbligatorio
Racc. per la scrittura	Specifico per l'editoria; raccomandato per la produzione di immagini raster finali

13. Il formato TIFF è il capostipite dei formati raster professionali, pur essendo ancora considerato appartenente alla categoria dei formati generali per le immagini raster. Nato con poche varianti e metadati prevalentemente per rappresentare immagini pronte sia per l'invio telematico (tramite fax) che per la stampa professionale –monocromatica o "offset"– è stato successivamente esteso dalla Adobe, fino a diventare uno standard aperto e *de iure*, con moltissime caratteristiche aggiuntive:

- segmentazione dell'immagine nel file per linee ovvero per riquadri;[22]
- segmentazione a più livelli sovrapposti;[23]
- spazi-colore con un qualsivoglia numero di canali (inclusa la trasparenza, o canale *alfa*);
- metadati aggiuntivi circa la rappresentazione spaziale (unità di misura, ecc.);
- metadati aggiuntivi circa le condizioni ideali per la visualizzazione (caratteristiche del monitor) o per la stampa professionale (intento di rappresentazione, codici di particolari colori "spot", ecc.);
- compressione secondo vari algoritmi, generalmente *lossless*.

Infine, anche nelle immagini TIFF –come per le JPEG– possono essere inseriti metadati EXIF.

GIF	FORMATO DI FILE
Nome completo	Graphic Image file Format

[22] Utili per ottimizzarne l'archiviazione su alcuni storage, la trasmissione attraverso specifici canali, la robustezza in caso di corruzione.
[23] Utile per immagini in fase di post-produzione, cioè quando sono semilavorati le cui modifiche devono essere reversibili.

Firmato digitalmente da ROBERTO FRACCIA

Estensione/i	.gif
Magic number	GIF89a; GIF87a
Tipo MIME	image/gif
Sviluppato da	CompuServe
Tipologia di standard	deprecato, proprietario (libero), *de iure*, binario, muto
Livello metadati	1
Derivato da	—
Revisione	89a (1989)
Riferimenti	• W3C, *Graphics Interchange Format™*, ©1990 CompuServe
Conservazione	No
Racc. per la lettura	Generico con riconoscimento obbligatorio
Racc. per la scrittura	Sconsigliato, tranne che in due casi legati al web

14. Il formato GIF venne introdotto nella fine degli anni '80 per rappresentare immagini fotorealistiche quando le capacità dei computer di visualizzare simultaneamente molti colori erano limitate. Alcune delle novità tecniche di questo formato sono sopravvissute sino ad oggi, tanto che vi sono ancora molti casi d'uso soprattutto nelle pagine web. Anche se esistono oggi formati molto più adeguati per le immagini fotorealistiche, il formato, implementando fra le altre cose un ana compressione *lossless*, è ancora tecnicamente valido per immagini con le seguenti caratteristiche:

- numero colori fino a un massimo di 256, scelti da una tavolozza con 32 bit di profondità;[24]
- supporto per una trasparenza assente ovvero totale,[25] senza diversi gradi di opacità;
- supporto per più immagini che si alternano in sequenza (con cadenza preselezionata) per rappresentare uno sprite dotato di caratteristiche di animazione basilari (si parla, in questo caso di "GIF animate");[26]

Le immagini con bassissimi requisiti di animazione, trasparenza e numero di colori (tipicamente loghi o porzioni di elementi grafici minimalisti), come quelle che si trovano in diversi siti web, spesso salvate in questo formato.

[24] La tavolozza è quella di un generico modello RGB con 8 bit/canale, per un totale di $2^{8+8+8} = 2^{32} \approx 16.8$ milioni di colori.
[25] Nel GIF la trasparenza è rappresentata da uno dei 256 colori della tavolozza, che può essere indicato come tale nei metadati interni.
[26] Le GIF animate sono ancora vincolate ad avere un massimo di 256 colori per fotogramma (inclusa la trasparenza), anche se i colori scelti possono cambiare da fotogramma a fotogramma.

Firmato digitalmente da ROBERTO FRACCIA

16. A causa della sua obsolescenza, se ne sconsiglia l'uso per nuove immagini, salvo in cui l'immagine da archiviare sia destinata all'uso in pagine web e rientri, nella sua forma originaria (o formato di partenza) all'interno dei vincoli sopraelencati.

EXR	FORMATO DI FILE
Nome completo	OpenEXR™
Estensione/i	.exr
Magic number	v/1 0x01
Tipo MIME	image/x-exr
Sviluppato da	Industrial Light and Magic
Tipologia di standard	aperto, estendibile, *de facto*, binario
Livello metadati	4
Derivato da	–
Revisione	2013
Riferimenti	• www.openexr.com/documentation • WetaDigital, *The Theory of OpenEXR Deep Samples*, 2013
Conservazione	Sì, senza compressione
Racc. per la lettura	Speciale; raccomandato in ambito cinetelevisivo
Racc. per la scrittura	Speciale; raccomandato in ambito cinetelevisivo

17. Il formato OpenEXR è stato recentemente inventato ed è oggi mantenuto, dalla comunità dei creativi dell'animazione cinematografica ma, a causa della sua versatilità e del supporto per un numero qualsiasi e facilmente estendibile di metadati, è oggi fortemente consigliato per la produzione di immagini raster –sia finali che, soprattutto, semilavorati– per la grafica e la produzione cinetelevisiva. A causa del formato specifico, non è richiesto il suo riconoscimento al di fuori delle organizzazioni dei sopracitati settori.
18. OpenEXR supporta immagini raster con le seguenti caratteristiche:

- segmentazione dell'immagine in vari modi diversi (per linee, a tasselli, per strati);
- supporto di più spazi-colore, inclusi astratti con un numero qualsivoglia elevato di canali (ciascuno associato ai propri metadati);
- supporto per un numero qualsivoglia elevato di livelli, ciascuno dotato dei propri metadati;
- data, ora ed eventuale posizione geografica della creazione;
- nome o altre caratteristiche dell'applicazione creatrice, ovvero dell'autore (se umano);
- eventuale supporto di vari algoritmi di compressione (sia *lossy* che *lossless*);
- supporto di metadati interni la cui tassonomia rientra in *namespace* estendibili.

Firmato digitalmente da ROBERTO FRACCIA

19. Inoltre, grazie alla versatilità nel numero di livelli e di canali di colore (e la possibilità di identificarli ciascuno con un nome), è possibile memorizzare nei punti di un'immagine raster salvata in OpenEXR non soltanto il colore, quanto piuttosto informazioni relative ad altre caratteristiche tecniche, fisiche o cinetiche dell'immagine, rappresentabili punto per punto. Esempi sono:

- il cosiddetto "deep EXR", ove più livelli sovrapposti mantengono una dei medesimi oggetti a diversi gradi di "profondità" rispetto ad immagini piane;
- le *texture*, che sono comuni raster, le cui coordinate cartesiane sono chiamate (*u*,*v*), che rappresentano una "pelle" da avvolgere intorno ad una superfice artificiale tridimensionale (come quelle rappresentate in formati descritti in §2.7) mediante una trasformazione conforme che prende il nome, appunto, di mappa *uv*.

20. In alcuni casi, l'immagine tradizionalmente costituita da un raster ove i punti rappresentano dei colori è contenuta in un primo livello, mentre in altri livelli sono rappresentate altre quantità relative alla medesima immagine. Due esempi, estremamente riduttivi, di tali quantità, utili particolarmente nella produzione di effetti speciali digitali (VFX) e nell'animazione in CG (dall'inglese, "computer-grafica"), sono:

- *velocity map*, ove i 2 o 3 canali (*u*,*v*,*w*) associati ad ogni punto rappresentano le componenti cartesiane della velocità istantanea del punto della superfice;
- *optical map*, ove i canali (uno o più) associati ad ogni punto rappresentano caratteristiche ottiche del materiale in quel punto, quali ad esempio opacità/trasparenza, riflettanza, assorbanza, emittanza, ecc.

21. Per quanto riguarda i metadati interni, purtroppo, la mancanza di un registro unificato è causa del proliferare incontrollato degli stessi: unica pecca per un formato altrimenti validissimo e fortemente consigliato per la produzione di *qualsiasi* tipo di immagine raster.

JPEG2000	FORMATO DI FILE
Nome completo	JPEG 2000
Estensione/i	.png
Magic number	0x89 PNG 0x0D0A1A0A
Tipo MIME	image/jp2
Sviluppato da	Joint Photographic Experts Group
Tipologia di standard	aperto, estendibile, *de iure*, binario
Livello metadati	3
Derivato da	–
Revisione	2020/1

Firmato digitalmente da ROBERTO FRACCIA

Riferimenti	• RFC-3745 Famiglia di standard **15444** della ISO: • ISO 15444-1:2016 • ISO 15444-2:2004 • ISO 15444-6:2013 • ISO 15444-6:2011 • ISO 15444-12:2015
Conservazione	No
Racc. per la lettura	Speciale; raccomandato nell'elaborazione professionale di immagini in vari ambiti
Racc. per la scrittura	Speciale; raccomandato nell'elaborazione professionale di immagini in vari ambiti

22. Il formato JPEG2000 utilizza una compressione basata su trasformata *wavelet*, cosiddetta multi-risoluzione, poiché l'evidenza informatica ivi rappresentata codifica prima i dettagli "grossolani" (cd. a bassa frequenza) dell'immagine, poi i dettagli via via più "fini" (cd. ad alte frequenze). A fronte di una maggiore complessità nella produzione (i.e. nella compressione) dell'immagine, il vantaggio tecnologico offerto da questo formato risiede nel fatto che la decodifica successiva dell'immagine (i.e. la sua decompressione) può avvenire anche non integralmente e interrompersi a un certo livello. In tal caso viene riprodotta una versione "a banda ristretta", cioè a risoluzione inferiore dell'immagine originale, in quanto sono state usate componenti a bassa frequenza. L'usodel formato è dunque preferibile laddove l'utilizzo professionale sia vincolato da uno o più dei seguenti fattori:

- immagini di dimensioni molto grandi, comparate a
- basse capacità computazionali del dispositivo di visualizzazione;
- canale di comunicazione tra lo storage ove è archiviata l'immagine e il dispositivo di visualizzazione.

DICOM	FORMATO DI PACCHETTO
Nome completo	Digital Imaging and Communications in Medicine
Estensione/i	
Magic number	128 byte qualsiasi, seguiti da DICM
Tipo MIME	image/dicom
Sviluppato da	National Electrical Manufacturers Association
Tipologia di standard	aperto, estendibile, *de iure*, binario
Livello metadati	2
Derivato da	–
Revisione	2018
Riferimenti	• dicom.nema.org/medical/dicom, PS3.10 • dicom.nema.org/medical/dicom, capitolo 7
Conservazione	Sì, se lo sono tutti i file del pacchetto

Firmato digitalmente da ROBERTO FRACCIA

Racc. per la lettura	Speciale; raccomandato in ambio diagnostica sanitaria
Racc. per la scrittura	Speciale; raccomandato in ambio diagnostica sanitaria

23. Il formato DICOM consente di aggiungere alle immagini raster diversi metadati relativi all'aspetto sanitario del loro contenuto, quali ad esempio un elenco di metadati facoltativi e non esaustivi comprende:

- il nome degli specialisti che hanno eseguito l'acquisizione, l'elaborazione o la refertazione,
- il nome e modello delle apparecchiature di acquisizione e parametri elettronici, fisico-chimici, meccanici impiegati per un dato esame diagnostico,
- la data, l'ora e il nome della struttura ove sia stato effettuato l'esame diagnostico,
- eventuali commenti sul pacchetto di immagini nella sua interezza (ad esempio il testo del referto), sulla specifica immagine, o su una porzione della stessa.

DNG	FORMATO DI FILE
Nome completo	Adobe® Digital Negative
Estensione/i	.dng
Specializzazione di	TIFF/EP
Tipo MIME	image/x-adobe-dng
Sviluppato da	Adobe Systems
Tipologia di standard	proprietario (brevettato), estendibile, *de iure*, binario
Livello metadati	4
Derivato da	TIFF™
Revisione	10.1.0.0 (2017)
Riferimenti	• Adobe, *Digital Negative (DNG) Specification* v1.4.0.0, 2012
Conservazione	No
Racc. per la lettura	Speciale; raccomandato in ambito fotografico e cinetelevisivo
Racc. per la scrittura	Speciale; raccomandato in ambito fotografico e cinetelevisivo

24. Il formato DNG ("negativo digitale") di Adobe consiste in una specializzazione del formato TIFF, dotato di diverse estensioni relative alla quantità di metadati di accompagnamento (che include, tra l'altro, l'intera gamma di metadati EXIF e XMP) ma soprattutto consente di memorizzare immagini grezze ("raw") provenienti da sensori digitali con diverse caratteristiche elettroniche e geometriche. La procedura di conversione effettuata a monte permette di transcodificare un'immagine raster altrimenti memorizzata in formati di file per lo più proprietari del costruttore della fotocamera o cinepresa, mediante un applicativo che, al momento della

Firmato digitalmente da ROBERTO FRACCIA

transcodifica, comprende il formato nativo e le informazioni sullo specifico modello dell'apparato di acquisizione. Il risultato è un'immagine visivamente fedele, identica all'originale, ma archiviata in un formato aperto e interoperabile, non più soggetto all'obsolescenza tecnologica né dell'apparato di acquisizione originario, né del formato di file proprietario di origine.

PSD	FORMATO DI FILE
Nome completo	Adobe® *Photoshop*® Standard Baseline file
Estensione/i	.psd
Magic number	8BPS
Tipo MIME	image/x-psd
Sviluppato da	Adobe Systems
Tipologia di standard	proprietario (libero), estendibile, *de facto*, binario
Livello metadati	4
Derivato da	–
Revisione	2016
Riferimenti	• www.adobe.com • FSDeveloper.com, *Adobe Photoshop File Formats Specification* 2006 • github.com/layervault/psd.rb
Conservazione	No
Racc. per la lettura	Specifico; obbligatorio in ambito beni culturali e comunicazione
Racc. per la scrittura	Specifico; obbligatorio in ambito beni culturali e comunicazione

25. Il formato nativo di Adobe *Photoshop*® si è evoluto notevolmente nel tempo e comprende attualmente la possibilità non solo di archiviare immagini a più livelli e con elevatissima variabilità tecnica, [27] ma anche informazioni vettoriali e tridimensionali di complemento alle immagini raster, che coadiuvano il loro utilizzo in molteplici contensti industriali, quali il design, la computer grafica (CG), l'architettura e la postproduzione cinetelevisiva. Si raccomanda l'utilizzo di questo formato per la creazione di semilavorati, particolarmente quando vadano elaborati dal particolare software applicativo in oggetto. Per l'archiviazione a lungo termine e la conservazione invece, si consiglia di riversare il contenuto in altri formati più aperti e interoperabili (quali OpenEXR, DNG o TIFF).

ARRIRAW	FORMATO DI FILE
Nome completo	ARRIRAW
Estensione/i	.ari
Magic number	ARRI 0x12345678; ARRI 0x78563412

[27] Si segnala la presenza un dialetto del formato PSD specificatamente per archiviazione e riutilizzo di immagini di grandissime dimensioni: il *Photoshop Large Format* (formato molto simile all'originario, che adotta l'estensione di file .psb).

Firmato digitalmente da ROBERTO FRACCIA

Tipo MIME	image/arriraw
Sviluppato da	Arnold & Richter Cine Technik GmbH
Tipologia di standard	proprietario (libero), estendibile, *de iure*, binario
Livello metadati	4
Derivato da	–
Revisione	2018
Riferimenti	• documentazione registrata SMPTE RDD30:2014 • documentazione registrata SMPTE RDD31:2014
Conservazione	No
Racc. per la lettura	Speciale; riprese cinematografiche
Racc. per la scrittura	Speciale; sconsigliata la produzione al di fuori dell'ambito cinematografico

26. Il formato ARRIRAW è un formato proprietario della ARRI GmbH, ma aperto, utilizzato attualmente come formato nativo "*raw*" per le sue cineprese digitali, che è stato candidato per diventare standard SMPTE. Nonostante si tratti di un formato proprietario, ne è un esempio virtuoso, in quanto esso supporta più tipologie di codifiche di immagine, nonché di metadati avanzati a contorno dell'immagine stessa, quali le informazioni colorimetriche (codifica dello spazio-colore, parametri di correzioni impostati direttamente sulla cinepresa, importati *una tantum* da file, ovvero comunicati in tempo reale da un'applicazione con connessione di rete diretta sulla cinepresa), quelle relative all'area attiva del fotogramma, alla velocità di ripresa mediante TimeCode (il formato ne supporta fino a 7 tipi differenti e indipendenti fra loro), ai metadati di produzione, ecc. In teoria, il formato ARRIRAW potrebbe essere utilizzato per produrre nuove immagini raster in una miriade di codifiche e di formati.

DPX	FORMATO DI FILE
Nome completo	Digital Picture Exchange
Estensione/i	.dpx
Magic number	SDPX, XPDS
Tipo MIME	image/x-dpx
Sviluppato da	Society of Motion Picture and Television Engineers
Tipologia di standard	aperto, estendibile, *de iure*, binario
Livello metadati	4
Derivato da	Kodak® Cineon™
Revisione	2.0 (2014)
Riferimenti	• standard SMPTE ST268:2014
Conservazione	No
Racc. per la lettura	Specifico; obbligatorio in ambito cinetelevisivo

Firmato digitalmente da ROBERTO FRACCIA

Racc. per la scrittura	Specifico; nessuna raccomandazione

27. Il formato DPX (originariamente sviluppato da Kodak come evoluzione del formato Cineon® usato nell'omonimo scanner digitale per le pellicole cinematografiche 35mm e successivamente divenuto uno standard SMPTE) permette la rappresentazione di immagini raster con differenti caratteristiche tecniche, oltre a un considerevole numero di metadati. L'attuale versione 2.0 suddivide i metadati in quattro categorie: generici, cinematografici, televisivi e "utente". Tra i metadati delle categorie cinetelevisive vi è la possibilità di rappresentare indicazioni per collocare con precisione l'immagine come fotogramma di una particolare sequenza video, quali:

- numerazione del fotogramma relativa all'inizio della sequenza,
- TimeCode (con relativi *framerate* e modalità di scansione del fotogramma, cfr. §2.10),
- KeyKode™ del forogramma rispetto al rullo di pellicola fotochimica da cui è stato scansionato digitalmente (con relativa *film-speed*).

28. Il formato si presta dunque ad una rappresentazione di documenti video mediante pacchetti di file, ove ciascun fotogramma è archiviato in un file separato (cfr. pacchetto DI basato su DPX, cfr. §2.12). In linea di principio il formato DPX ammette tra i metadati anche quelli che associano colorimetria digitale rappresentata nel raster dalla densitometria dell'emulsione di partenza (da cui il fotogramma è stato scansionato) o di destinazione (sulla quale s'intende possa essere stampato digitalmente), anche se pochissimi applicativi per la postproduzione cinematografica ne fanno realmente uso. Nonostante il DPX sia stato l'indiscusso formato di riferimento per la produzione, postproduzione e archiviazione digitale di contenuti cinematografici sin dall'avvento del Digital Intermediate (*DI*, cfr. §2.12), tre fattori ne hanno rapidamente ridotto l'importanza:

- il declino della produzione cinematografica su pellicola e la consistente riduzione di processi di scansione digitale di tali pellicole (ora quasi esclusivamente effettuati a scopo di restauro e conservazione);
- il mancato utilizzo di moltissimi metadati rappresentabili nel formato DPX da parte di gran parte dei software applicativi, che avrebbe invece incrementato l'efficacia di tale formato;
- la comparsa di nuovi standard tecnologici per la rappresentazione dell'immagine digitale, quali ad esempio l'elevata latitudine di posa (*HDR*). A tale scopo l'SMPTE sta sviluppando una nuova versione più moderna del formato DPX.

Firmato digitalmente da ROBERTO FRACCIA

29. Mentre si obbliga agli enti tecnici operanti nel settore della postproduzione, archiviazione e conservazione cinematografica di leggere immagini nel formato DPX, allo scopo di preservare l'accessibilità a contenuti provenienti da archivi in pellicola già digitalizzati o archivi digitali di DI basati su DPX, si raccomanda fortemente di considerare formati alternativi, quali ad esempio OpenEXR, ovvero i pacchetti di master interoperabile (IMF, cfr. §2.12).

ACES	
Nome completo	Academy Color Encoding System
Estensione/i	.exr, .mxf, .amf, .clf
Tipologie MIME	image/exr, application/mxf
Sviluppato da	Academy of Motion Picture Arts and Sciences
Tipologia di standard	aperto, estendibile, retrocompatibile, *de iure*
Derivato da	–
Revisione	1.1.0 (2018)
Riferimenti	Standard e bollettini tecnici dell'AMPAS: • TB-2014-012, *ACES version 1.0 component names* Famiglia di standard **ST2065** della SMPTE: • ST2065-1:2012, *Academy Color Encoding Specification* • ST2065-4:2013, *ACES image container file layout* • ST2065-5:2016, *mapping ACES into MXF container* • ST2067-50:2018, *IMF – Application #5: ACES* • www.oscars.org/aces • www.acescentral.com • W. Arrighetti, 'The ACES: a professional color-management framework for production, post-production and archival of still and motion pictures', *Journal of Imaging*, Vol.3, №4, pp.189–225, MDPI, 2017
Conservazione	Sì
Racc. per la lettura	Speciale; consigliato in post-produzione cinetelevisiva
Racc. per la scrittura	Speciale; consigliato in post-produzione, archiviazione e conservazione di contenuti cinetelevisivi in ACES

30. Il sistema *Academy Color Encoding System* (*ACES*), standard SMPTE introdotto dall'AMPAS, permette di descrivere in maniera unificata gli spazi-colore e i processi produttivi di elaborazione e trasporto del colore digitale nelle applicazioni professionali in campo cinetelevisivo. ACES si prefigge come una possibile soluzione alla rappresentazione di immagini raster (e video) catturate da dispositivi

Firmato digitalmente da ROBERTO FRACCIA

e camere con molteplici colorimetrie (spesso proprietarie), al trasporto di metadati colorimetrici tra processi dominati da svariati *vendor*, e visualizzabili con una moltitudine di tecnologie di visualizzazione (p.es. LED, OLED, plasma, ecc., così come HDR+, Dolby Vision,® HLG, ecc.). Il trasporto di file codificati con la colorimetria ACES può avvenire sia con il formato OpenEXR con l'aggiunta di specifici vincoli e metadati[28] (standard ST2065-4), sia imbustando una sequenza di fotogrammi, già nel formato EXR, all'interno di un contenitore MXF (cfr. standard ST2065-5 e §2.12) anch'esso con determinati vincoli e metadati. Ulteriori informazioni colorimetriche in ACES possono essere rappresentate accompagnando, il contenuto audiovisivo in un pacchetto di file contenente uno o più *sidecar file* nel formato AMF (cfr. §2.12).

2.6.1 Raccomandazioni per la produzione di documenti

1. Come già discusso sopra all'inizio della sezione, i formati di immagini raster vanno distinti innanzi tutto tra le finalità generiche e specializzate — queste ultime differenti a seconda dell'ambito: sanità, architettura e urbanistica, grafica e pubblicità (inclusa la produzione online), intrattenimento (inclusi l'animazione o CG, così come produzione, postproduzione ed effetti speciali cinetelevisivi).
2. Per i formati generici (PNG, JPEG, TIFF, GIF) sussiste in generale l'obbligo di riconoscimento. Nonostante tale obbligo in merito ai formati generali, le singole PP.AA., qualora accettino documenti informatici in formati di immagini raster generici tra quelli sopra elencati per un loro procedimento amministrativo o a scopo di conservazione, possono decidere di limitare ulteriormente l'accettazione di tali formati ad un loro sottoinsieme, specificatamente allo scopo di ridurre o uniformare i formati dei documenti.
3. Per la produzione di immagini raster, invece, la scelta dell'uno piuttosto che dell'altro formato generico, ovvero di uno di tali formati invece di uno specializzato, deve essere motivata da motivazioni tecniche ovvero da una valutazione di interoperabilità. In particolare si raccomanda:

- Il formato TIFF per immagini raster –generate o riversate in tale formato– dove la rappresentazione fedele del documento sia un vincolo tecnico o giuridico e dove la capacità di complementare l'immagine con trasparenze,

[28] Il vincolo principale è nell'assenza di compressione e nella codifica nello spazio-colore ACES2065-1 (standard ST2065-1); devono inoltre essere presenti alcuni metadati colorimetrici facoltativi del formato OpenEXR, più un metadata booleano specifico di ACES.

Firmato digitalmente da ROBERTO FRACCIA

livelli aggiuntivi e un certo livello di "metadati tecnici" (e.g. spazio-colore, impostazioni di stampa o scansione, raccordo con dimensioni fisiche di rappresentazione, etc.) costituisca un valore aggiunto.

- Il formato JPEG per la produzione di immagini originali e rettangolari il cui scopo sia meramente rappresentativo e non probatorio; il livello di compressione per la produzione di tali immagini sarà dunque scelto in maniera adeguata a non compromettere lo scopo rappresentativo del documento.
- Il formato JPEG per il riversamento di immagini raster rettangolari ove la conservazione della qualità originale dell'immagine non costituisca un impedimento giuridico o non sia un vincolo esatto; in particolar modo si preferisca tale formato per immagini di provenienza fotografica, scegliendo anche in questo caso un adeguato livello di compressione.
- Il formato PNG per immagini raster –generate o riversate in tale formato– ove sia importante il mantenimento della qualità –rispettivamente massima o originale– solo relativamente ad una rappresentazione su schermi digitali non professionali. Sono un esempio di tale esigenza la produzione di immagini o fotografie digitali per l'utilizzo su pagine web o sulle GUI di software applicativi, così come loghi e altri simboli grafici, spesso coadiuvati da effetti di trasparenza.
- Il formato GIF per immagini raster che soddisfano i requisiti del formato precedente (PNG) salvo l'appartenenza all'ambito fotografico, ma abbiano in più almeno una delle seguenti caratteristiche tecniche:
    - utilizzo di un numero complessivo di valori colorimetrici non superiore a 256;
    - assenza di trasparenze, ovvero
    - impiego di soli due livelli di trasparenza: 'trasparenza totale' e 'opacità totale';
    - piccola animazione costituita da pochi fotogrammi, riprodotti ciclicamente o una sola volta, ove ogni fotogramma soddisfi le precedenti caratteristiche.

4. Per quanto riguarda settori specifici, si raccomanda invece l'utilizzo di formati specializzati nei settori produttivi di riferimento, quali editoria, grafica, pubblicità, sanità, edilizia, architettura, intrattenimento, produzione cinetelevisiva. Si raccomandano perciò le seguenti adozioni:

- Il formato OpenEXR (anche detto, colloquialmente, "EXR") per immagini raster relative a produzione, postproduzione, archiviazione e soprattutto conservazione di contenuti cinetelevisivi, pubblicitari, videoludici, animazione e beni culturali — che si tratti di semilavorati, master o

Firmato digitalmente da ROBERTO FRACCIA

documenti definitivi. Il formato sia inoltre corredato adeguatamente dal più ampio spettro possibile di metadati a scopo archivistico.

- Formato DICOM per tutte le immagini diagnostiche di provenienza sanitaria, adeguatamente corredato dai metadati di produzione e refertazione,
- Formato JPEG2000 per le immagini raster di grandi dimensioni di competenza territoriale (e.g. immagini satellitari, demaniali, catastali), urbanistico e militare.
- Formato DNG per scatti provenienti da fotocamere o cineprese digitali — siano essi generati o riversati dai formati nativi in tale formato.
- Formato DPX per fotogrammi provenienti direttamente da scansioni digitali di pellicole cinematografiche non ulteriormente elaborate (per le quali si preferisce un riversamento nel formato OpenEXR durante le fasi della postproduzione).
- Formato ARRIRAW per le immagini provenienti dal girato originale di cinecamere ARRI (quali quelle della famiglia ALEXA ovvero AMIRA) — salvo quando esigenze di produzione cinetelevisiva richiedano che le camere *formino* il loro girato direttamente in formati video che adottano compressione *lossy*. [29]
- Formato PSD per immagini definitive provenienti da, ovvero semilavorati destinati all'elaborazione da parte di software di fotoritocco specializzati che supportino tale formato — nativamente o per compatibilità.

5. Tra i formati sopra individuati, il PNG e le varianti di TIFF e OpenEXR (EXR) senza ausilio di compressione, ovvero con algoritmi di compressione privi di perdita (*lossless*), sono i formati più adatti alla conservazione. Possono essere adatti alla conservazione anche il formato JPEG ovvero le varianti di TIFF e EXR che adottino algoritmi di compressione, ma solo qualora le immagini siano state nativamente generate in codesti formati (p.es. provenienti da fotocamere ovvero scanner digitali). Sono dunque esclusi dalla conservazione i riversamenti di immagini in formati che aggiungono (o cambiano) algoritmi di compressione adottati. Gli eventuali algoritmi di compressione adottati in conservazione devono tuttavia essere algoritmi aperti, previsti e pienamente descritti nelle specifiche tecniche dei formati stesso (ovvero nelle cui specifiche tecniche sono riportati i nomi degli standard relativi a codesti algoritmi di compressione).

[29] Ad esempio, contenitori QuickTime o MXF (§2.12) che imbustano video Apple® ProRes® ovvero Avid® DNxHD™, cfr. §2.10.

Firmato digitalmente da ROBERTO FRACCIA

2.7 Immagini vettoriali e modellazione digitale

1. Si chiamano vettoriali le immagini rappresentate nel file mediante una descrizione algoritmica della geometria e del colore che le compone, utilizzando tecniche descrittive più o meno complesse. I modelli multidimensionali sono una generalizzazione delle immagini vettoriali utilizzando tre o più dimensioni (a prescindere dal problema della visualizzazione, che è spesso demandato alle applicazioni più o meno specializzate).
2. La descrizione delle immagini vettoriali è fatta in uno spazio geometrico virtuale, mediante coordinate tipicamente adimensionali, sebbene nei metadati interni di alcuni tipi di file impiegati, e/o nelle informazioni metriche usate dalle primitive, possono essere presenti riferimenti a dimensioni reali. Anche la rappresentazione di caratteristiche quali colore, trasparenze o riflettanze può avvenire mediante una o più delle seguenti tecniche:

- coordinate di spazi-colore riferiti ad ambienti a luce emessa o riflessa (in inglese, rispettivamente, *output-referred* o *scene-referred*), ovvero ad altri tipi di colorimetrie.
- etichette di colore che rimandano a specifici cataloghi di vernici o altri coloranti (p.es. "blu cobalto", "Pantone®33M", "smalto dorato", ecc.),
- etichette che rimandano a cataloghi di materiali, tipicamente specifici per applicazione o riferiti altrove mediante file o etichette che rimandano a basi di dati esterne (p.es. "mogano laminato", "calcestruzzo", "cristallo smerigliato", "ebano lucido", "lino", "tartan", ecc.).

3. La potenziale multidimensionalità rappresentata in questi file, e la loro caratteristica intrinseca di descrivere immagini scomposti in oggetti distinti (tipicamente primitive geometriche con caratteristiche aggiuntive quali nomi/etichette, colori, trasparenze, collegamenti logici ad altri oggetti, ecc.) consente di salvare anche informazioni circa l'animazione –automatica o programmabile– di alcuni oggetti rispetto ad altri.
4. I formati di file più usati e specifici per immagini vettoriali sono: SVG, Adobe® *Illustrator*® (.ai), Encapsulated PostScript™ (.eps).
5. I modelli digitali sono un'estensione delle immagini vettoriali (cfr. §2.7) ma a spazi con tre o più dimensioni. Anche in questo caso gli oggetti virtuali sono descritti in maniera geometrica e corredati da metadati. Le applicazioni principali per questi file sono la progettazione edile e industriale, l'architettura, l'intrattenimento e le scienze in genere.
6. I formati di file più usati per modelli bi- e tridimensionali sono ben distinti tra categorie aperte e categorie chiuse (sia rispetto alle specifiche che rispetto alla proprietà intellettuale — cfr. §2.7):

Firmato digitalmente da ROBERTO FRACCIA

Tra i primi ci sono Autodesk® DXF, Autodesk® FBX, Blender (.blend), Wavefront OBJ, Google SketchUp (.skp), Stereolitography (.stl); tra i secondi, invece, figurano Autodesk® *AutoCAD*® (.dwg), Autodesk® *Maya*® (.ma, .mb), Autodesk® *3ds Max*® (.3ds), Maxon® *Cinema4D* (.c4d).

SVG	FORMATO DI FILE
Nome completo	Scalable Vector Graphics
Estensione/i	.svg, .svgz
Specializzazione di	XML (*namespace* svg)
Tipo MIME	image/svg+xml, image/svg+xml+zip
Sviluppato da	World Wide Web Consortium
Tipologia di standard	aperto, estendibile, *de jure*, testuale
Livello metadati	4
Derivato da	–
Revisione	1.1 (second edition)
Riferimenti	• W3C Recommendation *SVG 1.1 (2nd Ed.)*, 16 agosto 2011 • github.com/W3C/svgwg
Conservazione	Sì; cfr. §2.8
Racc. per la lettura	Generico; obbligatorio
Racc. per la scrittura	Generico; fortemente raccomandato

7. Il formato SVG, basato su XML, descrive un'immagine vettoriale componente per componente, utilizzando l'estendibilità del linguaggio per "etichettare" opzionalmente alcune parti di queste componenti affinché possano essere referenziate da altri documenti o applicativi (ad es., una pagina web in HTML e il suo foglio di stile CSS allo scopo di migliorare l'interattività con le immagini vettoriali). Data la sua versatilità e l'apertura dello standard è il formato fortemente raccomandato per l'uso, la trasmissione e la conservazione di tutte le immagini vettoriali.
C'è una nuova versione proposta per essere la futura SVG 2.0; essa supporta alcune caratteristiche quali l'animazione dei componenti. Tale versione, tuttavia, non è allo stato attuale raccomandata.

ILLUSTRATOR	FORMATO DI FILE
Nome completo	Adobe® *Illustrator*® artwork
Estensione/i	.ai
Specializzazione di	PDF, Encapsulated PostScript™
Tipo MIME	application/illustrator
Sviluppato da	Adobe Systems
Tipologia di standard	proprietario (libero), *de facto*, binario
Livello metadati	3

Firmato digitalmente da ROBERTO FRACCIA

Derivato da	Adobe® Encapsulated PostScript™, Adobe® PDF
Revisione	2019
Riferimenti	• Adobe Developer Support, *Adobe Illustrator File Format Specification*, 1998
Conservazione	No; cfr. §2.8
Racc. per la lettura	Specifico; nessuna raccomandazione
Racc. per la scrittura	Specifico; non raccomandato salvo che per scambio di semilavorati (a breve termine) tra reparti di design

8. Il formato proprietario dell'applicativo di disegno vettoriale Adobe® *Illustrator*® è in realtà un contenitore di un tipo specializzato di documento PDF ovvero di Encapsulated PostScript™, contenente estensioni particolari interpretabili dall'applicativo. Il formato è evoluto parecchio con le versioni successive di *Illustrator*®, che però ha sempre mantenuto la retrocompatibilità totale. Essendo l'applicativo molto diffuso tale formato è qui indicato perché è uno standard di riferimento per documenti in particolari ambiti (editoria e grafica pubblicitaria). Mentre è un formato consigliato per dei semilavorati (qualora vadano elaborati tramite *Illustrator*®), si sconsiglia di utilizzarlo per la produzione di documenti destinati alla conservazione, valutando piuttosto un riversamento dei documenti esistenti in altro formato più interoperabile (e.g. SVG).

ENCAPSULATED POSTSCRIPT	FORMATO DI FILE
Nome completo	Encapsulated PostScript®
Estensione/i	.eps
Specializzazione di	PostScript®
Tipo MIME	image/eps, application/eps
Sviluppato da	Adobe Systems
Tipologia di standard	proprietario (libero), *de facto*, binario, deprecato
Livello metadati	1
Derivato da	PostScript®
Revisione	3.0 (1992)
Riferimenti	• Adobe, *Encapslutated PostScript File Format Specifications*, v3.0 (1992)
Conservazione	No; cfr. §2.8
Racc. per la lettura	Specifico; raccomandato nei reparti di design
Racc. per la scrittura	Specifico; non raccomandato

9. Il formato EPS (Encapsulated PostScript™) è un dialetto del linguaggio PostScript™ (cfr. §2.1) con alcune distinzioni, come ad esempio la rappresentazione di un oggetto all'intero di una regione rettangolare confinata in una singola pagina

Firmato digitalmente da ROBERTO FRACCIA

e la possibilità di memorizzare una "pre-visualizzazione" raster (cd. *preview*) dell'intero contenuto. Di fatto, il formato è utilizzato il più delle volte per rappresentare singoli disegni o immagini da allegare successivamente a documenti PostScript™ impaginati ovvero, per via dell'apertura del formato, importarlo in altri applicativi di elaborazione vettoriale. Dato che il contenuto del documento è descritto nel linguaggio omonimo, orientato alle primitive di stampa, i file EPS non descrivono le immagini vettoriali come "oggetti" nell'accezione moderna, non supportando scenari di utilizzo più modulari o estendibili, come invece permette la scelta di formati più evoluti, quali ad esempio l'SVG. Il formato Encapsulated PostScript™ è dunque raccomandato in lettura per aprire documenti già esistenti, ma si sconsiglia la produzione di altri documenti in tale formato, invitando inoltre le PP.AA. a valutare il riversamento dei file esistenti in altri formati interoperabili (e.g. SVG).

ODG	FORMATO DI FILE
Nome completo	Open Document Graphics
Estensione/i	.odg
Magic number	XML imbustato dentro ZIP
Tipo MIME	application/vnd.oasis.opendocument.graphics
Sviluppato da	Organization for the Advancement of Structured Information Standards
Tipologia di standard	aperto, estendibile, *de iure*, binario
Livello metadati	3
Derivato da	–
Revisione	1.2 (2015)
Riferimenti	Famiglia di standard **26300** della ISO/IEC: • ISO/IEC 26300-1:2015, *ODF for Office Applications v1.2 – Part 1: OpenDocument Schema* • ISO/IEC 26300-3:2015, *ODF for Office Applications v1.2 – Part 3: Packages* • OASIS, *Open Document Format for Office Applications (OpenDocument)*, v1.2 (2015)
Conservazione	No; cfr. §2.8
Racc. per la lettura	Generico; raccomandato solo a scopo di riversamento
Racc. per la scrittura	Sconsigliato

10. Il formato ODG è il dialetto del formato OpenDocument (cfr. §2.3) per le immagini vettoriali; è incluso in questo elenco prevalentemente perché è completamente aperto ed è un necessario complemento agli altri dialetti, anche se il suo principale impiego è come allegato presente all'interno di testi impaginati (.odt), fogli di calcolo (.ods) e presentazioni multimediali (.odp).

Firmato digitalmente da ROBERTO FRACCIA

DXF	FORMATO DI FILE
Nome completo	AutoCAD® Drawing Interchange Format
Estensione/i	.dxf
Magic number	– / AutoCAD Binary DXF 0x0D0A1A00
Tipo MIME	image/vnd.dxf
Sviluppato da	Autodesk
Tipologia di standard	proprietario, libero, *de facto*, testuale e binario
Livello metadati	2
Derivato da	–
Revisione	2020/1
Riferimenti	• Autodesk, *DXF Reference*, 2011
Conservazione	No; cfr. §2.8
Racc. per la lettura	Specifico; nessuna raccomandazione
Racc. per la scrittura	Specifico; sconsigliato in archiviazione/conservazione

11. Pur trattandosi di un formato testuale (che descrive gli oggetti che compongono il modello o l'immagine mediante *primitive grafiche*) DXF permette una compressione facoltativa allo scopo di ridurre l'occupazione digitale del file. Tuttavia il numero di primitive grafiche utilizzate in questo formato non permette una rappresentazione con il medesimo livello semantico o di dettaglio tecnico di altri formati (p.es. i colori o i materiali); di conseguenza il formato non è completamente interoperabile con essi o con i loro applicativi.

DWF	FORMATO DI FILE
Nome completo	AutoCAD® Design Web Format
Estensione/i	.dwfx, .dwf
Magic number	–
Tipo MIME	model/vnd.dwf, drawing/dwf, image/dwf
Sviluppato da	Autodesk
Tipologia di standard	aperto, estendibile, *de iure*, testuale
Livello metadati	3
Derivato da	Open Packaging Convention
Revisione	6.0
Riferimenti	• Autodesk Knowledge Network, *About DWF and DWFx Files* • ISO/IEC 29500-2:2012
Conservazione	No; cfr. §2.8
Racc. per la lettura	Specifico; raccomandato in applicazioni CAD

Firmato digitalmente da ROBERTO FRACCIA

Racc. per la scrittura	Specifico; raccomandato per scambio e archiviazione di disegni e modelli tecnici in ambito CAD

12. Il formato DWF è stato specificatamente pensato per l'interoperabilità; è infatti basato, dalla versione 6.0, sullo standard ISO/IEC 29500-2 dell'*open packaging* (lo stesso usato da OOXML, §2.3), e dunque costituito da un file ZIP contenente più file differenti (XML per la descrizione del modello; PNG per le *preview* e le *texture*). Pur trattandosi di un formato testuale (che descrive gli oggetti che compongono il modello o l'immagine mediante *primitive grafiche*) il medesimo formato permette anche la compressione allo scopo di ridurre l'occupazione digitale del file. È spesso utilizzato come formato di interscambio e, tra tutti i formati imparentati, è quello con le specifiche più aperte, perciò è utilizzabile anche per archiviazione e conservazione.

DWG	FORMATO DI FILE
Nome completo	Autodesk® AutoCAD® Drawing
Estensione/i	.dwg, .dwt
Magic number	AC1032 (le ultime cifre variano con versione)
Tipo MIME	application/acad, image/vnd.dwg
Sviluppato da	Autodesk
Tipologia di standard	proprietario, libero, *de facto*, binario
Livello metadati	2
Derivato da	–
Revisione	DWG 2018
Riferimenti	• Autodesk, *AutoCAD .dwg file format* • Open Design, *Specification for .dwg*, v5.4.1 (2018)
Conservazione	Sì; cfr. §2.8
Racc. per la lettura	Specifico; nessuna raccomandazione
Racc. per la scrittura	Specifico; sconsigliato in archiviazione/conservazione

13. Il formato DWG è anch'esso proprietario ma ampiamente utilizzato per lo scambio di immagini vettoriali (prevalentemente bidimensionali) nel campo del disegno tecnico e dell'architettura.

FBX	FORMATO DI FILE
Nome completo	Autodesk® FBX®
Estensione/i	.fbx
Magic number	AC1032
Tipo MIME	model/vnd.fbx
Sviluppato da	Autodesk

Firmato digitalmente da ROBERTO FRACCIA

Tipologia di standard	proprietario (libero), chiuso, estendibile, *de facto*
Livello metadati	3
Derivato da	—
Revisione	2019 Extension 2
Riferimenti	• Autodesk Knowledge Network, *Autodesk FBX Files* • Blender Foundation, *FBX Binary file format specification*
Conservazione	Sì; cfr. §2.8
Racc. per la lettura	Specifico; raccomandato per modelli di progettazione
Racc. per la scrittura	Specifico; sconsigliato in archiviazione/conservazione

14. Il formato FBX, proprietario e chiuso ma completamente libero nel suo utilizzo, è utilizzato da vari applicativi di modellazione tridimensionale (ambito CAD e altro) prevalentemente come formato di interscambio. La sua estrema versatilità e il supporto del formato da parte di diversi applicativi professionali lo renderebbero adatto anche per archiviazione e conservazione, se non fosse per l'assenza di specifiche tecniche condivise.

STL	FORMATO DI FILE
Nome completo	Stereolithography file format
Estensione/i	.stl
Magic number	solid; —
Tipo MIME	model/stl, model/x.stl-ascii|binary
Sviluppato da	3D Systems (Albert-Battaglin Consulting Group)
Tipologia di standard	proprietario (libero), estendibile, *de facto*
Livello metadati	1
Derivato da	—
Revisione	2.0 (2009)
Riferimenti	• J.D. Hiller, H. Lipson, *STL 2.0: a proposal for a universal multi-material additive manufacturing file format*, 2009 • all3dp.com/what-is-stl-file-format-extension-3d-printing
Conservazione	No
Racc. per la lettura	Specifico; obbligatorio nel campo della stampa 3D
Racc. per la scrittura	Specifico; raccomandato nel campo della stampa 3D

15. Il formato STL (da non confondersi con l'omonimo formato per sottotitoli, cfr. § 2.11) è uno dei tanti standard *de facto* ed interoperabili per la modellazione

Firmato digitalmente da ROBERTO FRACCIA

tridimensionale industriale; recentemente si è affermato come formato d'elezione per la trasmissione di modelli per produzione tramite le tecniche di "stampa 3D" o stereolitografia. In quanto formato completamente aperto si consiglia il suo utilizzo per la produzione di prototipi con tale destinazione d'uso o loro archiviazione, anche se la mancanza di caratteristiche più avanzate (adatte alla prototipazione professionale (e.g. in ambito ingegneristico) non lo rendono un candidato ideale per qualunque modello tridimensionale.

2.7.1 Raccomandazioni per la produzione di documenti

1. Si raccomanda la creazione di immagini vettoriali e modelli tridimensionali in formati aperti ed interoperabili: per le immagini vettoriali sullo standard SVG del W3C viene adottato in un numero sempre crescente di contesti ed è oltretutto in continuo aggiornamento con nuove funzionalità.

2.8 Caratteri tipografici

1. Un esempio specializzato di immagine vettoriale –in questo caso bidimensionale e monocromatica– è costituita dal singolo "glifo" (i.e. carattere tipografico), per il quale possono essere rappresentate forme distinte nello stesso file. All'interno di un file di fonti tipografiche (*font* in inglese) esiste una tabella ove, per un sottoinsieme di tutti i possibili caratteri tipografici rappresentabili da un sistema operativo (e codificati mediante codici numerici negli standard ASCII, UNICODE, ovvero UTF-8 e UTF-16), è contenuta la rappresentazione vettoriale del glifo corrispondente al carattere. In un file di font ai caratteri può corrispondere più di un glifo, che rappresenta varianti di quel carattere a seconda del tipo (e.g. tondo o corsivo), del peso (e.g. sottile, regolare, grassetto, nero), di altri fattori stilistici (e.g. numerali vecchio stile o meno) e, in alcuni casi, della dimensione/grandezza del carattere per tener conto del cosiddetto "aggiustamento ottico". In alcuni casi tali variazioni stilistiche dei glifi sono mantenute in file separati (ad esempio un file per ciascuna combinazione di tipi e pesi), che vanno a costituire dunque un "pacchetto di font" (cfr. definizioni date in §1.1.2).
2. Le seguenti famiglie di caratteri tipografici –organizzati in macro-tipologie– sono considerati "standard" da diversi organi di settore (come il W3C) — si leggano le raccomandazioni più sotto:

Firmato digitalmente da ROBERTO FRACCIA

- "bastoni": sans-serif, Arial, Helvetica, Trebuchet, Verdana, Lucida Sans, Comic Sans;
- con grazie: serif, Times, Times New Roman, Palatino, Georgia;
- larghezza fissa: monospace, Courier, Courier new, Lucida Console;
- simboli: Symbol, Zapf Dingbats, Webdings, Wingdings.

3. I caratteri tipografici di cui al punto precedente sono chiamati, all'interno delle Linee guida di cui questo Allegato fa parte, "font interoperabili". Le PP.AA. che producono documenti informatici il cui contenuto dipende anche dai caratteri tipografici impiegati, si impegnano a prendere le misure tecnico-organizzative del caso (inclusa l'effettuazione di una valutazione di interoperabilità, cfr. §3.1), affinché la produzione di tali documenti includa i caratteri tipografici utilizzati nel file stesso ovvero sia costituito da un pacchetto di file contenente anche i caratteri tipografico. Qualora ciò non sia tecnicamente possibile, le PP.AA. si adoperano per utilizzare solamente caratteri tipografici interoperabili.
4. I formati più diffusi e interoperabili di font tipografici sono

d) TrueType (.ttf) e la sua evoluzione, OpenType (.otf), utilizzati negli applicativi dei principali SO tradizionali e mobile;
e) Web Open Font Format (.woff, .woff2), usati per le pagine web.

OpenType	Formato di file
Nome completo	OpenType®
Estensione/i	.otf
Magic number	OTTO 0x00
Tipo MIME	font/otf, application/x-font-otf
Sviluppato da	Microsoft, Adobe, Apple, Google
Tipologia di standard	proprietario (libero), *de iure*, binario
Livello metadati	3
Derivato da	TrueType®
Revisione	1.8.3
Riferimenti	• ISO/IEC 14496-22:2015 • Microsoft OpenType® specifications 1.8.3 (2018) • RFC-2361
Conservazione	Sì
Racc. per la lettura	Generico; obbligatorio
Racc. per la scrittura	Specifico; obbligatorio

TrueType	Formato di file
Nome completo	TrueType®
Estensione/i	.ttf

Firmato digitalmente da ROBERTO FRACCIA

Magic number	true 0x00
Tipo MIME	font/ttf, application/x-font-ttf
Sviluppato da	Apple, Microsoft
Tipologia di standard	proprietario (libero), *de facto*, binario
Livello metadati	1
Derivato da	Adobe Type-1
Revisione	1994
Riferimenti	• Apple Developer, *TrueType™ Reference Manual* • Microsoft Typography webpage
Conservazione	Sì
Racc. per la lettura	Generico; obbligatorio
Racc. per la scrittura	Specifico; valutare utilizzo del formato OpenType

WOFF	FORMATO CONTENITORE
Nome completo	Web Open Font Format
Estensione/i	.woff2; .woff
Magic number	wOF2; wOFF
Tipo MIME	font/woff2, application/font-woff
Sviluppato da	Mozilla Foundation, Opera Software, Microsoft
Tipologia di standard	proprietario (libero), *de iure*, binario
Livello metadati	1
Derivato da	OpenType®
Revisione	2.0
Riferimenti	• W3C Recommendation, *WOFF 2.0*, 2018 • W3C Recommendation, *WOFF 1.0*, 2012 • github.com/W3C/woff
Conservazione	Sì
Racc. per la lettura	Specifico; raccomandato per tipografia di contenuti web
Racc. per la scrittura	Specifico; raccomandato per caratteri nonstandard in pagine web

2.8.1 Raccomandazioni per la produzione di documenti

1. Sia per l'utilizzo applicativo che per quello web si fanno le seguenti due raccomandazioni:

Firmato digitalmente da ROBERTO FRACCIA

a) Qualora di adoperino caratteri tipografici standard (come indicati all'inizo della sezione) i punti seguenti non costituiscono più raccomandazioni.
b) Si includano sempre i file dei caratteri tipografici utilizzati nel documento (quando tali caratteri possono essere imbustati nel formato del documento),[30] ovvero si formi un pacchetto di file (cfr. §1.1.1) che comprenda anche tali caratteri tipografici.
c) Qualora i caratteri tipografici siano utilizzati per rappresentare testi scritti (come semplice collezione di simboli), scegliere solo caratteri tipografici che contengano un numero sufficiente di glifi a rappresentare *almeno* i caratteti alfanumerici, di interpunzione e diacritici del linguaggio utilizzato, della lingua italiana e di quella inglese inglese.
d) Ottemperare, se possibile, alla raccomandazione 1. per i caratteri alfanumerici, di interpunzione e diacritici di tutte le lingue dell'Unione Europea;[31]
e) Qualora dei caratteri tipografici non standard siano utilizzati per rappresentare testi scritti, mettere in atto tutte le metodiche tecniche e operative previste dai formati di file e di pacchetti utilizzati affinché, nel caso in cui i file dei caratteri tipografici non siano disponibili, l'applicativo usato per visualizzare, stampare o riprodurre il documento possa effettuare sostituzioni dei caratteri tipografici[32] con altri caratteri standard, senza che ciò risulti in una variazione sostanziale del contenuto informativo del documento.

2. Per ogni altra considerazione riguardo l'uso dei caratteri tipografici nei documenti informatici si rimanda alle *Linee guida sull'accessibilità* e alle *Linee guida di design*, anch'esse emanate dall'Agenzia per l'Italia Digitale.

2.9 Audio e musica

1. La rappresentazione digitale dei segnali audio è divisa in due categorie: quella per "forme d'onda" e quella, più indiretta, per metadati. Nel primo caso il segnale sonoro è rappresentato mediante un'approssimazione digitale dell'onda sonora, registrata o riprodotta. In fase di registrazione del sonoro la forma d'onda si ottiene mediante campionamento (misurato in numero di campioni per secondo, o *sample rate*) e quantizzazione (misurato in bit per campione); il prodotto di tali misure

[30] Come accade, ad esempio per alcuni tipi di file PDF (§2.1) di pacchetti IMF ovvero DCP (§2.12).
[31] Le raccomandazioni 1. e 2. servono a confermare, a priori, che il carattere tipografico può potenzialmente rappresentare altri caratteri tipografici e alfabetici qualora il testo andasse modificato ovvero tradotto in altra lingua.
[32] Tali sostituzioni possono avvenire anche a catena, purché terminino sempre con un carattere tipografico standard (denominato, in inglese, *fallback* font). Si consideri, come esempio, la seguente catena di sostituzioni tipografiche: Minion Pro > Minion Std > Noto Serif > Albertina > Times New Roman > Times > serif.

Firmato digitalmente da ROBERTO FRACCIA

costituisce il data-rate audio (anche detto *bit-rate* perché misurato in bit per secondo). Un file o un flusso audio può rappresentare le forma d'onda di più sorgenti sonore contemporaneamente — dette "canali".
2. I campioni audio di una forma d'onda possono subire una compressione digitale allo scopo di ridurne le dimensioni occupate. I formati più noti per la memorizzazione di tali segnali audio sono il Waveform RIFF (.wav), MP3, FLAC, OGG e Broadcast Wave (.bwf).
3. Nel secondo caso, invece, il file contiene una rappresentazione temporale di suoni pre-campionati (che possono essere contenuti nel medesimo file, o riferendosi a file esterni contenenti le loro forme d'onda) e degli eventuali effetti associati a tali campioni ovvero alla loro riproduzione. L'applicazione principale per tali file è la rappresentazione di brani musicali, ove il timbro di ciascuno strumento è associato a banche dati generiche di suoni (che obbediscono a standard quali General MIDI) ovvero salvato come forma d'onda esterna, mentre il file audio contiene la partitura completa, nota per nota. Appartengono a questa tipologia i file musicali registranti uno standard quale il MIDI (.mid).

WAV	FORMATO CONTENITORE
Nome completo	[Broadcast] Waveform File
Estensione/i	.wav, .bwf, .rf64
Magic number	WAVE, RIFF
Tipo MIME	audio/wave
Sviluppato da	IBM; Microsoft
Tipologia di standard	proprietario, libero, *de iure*, binario
Livello metadati	3
Derivato da	Resource Interchange File Format (RIFF)
Revisione	2018
Riferimenti	• Microsoft, *Multimedia Data Standards Update* (1994) • RFC-2361 • EBU Recommenation R111 (2007) • EBU – Tech 3285-1, *Broadcast Wave (BWF)* (2011) • EBU – Tech 3306 , *RF64* (2018) • soundfile.sapp.org/doc/WaveFormat
Conservazione	Sì, senza compressione
Racc. per la lettura	Generico; obbligatorio per audio qualunque
Racc. per la scrittura	Generico; fortemente raccomandato per audio qualunque

Firmato digitalmente da ROBERTO FRACCIA

MP3	Formato di file / Codec
Nome completo	MPEG-1, Layer 3
Estensione/i	.mp3
Magic number/FourCC	0xFFFB30; ID3 / mp3
Tipo MIME	audio/mpeg
Sviluppato da	Moving Pictures Expert Group
Tipologia di standard	aperto, estendibile, *de iure*, binario
Livello metadati	4
Derivato da	MPEG-ES
Revisione	1998
Riferimenti	• ISO/IEC 11172-3:1993 • ISO/IEC 13818-3:1998 • mpgedit.org/mpgedit/mpeg_format/MP3Format.html
Conservazione	No
Racc. per la lettura	Generico; obbligatorio
Racc. per la scrittura	Generico; raccomandato per contenuti musicali

AIFF	Formato di file
Nome completo	Audio Interchange File Format
Estensione/i	.aiff, .aifc, .aif
Magic number	AIFF; AIFC
Tipo MIME	audio/aiff
Sviluppato da	Moving Pictures Expert Group
Tipologia di standard	proprietario (libero), estendibile, *de facto*, binario
Livello metadati	3
Derivato da	Electronic Arts® Interchange File Format (IFF)
Revisione	1.3 (1991)
Riferimenti	• Apple Developer, *Audio Interchange File Format: "AIFF"* • www-mmsp.ece.mcgill.ca/Documents/AudioFormats/AIFF
Conservazione	No
Racc. per la lettura	Nessuna raccomandazione
Racc. per la scrittura	Nessuna raccomandazione

FLAC	Formato di file / Codec
Nome completo	Free Lossless Audio Codec
Estensione/i	.flac

Firmato digitalmente da ROBERTO FRACCIA

Magic number/FourCC	fLaC / FLAC
Tipo MIME	audio/flac
Sviluppato da	comunità open source
Tipologia di standard	aperto (licenze GNU GPL e BSD), *de facto*, binario
Livello metadati	3
Derivato da	–
Revisione	1.3.2 (2017)
Riferimenti	• xiph.org/flac
Conservazione	Sì
Racc. per la lettura	Specifico; raccomandato
Racc. per la scrittura	Specifico; raccomandato

RAW — FORMATO DI FILE

Nome completo	Audio “Raw”
Estensione/i	.pcm, .raw, .sam, …
Magic number	–
Tipo MIME	audio/basic
Sviluppato da	comunità open source e altri *vendor*
Tipologia di standard	aperto, *de facto*, muto, binario
Livello metadati	1
Derivato da	–
Revisione	–
Riferimenti	• www.fmtz.com/misc/raw-audio-file-formats • en.wikipedia.org/wiki/Au_file_format • www-mmsp.ece.mcgill.ca/Documents/AudioFormats/AU
Conservazione	Sì
Racc. per la lettura	Specifico; raccomandato per le registrazioni ambientali
Racc. per la scrittura	Specifico; raccomandato per le registrazioni ambientali

VORBIS — CODEC

Nome completo	Vorbis
Profili	–
Codice FourCC	vorb
Sviluppato da	comunità open source
Tipologia di standard	aperto, *de facto*

Firmato digitalmente da ROBERTO FRACCIA

Derivato da	–
Revisione	2015
Riferimenti	• Xiph.Org, *Vorbis I specification*, 2015 • xiph.org/vorbis
Conservazione	No
Racc. per la lettura	Specifico; raccomandato
Racc. per la scrittura	Nessuna raccomandazione

MusicXML — FORMATO DI FILE

Nome completo	MusicXML™
Estensione/i	.musicxml
Specializzazione di	XML
Tipo MIME	application/vnd.recordare.musicxml
Sviluppato da	W3C Music Notation Community Group
Tipologia di standard	aperto, estendibile, *de facto*, testuale
Livello metadati	4; cfr. §2.8
Derivato da	MakeMusic® MusicXML, MuseData™, Humdrum™
Revisione	3.1 (2017)
Riferimenti	• W3C Community Group Final Report, *MusicXML 3.1*, 2017 • www.musicxml.com
Conservazione	Sì
Racc. per la lettura	Specifico; raccomandato per le partiture musicali
Racc. per la scrittura	Specifico; fortemente consigliato per partiture musicali

MIDI — FORMATO DI FILE

Nome completo	Musical Instrument Digital Interface
Estensione/i	.mid, .midi
Magic number	MThd
Tipo MIME	audio/midi, application/x-midi
Sviluppato da	MIDI Manufacturers Association (MMA)
Tipologia di standard	aperto, estendibile, *de facto*, binario
Livello metadati	1
Derivato da	–
Revisione	1.1

Firmato digitalmente da ROBERTO FRACCIA

Riferimenti	• www.midi.org/specifications • McGill, *Standard MIDI-File Format Spec. 1.1*. • McGill, *Standard MIDI Files ("SMF")*. • RFC-6295 • *General MIDI ("GM") Specifications*: GM1, Roland® *GS*, Yamaha® *XG*, GM2.
Conservazione	Sì, purché adottando solo strumenti General MIDI
Racc. per la lettura	Specifico; obbligatorio per la riproduzione di musica strumentale; raccomandato per partiture musicali
Racc. per la scrittura	Specifico; raccomandato per partiture musicali con orchestrazione rappresentabile da questo standard

2.9.1 Raccomandazioni per la produzione di documenti

1. Per quanto riguarda la creazione di documenti audio (di entrambe le categorie elencate all'inizio della sezione) si raccomanda la scelta di formati interoperabili ed aperti: di conseguenza tutti i formati elencati –ad eccezione di AIFF– soddisfano tale caratteristica. Il wave, essendo in realtà un contenitore, è poi soggetto alla scelta del codec per rappresentare il contenuto audio. In questo caso si raccomandano codec aperti (come il "*raw*" non compresso, ovvero il PCM o il μ-law). La scelta di formati "*raw*," sebbene dettata spesso da esigenze contingenti, andrebbe evitata in quanto tali formati sono notoriamente muti (cfr. §1.2.2) e quindi può essere difficile ricostruire le caratteristiche, sia ambientali che tecniche, di registrazione e di campionamento.
2. Resta appannaggio delle singole organizzazioni valutare i parametri qualitativi in merito ai codec audio impiegati (ove sussistano come parametri variabili), tenendo conto ancora una volta di eventuali vincoli normativi, amministrativi e tecnologici. La scelta a priori dei parametri qualitativi può aiutare a standardizzare un processo e verificare che tutti gli organi coinvolti possano leggere o scrivere file con tali parametri.
3. Tra i formati sopra individuati, il WAV (con codifica PCM non compressa) e tutti i formati "*raw*" senza ausilio di compressione sono i formati più adatti alla conservazione. Nei casi in cui non si può evitare la compressione della forma d'onda, può essere adottato anche il formato FLAC.

Firmato digitalmente da ROBERTO FRACCIA

2.10 Video

1. Un file (ovvero un flusso) video *strictu sensu* rappresenta una sequenza ordinata di immagini raster (dette fotogrammi — *frame* in inglese) riprodotte ad una velocità temporale fissa, espressa in numero di fotogrammi al secondo (alle volte si usa la sigla "fps" o, più impropriamente, l'unità di misura Hertz, "Hz"). Per il resto si applicano al video le stesse descrizioni relative alle immagini raster: risoluzione, profondità di colore, colorimetria, ecc.
2. Anche nel video, come per le immagini statiche e l'audio, è possibile implementare diversi algoritmi di compressione allo scopo di ridurre le dimensioni del file ovvero del flusso digitale. Quando la compressione riguarda individualmente e separatamente ogni singolo fotogramma si parla di compressione *intra*-frame (che è concettualmente identica a quella applicata alle immagini raster); quando la compressione utilizza le informazioni residue di un fotogramma (calcolate rispetto ai fotogrammi precedenti o antecedenti) si parla invece di compressione *inter*-frame.
3. Quest'ultima tipologia di compressione utilizza modelli matematici e statistici tipicamente più sofisticati di quelli usati nella prima tipologia, il che rende spesso l'operazione di codifica più lunga e laboriosa di quella di decodifica. Per il motivo di cui al punto precedente, la compressione inter-frame è raccomandata per applicazioni ove la tecnologia, le tempistiche e i costi si distribuiscano in modo da avere una generazione del video più lunga, laboriosa e in generale dispendiosa, a fronte di una minore complessità di decompressione a carico dei dispositivi riproduttori[33].
4. Al contrario, la compressione intra-frame, isolando ogni fotogramma in un'evidenza compressa a se stante, pur non fornendo in generale gli stessi rapporti di compressione di quella inter-frame, la rendono spesso –ma non sempre– preferibile in due particolari casi d'uso:

- quando sia frequente la riproduzione casuale del documento video, che consiste nel saltare da un punto all'altro della *timeline*[34] (discontinuità temporale) piuttosto che riprodurla sequenzialmente;
- quando il documento debba potersi modificare (cioè aggiungendo, inserendo, sostiutendo o eliminandone sue parti dalla timeline) senza alterarne la qualità.

5. Algoritmi di compressione intra-frame molto diffusi –non necessariamente associati a specifici formati di file– includono l'MJPEG, l'AVC-Intra (di proprietà di

[33] La compressione inter-frame favorisce dunque gli scenari d'uso ove la codifica (compressione) è effettuata una tantum da dispositivi centralizzati e computazionalmente potenti, a fronte di una riproduzione (decompressione) in serie, effettuata da una moltitudine di dispositivi riproduttori "*consumer*" con caratteristiche tecnologiche inferiori (inclusa la necessità di risparmio energetico). Un esempio tipico è la riproduzione cine-televisiva o in streaming on-demand, ove i riproduttori spaziano dai televisori ai *tablet*, agli *smartphone*.
[34] La timeline verrà definita in §2.12.

Firmato digitalmente da ROBERTO FRACCIA

Panasonic®), la famiglia di codec proprietari ProRes® della Apple®, i vari video-codec ("VC") della SMPTE e il derivato proprietario dal codec VC-3: la famiglia DNxHD® della Avid®.

6. Algoritmi di compressione inter-frame largamente diffusi sono invece MPEG-2, MPEG-4, H.264 (e una sua variante proprietaria: AVCHD), XAVC (detto anche impropriamente "H.265") e la famiglia XDCAM™, anch'essa proprietaria e da non confondere con i formati del pacchetto di file usato nella medesima famiglia di prodotti (e in questo Allegato indicato in maniera tipograficamente diversa come "XDCAM", cfr. §2.12).

HEVC / H.265	CODEC
Nome completo	High Efficiency Video Coding
Profili	Main, High; 13 livelli
Codice FourCC	hevc, h265, x265
Sviluppato da	Joint Collaborative Team on Video Coding (JCT-VC)
Tipologia di standard	proprietario (*royalty* per varie tipologie d'uso), *de iure*
Derivato da	MPEG-H Part 2
Revisione	2018
Riferimenti	• ISO/IEC 23008-2:2017 • ISO/IEC 23008-2/Amd-1:2018 • ITU-T Recommendation H.265 (2018) • ETSI TS-126-114 v15.7.0 (2019) • x265.org/hevc-h265
Conservazione	No
Racc. per la lettura	Generale; raccomandato
Racc. per la scrittura	Generale; sconsigliato per archiviazione

H.264 / AVC	CODEC
Nome completo	Advanced Video Coding
Profili	21 profili e 20 livelli
Codice FourCC	h264, x264, avc1, davc, vssh, v264
Sviluppato da	Joint Collaboration Team on Video Codec (JCT-VC)
Tipologia di standard	proprietario (*royalty* per uso commerciale), *de iure*
Derivato da	MPEG-4 Part 2 (Visual), H.263
Revisione	2014
Riferimenti	• ISO/IEC 14496-10:2014 • ITU-T Recommendation H.264 (2019) • ETSI TS-126-114 v15.7.0 (2019) • x265.org/hevc-h265
Conservazione	Sì, purché con profili e livelli almeno "High"

Firmato digitalmente da ROBERTO FRACCIA

Racc. per la lettura	Generale; obbligatoria la lettura
Racc. per la scrittura	Generale; raccomandato per archiviazione o conserva- zione di contenuti non cinetelevisivi ovvero master cinetelevisivi già sottoposti a elaborazione finale

MP4V	CODEC
Nome completo	MPEG-4 Part 2 MPEG-4 Visual
Profili	21 profili (tra cui SP, ASP, SStP)
Codice FourCC	mp4v, mp42, avc1, v264
Sviluppato da	Video Coding Experts Group (VCEG), Moving Picture Experts Group (MPEG)
Tipologia di standard	proprietario (*royalty* per uso commerciale), *de iure*
Derivato da	H.263, MPEG-2 Part 2
Revisione	2014
Riferimenti	• ISO/IEC 14496-2:2004
Conservazione	No
Racc. per la lettura	Generale; obbligatoria la lettura
Racc. per la scrittura	Generale; raccomandato per archiviazione non a lungo termine; sconsigliato in conservazione ovvero quando sono necessari ulteriori metadati

H.263	CODEC
Nome completo	H.263 (XviD)
Profili	vari profili
Codice FourCC	h263, s263
Sviluppato da	Video Coding Experts Group
Tipologia di standard	proprietario (*royalty* per uso commerciale), *de iure*
Derivato da	MPEG-2 Part 2
Revisione	2006
Riferimenti	• ITU-T Recommendation Y.4414/H.263 (2005) • ETSI TS-126-141 v15.0.0 (2018)
Conservazione	No
Racc. per la lettura	Generale; obbligatoria la lettura
Racc. per la scrittura	Generale; sconsigliata la produzione

Firmato digitalmente da ROBERTO FRACCIA

MPEG2	CODEC
Nome completo	MPEG-2 Part 2
Profili	7 profili e 4 livelli
Codice FourCC	mp2v
Sviluppato da	Video Coding Experts Group, Moving Picture Experts Group
Tipologia di standard	aperto, *de iure*
Derivato da	MPEG-1
Revisione	2018
Riferimenti	• ISO/IEC 13818-2:2013
Conservazione	Sì
Racc. per la lettura	Generale; obbligatoria la lettura
Racc. per la scrittura	Generale; sconsigliato per archiviazione e conserva-zione di contenuto cinetelevisivo professionale

DNxHD	CODEC
Nome completo	DNxHD® / DNxHR™ [35]
Profili	vari *bit-rate* in Mb/s / LB,SQ,HQ,444,HQX
Codice FourCC	AVdn
Sviluppato da	Avid
Tipologia di standard	proprietario (licenza commerciale), *de facto*
Derivato da	SMPTE VC-3
Revisione	Codecs LE 2.7.3 (2018)
Riferimenti	• www.avid.com • avid.force.com Famiglia **ST2019** di standard/raccomandazioni SMPTE: • ST2019-1:2014
Conservazione	No
Racc. per la lettura	Speciale; consigliato in post-produzione cinetelevisiva
Racc. per la scrittura	Speciale; sconsigliato per archiviazione/conservazione

7. Il codec audio/video proprietario, indicato semplicemente come DNxHD®, dotato di compressione *lossy* e intra-frame, consiste in una specializzazione di alcuni profili del codec aperto VC-3 standardizzato dalla SMPTE (descritto altrove in questa sezione), adattato per l'utilizzo nella post-produzione non-lineare di documenti audiovisivi professionali. In particolar modo le essenze audio video sono vincolate a un insieme discreto di risoluzioni spaziali, profondità di colore, *framerate* e bit-rate costanti o variabili, ottimizzati per contenuti in risoluzione HD (1920×1080 punti,

[35] I nomi commerciali dei codec sono acronimi di '**D**igital **N**onlinear E**x**tensible **H**igh **D**efinition' e '**H**igh Dynamic **R**ange' rispettivamente.

Firmato digitalmente da ROBERTO FRACCIA

si parla in questo caso di codec DNxHD®) e l'UltraHD 4K (3840×2160, si parla in questo caso di codec DNxHR™) che andranno successivamente montati e post-processati (ad esempio tramite operazioni di *color-grading* –in HDR o meno– *compositing*), possibilmente mediante operazioni "non-distruttive", cioè riducendo il più possibile l'impatto che tali procedimenti di post-produzione avranno sulla qualità del documento masterizzato. La produzione del formato è chiusa e proprietaria, sebbene sia uno standard de facto del settore cinetelevisivo che diversi applicativi hardware e software sono in grado sia di produrre che di riprodurre. Nella loro declinazione nativa, le essenze audio/video con codec DNxHD® sono imbustate in un contenitore MXF (descritti nel §2.12) anch'esso dotato di particolari metadati. Tali metadati coadiuvano e semplificano il collegamento logico delle essenze audiovisive che, contenute in file separati, vengono associate insieme temporalmente da parte degli applicativi di montaggio non-lineare. È tuttavia possibile imbustare essenze DNxHD® n altri formati *wrapper*, come ad esempio il QuickTime.

ProRes	Codec
Nome completo	ProRes®
Profili	Proxy, LT, 422, HQ, 4444, XQ, RAW
Codice FourCC	apco, apcs, apcn, apch, ap4h, ap4x, aprh/aprn
Sviluppato da	Apple Incorporated
Tipologia di standard	proprietario (*royalty* per la produzione), *de facto*
Derivato da	Apple Intermediate Codec
Revisione	2018
Riferimenti	• Apple, *ProRes White Paper* (2018) • Apple, *ProRes RAW White Paper* (2018)
Conservazione	No
Racc. per la lettura	Speciale; raccomandato nel montaggio cinetelevisivo
Racc. per la scrittura	Sconsigliato per l'archiviazione o conservazione.

8. L'Apple ProRes® è un codec audio/video proprietario dotato di compressione *lossy* e intra-frame, specializzato anch'esso per il montaggio non-lineare di documenti audiovisivi professionali. È dotato di diversi profili cui sono associate profondità di colore e bit-rate predeterminati (mentre non vi sono vincoli alla risoluzione o al *framerate* come accade per altri codec)

AV1	Codec
Nome completo	AOMedia Video 1
Profili	3 profili e 10 livelli
Codice FourCC	av01
Sviluppato da	Alliance for Open Media

Firmato digitalmente da ROBERTO FRACCIA

Tipologia di standard	aperto, *de facto*
Derivato da	VP9, VP10
Revisione	2018
Riferimenti	• aomediacodec.github.io/av1-spec
Conservazione	No
Racc. per la lettura	Speciale; raccomandato per contenuti in *streaming* web
Racc. per la scrittura	Speciale; sconsigliato per archiviazione/conservazione

DASH / VP9 — CODEC

Nome completo	Video Partition structured video codec #9
Profili	–
Codice FourCC	VP90
Sviluppato da	Google
Tipologia di standard	proprietario (libero), *de facto*
Derivato da	VP8
Revisione	2014
Riferimenti	• Google, *VP9 bitstream & decoding process specification* v0.6 (2016) • ISO/IEC 14496-12:2015 • ISO/IEC 14496-12:2015 /Amd 2:2018 • Standard SMPTE ST2086:2014 • www.webmproject.org/vp9 • github.com/webmproject/vp9-dash
Conservazione	Sì
Racc. per la lettura	Speciale; raccomandato per contenuti in *streaming* web
Racc. per la scrittura	Speciale; sconsigliato per archiviazione/conservazione

CINEFORM — CODEC

Nome completo	SMPTE Video Codec #5
Profili	3 profili e 10 livelli
Codice FourCC	CFHD
Sviluppato da	Society of Motion Picture and Television Engineers
Tipologia di standard	aperto, *de iure*
Derivato da	GoPro® CineForm™
Revisione	2016
Riferimenti	Famiglia **ST2073** di standard SMPTE: • ST2073-1:2014, RP2073-2:2017, ST2073-3:2015, ST2073-4:2015, ST2073-5:2015, ST2073-6:2015 • gopro.github.io/cineform-sdk
Conservazione	No
Racc. per la lettura	Speciale; consigliato in post-produzione cinetelevisiva

Firmato digitalmente da ROBERTO FRACCIA

Racc. per la scrittura	Speciale; sconsigliato per archiviazione/conservazione

VC-3	CODEC
Nome completo	SMPTE Video Codec #3
Profili	–, HQ
Codice FourCC	AVdn
Sviluppato da	Society of Motion Picture and Television Engineers
Tipologia di standard	aperto, *de iure*
Derivato da	SMPTE VC-2 (“Dirac Pro”)
Revisione	2002
Riferimenti	Famiglia **ST2019** di standard/prassi SMPTE: • ST2019-1:2014, RP2019-2:2016, ST2019-4:2014
Conservazione	Sì
Racc. per la lettura	Speciale; consigliato in post-produzione cinetelevisiva
Racc. per la scrittura	Speciale; consigliato in post-produzione cinetelevisiva

HDCAM	CODEC
Nome completo	HDCAM
Profili	–, SR [Lite], SQ, HQ; diversi *bitrate*
Codice FourCC	—
Sviluppato da	Society of Motion Picture and Television Engineers
Tipologia di standard	proprietario (libero), *de iure*
Derivato da	Sony HDCAM™
Revisione	2005
Riferimenti	• Standard SMPTE ST367M:2001 *Type D-11 HDCAM picture compression and data stream format* • Standard SMPTE ST368:2002, *for digital television tape recording – 12.65mm Type D-11 format*
Conservazione	No
Racc. per la lettura	Speciale; consigliato per riprodurre e riversare repertori in nastri digitali HDCAM™ (formato D-11)
Racc. per la scrittura	Speciale; sconsigliato per la produzione di nastri

DIRAC Pro	CODEC
Nome completo	SMPTE Video Codec #2 “Dirac Pro”
Profili	–, SR [Lite], SQ, HQ

Firmato digitalmente da ROBERTO FRACCIA

Codice FourCC	Bbcd
Sviluppato da	Society of Motion Picture and Television Engineers
Tipologia di standard	aperto, *de iure*
Derivato da	BBC "Dirac"
Revisione	2016
Riferimenti	Famiglie **ST2042** e **ST2047** di standard SMPTE: • ST2042-1:2090, RP2042-2:2009, RP2042-3:2010,
Conservazione	No
Racc. per la lettura	Speciale; consigliato in post-produzione cinetelevisiva
Racc. per la scrittura	Speciale; sconsigliato per archiviazione/conservazione

XAVC — CODEC

Nome completo	XAVC™
Profili	H.264 livello 5.2
Codice FourCC	Xavc
Sviluppato da	Sony
Tipologia di standard	proprietario (*royalty* per uso commerciale), *de facto*
Derivato da	MPEG-2, H.263, MPEG-4 Part 2
Revisione	2018
Riferimenti	• www.xavc-info.org, *XAVC profiles and Operating Points* v1.20 (2016)
Conservazione	No
Racc. per la lettura	Speciale; consigliato in post-produzione cinetelevisiva
Racc. per la scrittura	Da *non* utilizzare per la produzione di documenti.

XDCAM — CODEC

Nome completo	XDCAM™
Profili	DVCAM, IMX, SD, EX, HD422, HD, SD422
Codice FourCC	xdv1, xdv2, …, xdv9, xdva
Sviluppato da	Sony
Tipologia di standard	proprietario (*royalty* per uso commerciale), *de facto*
Derivato da	MPEG-4 Part 2, MPEG-2 Part 2, DV
Revisione	2018
Riferimenti	• sonybiz.net
Conservazione	No
Racc. per la lettura	Speciale; consigliato in post-produzione cinetelevisiva
Racc. per la scrittura	Speciale; sconsigliato per archiviazione/conservazione

Firmato digitalmente da ROBERTO FRACCIA

BRAW	FORMATO DI FILE
Nome completo	Blackmagic RAW
Profili	XXXXX
Codice FourCC	Braw
Sviluppato da	Blackmagic Design
Tipologia di standard	proprietario
Derivato da	CinemaDNG™
Revisione	2018
Riferimenti	• www.blackmagicdesign.com
Conservazione	No
Racc. per la lettura	Speciale; consigliato in post-produzione cinetelevisiva
Racc. per la scrittura	Speciale; sconsigliata la produzione

AVC-INTRA	CODEC
Nome completo	AVC-Intra™
Profili	2 *bit-rate* e 6 risoluzioni
Codice FourCC	ai[5|1][p|q|2|3|5|6]
Sviluppato da	Sony
Tipologia di standard	proprietario (*royalty* per uso commerciale), *de iure*
Derivato da	MPEG-4 Part 10
Revisione	2014
Riferimenti	• prassi raccomandata SMPTE RP2027:2012 • ISO/IEC 14496-10:2014
Conservazione	No
Racc. per la lettura	Speciale; raccomandata la lettura
Racc. per la scrittura	Da *non* utilizzare per la produzione di documenti.

9. AVC-Intra deriva dal profilo High 10 Intra di H.264.

MJPEG	FORMATO DI FILE / CODEC
Nome completo	Motion JPEG
Profili	A, B
Codice FourCC	mjpg, mjpa, mjpb
Sviluppato da	comunità open source
Tipologia di standard	aperto, *de facto*
Derivato da	JPEG
Revisione	1998
Riferimenti	• RFC-2435
Conservazione	Sì
Racc. per la lettura	Generico con obbligo in lettura

Firmato digitalmente da ROBERTO FRACCIA

Racc. per la scrittura	Generico; consigliato per contenuti non cinetelevisivi che non necessitano di ulteriori metadati

10. Il formato MJPEG, come recita il suo stesso acronimo, «Motion JPEG», è un formato video ove l'essenza video è codificata come una sequenza di immagini raster nel formato JPEG, adottando dunque una compressione *lossy* e intra-frame. Nonostante il formato sia datato, la sua semplicità di codifica lo rende ancora raccomandato in tutti gli utilizzi non professionali ove il documento informatico non abbia particolari requisiti di qualità (o comunque requisiti di qualità non superiore a quella della compressione JPEG scelta per l'essenza MJPEG).

2.10.1 Raccomandazioni per la produzione di documenti

1. I file e i flussi multimediali –e in particolar modo quelli video– contengono evidenze con caratteristica peculiare rispetto a tutte le altre tipologie di file: i flussi video (compressi o meno che siano) hanno una dimensione digitale elevata e, tipicamente, richiedono anche una banda passante minima in caso vadano formati, riprodotti o addirittura elaborati in tempo reale. Pe questo motivo le scelte dei formati avranno un'elevata variabilità in base alla finalità d'uso e ai vincoli tecnologici ad esse collegati.[36]
2. Lo strumento della valutazione di interoperabilità (cfr. §3.1) può venire in contro alla risoluzione *ex ante* delle problematiche di cui al punto precedente, allo scopo di individuare prima i codec da usare per far fronte a tutte le esigenze e vincoli (normativi, amministrativi e tecnologici) in merito al documento video, durante il corso di tutto il suo ciclo vita.
3. Ciò detto, i codec da preferire per creare nuove evidenze video di uso generico – cioè avulse da casi d'uso peculiari di specifici settori quali la produzione, postproduzione e conservazione dei contenuti audiovisivi– sono quelli aperti e standard de iure, quali:

[36] Ad esempio, un'evidenza video potrebbe essere usata da un certo numero di utenze poco dopo la sua formazione, che richiedono tecnologie di elaborazione in tempo reale, a fronte delle quali è necessaria la produzione o la transcodifica in un codec ad elevato rapporto di compressione. Potrebbe anche esserci un vincolo di conservazione dell'evidenza originale piuttosto che di quella elaborata, che potrebbe avere o meno diversi requisiti di qualità. A fronte di questa seconda finalità, potrebbe essere pensato un procedimento per cui l'evidenza originale viene formata impiegando un codec senza compressione e la massima risoluzione possibile, mentre il file elaborato segue un ciclo vita diverso, al termine del quale possa o debba essere distrutto. Qualora anche il file elaborato vada conservato, potrebbe essere necessario prevedere un solo flusso, a fronte del quale andrebbe effettuata una scelta diversa riguardo alla transcodifica intermedia, allo scopo di assolvere ai vincoli qualitativi iniziali.

Firmato digitalmente da ROBERTO FRACCIA

- MPEG4 Part-10 (colloquialmente indicato con il nome di "H.264") in quanto largamente diffuso soprattutto negli apparati di riproduzione software e hardware. Tale codec è da preferirsi per contenuti già montati e ricondotti ad una risoluzione e una qualità accettabile per tutto il ciclo vita del documento.
- MPEG2 Part-2 qualora il ciclo vita del documento video e le sue finalità d'uso impongano privilegiare la semplicità computazionale dell'algoritmo di decompressione rispetto a fattori quali la qualità o la dimensione binaria dell'evidenza.
- Qualunque codec senza compressione, ovvero con una compressione priva di perdite. In tali casi sono valutabili tutte le rappresentazioni del documento video mediante sequenze di file (cfr. §2.12), ove i singoli file adottano formati con i medesimi requisiti di interoperabilità (cfr. §2.6) inclusa l'assenza di compressione ovvero la compressione *lossless*.

4. Nel caso di esigenze specifiche, si possono valutare anche altri codec, quali ad esempio:

- VP9 (anche detto "DASH") qualora il contenuto sia stato generato per applicazioni multipiattaforma (prevalentemente online) e non sia soggetto ad ulteriori modifiche.
- VC-3 (in particolar modo la sua variante "commerciale": l'Avid® DNxHD®) qualora il contenuto sia destinato al montaggio video (incluse successive archiviazioni del girato originale) e in assenza di ulteriori vincoli tecnologici.

5. Resta appannaggio delle singole organizzazioni valutare i parametri qualitativi in merito ai codec audio impiegati (ove sussistano come parametri variabili), tenendo conto ancora una volta di eventuali vincoli normativi, amministrativi e tecnologici. La scelta a priori dei parametri qualitativi può aiutare a standardizzare un processo e verificare che tutti gli organi coinvolti possano leggere o scrivere file con tali parametri.
6. I codec video più adatti alla conservazione –comunque tutti dotati di compressione con perdita– sono l'MPEG-4 Part-10

2.11 Sottotitoli, didascalie e dialoghi

1. Astrattamente, esiste una terza rappresentazione del suono legata ai *dialoghi* (rispetto a quelle descritte in §2.9) che consiste nella trascrizione più o meno letterale di ciò che una o più voci esprimono in una linea temporale, più eventualmente altre informazioni di contesto e ambiente.

Firmato digitalmente da ROBERTO FRACCIA

2. La necessità di rappresentare il parlato in una forma leggibile è prevalentemente legata a quattro casi d'uso, in alcuni casi concorrenti fra loro:

a) conservare dialoghi in forma scritta, eliminando la complessità tecnica o giuridica di conservare una registrazione multimediale degli stessi;
b) arricchire un dialogo con ulteriori informazioni quali, ad esempio, il nome (o la qualifica) dei partecipanti, il momento esatto e la *consecutio* temporale con cui le frasi sono pronunciate;
c) complementare il dialogo con informazioni relative all'ambiente o al contesto, a beneficio di spettatori ipoudenti o non-udenti, come nel caso di riproduzioni audiovisive;
d) fornire la traduzione di testi e dialoghi in lingue diverse da quella o quelle determinate preventivamente per i destinatari individuati per un particolare contenuto audiovisivo.

3. Le trascrizioni giuridiche ottemperano complessivamente ai casi d'uso 1 e 2 (e 4 in caso di testimoni stranieri, ove siano effettuate da traduttori giurati). Invece le trascrizioni di dialoghi in ambito cinetelevisivo –chiamate in inglese, nella loro accezione più generale, *timed-text*– si dividono tradizionalmente in tre categorie:

- sottotitoli (in inglese *subtitles*, abbreviati in *"subs"*) — ottemperano al solo caso d'uso 4;
- sottotitoli per non-udenti (in inglese *deaf or hard-of-hearing*, ovvero *DHH*) — ottemperano al solo caso d'uso 3;
- didascalie (in inglese *closed captions*, ovvero *CC*) — ottemperano al caso d'uso 2 sebbene, sovente combinati con tipologie di sottotitoli di cui sopra, ottemperino anche ai casi 3 o 4.

4. Il settore dell'intrattenimento sta venendo rivoluzionato dalla comparsa di innovativi servizi di fruizione tramite internet dei contenuti audiovisivi sotto forma di flussi multimediali (i cosiddetti servizi SVOD, cioè *streaming video on-demand*); tali servizi consentono, tra le altre cose, una *localizzazione*[37] molto più puntuale, precisa e multilingua, che li rende ancora più pervasivi e globali.
5. La normativa di riferimento per sottotitoli e didascalie dal punto di vista di accessibilità e qualità (soprattutto quando sono mostrate in sincronia e sovraimpressione, rispettivamente, con essenze audio e video) è regolamentata in particolare dalla norma ISO/IEC 20071-23 del 2018.

TTML	FORMATO DI FILE
Nome completo Timed Text Markup Language	

[37] La localizzazione è un processo riadattamento incrociato (in inglese *versioning*) di un contenuto rispetto a molteplici territori. Quando ciò riguardi il solo adattamento linguistico (anziché comprendere anche aspetti culturali, religiosi, giuridici) di audiovisivi, si parla più semplicemente di r*iedizione*, che comprende il video, il *doppiaggio* per l'audio e la sottotitolazione (trascrizione di dialoghi e didascalie).

Firmato digitalmente da ROBERTO FRACCIA

Estensione/i	.ttml, .dfxp
Specializzazione di	XML (*namespace* tt, tt[p|s|m] e altri)
Tipo MIME	application/ttml+xml
Sviluppato da	World Wide Web Consortium Society of Motion Picture and Television Engineers
Tipologia di standard	aperto, estendibile, retrocompatibile, *de iure*, testuale
Livello metadati	4
Derivato da	Distribution Format Exchange Profile (DFXP)
Revisione	1.0 (2018)
Riferimenti	• W3C Recommendation *TTML 2*, 2018 • W3C Recommendation *TTML 1 (3rd Ed.)*, 2018 • ETSI EN-303-560 v1.1.1 (2018) Famiglia **2052** di standard/raccomandazioni SMPTE: • OV2052-0:2013 • ST2052-1:2013 • ISO/IEC 14496-30:2018 • EBU – Tech 3380, *EBU-TT-D subtitling distribution format* v1.0.1 (2018)
Conservazione	Sì; cfr. §2.8
Racc. per la lettura	Speciale; obbligatorio in campo cinetelevisivo
Racc. per la scrittura	Speciale; raccomandato in campo cinetelevisivo

6. Il formato TTML (precedentemente chiamato DFXP) è, ad oggi, la declinazione più generica e completa relativamente alle possibilità tecniche e operative di aggiungere ad un documento audiovisivo una o più trascrizioni differenti. Il formato, adottato sempre di più come standard a livello europeo (*de iure*: cfr. norma EN-303-560 della ETSI) e internazionale[38] supporta qualunque tipo di lingua scritta e sue eventuali caratteristiche diacritiche (, integrando informazioni sulla presentazione dei sottotitoli all'interno del riquadro del video (posizione,[39] colore, dimensione, parametri tipografici completi), relativamente all'asse temporale (apparizione, scomparsa e altri effetti di animazione).

IMSC1	FORMATO DI FILE
Nome completo	Internet Media Subtitles and Captions
Estensione/i	.ttml

[38] Esistono diversi standard *de facto*, quali ad esempio le Linee guida di NETFLIX sulla sottotitolazione (in inglese).
[39] È anche possibile specificare la profondità ("*Z-depth*") rispetto alla parallasse nel caso di sottotitoli su contenuti stereoscopici (S3D).

Firmato digitalmente da ROBERTO FRACCIA

Specializzazione di	TTML
Tipo MIME	application/ttml+xml
Sviluppato da	World Wide Web Consortium
Tipologia di standard	aperto, estendibile, retrocompatibile, *de iure*, testuale
Livello metadati	4
Derivato da	W3C Timed Text Markup Language, versione 2
Revisione	1.1 (2018)
Riferimenti	• W3C Recommendation, *TTML profiles for IMSC 1.1*, 2018 • Netflix, *What does a properly formatted TTML file look like?* • Netflix, *Italian Timed Text Style Guide*, 2018
Conservazione	Sì; cfr. §2.8
Racc. per la lettura	Speciale; raccomandato in campo cinetelevisivo
Racc. per la scrittura	Speciale; raccomandato in campo cinetelevisivo

7. Il W3C ha deciso di standardizzare ulteriormente il generico formato TTML, derivando perciò le specifiche IMSC1 adottate, tra le altre cose dal formato di master interoperabile (IMF, cfr. §2.12). IMSC1 ha due profili: uno ove i sottotitoli sono rappresentati mediante solo testo, l'altro ove sono sottotitolo è rappresentato da un'immagine (tipicamente nel formato PNG con supporto completo del canale alfa, cfr. §2.6). L'esigenza di introduzione di questo profilo è stata necessaria per il diffondersi di notevoli dialetti di TTML da parte di diversi organi di standardizzazione, che hanno portato il formato originale –originariamente disegnato per essere il più interoperabile possibile– a creare notevoli problemi di compatibilità.[40] Il profilo IMSC1, oltretutto, è stato concepito anche per ottemperare ad esigenze proprie della distribuzione dei contenuti, quali l'adattamento dei dialoghi a diverse revisioni del contenuto audiovisivo, alla riedizione dei dialoghi in altre lingue o secondo esigenze diverse (cfr. distinzioni fra le varie tipologie di dialoghi sincronizzati all'inizio della sezione), alla transcodifica dei sottotitoli in altro formato.

EBU-TT	FORMATO DI FILE
Nome completo	EBU Timed Text (EBU-TT)
Estensione/i	.xml
Specializzazione di	XML (*namespace* ebutt[m|s|dt])

[40] Tale problema si è aggravato per il fatto che –come accade anche per molti altri formati di file per sottotitoli e didascalie– vi è un elevato riutilizzo della medesima estensione di file per formati anche molto diversi fra loro, cfr. §1.1.3.

Firmato digitalmente da ROBERTO FRACCIA

Tipo MIME	application/ttml+xml
Sviluppato da	European Broadcasting Union
Tipologia di standard	aperto, estendibile, retrocompatibile, *de iure*, testuale
Livello metadati	2
Derivato da	W3C Timed Text Markup Language, versione 1
Revisione	1998
Riferimenti	Famiglia **33x0** di standard tecnici EBU (2017): • Tech 3350, *part 1: subtitling format* v1.2 • Tech 3360, *part 2: mapping EBU STL to EBU-TT* v1.0 • Tech 3370, *part 3: mapping EBU STL to EBU-TT* v1.0 • Tech 3380, *subtitling distribution format* v1.0.1 (2018) • Tech 3390, *part M: metadata definitions* v1.0
Conservazione	No; cfr. §2.8
Racc. per la lettura	Speciale; obbligatorio in campo cinetelevisivo
Racc. per la scrittura	Speciale; raccomandato il campo cinetelevisivo ove richiesto da applicativi o capitolati

8. La EBU ha adattato il formato TTML agli specifici vincoli del mondo dell'audiovisivo, definendo così una specifica del medesimo formato, chiamato **EBU-TT**.
Analogamente, anche la SMPTE, ha definito una specifica TTML per i medesimi scopi, chiamata **SMPTE-TT**, che però è stata adottata prevalentemente dalla versione dei pacchetti per il cinema digitale (DCP) e quindi raccomandata in altra sezione di questo Allegato ad essi dedicata, cfr. §2.12.

STL	FORMATO DI FILE
Nome completo	EBU Subtitling Data Exchange Format
Estensione/i	.STL
Magic number	0x3?3?3? STL
Tipo MIME	—
Sviluppato da	European Broadcasting Union
Tipologia di standard	aperto, estendibile, *de iure*, binario
Livello metadati	1
Derivato da	—
Revisione	1.0 (1991)
Riferimenti	• EBU – Tech 3264 (1991)

Firmato digitalmente da ROBERTO FRACCIA

Conservazione	No
Racc. per la lettura	Speciale; raccomandato in campo cinetelevisivo
Racc. per la scrittura	Speciale; sconsigliato per la produzione e archiviazione

9. Il formato STL (da non confondersi con l'omonimo formato per modelli 3D per applicazioni stereolitografiche, cfr. §2.7) è stato per anni lo standard di riferimento in campo cinetelevisivo, perciò un grandissimo numero di contenuti risultano dotati di sottotitoli e didascalie in questo formato, in svariate lingue. Il formato tuttavia contiene solo indicazioni relative ai TimeCode ove i sottotitoli appaiono e scompaiono, al testo della lingua e a pochissime indicazioni visive su come presentare i sottotitoli, peraltro ampiamente non sempre utilizzate o rispettate dagli applicativi rispettivamente di creazione e riproduzione video.

2.11.1 Raccomandazioni per la produzione di documenti

1. Per la produzione di sottotitoli e didascalie in ambito cinetelevisivo, così come per finalità di conservazione, si raccomanda l'utilizzo del formato TTML del W3C, conforme al profilo IMSC1 e senza la specifica di caratteri tipografici esterni.

2.12 Contenitori e pacchetti di file multimediali

1. La registrazione e riproduzione di immagini e suoni contemporaneamente necessita innanzi tutto del sincronismo tra gli elementi costituenti un flusso multimediale. Per questo motivo tali flussi o file (a seconda del livello di astrazione adattato) sono disposti in una "linea temporale virtuale" (*timeline*, in inglese) che adotta un riferimento temporale autonomo[41] chiamato TimeCode.
2. Un esempio di sintassi per un TimeCode sincronizzato con un flusso video digitale (la cui unità indivisibile è il fotogramma) è, ad esempio, "**04:23:56:**07"[42]. Un esempio di sintassi per un TimeCode sincronizzato con un flusso audio digitale

[41] Per analogia, mentre la datazione di un'evidenza informatica mediante marcatura temporale è un riferimento temporale "assoluto", la temporizzazione di uno specifico punto della timeline è un riferimento temporale "relativo", che diviene assoluto solo nel momento in cui la riproduzione della timeline inizia ad un determinato istante temporale.
[42] Leggasi «4 ore, 23 minuti, 56 secondi e 7 fotogrammi» (i fotogrammi si azzerano al secondo in base al numero di fps, cfr. §2.10).

Firmato digitalmente da ROBERTO FRACCIA

(la cui unità indivisibile è il campione sonoro) è, ad esempio, "**00:06:32.**01436"[43]. Più in generale i TimeCode sono normati da standard di riferimento, quali la raccomandazione BT.1366 della ITU, la famiglia di standard **ST12** della SMPTE, la EBU *Tech 3097*.

3. Nel caso multimediale un flusso o file contiene spesso evidenze informatiche diverse per audio, video, e altri tipi di metadati (quali ad esempio sottotitoli, informazioni per i non udenti, uno o più TimeCode di riferimento, ecc.), che sono complessivamente chiamate essenze. Esse –ciascuna potenzialmente codificata con parametri e algoritmi diversi– sono racchiuse in un unico file contenitore, il quale ne facilita il sincronismo (eventualmente grazie alla presenza di una o più essenze TimeCode) e le descrive allo scopo di migliorarne la riproduzione o l'utilizzo.

4. Le essenze possono a loro volta contenere più *canali*. Nel caso dell'audio essi sono associati ad un particolare dispositivo di riproduzione ovvero alla direzione spaziale della sorgente sonora, p.es. canale dei totali sinistra (L_t), canale centrale (C), canale degli effetti a bassa frequenza (LFE), canale per il surround di destra (R_s). Nel caso di immagini statiche o video, i canali possono codificare un singolo canale cromatico dello spazio-colore riprodotto (cfr. §2.6), ad es. rosso (R), verde (G), blu (B) ovvero uno di due stereogrammi (occhio destro e occhio sinistro):

5. Così come una partitura musicale descrive per prima cosa tutti gli strumenti coinvolti e contiene le informazioni –sia comuni che specifiche per ogni parte– affinché un'orchestra possa rieseguire il brano, allo stesso modo un contenitore multimediale può contenere uno o più dei seguenti fattori (la cui presenza possibile e/o obbligatoria dipende dallo specifico formato della busta, cfr. §1.1.1):

- informazioni globali circa il documento multimediale (e.g. titolo del film/brano, nome dell'autore/regista, anno di produzione, durata nominale, livello di censura, data/ora di masterizzazione del file, ecc.);
- numero e tipologia delle essenze presenti e loro suddivisione in "tracce" per la riproduzione; per ciascuna essenza possono essere presenti altri metadati come, ad esempio:
  - nome o altro tipo di descrizione dell'essenza;
  - codec dell'essenza (ad esempio tramite codice FourCC);
  - velocità dell'essenza video (fotogrammi/secondo) o audio (campioni/secondo);
  - nome e numero di canali dell'essenza video (e.g. RGB, RGBα, CMYK, …; occhio destro/sinistro) o audio (e.g. monoaurale, stereo, quadrifonico, '5.1', '7.1', Dolby-E®, '22.1', Dolby® Atmos™, …);
  - in caso di essenza multi-canale, eventuale nome dei singoli canali;

[43] Leggasi «6 minuti, 32 secondi e 1436 campioni» (i campioni si azzerano al secondo in base al sample rate: p.es. 44100Hz, cfr. §2.9).

Firmato digitalmente da ROBERTO FRACCIA

    - profondità digitale dell'essenza immagine/video (bit/pixel) o audio (bit/campione);
    - *data-rate* minimo, medio e/o massimo di ciascun essenza.
    - lingua utilizzata per il parlato nell'audio (se presente) ovvero nei sottotitoli;
- 1 essenza video (nel caso di video stereoscopico potrebbe essere presente un'unica essenza con due canali, ovvero due essenze video distinte — una per ciascuno stereogramma, associati rispettivamente all'occhio destro e sinistro;
- 3 essenze audio (e.g. 'suoni ed effetti', 'colonna sonora italiana', 'colonna sonora inglese');
- 5 essenze sottotitoli (e.g. 'sottotitoli in italiano', 'sottotitoli in italiano per non-udenti', 'didascalie in inglese, 'sottotitoli in francese', 'didascalie in tedesco per non-udenti').
- 1 essenza TimeCode[44].

6. Come primo vantaggio, l'utilizzo di un formato contenitore consente ad applicazioni di conservazione e archiviazione di estrapolare molte informazioni da un file complesso e di grandi dimensioni (quale spesso è il file multimediale) senza dover implementare tutti i possibili codec necessari per decodificarne le essenze audio\video (cosa necessaria, invece, per poter riprodurre il file). Inoltre, il formato contenitore separa molto nettamente, al suo interno, le evidenze informatiche delle singole essenze, permettendone un'estrapolazione segmentata, molto più efficace e spesso anche con economia di spazio di archiviazione e tempi di elaborazione.
7. In alcuni casi di pertinenza multimediale, ad esempio, una o più essenze vengono ricodificate allo scopo di alternarne il *data-rate* o semplicemente per cambiare il codec utilizzato: si parla in tal caso, di *transcoding* delle essenze. Quando si cambia una o più essenze per un file multimediale (ad esempio per togliere una colonna sonora non più necessaria, aggiungere una traccia sottotitoli, ovvero sostituire una traccia video monoscopica con una stereoscopica) si parla di *re-wrapping*. Quando infine si cambia il formato di busta contenente l'intero file multimediale, ma mantenendo invariate le essenze, si parla di *trans-wrapping* — che è tipicamente un'operazione molto meno computazionalmente onerosa.

[44] Un esempio in cui sono presenti più tracce TimeCode è quando sono necessari più riferimenti temporali diversi (allo scopo di sincronizzare il flusso con altri sistemi informativi o altri flussi): ad esempio potrebbe essere presente un TimeCode "assoluto" espresso in orario diurno sulle 24 ore e uno "relativo" a un inizio temporale arbitrario rappresentato da "**00:00:00:**00".

Firmato digitalmente da ROBERTO FRACCIA

Figura 1 Esempio di una timeline semplice di un file multimediale con una traccia video (monoscopica) e una traccia audio biaurale (2 canali stereo).

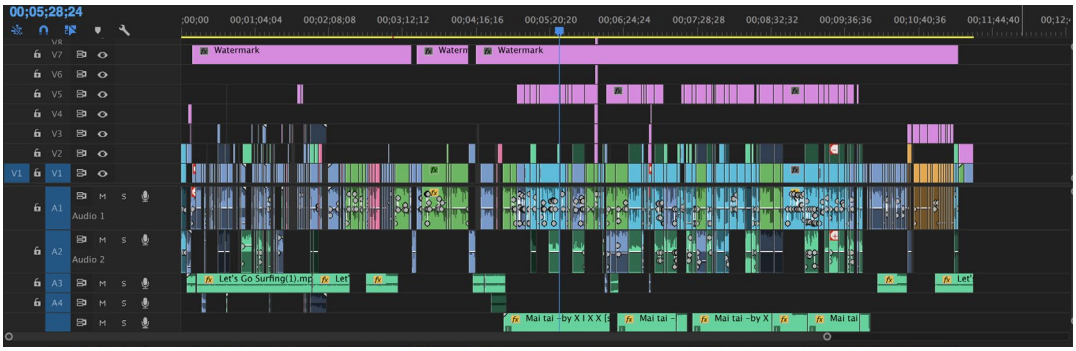


Figura 2 Esempio di una timeline di un file multimediale più complesso, con 9 tracce video (di cui una stereoscopica), 18 tracce audio mono o biaurali (cioè a 1 o 2 canali), 1 traccia TimeCode e diverse tracce sottotitoli nascoste.

8. Un'alternativa all'impiego di buste multimediali (cfr. §1.1.1) come sopra descritta è costituita dall'organizzazione delle singole essenze in file separati, poi riorganizzati in un pacchetto di file, ove le essenze siano logicamente associate fra loro in vari modi, come definito nel §1.1.2. Esempi di pacchetti multimediali sono ad esempio il pacchetto di master interoperabile (IMP), il pacchetto per il cinema digitale (DCP) e il pacchetto XDCAM, cfr. §2.12.
9. Per quanto riguarda le essenze video –nel caso di semilavorati o master di elevata qualità– è spesso preferito l'impiego della sola *naming convention*, ove ogni fotogramma del video è contenuto in un file separato, mentre i file sono numerati in sequenza cronologica (rispetto alla loro timeline relativa), costituendo dunque un pacchetto chiamato "sequenza di fotogrammi" (*frame sequence*, ovvero *frame-per-file* in inglese). Formati di immagini raster spesso adottati per tali sequenze di fotogrammi sono l'OpenEXR, il DPX (§2.6), così come il TIFF (soprattutto nei pacchetti DCDM), e il CinemaDNG (§2.12).

Firmato digitalmente da ROBERTO FRACCIA

MXF	FORMATO CONTENITORE
Nome completo	Material Exchange Format
Estensione/i	.mxf
Magic number	–
Tipo MIME	application/mxf
Sviluppato da	Society of Motion Picture and Television Engineers
Tipologia di standard	aperto, estendibile, *de iure*, binario
Livello metadati	4
Derivato da	–
Revisione	2018
Riferimenti	• RFC-4539 (2006) Documenti SMPTE, prevalentemente standard ('ST'): • base: ST377; EG41, EG42 • schemi operativi: ST378, ST390–393, ST407, ST408 • contenitori: ST379, ST381–389, ST394, ST405 • registri e dizionari di metadati: ST380, ST436; RP210, RP224 • www.smpte.org
Conservazione	Sì, solo usando codec adatti alla conservazione
Racc. per la lettura	Speciale; obbligo in lettura in tutti i settori audiovisivi
Racc. per la scrittura	Speciale; raccomandato per la produzione, lo scambio e l'archiviazione di contenuti cinetelevisivi

10. Il formato contenitore MXF è stato introdotto dalla SMPTE in un tentativo di standardizzare un formato per contenuti e flussi (cfr. §1.1.1) audiovisivi professionali che fosse utilizzabile lungo l'intera filiera cinetelevisiva, supportando il maggior numero di procedimenti: dalla produzione dei contenuti (camere digitali e animazione), attraverso tutte le fasi della post-produzione, sino alla distribuzione su diverse piattaforme (cinema digitale, televisione digitale terrestre e satellitare, streaming via internet, ecc.) e successiva archiviazione. Il formato MXF è regolamentato da diversi standard dell'SMPTE (fare riferimento alla tabella qui sopra), ma il principale fra loro è l'ST377. Il contenitore è professionale in quanto estremamente flessibile nell'imbustare più essenze di tipologie differenti, e supportare un'ampia gamma di metadati interni, associabili a diversi livelli semantici del contenuto, incluse specifiche posizioni della timeline)[45]. I metadati supportati sono estendibili: oltre ad una serie di metadati minimi supportati, la SMPTE mantiene

[45] Metadati associabili a particolari posizioni della *timeline* sono, ad esempio, commenti e annotazioni di montatori, coloristi, tecnici digitali o assistenti alla regia; l'elenco delle persone reali (e.g. ospiti, attori) ovvero finzionali (personaggi) inquadrati in quel momento.

Firmato digitalmente da ROBERTO FRACCIA

un registro ove ad ogni semantica è associato un codice binario (*UL*, ovvero *unified label* in inglese). Il registro è consultabile applicativamente o interattivamente sul sito smpte-ra.org, ovvero direttamente sotto forma di XML (§2.2). Per supportare molteplici casi di utilizzo, procedure di elaborazione e di tecnologie di stoccaggio e trasporto dei contenuti e dei flussi multimediali, le essenze stesse possono essere disposte in una molteplicità di strutture differenti all'interno dell'evidenza informatica complessiva. Ad esempio, la registrazione simultanea e in tempo reale, nel medesimo file MXF, di due flussi video provenienti da una cinepresa stereoscopica e di flussi audio provenienti da più microfoni disposti in scena, prevede che le essenze audio e video siano disposte in maniera "interlacciata": il contenitore MXF avvolge perciò, sequenzialmente, ciascun fotogramma, seguito dalle essenze audio relative alla durata del medesimo fotogramma, seguito dal fotogramma successivo e così via.

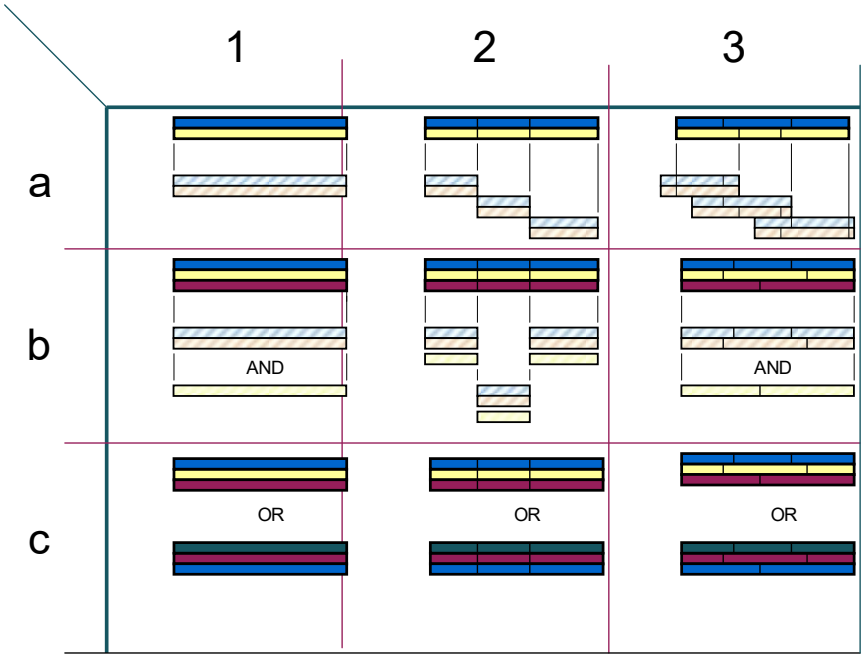


Figura 3 Tassonomia degli schemi operativi del formato MXF: sulle ascisse è rappresentata la complessità della timeline (indicata con un numero ordinale); sulle ordinate quella dei pacchetti (indicata con una lettera minuscola).

11. Per completare la descrizione di insieme del formato MXF, la SMPTE fornisce degli schemi operativi (*operational patterns* in inglese, abbreviati in **OP**), per i quali si invita a far riferimento ai relativi standard in tabella (oltre che allo standard principale ST377). In questi schemi operativi una timeline è astratta ulteriormente separando la suddivisione (e la "complessità") delle sue tracce e canali, dall'insieme di file ("pacchetti materiali") da cui è logicamente composta. In una tale tassonomia un contenuto multimediale (un'unica timeline) è rappresentato da un *pacchetto di contenitori MXF*, ciascuno contenente una o più essenze. La costruzione della

Firmato digitalmente da ROBERTO FRACCIA

timeline logica del contenuto a partire dai file MXF costituenti può avvenire in modi diversi, la cui complessità dipende da una duplice organizzazione virtuale. Da una parte vi è quella delle essenze lungo la timeline (cfr. l'elenco alfabetico per righe, di complessità crescente, in **Figura 2**):

a. ogni istante della timeline è riferito a una o più essenze contenute in un unico file;
b. ogni istante della timeline è riferito a più essenze contenute in uno o più file;[46]
c. vi sono due o più timeline alternative[47], ciascuna delle quali è riferita a una o più essenze contenute in uno o più file;

Dall'altra vi è l'organizzazione di come le varie essenze della timeline siano distribuite in un pacchetto di uno o più file (cfr. l'elenco numerico per colonne, di complessità crescente, nella medesima **Figura 2**):

1. il pacchetto contiene essenze usate interamente e della medesima durata della timeline;[48]
2. il pacchetto contiene più sequenze di essenze, usante interamente, adiacenti fra loro lungo la timeline;[49]
3. il pacchetto contiene più sequenze di essenze, ciascuna delle quali (contenuta in file differenti) può essere usata parzialmente o interamente.[50]

12. Ad esempio, lo schema operativo **OP**1a corrisponde a quello della singola clip audio\video con le cui essenze sono tutte di pari durata[51], dove cioè un singolo file contiene all'interno l'audio, il video e gli eventuali sottotitoli e può quindi essere riprodotto autonomamente dall'inizio alla fine. Lo schema operativo **OP**3c, invece, prevede un montaggio asincrono tra le varie tracce, con i contenuti potenzialmente estratti da essenze di durata più lunga e contenuta in diversi file del pacchetto e, in più, la possibilità che vi siano più montaggi alternativi tra cui scegliere. Gli schemi operativi permettono di indicare queste differenti tipologie mediante metadati nei file MXF costituenti il pacchetto, ma anche di vincolarli logicamente fra di loro, cosa particolarmente utile sia nel caso in cui i file perdano l'affinità per referenza

[46] Nel gergo del montaggio audiovisivo, si dice che tali essenze sincronizzate sono 'in *gang*' (letteralmente, "raggruppate") fra loro.
[47] La selezione di una delle timeline alternative, o il passaggio dall'una all'altra, non fanno parte dello schema operativo, anche se ciò è solitamente computo in automatico dall'applicazione che riproduce il contenuto, ovvero da una scelta manuale dello "spettatore".
[48] In questo caso la timeline è fatta da una sola sequenza (o "taglio"), la cui riproduzione coinvolge per intero le essenze di uno o più file.
[49] In questo caso la timeline è fatta da più sequenze (o "tagli"), fra loro contigue nel tempo, come avviene nel caso d'uso della *playlist*.
[50] Questo è lo scenario tipico usato nel montaggio audiovisivo, ove porzioni di clip "sorgenti" sono montate in una timeline, tipicamente separate da tagli netti.
[51] Un altro schema operativo non descritto in Figura è l'**OP**-Atom: una variante dell'**OP**1a ove le essenze sono inoltre tutte auto-contenute in un singolo file.

Firmato digitalmente da ROBERTO FRACCIA

(venendo archiviati in percorsi differenti o non stabili nel tempo), sia nel caso di successive modificazioni del contenuto. In quest'ultimo caso, modifiche parziali del contenuto multimediale vengono effettuate sui soli file MXF che contengono le essenze interessate, senza ricostruire o modificare il contenuto nella sua interezza. Più avanti sono descritti alcuni pacchetti di file che implementano proprio questa flessibilità degli schemi operativi del contenitore MXF: il formato di master interoperabile (IMF) e il pacchetto di cinema digitale (DCP).

13. Per tutti i motivi sopra esposti il contenitore MXF è fortemente raccomandato come formato contenitore d'elezione per la produzione e il riversamento di qualunque contenuto multimediale (audio, video, dialoghi), accompagnato ovviamente da una scelta adeguata dei codec da impiegare.

MP4	FORMATO CONTENITORE
Nome completo	MPEG-4, Part 14
Estensione/i	.mp4, .m4a, .m4v
Magic number	0x00000000 ftyp
Tipo MIME	video/mp4, audio/mp4
Sviluppato da	Society of Motion Picture and Television Engineers
Tipologia di standard	aperto, estendibile, retrocompatibile, *de iure*, binario
Livello metadati	3
Derivato da	Apple® QuickTime™, MPEG-4 Part 12
Revisione	2018
Riferimenti	• ISO/IEC 14496-14:2018 • ISO/IEC 14496-12:2015 • RFC-4337 (2006) • mp4ra.org
Conservazione	Sì
Racc. per la lettura	Generico; obbligatorio
Racc. per la scrittura	Generico; altamente consigliato per la produzione audiovisiva generica di contenuti auto-consistenti

14. La parte 14 del gigantesco standard MPEG-4 della ISO, ma anche contenuta nella RFC-4337 (più colloquialmente chiamata *MP4*) descrive uno standard *de iure* derivato moltissime sue caratteristiche dal formato Apple QuickTime (si legga sotto). Per questo motivo, e anche a causa della sua elevata versatilità sia nel numero e tipologie di essenze supportate al suo interno, che per la capacità di includere molteplici metadati interni nel file, è obbligatoria la capacità di leggere tale contenitore da parte di qualunque organizzazione, mentre è fortemente consigliato di adottarlo per la produzione di documenti solo video o audiovisivi — laddove non sia preferibile un formato con gradi di interoperabilità ancora maggiori — quale IMF ad esempio (sotto descritto).

Firmato digitalmente da ROBERTO FRACCIA

IMF	FORMATO DI PACCHETTO
Nome completo	Interoperable Master Format
Estensione/i	[.pkl|cpl], .xml, .mxf, …
Tipologie MIME	application/xml, /mxf, …
Sviluppato da	Society of Motion Picture and Television Engineers
Tipologia di standard	aperto, estendibile, retrocompatibile, *de iure*
Livello metadati	4
Derivato da	SMPTE Digital Cinema Package
Revisione	2019
Riferimenti	Famiglia di standard **ST2067** della SMPTE: • base: ST2067-1, ST2067-2:2013, ST2067-3:2016, ST2067-5:2012, ST2067-101:2017, ST2067-102:2014, ST2067-200:2018; • audio: ST2067-6:2012, ST2067-8:2013; • applicazioni: ST2067-10, ST2067-20:2013, ST2067-21:2016, ST2067-30:2013, ST2067-40:2017, ST2067-50:2018 • SMPTE RDD47:2019, *Isochronous Stream of XML Documents (ISXD) plugin* • SMPTE Report, *TTML features for IMF Data essence*, 2012 • www.smpte.org • www.imfug.com
Conservazione	Sì, con Applicazioni IMF che usano codec conservabili
Racc. per la lettura	Speciale; obbligatorio per il trattamento e l'interscambio di master e semilavorati cinetelevisivi
Racc. per la scrittura	Speciale; obbligatorio per interscambio, archiviazione e conservazione di contenuti cinetelevisivi.

15. Il formato master interoperabile (IMF) è descritto dalla famiglia di standard **ST2067** della SMPTE ed è nato dall'esigenza condivisa dai maggiori studi cinetelevisivi del mondo di gestire e conservare contenuti audiovisivi in maniera organizzata e attenta all'impatto che tale tipo di documenti, –per effetto delle loro grandi dimensioni informatiche– hanno nei processi di produzione, trasferimento, archiviazione, localizzazione e distribuzione internazionale. Una metodologia che è stata seguita nell'individuazione di tale formato è quella di massimizzare il riutilizzo di porzioni di contenuti audiovisivi che sono identici fra l'oro, archiviate nello stesso formato di pacchetto. Ciò avviene immancabilmente nelle riedizioni del medesimo contenuto (in caso di doppiaggio e altri adattamenti), nonché quando lo stesso master viene trasferito tra più enti durante le fasi di post-produzione, distribuzione e archiviazione.

Firmato digitalmente da ROBERTO FRACCIA

16. Un documento informatico in tale formato è chiamato 'pacchetto master interoperabile' (*IMP*) e comprende sempre dei contenuti multimediali rappresentati nel tempo lungo una timeline (cfr. §2.10 articolo 1), chiamata *composizione*.
17. IMF utilizza ampiamente le caratteristiche di estendibilità offerte dal formato XML (usato per file sidecar di un IMP, che ne contengono i metadati globali), così come l'interoperabilità della busta MXF e dei suoi schemi operativi, per contenere le essenze audio, video, oltre ai dialoghi e ad altri metadati "temporali" (cioè localizzati cronologicamente in punti specifici della timeline).
18. Un IMP contiene sempre almeno i seguenti file XML:

- un 'elenco di impacchettamento' (PKL, *packing list* in inglese), che contiene il nome completo di un dato pacchetto, l'UID ad esso associato e altri suoi metadati, oltre nome, dimensione, impronta crittografica (cfr. §2.16) e UID associati a ciascuno dei file facenti parte dell'IMP;
- una 'scaletta della composizione' (CPL, *composition playlist* in inglese) che descrive come la timeline del contenuto sia composta a partire dalle risorse (file) indicizzate nella PKL del medesimo pacchetto e, opzionalmente, anche da PKL di altri pacchetti.

19. Un pacchetto master interoperabile è un pacchetto di file in base alla definizione data in §1.1.1, ma la sua CPL, potendo riferirsi anche ad altre PKL oltre alla propria, può descrivere il contenuto di una composizione utilizzando anche contenitori multimediali appartenenti ad altri IMP. Un pacchetto IMF che faccia uso di altre PKL oltre la propria viene chiamato 'pacchetto complementare' (*supplemental package*, in inglese),[52] in quanto dipende da uno o più IMP differenti dal proprio. Il caso d'uso degli IMP complementari è quello di riedizioni o adattamenti successivi del medesimo contenuto, quali:

- doppiaggio (i.e. cambio della lingua parlata);
- aggiunta, o cambio, di *timed text* (i.e. sottotitoli di vario tipo, cfr. § 2.11);
- sostituzione di cartelli e altre parti di video ove vada inserito un testo in una lingua differente (*texted*), o ne vada aggiunto ove non era presente (*textless*);
- riedizione di parti del contenuto audiovisivo per altre finalità di adattamento;
- aggiunta o sostituzione di marche, loghi, o interi titoli di testa o di coda;
- sostituzione dell'intero contenuto con altre codifiche con diverse specifiche tecniche (ad esempio video stereoscopico, HDR/WCG, HFR;[53] audio con diverso numero di canali, ecc.).

20. IMF ammette anche altri tipi di file sidecar opzionali, sempre in XML, quali:

[52] In tal caso la CPL di un pacchetto complementare si dice essere un *versioning file* (*VF*) — mentre invece un pacchetto IMF che si riferisce soltanto alla propria PKL (e quindi ai suoi file MXF), si dice essere –almeno tecnicamente– nella 'versione originale' (*OV*).
[53] Acronimi commerciali che stanno rispettivamente per *high dynamic range*, *wide colour gamut* e *high frame rate*.

Firmato digitalmente da ROBERTO FRACCIA

- un 'elenco dei profili d'uscita' (OPL, *output profile list* in inglese), che contiene informazioni tecniche su come generare file multimediali auto-consistenti in altri formati di file, incluse informazioni sul formato video (risoluzione, rapporto d'aspetto, ritagli e ingrandimenti) e audio (numero di canali e lingue impiegate) da utilizzare;[54]
- una 'mappa di composizione accessoria' (SCM, *sidecar composition map*), che può racchiudere commenti, annotazioni, ovvero metadati "globali" associabili all'IMP nella sua interezza — particolarmente utile ai fini dell'archiviazione a lungo termine di qualunque tipi di informazione accessoria riguardo al contenuto audiovisivo stesso.

21. Gli eventuali sottotitoli, così come i metadati associabili a particolari punti della timeline (cosiddetti "locali") sono entrambi rappresentati come tracce in un IMP, venendo codificati in XML imbustati ciascuno in file MXF facenti parte del pacchetto. Il dialetto XML dei sottotitoli è sempre TTML o sue ulteriori specializzazioni (cfr. §2.11).
22. Gli altri tipi di metadati locali sono codificabili in file XML senza ulteriori vincoli di specializzazione, associati a particolari istanti della timeline e raggruppati in uno o più buste. Ciascun siffatto contenitore di metadati costituisce un *flusso isocrono di documenti XML* (ISXD). Si raccomanda di avere un file MXF separato per ogni tipologia macroscopica di metadati.[55]
23. Allo scopo di incrementare l'interoperabilità, accanto agli standard che descrivono i componenti generici di IMF, ve ne sono altri che descrivono i suoi schemi operativi, chiamati "Applicazioni". In questi documenti vengono descritti ulteriori vincoli tecnici che armonizzano gli IMP formati per determinate finalità, come ad esempio i codec da usare per le essenze, la loro risoluzione, le specifiche sugli spazi-colore e altre informazioni colorimetriche, la suddivisione delle tracce audio multicanale in "campi sonori", la compressione audio-video, il formato dei sottotitoli, e così via. Molte di queste Applicazioni sono diventate standard di consegna per diversi attori del mercato cinetelevisivo, soprattutto nel campo SVOD (distribuzione a consumo via etere/satellite/internet).
24. Sebbene IMF resti un formato specifico per i settori cinetelevisivi, all'interno di questi è fortemente raccomandata la produzione di documenti in questo formato: sia nei casi di documenti "semilavorati", per i quali siano cioè previsti ulteriori

[54] Bisogna ricordare che, sebbene IMF sia un formato adatto per la post-produzione e l'archiviazione, il suo uso principale è come master cinetelevisivo, da intendersi successivamente convertito in formati specifici agli scopi di post-produzione, distribuzione e conservazione.
[55] Ad esempio 4 file MXF per contenere 4 differenti ISXD: uno con l'elenco dei nomi di attori e/o personalità presenti in ad ogni cambio di scena; uno con informazioni di produzione ad ogni cambio scena (illuminazione, ottiche, parametri delle configurazioni della cinepresa); uno con parametri relativi al restauro fotogramma per fotogramma (difetti fisici della pellicola sia riparati che solo individuati, finestra del fotogramma completo da cui è estratto il fotogramma cinetelevisivo, ecc.); uno con informazioni di postproduzione e visualizzazione in tempo reale (correzione del colore in HDR, parametri degli effetti speciali, coordinate giroscopiche della camera, ecc.).

Firmato digitalmente da ROBERTO FRACCIA

adattamenti quali montaggio, doppiaggio o altro; sia qualora il contenuto sia destinato ad archiviazione a lungo termine e conservazione. Le PP.AA. di settore sia adoperano per adottare il formato IMF per tali scopi nel minor tempo possibile.
25. Per le organizzazioni che manipolano un elevato numero di IMP, si raccomanda l'uso di un applicativo di gestione dei contenuti che –sfruttando i file sidecar di cui all'articolo 18– consenta una migliore razionalizzazione degli storage contenenti tali contenuti, tramite il tracciamento completo dei file costituenti ogni pacchetto IMP.

MATROSKA	FORMATO CONTENITORE
Nome completo	Matroska
Estensione/i	.mkv, .mka, .mks, .mk3d
Magic number	0x1A45DFA3
Tipo MIME	video/x-matroska, audio/x-matroska
Sviluppato da	comunità open source
Tipologia di standard	aperto (licenza CC BY 4.0), *de facto*, binario
Livello metadati	3
Derivato da	Multimedia Container Format (MCF), Extensible Binary Meta Language (EBML)
Revisione	1.4.9 (20 aprile 2017)
Riferimenti	• www.matroska.org • github.com/Matroska-Org • matroska-org.github.io
Conservazione	No
Racc. per la lettura	Generale con obbligo in lettura
Racc. per la scrittura	Generale; raccomandato per la produzione non cinetelevisiva di contenuti cronologicamente continui

26. Il contenitore Matroska è un altro formato estremamente versatile capace di contenere molteplici essenze di vario tipo. Se ne raccomanda inoltre l'uso in tutti i campi della produzione audiovisiva, salvo nei casi d'uso specifici della post-produzione o sua archiviazione, dove sono preferibili formati contenitori più professionali, quali MXF ovvero MP4.

WEBM	FORMATO CONTENITORE
Nome completo	WebM
Estensione/i	.webm, .weba
Magic number	0x1A45DFA3
Tipo MIME	video/webm, audio/webm
Sviluppato da	Google; On2 Technologies
Tipologia di standard	proprietario (licenza tipo BSD), *de facto*, binario
Livello metadati	1
Derivato da	Matroska, VP9 (video), Vorbis (audio)

Firmato digitalmente da ROBERTO FRACCIA

Revisione	2018
Riferimenti	• www.webmproject.org • www.matroska.org • www.vorbis.com
Conservazione	No
Racc. per la lettura	Generico; raccomandata la lettura
Racc. per la scrittura	Generico; raccomandata la produzione per brevi clip finalizzate alla distribuzione via internet

27. Il contenitore WebM è ad oggi uno degli standard de facto per la condivisione di contenuti audiovisivi sottoforma di flussi in *streaming* via internet. È in pratica costituito dalla combinazione di una busta Matroska, del codec VP9 per le essenze video e di quello Vorbis per le essenze audio.

MPEG2-TS	FORMATO CONTENITORE
Nome completo	MPEG-2 Transport Stream
Estensione/i	.ts, .m2ts
Magic number	G
Tipo MIME	video/MP2T
Sviluppato da	Moving Picture Experts Group
Tipologia di standard	aperto, estendibile, *de iure*, robusto, binario
Livello metadati	1
Derivato da	MPEG-2
Revisione	2018
Riferimenti	• ISO/IEC 13818-1:2018 • ITU-T Recommendation H.222.0 (2018) • ETSI TS-101-154 v2.6.1 (2019)
Conservazione	No
Racc. per la lettura	Generale raccomandato
Racc. per la scrittura	Speciale; raccomandato per la produzione finale di contenuti cronologicamente continui

MPEG2-PS	FORMATO CONTENITORE
Nome completo	MPEG-2 Program Stream
Estensione/i	.mpg, .mpeg, .vob, .m2p
Magic number	0x0001BA
Tipo MIME	video/MP2P
Sviluppato da	Moving Picture Experts Group
Tipologia di standard	aperto, estendibile, *de iure*, binario
Livello metadati	1
Derivato da	MPEG-2
Revisione	2018

Firmato digitalmente da ROBERTO FRACCIA

Riferimenti	• ISO/IEC 11172-3:1993 • ISO/IEC 13818-1:2018 • ITU-T Recommendation H.222.0 (2018)
Conservazione	No
Racc. per la lettura	Generale; raccomandato
Racc. per la scrittura	Speciale; sconsigliato per archiviazione/conservazione

28. L'*MPEG-2 Transport Stream* (*TS*) e *Program Stream* (*PS*) sono due formati busta utilizzati per contenere essenze audiovisive, in due scenari di utilizzo diversi:

- MPEG2-TS, introdotto originariamente per una riproduzione sequenziale sotto forma di flusso digitale (cfr. §1.1.1) trasmesso attraverso un canale di comunicazione non affidabile, quale ad esempio il "digitale terrestre";[56] per questo motivo l'MPEG2-TS è dotato di messaggi di verifica dell'integrità legati a meccanismi di protezione del flusso digitale. Adotta inoltre una disposizione interlacciata delle essenze per migliorare le prestazioni dovute allo scenario d'uso della riproduzione sequenziale.
- MPEG2-PS, introdotto originariamente per la distribuzione televisiva aerea o via cavo, è disegnato per contenere flussi audiovisivi digitali (cfr. §1.1.1, con estensioni preferite .mpg e .mpeg), insieme ai metadati necessari al mantenimento della sincronia, al controllo di qualità della banda impiegata e all'organizzazione del canale di comunicazione di tipo televisivo (e.g. supporta il numero e il nome del programma/canale, ecc.). L'MPEG2-PS è disegnato per la riproduzione casuale ed è adottato come contenitore per le evidenze informatiche nei dischi di formato DVD e simili (adottando, in questo caso, l'estensione .vob).

29. Inizialmente questi formati di busta supportavano codec della famiglia MPEG-2, anche se è possibile utilizzare altri tipi di codec.

AVI	FORMATO DI FILE
Nome completo	Advanced Video Interleave
Estensione/i	.avi
Magic number	RIFF
Tipo MIME	video/avi, video/msvideo
Sviluppato da	Microsoft Corporation
Tipologia di standard	proprietario (libero), *de iure*, binario
Livello metadati	3
Derivato da	Resource Interchange File Format (RIFF)
Revisione	2008

[56] Cioè i canali di comunicazione che seguono gli standard di comunicazione denominati **DVB** della ITU e della EBU.

Firmato digitalmente da ROBERTO FRACCIA

Riferimenti	• Microsoft, *AVI RIFF File Reference*, vs.85 (2008) • RFC-2361 • Hackaday, *AVI File Format*
Conservazione	No
Racc. per la lettura	Generale con obbligo in lettura
Racc. per la scrittura	Generale; sconsigliata la produzione

30. Il formato di busta AVI è una declinazione del più generico formato contenitore RIFF (da cui derivano anche WAVE e AIFF nel campo audio, cfr. §2.9). È stato, storicamente, uno dei primi formati di contenitore destinato a documenti audiovisivi e dunque a supportare l'uso di codec molteplici per le sue essenze. La mancanza di particolari metadati professionali, tuttavia, oltre ad una poca descrizione dei codec impiegati, lo rendono poco adatto ad usi professionali, perciò se ne sconsiglia l'uso per la creazione di nuovi file laddove vi sia un'alternativa possibile.

OGG	FORMATO CONTENITORE
Nome completo	Ogg encapsulated format
Estensione/i	.ogg, .oga, .ogv
Magic number	OggS
Tipo MIME	audio/ogg, video/ogg, application/ogg
Sviluppato da	comunità open source
Tipologia di standard	aperto (licenza tipo BSD), *de iure*, binario
Livello metadati	3
Derivato da	–
Revisione	0 (2003)
Riferimenti	• RFC-3533 • RFC-5334 • xiph.org/vorbis
Conservazione	No
Racc. per la lettura	Speciale; raccomandata lettura
Racc. per la scrittura	Speciale; sconsigliata post-produzione cinetelevisiva

31. Il formato OGG è un contenitore completamente aperto ed estremamente versatile, raccomandato per l'archiviazione di essenze audio, ma al di fuori del caso d'uso cinetelevisivo, dove si raccomandano altri forati di file.

QUICKTIME	FORMATO CONTENITORE
Nome completo	QuickTime™ File Format
Estensione/i	.mov, .qt
Magic number	0x00000000 moov

Firmato digitalmente da ROBERTO FRACCIA

Tipo MIME	video/quicktime
Sviluppato da	Apple
Tipologia di standard	proprietario, estendibile, *de facto*, deprecato
Livello metadati	4
Derivato da	–
Revisione	2016
Riferimenti	• Apple, *QuickTime File Format Specifications* (2016)
Conservazione	No
Racc. per la lettura	Generale; raccomandata la lettura
Racc. per la scrittura	Generale; sconsigliata la produzione

32. Il contenitore QuickTime, di proprietà della Apple, è stato a lungo uno dei contenitori più usati per le essenze multimediali, grazie soprattutto alla sua estendibilità. Nonostante si tratti di un formato aperto (la Apple pubblica e revisiona continuamente le sue specifiche tecniche), ne detiene la proprietà intellettuale e ne ha solo parzialmente liberalizzato la produzione al di fuori di applicativi o dispositivi hardware di proprietà della Apple o vincolati da accordi di licenza. Per questo motivo, nonostante ne sia fortemente consigliata la capacità di riproduzione da parte di tutte le organizzazioni che utilizzano, elaborano, o producono contenuti audiovisivi, la produzione di nuovi contenuti in questo formato è fortemente sconsigliata (a meno che non sia l'unico formato supportato da specifici applicativi). Inoltre la smpte e la iso hanno derivato dal QuickTime il formato MP4, completamente aperto.

DCP	FORMATO DI PACCHETTO
Nome completo	SMPTE Digital Cinema Package
Estensione/i	[.pkl|cpl].xml, .mxf, …
Tipologie MIME	application/xml, /mxf, …
Sviluppato da	Society of Motion Picture and Television Engineers
Tipologia di standard	proprietario (libero), estendibile, *de iure*
Livello metadati	3
Derivato da	DCP della DCI (Digital Cinema Initiative) e *"InterOp"*
Revisione	1.3 (2018)

Firmato digitalmente da ROBERTO FRACCIA

Riferimenti	Famiglie di standard ('ST'), prassi raccomandate ('RP'), regole tecniche ('EG') **429–433** della SMPTE: • pacchetto: ST429-2:2009, ST429-3:2007, ST429-6:2006, ST429-7:2006, ST429-8:2007, ST429-9:2007 • video: ST429-4:2006, ST428-11:2009, ST428-21:2011, ST428-2:2006, EG432-1:2010; • audio: ST428-1:2006, ST428-2:2006, ST428-3:2006 • sottotitoli: ST429-5:2009, ST429-12:2008, ST428-21:2011; • www.smpte.org • www.dcimovies.com
Conservazione	No (cfr. §2.8 per i sottotitoli)
Racc. per la lettura	Speciale; raccomandato per la distribuzione e post-produzione cinematografica
Racc. per la scrittura	Speciale; raccomandato per distribuzione e (non criptato) per archiviazione di contenuti cinematografici

33. Il formato di pacchetto per il cinema digitale (DCP, *digital cinema package* in inglese) è un pacchetto di file il cui scopo è contenere una copia di contenuto cinematografico da distribuire nelle sale di proiezione. Esistono due tipi di standard DCP: quello della *Digital Cinema Initiatives* (DCI), ora obsoleto, e quello della SMPTE, più recente, che attualmente supporta tutte le novità tecniche.
34. Un DCP è costituito da file multimediali MXF, con schema operativo **OP**2b, contenenti separatamente almeno una traccia audio (in formato PCM non compresso) e una video (con compressione inter-frame di tipo *wavelet*),[57] più alcuni sidecar file in XML. Da questo punto di vista, l'architettura del pacchetto è simile a quella del formato di master interoperabile (IMF, sopra descritto). Ciò che rende le DCP peculiari sono i vincoli ai formati audiovisivi delle sale teatrali; la possibilità, mediante messaggi inseriti in specifici istanti della timeline della composizione, di comandare operazioni in sala quali il controllo del proiettore, del sistema di tende, sipari e luci, o di altri dispositivi di intrattenimento proprietari; la possibilità di cifrare l'intero contenuto sbloccandolo soltanto con una chiave crittografica (cfr. §2.16) generata in maniera sicura, tipicamente dallo stesso applicativo che ha masterizzato la DCP.
35. Le DCP cifrate hanno infatti tutti i loro file MXF cifrati, ciascuno mediante crittografia simmetrica (algoritmo AES) con *chiave-contenuto* a 256 bit. La chiave-contenuto di ciascun MXF è sempre archiviata e distribuita cifrata da una chiave pubblica (RSA), la cui corrispondente chiave privata è confidenzialmente mantenuta

[57] La compressione impiegata, visivamente priva di perdite (*visually lossless* in inglese), è la medesima utilizzata dall'algoritmo JPEG2000, cfr. §2.7.

Firmato digitalmente da ROBERTO FRACCIA

da dispositivi certificati dalla DCI — tipicamente dispositivi di masterizzazione o riproduzione del contenuto (attaccati ai proiettori delle sale cinematografiche), ai quali viene distribuita l'evidenza informatica contenente la chiave-contenuto da sbloccare per riprodurre il DCP. Tale evidenza è formata in un particolare file chiamato KDM (cfr. §2.16).

36. L'uso della crittografia per proteggere i DCP pone tuttavia diverse problematiche in merito all'archiviazione a lungo termine e alla conservazione dei documenti cinetelevisivi in tale formato: in seguito a smarrimento o a scadenza naturale dei certificati a chiave pubblica, infatti, non sarebbe più possibile generare altre KDM che potrebbero sbloccare la DCP.

37. Mentre da una parte si raccomanda che le organizzazioni dedicate alla produzione e riproduzione di opere cinematografiche compiute siano in grado di riprodurre almeno le DCP *non* cifrate, si sconsiglia alle medesime organizzazioni di produrre DCP, salvo per le seguenti finalità:

- DCP *non* criptate per finalità di archiviazione a lungo termine e conservazione del master dedicato alla proiezione cinematografica;
- DCP *criptate* per la sola finalità di distribuzione nelle sale cinematografiche.

85. Si sconsiglia di produrre DCP secondo lo standard DCI (ovvero secondo lo standard *de facto* e intermedio fra i due qui elencati, denominato "InterOp"), favorendo invece lo standard *de iure* SMPTE in quanto è l'unico a supportare, mediante aggiornamenti lenti ma costanti delle specifiche, le migliorie tecnologiche delle sale cinematografiche, sia in campo audio, che video, che intrattenimento di sala in generale.

39. Si raccomanda alle organizzazioni che archiviano un contenuto in formato DCP di archiviarne anche una versione in un formato indipendente dalle caratteristiche tecniche di una sala cinematografica digitale, quali quelli individuati in questo stesso capitolo.

DCDM	FORMATO DI PACCHETTO
Nome completo	Digital Cinema Distribution Master
Estensione/i	.tif/.tiff, .wav
Tipologie MIME	image/tiff, sound/wav
Sviluppato da	Society of Motion Picture and Television Engineers
Tipologia di standard	aperto, estendibile, retrocompatibile, *de iure*
Livello metadati	2
Derivato da	Tagged Information File Format
Revisione	1.3 (27 giugno 2018)

Firmato digitalmente da ROBERTO FRACCIA

Riferimenti	Famiglia **ST428** di standard/prassi SMPTE: • video: ST428-1:2006, ST428-5:2010, ST428-9:2008, RP428-6:2009; Adobe® TIFF™ Revision 6.0 (1992) • audio: ST428-2:2006, ST428-3:2006, ST428-4:2010, ST428-3:2006; EBU – Tech 3285-1 2.0 (2001) • sottotitoli: ST428-7:2010, ST428-10:2008, ST429-5: 2009; ST428-5:2010 • www.smpte.org
Conservazione	Sì (cfr. §2.8 per i sottotitoli)
Racc. per la lettura	Speciale; obbligatorio per la post-produzione e distribuzione cinematografica
Racc. per la scrittura	Speciale; raccomandato per l'archiviazione di contenuti per la distribuzione cinematografica, previa riversamento in pacchetto IMF Application #4

40. Il master per la distribuzione del cinema digitale (DCDM) è un altro formato basato su sequenze di fotogrammi, ove l'essenza audio è costituita da file WAVE monaurali (uno per ciascun canale stereo, 5.1 ovvero 7.1) mentre l'essenza audio è costituita da file TIFF adeguatamente formati (cfr. §2.6), che codificano l'immagine nello spazio-colore DCI *X'Y'Z'*, basato su *code-value* a numeri interi e sulla colorimetria riferita alla luce proiettata su uno schermo bianco, che però, da un punto di vista teorico, comprende ogni colore visibile da un "osservatore standard". Il pacchetto DCDM, così come il DCP sopra descritto, esistono in due versioni: uno primo standard *de facto* della DCI e il più recente standard *de iure* della SMPTE, cui ci si raccomanda di attenersi.
41. Sebbene la lettura del DCDM sia obbligatoria per le organizzazioni che si occupano della post-produzione e della masterizzazione per il cinema digitale, nonché fortemente consigliata per l'archiviazione a lungo termine dei contenuti cinematografici, si consiglia altresì la produzione dei futuri master cinematografici nel formato IMF, che presenta caratteristiche di maggior interoperabilità con le filiere contemporanee di distribuzione cinematografica, oltre a supportare un maggior numero di metadati e di resilienza alle riedizioni.
42. Si consiglia il riversamento di tutti i pacchetti DCDM in pacchetti IMF Application #4 (cosiddetta "*Cinema mezzanine*").

CINEMADNG	FORMATO DI FILE
Nome completo	Adobe® CinemaDNG™
Estensione/i	.dng; .wav
Specializzazione di	TIFF/EP
Tipo MIME	video/x-adobe-dng
Sviluppato da	Adobe Systems

Firmato digitalmente da ROBERTO FRACCIA

Tipologia di standard	proprietario (brevettato), estendibile, *de iure*, binario
Livello metadati	2
Derivato da	Adobe® DNG
Revisione	1.1.0.0 (2011)
Riferimenti	• Adobe, *CinemaDNG image data format specification* v1.1.0.0, 2011 • Adobe, *Digital Negative (DNG) Specification* v1.4.0.0, 2012
Conservazione	No
Racc. per la lettura	Speciale; fortemente raccomandato per archiviazione, conservazione e post-produzione fotocinematografica
Racc. per la scrittura	Speciale; fortemente consigliato per archiviazione/ conservazione fotografica; consigliato riversamento su IMF in caso cinematografico

43. Il formato CinemaDNG™ è una specifica aperta della Adobe per rappresentare il video professionale sotto forma di sequenze di fotogrammi, ove ciascun file è rappresentato come DNG.

D.I. BASATO SU EXR	FORMATO DI PACCHETTO
Nome completo	Digital Intermediate
Estensione/i	.exr; .wav
Tipologie MIME	image/exr, sound/wav
Sviluppato da	major film studio
Tipologia di standard	aperto, retrocompatibile, *de facto*
Livello metadati	2
Derivato da	–
Revisione	–
Riferimenti	• www.smpte.org
Conservazione	Sì
Racc. per la lettura	Speciale; obbligatorio in post-produzione cinetelevisiva
Racc. per la scrittura	Speciale; fortemente raccomandato per l'archiviazione cinetelevisiva; consigliato riversamento in IMF

D.I. BASATO SU DPX	FORMATO DI PACCHETTO
Nome completo	Digital Intermediate
Estensione/i	.dpx; .wav
Tipologie MIME	image/x-dpx, sound/wav
Sviluppato da	Technicolor; Kodak
Tipologia di standard	aperto, retrocompatibile, *de facto*, deprecato
Livello metadati	2

Firmato digitalmente da ROBERTO FRACCIA

Derivato da	—
Revisione	—
Riferimenti	—
Conservazione	No
Racc. per la lettura	Speciale; obbligatorio in post-produzione cinetelevisiva
Racc. per la scrittura	Speciale; consigliato per archiviazione di scansioni da pellicola cinematografica; consigliato riversamento in IMF, ovvero in DI basato su EXR

44. Il nome *Digital Intermediate* (*DI*) indica il processo di post-produzione cinematografica digitale che ha soppiantato l'analogo processo fotochimico su pellicola da 16mm, 35mm o 65mm. Agli albori della post-produzione digitale, quando la fotografia era prevalentemente su pellicola negativa e la proiezione nelle sale basata su pellicole positive, il processo DI cominciava con la scansione digitale del negativo già sviluppato –fotogramma per fotogramma– e terminava con la stampa digitale (*film-out*, in inglese) su pellicola internegativa o interpositiva di pari calibro, da cui venivano poi stampate le copie positive in 35mm o 70mm per la distribuzione. Con l'avvento predominante delle cineprese digitali da un lato del processo e i proiettori per il cinema digitale dall'altro, il termine di è oggi diventato semplice sinonimo di post-produzione interamente digitale. È rimasta comunque l'esigenza di memorizzare i contenuti video in pacchetti di file a "sequenza di fotogrammi" (cfr. §2.12) in quanto ciò rende più semplice la modifica di singole scene, parti di scene e persino fotogrammi individuali — sia dal punto divista dello storage ove il contenuto è memorizzato, che delle prestazioni degli applicativi impiegati. Per gli stessi motivi, le sequenze di fotogrammi non utilizzano compressione, o al più utilizzano algoritmi *lossless* (dunque, considerando la sequenza di fotogrammi come un unico flusso video, si tratta sempre di compressione intra-frame, cfr. §2.10). La suddivisione in "rulli" (cioè clip audiovisive della durata di 15–25 minuti circa[58]) è di solito rispettata dividendo le sequenze di fotogrammi in sottocartelle del medesimo pacchetto

45. L'audio viene invece codificato in uno o più file WAVE (cfr. §2.9), tipicamente monoaurali, uno per canale. Non esistono veri e propri documenti che descrivono tali specifiche, così come la loro archiviazione a lungo termine (storicamente in nastri digitali LTO mediante il formato di archiviazione TAR, cfr. §2.13): si tratta, dunque, di uno vero e proprio standard *de facto*.

46. Per quanto riguarda il formato di file usato per i singoli fotogrammi, il DI tradizionale ha da molto tempo adottato il formato DPX (creato dalla Kodak® come evoluzione del Cineon™ e standardizzato poi dalla SMPTE, cfr. §2.6), in quanto tale formato permette nativamente la rappresentazione digitale della densitometria di

[58] Considerando un framerate di 24fps tipico del cinema, questo equivale dai 20'000 ai 30'000 fotogrammi.

Firmato digitalmente da ROBERTO FRACCIA

una pellicola negativa scansionata, ovvero di una positiva stampata, oltre a supportare metadati tipici della postproduzione cinematografica.[59] Il formato DPX tuttavia, nonostante sia attualmente sotto revisione da parte di SMPTE, non è più adeguato agli standard di archiviazione multimediale moderni, a causa della poca efficacia nel mantenere metadati inerenti alle annotazioni o alla codifica colorimetrica. Per questo e altri motivi, come ad esempio le esigenze tecniche della computer-grafica (*CG*) e degli effetti speciali digitali (*VFX*), i pacchetti DI contemporanei hanno abbandonato il formato DPX in favore di OpenEXR (anch'esso introdotto in §2.6).

47. Si raccomanda a tutti gli enti operanti nel settore della post-produzione cinematografica di poter leggere pacchetti di file di entrambe i tipo, anche se si sconsiglia fortemente la produzione di nuove sequenze di fotogrammi in formato DPX (in favore del formato OpenEXR). Per la produzione di nuovi pacchetti destinati all'archiviazione o conservazione, si raccomanda inoltre l'impiego dell'IMF (sopra descritto), per la sua maggiore capacità di interoperabilità e riusabilità.

AMF	FORMATO DI PACCHETTO
Nome completo	ACES Metadata File
Estensione/i	.amf
Tipologie MIME	application/amf+xml
Sviluppato da	Academy of Motion Picture Arts and Sciences
Tipologia di standard	aperto, estendibile, retrocompatibile, testuale
Livello metadati	3
Derivato da	ACESclip
Revisione	1.2 (2019)
Riferimenti	Standard e bollettini tecnici dell'AMPAS: • TB-2014-009, *ACES clip-level metadata file format* • S-2014-006, *A common file format for Look-Up Tables* • TB-2014-012, *ACES version 1.0 component names* • TB-2014-010, *design, integration and use of ACES LMT* • www.oscars.org/aces • www.acescentral.com
Conservazione	Sì
Racc. per la lettura	Speciale; consigliato in post-produzione cinetelevisiva

[59] Quali il TimeCode (cfr. §2.12) e il KeyCode™: quest'ultimo, in pratica, un UID che si associa al singolo fotogramma –addirittura della singola perforazione– al numero di serie di ogni rullo, insieme alla sua marca ed emulsione fotochimica.

Firmato digitalmente da ROBERTO FRACCIA

Racc. per la scrittura	Speciale; consigliato in post-produzione, archiviazione e conservazione di contenuti cinetelevisivi in ACES

48 Il formato ACESclip è un dialetto XML riservato ad un file *sidecar* che possa accompagnare diversi tipi di file video, all'interno di un processo di trasporto, elaborazione o archiviazione di contenuti che rispetti, colorimetricamente, il sistema ACES introdotto in §2.6. In particolare si consiglia di affiancare un file ACESclip (estensione .ACESclip.xml) sia a file con contenuti compatibili alle specifiche colorimetriche ACES (in pratica, il solo spazio-colore ACES2065-1 descritto nello standard ST2065-1).

XDCAM	FORMATO DI PACCHETTO
Nome completo	XDCAM™ package
Estensione/i	.mxf, .xml, …
Tipologie MIME	application/mxf, /xml, …
Sviluppato da	Sony Corporation
Tipologia di standard	proprietario (chiuso), *de facto*
Livello metadati	4
Derivato da	–
Revisione	–
Riferimenti	–
Conservazione	No
Racc. per la lettura	Speciale; raccomandato in post-produzione e distribuzione di contenuti cinetelevisivi
Racc. per la scrittura	Speciale; sconsigliata la produzione

49. Il formato di pacchetto proprietario XDCAM è utilizzato da alcune cinecamere della Sony Corporation, anche se il nome XDCAM™ si riferisce a una gamma ben più ampia di prodotti per il video professionale, inclusi dispositivi di archiviazione (*Professional Disc*, ovvero dischi P2) e di riproduzione. Come formato di pacchetto, XDCAM prevede una ramificazione in sottocartelle predefinite, l'uso di vari codec video (e.g. DV, MPEG-2 parte 2, MPEG-4 ovvero M4V), più alcuni file XML di contorno, che ne descrivono i metadati e il pacchetto d'insieme. A causa delle licenze d'uso legate al formato, se ne sconsiglia fortemente l'uso per la produzione di nuovi contenuti (salvo laddove il capitolato tecnico di consegna lo preveda come unica opzione per una data qualità oggettiva). Tuttavia, la sua ampia diffusione come standard *de facto* impone di considerarlo come formato da poter aprire da parte delle organizzazioni che si occupano di post-produzione o masterizzazione dei contenuti.

Firmato digitalmente da ROBERTO FRACCIA

2.12.1 Raccomandazioni per la produzione di documenti

1. Per quanto riguarda la produzione di documenti audiovisivi in generale, come verrà anche ribadito nel capitolo sul riversamento (§3.3), si raccomanda una valutazione di interoperabilità su tutti i formati di tutte impiegati in un documento informatico multimediale. In particolar modo, qualora il contenuto audiovisivo sia rappresentato da un pacchetto di file (ove, tipicamente, ciascun file descrive metadati, singole essenze o loro porzioni) andrà valutata l'interoperabilità del formato del pacchetto, seguito dall'interoperabilità di ogni file potenzialmente contenuto in esso. Per ciascun file andrà valutata l'interoperabilità del formato contenitore (wrapper, cfr. §1.1.1), se del caso, la tipologia di essenze in esso rappresentate e dunque l'interoperabilità dei codec usati da ciascuna essenza nel contenitore.
2. Relativamente ai soli formati di contenitori e pacchetti multimediali oggetto di questa sezione, si fanno le seguenti raccomandazioni:

- Per contenuti audiovisivi, prevalentemente di natura cinetelevisiva o comunque con destinazioni d'uso professionali –siano essi master per la distribuzione tramite i canali della televisione tradizionale o OTT– da sottoporre o meno a procedimenti di archiviazione o conservazione, si raccomanda particolarmente il formato master interoperabile (IMF). Tale formato di pacchetto di file consente, tecnicamente, una separazione delle essenze (anche relativamente a edizioni multiple e localizzazione); operativamente, può trasportare anche la separazione del contenuto in sue parti funzionali (e.g. marche e loghi iniziali, prologo, titoli di testa, "capitoli", titoli di coda, ecc.). In entrambe i casi, tali separazioni possono essere sfruttate in caso di riedizione, trasporto e archiviazione, allo scopo di minimizzare tempi, risorse computazionali e occupazione di storage, riducendo i costi infrastrutturali e migliorando al contempo le caratteristiche archivistiche del contenuto. Si raccomanda, tuttavia, di formare i pacchetti IMF secondo una specifica "Applicazione" (anch'esse standardizzate dalla SMPTE) relativa al dato contenuto, in modo da estendere l'interoperabilità con le aziende di settore che le adottano. Il formato IMF può invece non essere ideale quando si verificano una o più delle seguenti condizioni:
  - sia necessario conservare le essenze audiovisive senza perdita di qualità della compressione,
  - non via sia un'Applicazione IMF adeguata al processo, o
  - sia necessaria una modifica del contenuto per cui è preferibile l'utilizzo di sequenze di fotogrammi (cfr. qui sotto).

Firmato digitalmente da ROBERTO FRACCIA

- Per contenuti sempre con destinazioni d'uso professionale (prevalentemente cinetelevisivi) ove sia necessario preservare la massima qualità video (tramite assenza di compressione o l'uso di compressione *lossless*) e, al contempo, è preferibile un approccio basato su sequenze di fotogrammi, si raccomanda l'uso di DI basato su EXR.
- Per particolari casi d'uso cinetelevisivi, vincolati a specifiche regole tecniche, è possibile adottare altri formati, come ad esempio:
    - il pacchetto di cinema digitale (DCP) per la distribuzione finale dei film nelle sale cinematografiche;[60]
    - il DI basato su sequenze di DPX per contenuti scansionati da pellicole cinematografiche e non ulteriormente elaborati;
    - l'MPEG2 per la sola trasmissione dei contenuti come flussi in tempo-reale (e.g. televisione via cavo, satellitare, ovvero OTT).
- Per tutti gli altri tipi di contenuto, si raccomanda l'utilizzo di un solo file contenitore che racchiuda tutte le essenze e i metadati necessari comunque alla riproduzione del documento audiovisivo. In particolar modo, si raccomanda l'utilizzo del *wrapper* MXF, in quanto potenzialmente integrabile con funzionalità avanzate che rendono facilmente riutilizzabile un contenuto generico anche in ambiti professionali.
- Per contenuti audiovisivi generici, ove sia prioritario facilitarne la riproduzione da parte di applicativi di larga diffusione (anziché dotarlo di un contenitore professionale che supporti metadati interoperabili e una migliore facilità di riversamento), si raccomanda in particolar modo il *wrapper* MP4.

2.13 Archivi compressi

1. ***Nota Bene***: Alcuni dei pacchetti di file oggetto del presente Allegato sono di fatto creati, come ultimo passaggio, impacchettando una porzione di filesystem (cfr. §1.1.2) in un unico file compresso, utilizzando formati descritti nel presente capitolo o meno. Tali documenti sono dunque rappresentati, grazie a questo stratagemma tecnico, da un unico file anziché da un pacchetto — con indubbi vantaggi sia operativi che normativi.
2. Alcuni di questi formati mantengono l'estensione file del formato di archiviazione sopra descritto (e.g. .zip, .tar,.7z, …); altri utilizzano estensioni proprie (e.g. .docx/.xlsx/.pptx, .od*?*, .woff/.woff2, .jar, .apk, .ipa).

[60] Si sconsiglia di utilizzare il DCP come formato per archiviazione e conservazione per via della compressione jpeg2000 delle essenze video e, soprattutto, a causa della crittografia a chiave mista pubblica/privata con cui vengono formate le copie per le sale e che rischia, senza una corretta gestione delle chiavi crittografiche (cfr. §2.16), di rendere inutilizzabile il documento archiviato in DCP.

Firmato digitalmente da ROBERTO FRACCIA

3. Un tipico esempio ove sono impiegate entrambe le convenzioni è rappresentato quando il documento, originariamente costituito da più file, è riversato in un unico file mediante due passaggi distinti e consecutivi: prima viene "pacchettizzato" in un unico file; successivamente tale file viene compresso usando un formato a scelta tra una pluralità di formati (e i corrispondenti algoritmi di compressione). Molto diffuso è l'uso della pacchettizzazione in formato TAR seguita da compressione, ove si adottano due *naming convention* alternative: quella con 'doppia estensione' (all'estensione .tar viene concatenata quella dello specifico algoritmo di compressione) e quella ove un'unica estensione di file indica la concatenazione dei due formati. Tale dualismo si trova, ad esempio, per le compressioni GZIP (.tar.gz ovvero .tgz), BZIP2 (.tar.bz2 / .tbz), 7-Zip (.tar.7z / .t7z), LZMA (.tar.lzma / .tlz), XZ (.tar.xz e .txz), ecc.

TAR	FORMATO CONTENITORE
Nome completo	UNIX Standard Tape Archive (TAR)
Estensione/i	.tar
Magic number	ustar
Tipo MIME	application/x-tar
Sviluppato da	comunità open source
Tipologia di standard	aperto, retrocompatibile, *de iure*, binario
Livello metadati	1
Derivato da	PKZIP
Revisione	7 (2017)
Riferimenti	• IEEE 1003.1:2017, POSIX *base specifications, issue 7* • GNU, Basic Tar Format, (2017)
Conservazione	Sì, ma dipende dal contenuto della busta TAR
Racc. per la lettura	Generico; obbligatoria la lettura
Racc. per la scrittura	Generico; raccomandata la produzione per archivi su nastri digitali generici o file applicativi Linux/UNIX

ZIP	FORMATO CONTENITORE
Nome completo	Zip
Estensione/i	.zip, .zipx
Magic number	PK 0x[0304|0506|0708]
Tipo MIME	application/zip
Sviluppato da	PKWARE®
Tipologia di standard	proprietario (libero), retrocompatibile, *de iure*, binario
Livello metadati	3
Derivato da	PKZIP

Firmato digitalmente da ROBERTO FRACCIA

Revisione	6.3.5 (2018)
Riferimenti	• ISO/IEC 21320-1:2015 • PKWARE, *.ZIP File Format Specification*, v6.3.5 (2018)
Conservazione	Sì, ma dipende dal contenuto della busta ZIP
Racc. per la lettura	Generico; obbligatoria dalla versione 6.3.1 (2007)
Racc. per la scrittura	Generico; raccomandata la versione 6.3.1 o precedenti

GZIP	FORMATO CONTENITORE
Nome completo	GNU Zip
Estensione/i	.gzip
Magic number	0x01F8B
Tipo MIME	application/gzip
Sviluppato da	comunità open source
Tipologia di standard	aperto (GNU LGPL), retrocompatibile, *de iure*, binario
Livello metadati	1
Derivato da	PKZIP
Revisione	6.3.5 (2018)
Riferimenti	• RFC-1952 • RFC-6713 • www.zlib.org/rfc-gzip.html
Conservazione	Sì, ma ipende dal contenuto della busta GZIP
Racc. per la lettura	Generico; obbligatorio
Racc. per la scrittura	Generico; raccomandato per archivi contenenti applicativi Linux/UNIX

7-ZIP	FORMATO CONTENITORE
Nome completo	*7-Zip* compressed archive format
Estensione/i	.7z
Magic number	7z 0xBCAF271C
Tipo MIME	application/x-7z-compressed
Sviluppato da	Igor Pavlov
Tipologia di standard	aperto (GNU LGPL), retrocompatibile, *de facto*, binario
Livello metadati	3
Derivato da	compressione Lempel-Ziv-Markov (LZMA)
Revisione	18.06 (2018)
Riferimenti	• Pavlov I., LZMA SDK (2018)
Conservazione	Sì, ma ipende dal contenuto della busta 7-Zip

Firmato digitalmente da ROBERTO FRACCIA

Racc. per la lettura	Generico; consigliato
Racc. per la scrittura	Generico; consigliato

RAR	FORMATO CONTENITORE
Nome completo	Roshal Archive file format
Estensione/i	.rar; .r[00–99]
Magic number	Rar! 0x1A0700, Rar! 0x1A070100
Tipo MIME	application/java-archive
Sviluppato da	Eugene (algoritmo) e Alexander (applicativi) Roshal
Tipologia di standard	aperto (lettura), proprietario (scrittura), retrocompatibile, *de facto*
Livello metadati	3
Derivato da	compressione Lempel-Ziv-Storer-Szymański (LZSS)
Revisione	5.61 (2018)
Riferimenti	• www.rarlab.com • theunarchiver.com
Conservazione	No
Racc. per la lettura	Generico; altamente sconsigliato; valutare opportunità di riversamento in altro formati di archiviazione
Racc. per la scrittura	Generico; Sconsigliato.

JAR	FORMATO CONTENITORE
Nome completo	Java Archive file format
Estensione/i	.jar
Magic number	0x5F27A889
Tipo MIME	application/jar-archive
Sviluppato da	Verizon Media; Oracle Corporation
Tipologia di standard	proprietario (libero), retrocompatibile, *de facto*, binario
Livello metadati	3
Derivato da	ZIP
Revisione	2018
Riferimenti	• Oracle, JAR File Overview, 2018 • Oracle, JAR File Specification, 2018
Conservazione	Sì, ma dipende dal contenuto della busta JAR
Racc. per la lettura	Specifico; raccomandato in ambito ICT e sviluppo codice
Racc. per la scrittura	Specifico; raccomandato in ambito ICT e sviluppo codice in linguaggio Java

Firmato digitalmente da ROBERTO FRACCIA

ISO	FORMATO CONTENITORE
Nome completo	Immagine di volume ISO9660
Estensione/i	.iso
Magic number	CD001 (dal 32768,mo 34817,mo o 36865mo byte)
Tipo MIME	application/x-iso9660-image
Sviluppato da	International Organization for Standardization
Tipologia di standard	proprietario (libero), retrocompatibile, *de iure*, binario
Livello metadati	1
Derivato da	
Revisione	6.3.5 (2018)
Riferimenti	• ECMA-119, 3rd Ed. (2017) • ISO/IEC 13490-1:1995, […]: *General* • ISO/IEC 13490-2:1995, […]: *Volume & file structure* • ECMA-168, 2nd ed., 1994 • Famiglia di standard **13346** della ISO/IEC • ECMA-167, *Universal Disk Format (UDF)*, 3rd ed., 1997
Conservazione	Sì, ma dipende dal contenuto della busta ISO9660
Racc. per la lettura	Specifico; fortemente raccomandato in ambito ICT
Racc. per la scrittura	Specifico; raccomandato in ambito ICT per immagini normali e forensi di dispositivi di *storage* a blocchi

4. Questo standard descrive prevalentemente due oggetti che possono a livello logico contenersi l'una nell'altra:

1. un contenitore generico per la memorizzazione "byte per byte" di un'evidenza informatica costituente il volume di un dispositivo di *storage* a blocchi (tipicamente ad accesso casuale);
2. un filesystem (cfr. §1.1.2), la cui specifica è codificata nello standard deprecato ISO 9660;

4. Lo standard ISO 9660, obsoleto, è stato sostituito, sia come storage che come filesystem virtuale, da altri due standard: l'ISO 13490, che è prevalentemente un suo aggiornamento; l'ISO 13346, denominato *Universal Disk Format* (UDF), che introduce invece contenitore e filesystem nuovi. In passato, diverse estensioni furono introdotte –come standard *de facto* però– da alcune organizzazioni: le Apple ISO9660 Extensions (per il filesystem proprietario HFS+), l'IEEE P1282 ("Rock Ridge"), il Microsoft® "Joilet", l'IBM "El Torito". Come filesystem invece, l'ISO9660 (che continua a dare il nome al formato di file) e le sue estensioni furono originariamente impiegati per i dischi ottici di tipo CD, DVD e BluRay (BD) — nelle versioni "ROM"

Firmato digitalmente da ROBERTO FRACCIA

a sola-lettura o meno. Il formato, rappresentato in un unico file è stato utilizzato per distribuire immagini trasportabili di tali dischi, allo scopo di masterizzarli in un secondo momento. In una terza fase temporale, si è consolidato come standard *de facto* per conservare immagini "pseudoforensi" di versioni installabili o preinstallate di alcuni software, simulandone la distribuzione nell'obsoleto supporto informatico basato su disco.

VMDK	FORMATO CONTENITORE E DI PACCHETTO
Nome completo	Virtual Machine Disk Format
Estensione/i	.vmdk
Magic number	KDMV 0x[01|02]000000
Tipo MIME	application/x-vmdk
Sviluppato da	VMware (Dell Incorporated)
Tipologia di standard	aperto, retrocompatibile, *de facto*, binario o testuale
Livello metadati	3
Derivato da	ISO 660
Revisione	VMFS-5 (2011)
Riferimenti	• VMware, *Virtual Disk Format* (2011) • VMware, Virtual Disk Development Kit (VDDK) v6.7.1
Conservazione	Sì, ma dipende dal contenuto della busta VMDK
Racc. per la lettura	Usare SOS o applicativi commerciali nei reparti IT.
Racc. per la scrittura	Usare SOS o applicativi commerciali nei reparti IT.

5. Il formato VMDK, proprietario VMware ma standard *de facto*, permette di rappresentare uno storage a blocchi in formato "sparso" (cioè rappresentando solo i blocchi effettivamente inizializzati dal dispositivo), in uso da parte di macchine virtuali e container. È un formato sia di contenitore che di pacchetto perché è disponibile in due varianti: nella prima è un singolo file che contiene sia l'header con i metadati interni, sia il contenuto a blocchi vero e proprio dello storage virtualizzato. Nella seconda variante, invece, è costituito da un file di testo contenente i soli metadati più uno o più file binari contenenti solo la rappresentazione blocco per blocco di parti del dispositivo.

DMG	FORMATO CONTENITORE
Nome completo	Apple® Disk Image
Estensione/i	.dmg
Specializzazione di	Immagine di volume ISO9660
Tipo MIME	application/x-apple-diskimage
Sviluppato da	Apple Incorporated

Firmato digitalmente da ROBERTO FRACCIA

Tipologia di standard	proprietario (libero), retrocompatibile, *de facto*, binario
Livello metadati	3
Derivato da	Apple New Disk Image Format (NDIF, .img)
Revisione	–
Riferimenti	• newosxbook.com/DMG.html • Apple, *File System Programming Guide* (2018)
Conservazione	No
Racc. per la lettura	Nessuna raccomandazione
Racc. per la scrittura	Valutare riversamento in altri formati per dati semplici. Conservare/archiviare i file .dmg in caso di backup di applicativi nativi Apple (macOS®, iOS®, ecc.).

2.13.1 Raccomandazioni per la produzione di documenti

1. La raccomandazione circa i formati da utilizzare per la produzione di archivi compressi non può che essere dettata dalle finalità d'uso dell'archivio. Per il resto – con l'eccezione del formato RAR e del DMG di Apple– tutti i formati descritti in questa sezione sono sufficientemente aperti. Mentre la scelta su ZIP, GZIP (e loro varianti) piuttosto che 7-Zip è dettata spesso da esigenze tecniche specifiche degli algoritmi di compressione.

2.14 Documenti amministrativi

1. Sono qui elencati alcuni formati di file utilizzati per documenti amministrativi di utilizzo generale, da parte delle PP.AA. e di altri enti, su tutto il territorio nazionale, quali:

- fascicolo sanitario elettronico,
- fatturazione elettronica,
- protocollo informatico,
- asserzioni elettroniche legate a schemi di identificazione elettronica e a loro utilizzi in capo ad autenticazione, autorizzazione, sottoscrizione o altro.

Firmato digitalmente da ROBERTO FRACCIA

2. Si precisa che, per lo svolgimento di procedimenti amministrativi non contemplati in questa sezione, le PP.AA. posso utilizzare anche altri formati di file descritti sia nel resto di questo Allegato, sia non compresi da esso qualora, in quest'ultimo caso, i formati non siano sostituibili con formati previsti nell'Allegato e sia comunque stata fatta una valutazione di interoperabilità.[61]

FATTURAPA	FORMATO DI FILE
Nome completo	fattura elettronica FatturaPA
Estensione/i	.xml
Specializzazione di	XML
Tipo MIME	application/xml
Sviluppato da	Agenzia delle Entrate
Tipologia di standard	aperto, estendibile, *de iure*, testuale
Livello metadati	4
Derivato da	–
Revisione	1.2.1 (2018)
Riferimenti	• www.fatturapa.gov.it • *Specifiche tecniche operative del formato della fattura del sistema di interscamio* v1.2.1 (2018) • *Schema del file XML Fattura PA* v1.2.1 (2018) • Foglio di stile per visualizzare la fattura v1.2.1 (2018) • Agenzia delle Entrate, *Allegato A* del D.M. 55/2013
Conservazione	Sì
Racc. per la lettura	Specifico; consultare la normativa in materia
Racc. per la scrittura	Specifico; consultare la normativa in materia

3. La fattura elettronica è creata, trasmessa, elaborata e conservata centralmente dal Sistema di Interscambio (*SdI*) dell'Agenzia delle Entrate, ovvero da altri applicativi ad esso interconnessi. Il formato della fattura elettronica è costituito da un file XML nel dialetto FatturaPA, che comprende tutte le varianti di processo della fatturazione convenzionale, suddivisi in tre macro-aree:

- dati anagrafico-fiscali delle parti (prestatore/cedente e committente/cessionario),
- metadati relativi alla fattura elettronica stessa, alle valute e al suo trasporto nel SdI,

[61] Si veda in tal senso, per quanto riguarda il protocollo informatico le Linee guida cui questo Allegato afferisce, per quanto riguarda gli schemi di identificazione elettronica e i servizi fiduciari elettronici il §2.16 del presente Allegato, che rimanda alla normativa attualmente in vigore.

Firmato digitalmente da ROBERTO FRACCIA

- descrizione dei beni o servizi oggetto della fatturazione da un punto di vista fiscale,
- metadati inerenti all'eventuale trasporto fisico dei beni oggetto della fatturazione.

4. È anche prevista la possibilità di allegare alla fattura uno o più allegati che vengono codificati [62] e "immersi" all'interno del file (che diviene così un contenitore).

CDA2	FORMATO DI FILE
Nome completo	Clinical Document Architecture
Estensione/i	.xml
Specializzazione di	XML
Tipo MIME	application/xml
Sviluppato da	HL7 International
Tipologia di standard	proprietario (libero), estendibile, *de iure*, testuale
Livello metadati	2
Derivato da	HL7 CDA Rel. 1.0
Revisione	2.0 (2018)
Riferimenti	• ISO/HL7 27932:2005, *HL7 Clinical Document Architecture* • www.fascicolosanitario.gov.it/Standard-documentali • Foglio di stile per la consultazione interoperabile • Circolare AGID N°4/2017
Conservazione	Sì
Racc. per la lettura	Specifico; consultare la normativa in materia
Racc. per la scrittura	Specifico; consultare la normativa in materia

5. Il CDA è uno standard di markup basato su XML pensato per lo scambio informatico di documenti clinici ed è, inoltre, uno degli standard di riferimento per il Fascicolo Sanitario Elettronico (FSE), la cui normativa si può trovare sul sito ufficiale del FSE: www.fascicolosanitario.gov.it. Il CDA è uno standard definito originariamente da ANSI e successivamente sviluppato dall'organizzazione senza scopi di lucro Health Level 7. Il CDA specifica la sintassi e fornisce una struttura di base (data set di riferimento) per realizzare l'intera semantica di un documento clinico (guida implementativa). Un documento CDA è in grado di contenere qualunque tipo di informazione clinica; supporta inoltre testo non strutturato e può incorporare documenti nei formati PDF, DocumentML e RichText Format, così

[62] Per la precisione, la codifica binaria è ottenuta mediante algoritmo *Base64*, specificato in RFC-4648.

Firmato digitalmente da ROBERTO FRACCIA

come immagini di tipo JPEG e PNG. La versione 2 del CDA è stata adottata dallo standard ISO/HL7 27932 del 2005.

SEGNATURA DI PROTOCOLLO		FORMATO DI FILE
Nome completo	Segnatura di protocollo	
Estensione/i	.xml	
Specializzazione di	XML	
Tipo MIME	application/xml	
Sviluppato da	Agenzia per l'Italia Digitale	
Tipologia di standard	aperto, estendibile, *de iure*, testuale	
Livello metadati	2	
Derivato da	–	
Revisione	2013	
Riferimenti	• Allegato 6 alle Linee guida per la formazione, gestione e conservazione del documento informatico • Foglio di stile per visualizzare la segnatura (2018)	
Conservazione	Sì	
Racc. per la lettura	Specifico; si veda la normativa nelle presenti Linee guida	
Racc. per la scrittura	Specifico; si veda la normativa nelle presenti Linee guida	

6. La segnatura di protocollo è descritta nell'Allegato 6 delle presenti Linee guida.

ASSERZIONE SPID		FORMATO DI FILE
Nome completo	Asserzione SPID	
Estensione/i	.xml	
Specializzazione di	XML	
Tipo MIME	text/xml	
Sviluppato da	Agenzia per l'Italia Digitale	
Tipologia di standard	aperto, estendibile, *de iure*, testuale	
Livello metadati	2	
Derivato da	Security Assertion Markup Language, SSO profile; OpenID Connect	
Revisione	1.0 (2014)	
Riferimenti	• www.spid.gov.it • AGID, *Regolamento recante le Regole Tecniche* v1.0 (2014) • D.P.C.M. 24 ottobre 2014	
Conservazione	Sì	
Racc. per la lettura	Specifico; consultare normativa in materia	

Firmato digitalmente da ROBERTO FRACCIA

Racc. per la scrittura	Riservato alla federazione SPID, costituita da gestori di identità digitale, fornitori di servizi e *attribute authority*.

7. Le asserzioni legate al Sistema Pubblico di Identità Digitale (SPID), siano esse in linguaggio SAML (basato su XML), ovvero in formato JWT (basato su JSON), cfr. §2.3, sono da considerarsi un formato a se stante in quanto possono trasportate e, se adeguatamente gestite, conservare a lungo termine dati personali o sensibili di persone fisiche o giuridiche. Per tali motivi tali asserzioni sono normate da altre Regole Tecniche emanate dall'Agenzia per l'Italia Digitale.

2.15 Applicazioni e codice sorgente

1. Esistono una miriade di formati per codificare le applicazioni (altrimenti dette, impropriamente anche se a causa di una forzatura storica, *binari*). Tipicamente, tali formati dipendono dall'architettura dell'hardware e dal SO impiegato. Per tale motivo figurano tanto gli eseguibili Microsoft® (.exe, .com, .msi), quanto quelli macOS® (.pkg), quanto le *app* per dispositivi mobili, sia Android (.apk), che iOS® (.ipa). Oltre agli eseguibili, le porzioni di codice statico (.a, .lib) e dinamico (.so, .dll, .dylib) sono anch'esse dotate di formati specifici, largamente dipendenti dal SO.
2. La distinzione si semplifica nel caso dei codici sorgente scritti nei vari linguaggi di programmazione –interpretati o compilati– per i quali la tipologia di file è in realtà unica: un semplice file di testo (con codifica dei caratteri ASCII ovvero in qualche variante di UNICODE o UTF), la cui estensione (e, di conseguenza, anche il tipo MIME) da un'indicazione logica circa il linguaggio di programmazione o di *scripting* in cui sono codificate le proposizioni al suo interno.
3. Né il formato dei file contenenti le applicazioni, né i linguaggi di programmazione sono oggetto delle Linee guida di cui il presente Allegato è parte integrante. Si rimandano le PP.AA. alle *Linee guida sul riuso del software* per gli obblighi e le raccomandazioni in materia di sviluppo applicativo.

2.16 Applicazioni crittografiche

1. Per meglio chiarire il contesto, si premette che i servizi fiduciari elettronici sono normati da fonti di livello pari o superiore a quello delle presenti Linee guida, le quali contengono obblighi e raccomandazioni anche in merito ai formati di file utilizzati per tali servizi. Tali fonti, includenti le loro successive modificazioni, sono:

Firmato digitalmente da ROBERTO FRACCIA

- Regolamento (UE) Nº 910/2014 del Parlamento europeo e del Consiglio (regolamento "eIDAS");
- Decisioni di Esecuzione (UE) collegate con il regolamento eIDAS;
- articoli 20, 21, 24, 28, 35 e 36 del CAD;
- *Linee Guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate*, emanate con Determinazione AgID Nº121/2019;
- D.P.C.M. del 21 maggio 2013 (*Nuove Regole Tecniche Firma Elettronica Avanzata*).

2. I documenti informatici normati dalle suddette fonti, utilizzati per servizi fiduciari elettronici e altri servizi che impiegano la crittografia, al fine di aumentare le caratteristiche di confidenzialità, integrità, autenticità e non ripudio di evidenze informatiche, si classificano, generalmente, in:

a) buste crittografiche contenenti firme, sigilli o validazioni temporali elettroniche ed, eventualmente, i documenti informatici stessi a cui tali servizi fiduciari afferiscono;
b) certificati elettronici di creazione di firma, sigillo o validazione temporale elettronica;
c) certificati elettronici di autenticazione di siti web (WAC);
d) certificati elettronici di attribuzione o autenticazione;
e) certificati elettronici di certificazione;
f) richieste di sottoscrizione di certificato elettronico;
g) liste di revoca o di fiducia (di certificati elettronici);
h) buste contenenti chiavi crittografiche;
i) buste contenenti documenti cifrati elettronicamente;
j) buste contenenti impronte crittografiche;

3. Nel caso in cui la busta crittografica contenga solo la firma elettronica (o le firme elettroniche), senza il documento stesso a cui essa o esse si riferiscano logicamente, si parla di firma *detached*; quando invece la busta crittografica contiene sia il documento che la sua firma elettronica si parla di firma *enveloping*; quando, infine, il documento informatico costituisca esso stesso busta crittografica per la firma apposta, si parla di firma *enveloped*. La stessa distinzione nominativa si applica, *mutatis mutandis*, al sigillo elettronico ovvero alla validazione temporale elettronica.
4. Viene aggiunta una specifica relativa allo standard *de facto* dei file contenenti una o più impronte crittografiche in un formato puramente testuale (ASCII) e alcuni formati relativamente al trasporto di informazioni crittografiche in ambiti specifici.

CHECKSUM		FORMATO DI FILE
Nome completo	impronta crittografica	
Estensione/i	.sha2, .sha1, .md5, .ripemd160, …	

Firmato digitalmente da ROBERTO FRACCIA

Magic Number	–
Sviluppato da	–
Tipologia di standard	aperto, *de facto*, testuale
Livello metadati	1
Derivato da	XAdES
Revisione	–
Riferimenti	• SANS, *An introduction to file integrity checking on UNIX systems*, GIAC paper, 2003
Conservazione	No
Racc. per la lettura	Generale; obbligo di lettura come normale file di testo
Racc. per la scrittura	Generale; raccomandato la produzione di un'impronta *detached* così costituita in assenza di altri meccanismi di verifica dell'integrità impliciti nei formati o non collegati con essi da vincoli logici più forti e robusti.

5. Per quanto concerne le impronte crittografiche (anche dette *digest* o *thumbprint* in inglese) e le chiavi crittografiche, ove esse non siano utilizzate per finalità, ovvero non siano contenute in file il cui formato non è altrimenti definito da altre fonti normative, si raccomanda di adottare la seguente metodica per creare e archiviare un digest *detached* di file (il cui nome generico sia *nomefile.ext*):

a) scegliere una funzione di *hash* crittografico adeguatamente robusta (si raccomanda SHA-256 o superiore, come definito in RFC-6234 ovvero da Avvisi pubblicati da AgID) e rappresentare il nome dell'algoritmo mediante una stringa di caratteri alfanumerici minuscoli *hash*: senza interruzioni, caratteri di spaziatura o altri simboli (ad esempio, sha256 per SHA-256, ripemd160 per RIPEMD a 160 bit, md5 per MD5 e così via);
b) calcolare l'impronta crittografica dell'intero file con la funzione di *hash* di cui al punto 1;
c) creare un file chiamato *nomefile.ext.hash* (che avrà dunque estensione *.hash*), possibilmente nella medesima cartella ove si trova il file stesso;
d) salvare in questo file, mediante codifica ASCII a 7-bit (cfr. RFC-2045) la sola rappresentazione esadecimale (con cifre minuscole) dell'impronta di cui al punto 2; non andranno aggiunti altri caratteri (incluse spaziature e a-capo — *newline* in inglese), né prima né dopo l'impronta;
e) per quanto possibile, mantenere la località di referenza tra il file originale e quello contenente la sua impronta crittografica mediante i metodi esposti nel §1.1.2, cioè mantenendo sempre file e impronta nella medesima cartella, con la medesima *naming convention* definita ai punti 1 e 2 di questo elenco numerato.

Firmato digitalmente da ROBERTO FRACCIA

KDM	FORMATO DI FILE
Nome completo	Key Delivery Message
Estensione/i	.kdm.xml
Specializzazione di	XML
Tipo MIME	application/kdm+xml
Sviluppato da	Society of Motion Picture and Television Engineers
Tipologia di standard	aperto, retrocompatibile, *de iure*, testuale
Livello metadati	4
Derivato da	XML Digital Signature
Revisione	—
Riferimenti	Famiglia di standard **ST430** della SMPTE: • ST430-1:2006, *D-Cinema operations – KDM* • ST430-2:2006, *D-Cinema operations – Digital Certificate* • W3C Recommendation *XML Signature Syntax and Processing*, 2002 (deprecato)
Conservazione	No
Racc. per la lettura	Specifico; raccomandato per le sale cinematografiche
Racc. per la scrittura	Specifico; raccomandato nella produzione dei master cinematografici per la distribuzione nelle sale

6. Il formato DCP è un formato di busta contenente le cosiddette "chiavi di contenuto" nel contesto del cinema digitale (per i cui formati audiovisivi vedasi §2.12), cioè chiavi simmetriche AES a 256 bit di lunghezza), fino ad uno specifico server Digital Cinema, cui è concessa la facoltà di riprodurre il contenuto di un determinato pacchetto di cinema digitale (DCP) entro un intervallo di tempo finito e predeterminato. Per ogni DCP cifrato, infatti, le essenze di ciascun file MXF sono cifrate ciascuna con una chiave di contenuto. La sicurezza del DCP si ottiene cifrando ulteriormente tutte le chiavi di contenuto di un dato DCP mediante crittografia asimmetrica (RSA a 2048 bit di lunghezza), ove ciascun server è dotato di un HSM contenente sia la chiave privata della coppia (e il relativo certificato di creazione di sigillo elettronico avanzato) che un orologio indipendente anti-manomissione per la validazione temporale elettronica. Su tutti i KDM si appone un sigillo *enveloping* che protegge da contraffazione la specifica DCP da riprodurre (mediante sia l'UID del pacchetto stesso che le impronte crittografiche dei singoli file che lo costituiscono, cfr. §1.1.1), l'intervallo temporale durante il quale ne è concessa la riproduzione e, soprattutto, la copia cifrata delle sue chiavi di contenuto.

Firmato digitalmente da ROBERTO FRACCIA

3 Raccomandazioni sui formati di file

1. I formati da utilizzare nell'ambito delle presenti Linee guida sono quelli previsti nel §2 del presente Allegato. Nello scegliere tali formati di file, da utilizzare per i propri documenti informatici, le organizzazioni possono effettuare la valutazione di interoperabilità (§3.1) che prediliga formati aperti, non proprietari, standard *de iure*, estendibili, parlanti, completamente robusti, indipendenti dal dispositivo –secondo la classificazione fatta in §1.2.2– al fine di:

- prevenire il rischio della loro obsolescenza tecnologica (rischio che incrementa con il divergere delle caratteristiche del formato da quelle sopraelencate);
- mitigare il rischio del *vendor lock-in*,[63] che sussiste soprattutto per i formati proprietari, non codificati in standard *de iure*, o per quelli dipendenti dal dispositivo;
- facilitare il più possibile un loro futuro riversamento in altro formato, prediligendo caratteristiche quali l'estendibilità, la codifica testuale, la compatibilità in avanti e, in misura minore, la robustezza.

2. I formati di file, di contenitori, di pacchetti di file e di codec elencati nel §2 rappresentano, in generale, una famiglia allargata, con candidati più o meno adatti ad un particolare scopo. Nel caso dei codec video, allo scopo di indicare esempi di formati non interoperabili da utilizzare il meno possibile per conservazione o archiviazione, sono elencati anche alcuni codec chiusi o con particolari limitazioni d'uso dovute a licenze, brevetti o royalties, allo scopo di indicare esplicitamente le organizzazioni che avessero documenti multimediali con tali codec verso un riversamento o altra procedura di gestione documentale mirata.
3. Così come accade per i sistemi di archiviazione digitale (storage) –e per tutta la tecnologia in generale– non si può pensare che un formato di file, seppur revisionato nel tempo, possa essere perennemente attuale né di uso corrente. L'obsolescenza dei formati di file e dei dispositivi di archiviazione può essere mitigata soltanto mediante *riversamenti periodici* da una tecnologia verso un'altra; questo vale tanto per le tecnologie di storage che per i formati dei file.
4. Per questo motivo, si consiglia che le PP.AA. e le imprese che hanno necessità di archiviazione e riuso a lungo e lunghissimo termine dei documenti informatici, pianifichino in anticipo una strategia di selezione degli *storage* e dei formati di file che sia il più possibile congiunta, in modo da minimizzare il numero di riversamenti relativi a ciascuno di questi due fattori (ottimizzando la continuità operativa e, nel complesso, riducendo i costi derivanti da tali operazioni).

[63] Consiste, in questo caso, nell'impossibilità tecnologica e/o giuridica di elaborare file (inclusa la conversione in altri formati) senza l'ausilio del proprietario del formato: avvalendosi di sue consulenze, beni, tecnologie, proprietà intellettuale, licenze software o altro.

Firmato digitalmente da ROBERTO FRACCIA

3.1 Valutazione di interoperabilità

1. La valutazione di interoperabilità in merito ai formati dei file, prevista dalle Linee guida di cui il presente Allegato è parte integrante, può essere redatta da qualunque ente pubblico o privato tratti documenti informatici. La valutazione di interoperabilità è redatta con cadenza annuale dalle PP.AA. che trattino documenti informatici in formati diversi da quelli di cui al presente Allegato, ovvero conformi a questi formati ma utilizzati disapplicando gli obblighi e raccomandazioni ivi contenuti.
2. Allo scopo di effettuare la valutazione di interoperabilità, le organizzazioni effettuano una ricognizione di tutte le loro procedure amministrative e/o processi di business, allo scopo di individuare ogni tipologia di documenti informatici trattati (o trattabili). Il valore di questa ricognizione può andare ben al di là degli scopi di cui alle presenti Linee guida.
3. La valutazione di interoperabilità consiste in un dettagliato rapporto circa le seguenti azioni (obbligatorie se indicate in **grassetto**):

a) Includere nell'attività di classificazione (cfr. §1.2.2) un **censimento dei formati** di file e delle tipologie di storage attualmente utilizzati, con particolare riferimento a quelli non elencati nel §2 del presente Allegato.
b) Per ciascun formato di file adottato, elencare tutti i **dettagli tecnici** dei medesimi, quali ad esempio:
   - ♦ nome dei formati e, laddove applicabile, dei dialetti, profili, codec, schemi operativi;
   - ♦ suddivisione tra formati generici e specifici (cfr. §1.2.3);
   - ♦ versioni utilizzate nei documenti già esistenti, ovvero producibili dagli attuali applicativi;
   - ♦ altre caratteristiche tecniche non vincolate dalle specifiche di cui ai punti precedenti (e.g. lingue adottate nei testi, numero di canali audio, spazi-colore, risoluzione per immagini e video, *bitrate* massimo, algoritmi di cifratura, presenza di password, ecc.).
c) Elencare i **processi di riversamento** di formato attualmente in corso nell'organizzazione, con particolare riferimento ai software applicativi impiegati e alle procedure tecniche (automatiche, semiautomatiche o completamente manuali) adottate per configurare tali riversamenti, con lo scopo prioritario di rendere tali riversamenti riproducibili.
d) Elencare le motivazioni attuali che hanno portato alla scelta di ciascun formato di file per il trattamento dei documenti informatici. In particolar modo, se del caso, distinguere i formati di file tra quelli adottati per i documenti:

Firmato digitalmente da ROBERTO FRACCIA

- accettati "in entrata" dal pubblico ovvero da altre organizzazioni,
- utilizzati ad uso esclusivamente interno,
- pubblicati, ovvero prodotti "in uscita" verso altre organizzazioni,
- archiviati ovvero mandati in conservazione.

e) Valutare l'esistenza di standard o di iniziative di standardizzazione a livello internazionale, europeo e nazionale, relativamente alle tipologie di documenti informatici trattati.
f) Quantificare l'eventuale **necessità** di operare sui medesimi documenti informatici nell'arco di una finestra temporale futura.
g) Valutare gli scenari ove successive modificazioni o revisioni dei documenti vengano prodotte in formati diversi da quello originale.
h) Valutare la sussistenza di leggi o altri tipi di obblighi in merito alla **conservazione delle evidenze informatiche nel formato originale** di acquisizione o formazione.
i) Valutare i formati di file di **categorie specifiche**, nonché l'opportunità di riutilizzo dei documenti informatici di ciascuna classe (come da punto 1) da parte di PP.AA. e organizzazioni che operano al di fuori dello specifico settore per il quale il formato e i suoi scenari d'utilizzo sono stati prefigurati.
j) Dipendenza dei formati di file da:
   - licenze d'uso, marche e brevetti o altra **proprietà intellettuale**,
   - sistemi e architetture **proprietarie**, o comunque,
   - sistemi e architetture che, pur senza i suddetti vincoli, sono comunque associati a costi di manutenzione ordinaria o straordinaria, senza la quale diviene a rischio o è fortemente ridotta la capacità di elaborare i suddetti documenti.
k) Inserimento dell'obsolescenza dei formati di file e delle tecnologie di archiviazione all'interno di una più ampia strategia di trasformazione digitale dell'organizzazione.

Si faccia riferimento al Glossario delle presenti linee guida per la definizione dei termini non ulteriormente introdotti in questo Allegato (e che sono qui indicati in colore azzurro Italia).
4. La valutazione di interoperabilità, in quanto parte della gestione documentale, andrebbe effettuata periodicamente allo scopo di individuare tempestivamente cambiamenti delle condizioni espresse dai punti sopra elencati e permettere quindi di valutare eventuali azioni. È proprio nella ripetizione della valutazione di interoperabilità ad intervalli regolari che divengono manifesti i formati in via di obsolescenza (quando non già conservati in un formato obsoleto).

Firmato digitalmente da ROBERTO FRACCIA

3.2 Indice di interoperabilità

1. Allo scopo di coadiuvare la valutazione dei formati di file relativamente all'interoperabilità, l'Agenzia propone innanzi tutto un modello semplificato e quantitativo ove, ad ogni formato di file (anche quelli non elencati nel §2 di questo Allegato), viene associato un valore numerico. Tale valore assegnato al formato è dato dalla somma dei valori associati a tutte le caratteristiche di cui ai punti a)–g) del capitolo §1.2.2.
2. Nel caso di formati di pacchetti o contenitori, andrà fatta una valutazione per ogni componente e considerato come addendo il valore più basso (cioè peggiore) per ciascuna delle sue componenti.
Per un formato contenitore andrà valutato sia il formato della busta che il formato del suo contenuto, ad esempio per i contenitori multimediali (cfr. §2.12), il formato dei codec di ciascuna essenza ivi contenuta; per un formato di pacchetto andranno valutati i formati di tutti i file compresi nel pacchetto e, qualora il pacchetto comprenda dei file contenitori, valutarli con il medesimo criterio sopra esposto.
3. Sia per i formati contenitori che per quelli di pacchetto verrà usato come addendo, per caratteristica, il valore numerico peggiore tra quelli dei suoi file (o dei codec di ciascun file). Si prenda, a titolo di esempio, l'indice di interoperabilità di uno specifico pacchetto di file ove tutti i file utilizzino formati indipendenti dal dispositivo tranne un file multimediale, la cui busta e tutte le sue essenze sono anch'esse indipendenti dal dispositivo tranne una sola essenza audio (che ad esempio potrebbe richiedere la presenza di un dispositivo hardware proprietario per la sua decodifica). Il pacchetto andrà considerato comunque come "dipendente dal dispositivo" e quindi gli verrà applicato un modificatore pari a 0 (anziché a +3), proprio a causa della presenza dell'unico file il cui formato è dipendente dal dispositivo.
4. Considerando una scala che va dal file più interoperabile (con indice pari a 20) a quello meno interoperabile (indice pari a 0), un valore pari a 12 o superiore può essere considerato sufficiente dal punto di vista dell'impatto di tale formato relativamente ad interoperabilità e obsolescenza; valori inferiori indicano problematiche oggettive che vanno affrontate il prima possibile in ottica di riversamento o altre metodologie.
5. Si precisa che l'indice di interoperabilità è meramente indicativo, in quanto non tiene conto di alcuna peculiarità che un'organizzazione possa avere in merito a specifici formati di file. Ad esempio, l'utilizzo di formati chiusi, proprietari o dipendenti dal dispositivo dovrebbe essere sempre un fattore di esclusione almeno nella scelta di formati da usarsi per la formazione di nuovi documenti informatici.

Firmato digitalmente da ROBERTO FRACCIA

3.3 Riversamento

1. Il riversamento di formato, precedentemente introdotto, comporta il trasferimento di un documento informatico in un formato di file diverso: contestualmente, ciò può comportare anche una duplicazione da un sistema di storage ad un altro (volume, disco, nastro, filesystem, storage ad oggetti o altri). Quando si parla di riversamento di file, s'intende un riversamento di almeno il suo formato. Per quanto già detto nell'introduzione al §3, le strategie relative alla gestione dei formati e dei sistemi di storage vanno spesso di pari passo; perciò, può essere in alcuni casi operativamente ed economicamente vantaggioso effettuare i riversamenti di formato contestualmente a quelli di storage. I riversamenti vengono pianificati a seguito di una nuova valutazione di interoperabilità, considerando i costi e i benefici di una tale operazione.
2. Quando si effettua un riversamento finalizzato alla conservazione del file si può e, in certi casi previsti dalla legge, si deve, conservare anche la copia del file nel formato originario. In entrambe questi casi il file originario è conservato indipendentemente dal suo formato di file originario, purché sia conservata anche –in una forma logicamente e univocamente legata ad esso– copia conforme del medesimo in un formato adatto alla conservazione (tra quelli individuati al §2 del presente Allegato). Le considerazioni in questo e nei successivi paragrafi si applicano non solo ai formati di file, ma anche, *mutatis mutandis*, ai formati di buste, pacchetti di file, flussi binari e codec. Lo scopo del riversamento congiunto alla conservazione del documento nel formato originario è consentire la convalida di firme, sigilli o validazioni temporali elettroniche che, eventualmente già presenti nel documento originario, non potrebbero essere riportate –senza invalidarle– nel documento riversato.
3. Quando si effettua un riversamento finalizzato alla conservazione, il file riversato è una copia digitale di un documento digitale e, come tale, la conformità della copia è attestata in base alla normativa vigente, inclusa la certificazione di processo come riportata nell'Allegato 3 delle presenti Linee guida.
4. È importante che nella scelta dei nuovi formati di file (e, *mutatis mutandis*, di contenitori, pacchetti di file, flussi digitali e codec), così come nella scelta metodologica circa l'esecuzione del riversamento, si considerino le peculiarità tecniche del formato sorgente e di quello riversato, con particolare riferimento sia alla perdita di dati e metadati, sia alla diversa qualità o rappresentazione tecnica dei medesimi.
5. Quando si effettua un riversamento massivo finalizzato alla conservazione di più documenti informatici –a prescindere se sia conservato o meno il documento nel suo formato originario– il processo di riversamento include i passaggi indicati nel successivo elenco numerato. Tali passaggi –particolarmente 1 e 2– possono essere

Firmato digitalmente da ROBERTO FRACCIA

inquadrati come parte di un processo certificato di conformità della copia riversata (cfr. Allegato 3 delle presenti linee guida).

1. Il riversamento di un formato viene effettuato mediante un processo certificato che ne garantisce l'integrità (effettiva o per lo meno sostanziale, come intesa nel punto 2) e la riproducibilità. Ogni procedura di riversamento è descritta nel manuale di gestione e, se del caso (cfr. §3.1), nella valutazione di interoperabilità, in tutti i suoi dettagli tecnici, inclusi quelli sui formati di destinazione e quelli riversati.
2. Per le PP.AA., il riversamento avviene sempre in formati che ne migliorano l'interoperabilità, o comunque non la peggiorano (come, stabilito, ad esempio, mediante il calcolo dell'indice di interoperabilità), tenendo conto degli obblighi sulla specificità di formato introdotti in §2.2. In particolar modo *non* sono opportuni, relativamente alla classificazione di formati di cui al §1.2.2, i seguenti riversamenti, da un formato:
   - aperto verso formati chiusi,
   - non proprietario, ovvero proprietario a libero utilizzo, verso formati proprietari,
   - non dipendente dal dispositivo verso formati dipendenti da dispositivo,
   - formato parlante verso formati muti.
3. Per ogni file riversato di un processo massivo automatico ovvero semiautomatico il processo produce un'attestazione del riversamento specifico di quel file, ove le attestazioni circa documenti riversati come parte della medesima procedura vengono collezionati in un registro di riversamento, che contiene (globalmente rispetto alla particolare procedura e individualmente per ogni file elaborato) almeno:
   a. un riferimento temporale opponibile a terzi ai sensi dell'art. 41 del DPCM 22 febbraio 2013 relativo all'inizio o alla fine del riversamento (indicando chiaramente a quale dei due tempi ciascun riferimento temporale si riferisca);
   b. indicazioni sul sistema informativo impiegato (per esempio: nome, numero di revisione sia del sistema operativo che del software; nome della macchina e suoi indirizzi di rete o altri numeri identificativi unici delle componenti hardware; identificativi unici del software quali i numeri di licenza; nome o identificativo unico e orario di accesso al sistema operativo dell'utenza sotto cui l'applicativo ha agito);
   c. nome del file sorgente, posizione nel filesystem e metadati esterni (cfr. §1.1.2);

Firmato digitalmente da ROBERTO FRACCIA

   d. formato sorgente del file, sua versione del formato e metadati interni (cfr. §1.1.3);
   e. impronta crittografica del file sorgente;
   f. nome del file riversato, posizione nel filesystem e metadati esterni;
   g. formato di riversamento, sua versione e metadati interni convertiti dal punto d;
   h. impronta crittografica del file destinazione;
   i. in caso di file contenitori (come sorgente o destinazione), i metadati ai punti d, g[64] si intendono riferiti alla busta, cui si aggiunge elenco completo del contenuto della medesima (p.es. essenze e i codec impiegati per ciascuna di esse, con i loro eventuali metadati e profili); deve inoltre essere previsto –nei casi ove sia tecnicamente possibile– file con imbustamento nidificato (cfr. §1.1.1);
   j. in caso di pacchetti di file (come sorgente o destinazione), i controlli c–h[65] si intendono riferiti a ciascun file componente il pacchetto, cui si aggiunge l'indicazione dei metadati deducibili dall'intero pacchetto nella sua interezza, laddove non esplicitamente descritti negli eventuali file-manifesto (cfr. §1.1.1);
   k. eventuali errori tecnici, anomalie o ambiguità riscontrate durante il riversamento.

4. Nel rispetto delle leggi sulla privacy in vigore (D.Lgs. N°101 del 10 agosto 2018, del GDPR e loro successive modificazioni), il riversamento in altro formato di file costituisce un'ulteriore occasione per ottemperare agli obblighi in materia di adeguatezza, pertinenza, minimizzazione ed esattezza dei dati personali ivi contenuti, così come della liceità del loro trattamento e della loro eventuale pseudonimìa.
5. Qualora sussistano obblighi di legge (come nel caso della protezione dei dati personali o della conservazione sostitutiva) o altri tipi di vincoli nel preservare l'evidenza informatica costituita dal documento nella sua interezza, il documento nel formato originale viene conservato *insieme* a un suo riversamento in formato più interoperabile. Tale associazione logica deve anch'essa essere scritta nel registro di riversamento (ad esempio associando le impronte crittografiche dei due come indicate ai punti e,h[66] del punto 2).
6. Salvo in casi in cui siano applicabili le considerazioni di cui ai punti 3 o 4, un riversamento di formato altera l'evidenza informatica, intaccandone dunque l'integrità da un punto di vista strettamente tecnico; esistono tuttavia riversamenti di formato che mantengono il contenuto documentale *sostanzialmente* invariato (inclusi quelli discussi nei punti 3 o 4), costituendo

[64] Leggasi «al punto d più al punto g».
[65] Leggasi «i controlli dal c all'h».
[66] Leggasi «al punto e più al punto h».

Firmato digitalmente da ROBERTO FRACCIA

una valida possibilità per il riversamento. Tali possibilità di riversamento, qualora siano individuate, sono comprese nel manuale di gestione documentale. In esso viene descritto come il contenuto documentale viene sostanzialmente preservato, incluse le considerazioni sulla similitudine tra le due evidenze informatiche. Sono incluse anche una o più delle seguenti trasformazioni che, se applicabili, sono effettuate durante il riversamento:

- In caso il documento nel formato originale venga mantenuto per assolvere ad obblighi di legge o altro, specificare come i due file (l'originale e il riversato) vengano logicamente associati fra loro (come descritto al punto 4).
- Laddove le evidenze vengano modificate da algoritmi non reversibili (p.es. compressione con perdita) un'analisi puntuale o statistica dell'ammontare di informazione persa durante il riversamento (p.es. misurata in SNR minimi e massimi tra l'essenza sorgente e quella destinazione), con riferimento a standard di misura riconosciuti a livello internazionale, europeo o nazionale.
- In caso di perdita di metadati interni, indicare quali metadati si perdono e come essi vengano comunque riportati nel registro di riversamento.
- In caso metadati convertiti biunivocamente da un formato all'altro (incluso il caso in cui più metadati nel formato sorgente siano oggetto di accorpamenti o separazioni in altri metadati nel formato di destinazione), descrivere gli algoritmi che sono implementati per ciascun metadato.[67]
- In caso di metadati interni convertiti in maniera *non* invertibile, descrivere gli algoritmi impiegati (come al punto precedente), aggiungendo esplicitamente quali informazioni si perdono e come esse siano trasformate irreversibilmente.[68]
- In caso il formato destinazione ammetta dei metadati obbligatori che non hanno un analogo nel formato sorgente (ovvero ammetta metadati facoltativi che si ritiene comunque opportuno inserire nel

[67] A titolo di esempio, sia dato un campo 'Scadenza' nel formato sorgente e un campo 'NotAfter' nel formato destinazione, le cui sintassi sono, rispettivamente, il numero intero di giorni passati da un'*epoca* pari al 1 gennaio 2019 (fuso orario italiano: CEST) e una stringa di testo formattata come da RFC-3339 (in fuso orario UTC). Viene dunque specificato l'algoritmo, perfettamente invertibile, che mappa un valore di "42" in "2019-02-14T01:00:00Z".

[68] A titolo di esempio, sia dato un campo 'dimensione1' nel formato sorgente e un campo 'Width' nel formato destinazione. Nel manuale di riversamento, andrà giustificata la motivazione per cui un valore di "-42.58cm" nel formato sorgente, dotato di segno e unità di misura, viene mappato in "426" indicato implicitamente in millimetri e arrotondato al numero intero più vicino. È anche opportuno che sia indicato il motivo per cui un metadato relativo ad una dimensione (spaziale?) non meglio identificata sia (sempre?) mappato in un campo riservato alla 'larghezza' di qualcosa.

Firmato digitalmente da ROBERTO FRACCIA

formato riversato, anche se non hanno un analogo nel formato originario), specificare come gli vengono assegnati valori.

7. In alcuni casi,[69] imbustando un documento informatico in un contenitore aggiuntivo potrebbe mantenere integro il contenuto all'interno, perciò un riversamento in tal senso –cioè un semplice imbustamento del documento senza alterarlo– può essere reversibile. L'integrità del file nella sua interezza è tuttavia compromessa. Analogamente reversibile è invece includere un documento rappresentato da un file all'interno di un pacchetto di file. Entrambi le metodologie non risolvono i problemi di interoperabilità e obsolescenza originali per cui il riversamento è stato concepito, ma possono mitigarli, soprattutto se vengono scelti contenitori o pacchetti parlanti che compensano la mancanza di metadati nel formato originale.
8. Analogamente al punto 3, in alcuni casi, un documento che viene re-imbustato (cfr. §1.1.1), nel senso che il riversamento consiste nel sostituire la busta che lo conteneva con un'altra, potrebbe mantenere, in alcuni casi, l'integrità del contenuto della busta. Verrebbe persa comunque l'integrità della busta e, come per il punto 3, l'integrità del file nella sua interezza. Tuttavia questa metodologia potrebbe risolvere un problema di obsolescenza e interoperabilità legato al solo formato della busta usata in precedenza.

6. Quando si effettui un riversamento *non* finalizzato alla conservazione è comunque opportuno considerare i passaggi elencati al precedente punto 5, ad eccezione dei punti 1 e 2 del medesimo elenco, che si riferiscono al riversamento qualora inquadrato in processi di conservazione o certificazione di processo.

[69] Alcuni formati contenitori, imbustando un documento, si limitano ad aggiungervi una busta costituita da una o più evidenze informatiche in punti predeterminati del documento o essenza originale (tipicamente in testa e in coda, ma anche inseriti in parti centrali). Quando avviene tecnicamente un procedimento di questo tipo l'evidenza informatica imbustata è alterata *reversibilmente*, potendo quindi essere ricostruita bit a bit. Alcuni formati di contenitore di file, tuttavia, effettuano alterazioni irreversibili del contenuto, che dunque non rimane integro a seguito di un'operazione di "sbustamento" (in inglese, *unwrapping*).

Firmato digitalmente da ROBERTO FRACCIA

ISTITUTO COMPRENSIVO STATALE
"ADA NEGRI"
Via Don Milani 4 - 20086 MOTTA VISCONTI (MILANO)
Tel./Fax02.90000266
E- mail : miic872009@istruzione.it - miic872009@pec.istruzione.it
www.icmottavisconti.it
C.F. 90015610158 – C.M. MIIC872009

DELIBERA N. 11

Il Consiglio di Istituto dell' I.C. statale "A.Negri" – di Motta Visconti, riunitosi il g. 27/04/2022 c/o i locali della sede – Via Don Milani,4 – Motta Visconti;

Visto il D.P.R. 28 dicembre 2000 n.445 "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa" che al capo IV pone l'obiettivo della razionalizzazione della gestione dei flussi documentali coordinata con la gestione dei procedimenti amministrativi da parte delle Pubbliche Amministrazioni, al fine di migliorare i servizi e potenziare i supporti conoscitivi delle stesse secondo i criteri di economicità, efficacia e trasparenza dell'azione amministrativa;

Visto che il D.P.C.M. 31 ottobre 2000 "Regole tecniche per il protocollo informatico" prescrive che il Responsabile del servizio per la tenuta del protocollo informatico, della gestione informatica dei flussi documentali e degli archivi predisponga lo schema del Manuale di gestione e di conservazione dei documenti, e che ciascuna pubblica amministrazione adotti un proprio manuale;

Visto il Decreto del Ministro per l'Innovazione e le Tecnologie del 14 ottobre 2003, con il quale sono state approvate le linee guide per l'adozione del protocollo informatico e per il trattamento informatico dei procedimenti amministrativi;

Visto il D.Lgs. 7 marzo 2005 n.82 "Codice dell'amministrazione digitale";

Visto il DPCM 3 dicembre 2013 "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n.82 del 2005";

Ritenuto opportuno procedere all'aggiornamento del Manuale di gestione e di conservazione dei documenti e del corretto funzionamento del servizio per la tenuta del protocollo informatico approvato con delibera n. 59 del 12/06/2017;

all'unanimità dei presenti

DELIBERA

di approvare, per le motivazioni esposte in premessa, il Manuale per la gestione informatica dei flussi documentali e dell'archivio.

Letto, approvato e sottoscritto

IL SEGRETARIO

(Monica Castiglioni)

IL PRESIDENTE del CONSIGLIO d'ISTITUTO

(Alessio Belloni)

Visto: per l'affissione all'albo il 29/04/2022

Il Dirigente Scolastico
(Prof. Roberto Fraccia)

Firmato digitalmente da ROBERTO FRACCIA

Regolamento Europeo 679/2016 GDPR

Modello aggiornamento incarichi

Il presente modello **va compilato per i soli incarichi che hanno subito variazione** rispetto alla precedente ricognizione / compilazione; i campi lasciati in bianco si intendono rimasti invariati rispetto alla certificazione precedente.

Il presente modello, **firmato digitalmente**, va conservato congiuntamente al **Manuale di Gestione Documentale**, di cui costituisce aggiornamento annuale.

Data compilazione: _____ **Protocollo n. : _____**

Nome e cognome del Dirigente Scolastico: _____

Nome e cognome del Direttore S.G.A. : _____

Atto di nomina del Responsabile del servizio per la tenuta del Protocollo Informatico			
Nome e cognome			
Data		N. protocollo:	

Atto di nomina del sostituto del Responsabile della tenuta del Protocollo Informatico			
Nome e cognome			
Data		N. protocollo:	

Atto di nomina del Responsabile del servizio di Conservazione a norma			
Nome e cognome			
Data		N. protocollo:	

Atto di nomina del Responsabile della conservazione delle copie di sicurezza			
Nome e cognome			
Data		N. protocollo:	

Firmato digitalmente da ROBERTO FRACCIA

Amministratore di rete			
Nome e cognome			
Azienda			
Recapiti (mail e telefono)			
Data nomina		N. protocollo	

Amministratore di sistema			
Nome e cognome			
Azienda			
Recapiti (mail e telefono)			
Data nomina		N. protocollo	

Fornitore Registro Elettronico	
Fornitore Segreteria Digitale	

Incarico	Nome e cognome
Assistente amministrativo	
Assistente amministrativo	
Assistente amministrativo	
Assistente amministrativo	
Assistente amministrativo	
Assistente amministrativo	
Assistente amministrativo	
Assistente amministrativo	
Assistente amministrativo	
Assistente tecnico	
Assistente tecnico	

DPO (Data Protection Officier)			
Nome e Cognome			
Azienda			
Recapiti (mail e telefono)			
Data Nomina		N. protocollo	

Firmato digitalmente da ROBERTO FRACCIA

Ministero dell'Istruzione

Dipartimento per le risorse umane, finanziarie e strumentali
Direzione generale per i sistemi informativi e la statistica

Ministero della Cultura

Direzione Generale Archivi

Linee guida per la gestione documentale nelle Istituzioni scolastiche

Firmato digitalmente da ROBERTO FRACCIA

INDICE

Firmato digitalmente da ROBERTO FRACCIA

PREMESSA

In un quadro di riferimento in cui innovazione e tecnologia rappresentano *asset* strategici per la crescita del sistema Paese e in cui l'emergenza da Covid-19 ha determinato una crescente richiesta di servizi digitali, il Responsabile per la Transizione al Digitale (RTD) del Ministero e delle Scuole sta investendo nel percorso di trasformazione digitale dei servizi e dei relativi processi delle Istituzioni scolastiche.

Il digitale rappresenta uno degli elementi chiave nel raggiungimento di obiettivi di miglioramento della qualità dei servizi e di efficientamento dei modelli operativi, e conseguentemente nel percorso di ripensamento del modello di erogazione dei servizi del settore istruzione; per massimizzare il contributo della leva tecnologica è necessario però che la stessa sia integrata rispetto alla leva organizzativa (processi, ruoli, responsabilità) in cui esprime la propria funzione.

Oltre agli interventi di digitalizzazione dei servizi e processi istituzionali e amministrativi, il RTD sta lavorando nell'assicurare l'infrastruttura organizzativa e digitale alla base del modello di erogazione dei singoli servizi: la gestione documentale. A tal fine, il percorso intrapreso dal Ministero ha il duplice obiettivo di semplificare il lavoro del personale scolastico, fornendo istruzioni uniformi in merito alle modalità operative, e di garantire adeguatezza, dal punto di vista normativo, organizzativo e tecnologico, degli strumenti in uso presso le Istituzioni scolastiche. In tale contesto, si è avvertita la necessità di aggiornare e adattare le *Linee guida per gli archivi delle istituzioni scolastiche*, elaborate dalla Direzione Generale per gli Archivi del Ministero della Cultura nel dicembre del 2005.

Il Ministero ha pertanto definito un *framework* di riferimento che tiene conto di aspetti organizzativi e tecnologici omogenei, all'interno del quale le Istituzioni scolastiche si possono muovere per garantire una gestione uniforme e adeguata, anche dal punto di vista normativo, del processo di gestione documentale. Il *framework* proposto prevede la digitalizzazione di tutto il «ciclo di vita» dei documenti: dalla loro nascita (per creazione o acquisizione) fino alla conservazione e/o scarto, con l'obiettivo di consentire una graduale transizione da un sistema di tipo analogico e cartaceo ad un sistema esclusivamente digitale e «*paperless*».

Le presenti Linee guida di carattere generale descrivono, a livello macro, l'architettura del modello di funzionamento che l'Amministrazione intende proporre alle Istituzioni scolastiche, nonché i principali strumenti necessari per il presidio di tutte le attività inerenti al processo di gestione documentale. Sono parte integrante delle presenti Linee guida i relativi allegati (*format* di manuale per la gestione dei flussi documentali delle Istituzioni scolastiche, titolario di classificazione, massimario di conservazione e scarto).

Nel seguito del documento si fornisce una panoramica rispetto ai seguenti aspetti:

1. Quadro normativo di riferimento;
2. Principali indicazioni sulla gestione documentale;
3. Strumenti a supporto.

Firmato digitalmente da ROBERTO FRACCIA

1. QUADRO NORMATIVO DI RIFERIMENTO

Le principali disposizioni normative prese in considerazione ai fini della redazione delle presenti Linee guida e dei relativi allegati sono le seguenti:

D.P.R. 445/2000 e successive modificazioni	Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (TUDA)
D.Lgs. 42/2004 e successive modificazioni	Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137[1]
Linee Guida AgID	Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, adottate dall'AgID con Determinazione n. 407/2020 del 9 settembre 2020 ed in seguito aggiornate con Determinazione n. 371/2021 del 17 maggio 2021 (da attuare entro il 1° gennaio 2022)
L. 241/1990	Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi
D.Lgs. 196/2003 e successive modificazioni	Codice in materia di protezione dei dati personali
D.Lgs. 82/2005 e successive modificazioni	Codice dell'amministrazione digitale (CAD)
DPCM del 22 febbraio 2013	Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71
DPCM del 21 marzo 2013	Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni
Regolamento UE 910/2014 (Regolamento *eIDAS*)	Regolamento in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE

Oltre alle fonti elencate in tabella, sono state utilizzate ulteriori disposizioni normative e prassi adottate in materia, quali, a titolo esemplificativo, il D.Lgs. 33/2013 recante "*Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni.*" e la Delibera ANAC n. 1309 del 28 dicembre 2016, recante "*Linee Guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 c. 2 del D.Lgs. 33/2013*".

[1] Con riferimento al Codice dei beni culturali e del paesaggio, è bene precisare che le norme in materia di autonomia delle Istituzioni scolastiche (D.P.R. 8 marzo 1999, n. 275), conferendo personalità giuridica alle scuole che ne erano prive, hanno esteso a tutte la natura di ente pubblico. Pertanto, ogni Istituzione scolastica è destinataria dei medesimi obblighi discendenti dal Codice validi per tutti gli enti pubblici. In forza di questa normativa, gli archivi delle Istituzioni scolastiche sono beni culturali fin dall'origine (art.10, c.2-b D.lgs 42/2004, Codice dei beni culturali e del paesaggio) e come tali soggetti alla vigilanza (art. 18 del Codice citato) della Soprintendenza archivistica competente per territorio, la quale in tale ambito svolge anche funzioni di consulenza tecnica.

Firmato digitalmente da ROBERTO FRACCIA

2. PRINCIPALI INDICAZIONI SULLA GESTIONE DOCUMENTALE

2.1 MODELLO ORGANIZZATIVO

AREA ORGANIZZATIVA OMOGENEA

L'art. 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445 stabilisce che "*Ciascuna Amministrazione individua, nell'ambito del proprio ordinamento, gli uffici da considerare ai fini della gestione unica o coordinata dei documenti per grandi aree organizzative omogenee, assicurando criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna tra le aree stesse*".

L'Istituzione scolastica individua al proprio interno un'unica Area Organizzativa Omogenea (AOO), alla quale corrisponde un Registro unico di protocollo. Si rappresenta che esistono fattispecie peculiari quali, a titolo esemplificativo, gli Istituti Agrari con annessa Azienda Agricola, in cui si identificano due Aree Organizzative Omogenee differenti.

L'AOO può essere sotto-articolata in Unità Organizzative Responsabili (UOR), ovvero l'insieme di uffici che, per tipologia di mandato istituzionale e di competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato.

RUOLI E RESPONSABILITÀ

L'Istituzione scolastica, allo scopo di assicurare un trattamento uniforme dei documenti, una puntuale applicazione delle disposizioni ed un periodico monitoraggio delle modalità d'uso degli strumenti di gestione documentale, deve prendere al suo interno le seguenti figure:

- il **Responsabile della gestione documentale** ed il suo vicario, soggetti in possesso di idonei requisiti professionali o di professionalità tecnico-archivistica, preposti al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'art. 61 del D.P.R. 28 dicembre 2000, n. 445, che producono il pacchetto di versamento ed effettuano il trasferimento del suo contenuto nel sistema di conservazione[2];
- il **Responsabile della conservazione**, soggetto in possesso di idonee competenze giuridiche, informatiche ed archivistiche, che opera secondo quanto previsto dall'art. 44, comma 1-quater, del D.Lgs. 82/2005;
- il **Responsabile per la prevenzione della corruzione e della trasparenza**, al quale può essere presentata l'istanza di accesso civico, qualora la stessa abbia ad oggetto dati, informazioni o documenti oggetto di pubblicazione obbligatoria ai sensi del D.Lgs. 33/2013;
- il **Responsabile della protezione dei dati**, ai sensi dell'art. 37 del Regolamento UE 679/2016, che ha il compito di sorvegliare sull'osservanza della normativa in materia di protezione dei dati personali.

Inoltre, in aggiunta alle figure sopra elencate, si evidenzia la rilevanza di individuare il **Referente per l'indice delle Pubbliche Amministrazioni** (iPA), soggetto a cui il Dirigente Scolastico affida il compito, sia organizzativo che operativo, di interagire con il gestore dell'iPA per l'inserimento e la modifica dei dati dell'Istituzione scolastica, nonché per ogni altra questione riguardante la presenza della stessa presso l'iPA.

[2] Si precisa che, anche nell'ipotesi in cui il Responsabile della gestione documentale venga individuato in una figura diversa dal Dirigente Scolastico, alcuni compiti e responsabilità restano in capo allo stesso Dirigente, nel rispetto delle previsioni contenute nell'art. 4, comma 2, e nell'art. 25 del D.Lgs. 165/2001.

Firmato digitalmente da ROBERTO FRACCIA

2.2 CICLO DI VITA DEL DOCUMENTO

Il ciclo di vita del documento è articolato nei processi di produzione, gestione e conservazione:

- il **processo di produzione** del documento si sostanzia principalmente nell'acquisizione di documenti cartacei, informatici e/o telematici ovvero nella creazione degli stessi;
- il **processo di gestione** interessa tutte le attività a partire dalla registrazione del documento, alla classificazione, assegnazione e fascicolazione/archiviazione corrente;
- il **processo di conservazione** si sostanzia nel trasferimento dei documenti dall'archivio corrente all'archivio di deposito (dal quale possono eventualmente seguire l'attività di scarto e di delocalizzazione) e dall'archivio di deposito all'archivio storico.

Il sistema di produzione e gestione dei documenti adottato, anche ai fini della conservazione, è descritto all'interno del **manuale di gestione documentale**. Il manuale, che costituisce un adempimento obbligatorio per tutte le Pubbliche Amministrazioni, viene redatto da ciascuna Istituzione scolastica dettagliando le specifiche istruzioni operative adottate dalla stessa. Esso costituisce una guida dal punto di vista operativo per tutti coloro che gestiscono documenti all'interno della scuola, in modo tale da facilitare un corretto svolgimento di tutte le attività inerenti al ciclo di vita del documento.

Al fine di uniformare la gestione documentale tra le Istituzioni scolastiche e, allo stesso tempo, garantire *compliance* normativa, il Ministero ha predisposto un ***format* di manuale** che ciascuna Istituzione scolastica può utilizzare come strumento per la redazione del manuale di gestione documentale, adattandolo rispetto alle proprie specifiche esigenze e peculiarità amministrative e gestionali.

Per ulteriori informazioni in merito al ***Format* di manuale per la gestione dei flussi documentali delle Istituzioni scolastiche**, si veda la sezione "*Strumenti a supporto*".

PROCESSO DI PRODUZIONE E GESTIONE

Il processo di produzione e gestione è suddiviso in "*Acquisizione documento*" e "*Creazione documento*", al fine di distinguere rispettivamente le attività relative ai documenti in entrata dalle attività relative ai documenti elaborati dall'Istituzione scolastica.

Processo di produzione e gestione - Acquisizione documento

Firmato digitalmente da ROBERTO FRACCIA

Nella fase di **acquisizione**, l'Istituzione scolastica riceve il documento e verifica la competenza dello stesso.

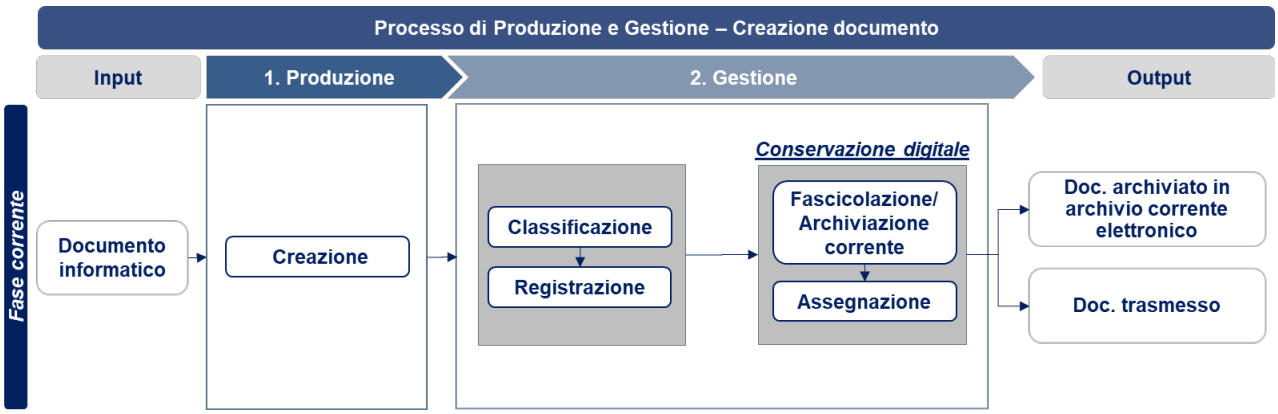
Se il documento è di competenza dell'Istituzione scolastica, l'operatore addetto alla protocollazione valuta se il documento è da protocollare e, in caso positivo, effettua tutte le attività funzionali alla registrazione di protocollo. In particolare, in seguito alla verifica della competenza del documento, provvede alla **classificazione** dello stesso sulla base del **titolario di classificazione**, previa verifica della presenza di categorie particolari di dati personali, di cui all'articolo 9 del Regolamento UE 679/2016. In seguito, procede ad effettuare la **registrazione** di protocollo per il documento in ingresso ed infine all'**assegnazione** del documento al personale competente.

Una volta che il documento è stato assegnato, segue la fase di **fascicolazione/archiviazione corrente**, in cui il documento viene inserito nel fascicolo di riferimento (nuovo o già esistente), all'interno dell'archivio corrente e secondo l'ordine cronologico di registrazione.

Le procedure da seguire per lo svolgimento di tutte le attività e i relativi *output* variano in base alla tipologia di documento acquisito (cartaceo o informatico), nonché alle specifiche modalità organizzative ed operative adottate dall'Istituzione scolastica (es. conservazione ibrida o conservazione sostitutiva).

Per ulteriori informazioni in merito al **Titolario di classificazione**, si veda la sezione "*Strumenti a supporto*".

Processo di produzione e gestione - Creazione documento



Nella fase di **creazione** si considera come *input* esclusivamente il documento di natura informatica. In tale fase, il documento viene elaborato, eventualmente revisionato ed infine approvato e sottoscritto dal responsabile. I documenti informatici prodotti, prima della loro sottoscrizione, sono convertiti in uno dei formati *standard* previsti dalla normativa vigente.

Il documento, una volta creato e perfezionato come descritto in precedenza, viene **classificato** sulla base del **titolario di classificazione** e protocollato, previa verifica della presenza di categorie particolari di dati personali, di cui all'articolo 9 del Regolamento UE 679/2016.

In seguito alla registrazione, segue la fase di **fascicolazione/archiviazione corrente**, in cui il documento viene inserito nel fascicolo di riferimento (nuovo o già esistente), all'interno dell'archivio corrente e secondo l'ordine cronologico di registrazione. Infine, il documento può essere oggetto di **assegnazione** o di pubblicazione.

Si precisa che l'archivio deve essere periodicamente sottoposto ad una selezione razionale. A tal fine si inserisce lo **sfoltimento**, attività eseguita nell'archivio corrente e propedeutica ad una corretta conservazione

Firmato digitalmente da ROBERTO FRACCIA

documentale, che consiste nella selezione ed estrazione dal fascicolo dell'eventuale carteggio di carattere transitorio e strumentale (ad es., appunti, promemoria).

PROCESSO DI CONSERVAZIONE

Il ciclo di gestione di un documento informatico termina con il suo versamento in un sistema di **conservazione** che è coerente con quanto disposto dal CAD e dalle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*".

In particolare, ai sensi dell'art. 34, comma 1-*bis* del CAD, come modificato dall'art. 25, comma 1, lett. e), del D.L. 76/2020 (c.d. "Decreto Semplificazione"), convertito con Legge n. 120/2020, le Pubbliche Amministrazioni possono procedere alla conservazione dei documenti informatici all'interno della propria struttura organizzativa, ovvero all'esterno, affidandola, in modo totale o parziale, nel rispetto della disciplina vigente, ad altri soggetti, pubblici o privati che possiedono i requisiti di qualità, di sicurezza e organizzazione individuati, nel rispetto della disciplina europea, nelle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" emanate da AgID[3].

La documentazione afferente a pratiche presenti nell'archivio corrente (ancora in fase di lavorazione) viene versata nell'archivio corrente del nuovo anno, mentre la documentazione relativa a pratiche per cui la lavorazione è stata conclusa viene versata nell'**archivio di deposito**, dove sono raccolti i documenti ancora utili per finalità amministrative o giuridiche, ma non più indispensabili per la trattazione delle attività correnti.

Nell'ambito dell'archivio di deposito avviene l'operazione di **scarto**, supportata dal **massimario di conservazione e scarto**, grazie al quale è prodotto annualmente l'elenco dei documenti per i quali è trascorso il periodo obbligatorio di conservazione e che, quindi, sono suscettibili di scarto archivistico.

La documentazione afferente a pratiche contenute nell'archivio di deposito da oltre 40 anni è soggetta al versamento nell'**archivio storico**, in cui vengono conservati i documenti storici di rilevanza storico-culturale, destinati alla conservazione permanente.

[3] L'AgID ha adottato con Determinazione n. 455/2021 il "*Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici*" e i relativi allegati. L'allegato A, in particolare, fissa i requisiti per l'erogazione del servizio di conservazione per conto delle Pubbliche Amministrazioni. Il regolamento prevede, inoltre, l'istituzione di un *marketplace* per i servizi di conservazione quale sezione autonoma del *Cloud Marketplace* cui possono iscriversi i soggetti, pubblici e privati, che intendono erogare il servizio di conservazione dei documenti informatici per conto delle Pubbliche Amministrazioni. L'iscrizione al *marketplace* non è obbligatoria ma i conservatori che intendono partecipare a procedure di affidamento da parte delle Pubbliche Amministrazioni devono ugualmente possedere i requisiti previsti nel suddetto regolamento e sono sottoposti all'attività di vigilanza di AgID.

Firmato digitalmente da ROBERTO FRACCIA

Dopo aver effettuato le operazioni di scarto e l'eventuale versamento nell'archivio storico, qualora risulti che l'archivio di deposito cartaceo è saturo, si procede con la fase di **delocalizzazione**, in cui si seleziona la documentazione da delocalizzare, selezionandola tra quella più prossima alla data di scarto, e, previa approvazione della Soprintendenza competente, si provvede ad inviare la stessa presso una struttura, se possibile interna, con sufficiente spazio negli archivi.

Per ulteriori informazioni in merito al **Massimario di conservazione e scarto**, si veda la sezione "*Strumenti a supporto*".

3. STRUMENTI A SUPPORTO

Le "***Linee guida sulla formazione, gestione e conservazione dei documenti informatici***", adottate con Determinazione AgID n. 407/2020 ed in seguito aggiornate con nuova Determinazione n. 371/2021, hanno l'obiettivo di aggiornare le regole tecniche in materia di formazione, protocollazione, gestione e conservazione del documento e, allo stesso tempo, incorporare in un'unica guida le regole tecniche e le circolari in materia. Le suddette Linee guida hanno introdotto elementi di novità nel quadro normativo di riferimento, che vanno nella direzione della **semplificazione** della gestione dei processi documentali e della **digitalizzazione** delle Pubbliche Amministrazioni.

Al fine di supportare le Istituzioni scolastiche nell'adeguamento alle evoluzioni del quadro normativo di riferimento, nonché di favorire una maggiore uniformità delle procedure operative in uso, il Ministero mette a disposizione delle scuole degli strumenti funzionali a presidiare l'intero processo della gestione documentale, che si descrivono di seguito.

3.1 *FORMAT* DI MANUALE PER LA GESTIONE DEI FLUSSI DOCUMENTALI DELLE ISTITUZIONI SCOLASTICHE

Il ***format* di manuale per la gestione dei flussi documentali delle Istituzioni scolastiche** (Allegato 1) rappresenta uno strumento di supporto alle Istituzioni scolastiche per la redazione del manuale di gestione documentale, che descrive il sistema di produzione e gestione dei documenti e contiene istruzioni di dettaglio per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Il *format* è articolato in capitoli che descrivono il modello organizzativo adottato dall'Istituzione scolastica per la gestione documentale e il processo di gestione del ciclo di vita del documento, dettagliandone alcuni aspetti specifici che risultano fondamentali per un adeguato svolgimento delle attività. Al fine di favorirne l'utilizzo da parte delle scuole, nonché di fornire alle stesse uno strumento operativo funzionale al presidio di tutto il processo, all'interno del *format* sono presenti **approfondimenti** specifici su tematiche particolarmente rilevanti per le Istituzioni scolastiche e ***focus*** sulle modalità di svolgimento di alcune **procedure operative**. Trattandosi di uno strumento che le scuole devono adattare rispetto alle loro caratteristiche, esigenze e necessità, nel *format* sono evidenziati in giallo specifici punti in cui l'Istituzione scolastica deve integrare il *format* con ulteriori informazioni ed in grigio specifici passaggi afferenti a procedure operative per le quali è facoltà della singola Istituzione scolastica definirne in maniera autonoma le modalità di attuazione.

Approfondimenti su tematiche rilevanti

Tra le tematiche particolarmente rilevanti da gestire per le Istituzioni scolastiche, si evidenziano le seguenti, che sono oggetto di approfondimento all'interno del *format*.

- **Firme elettroniche** (cfr. par. 4.6.1. "*Le firme elettroniche*"): vengono dettagliate le diverse tipologie di sottoscrizione elettronica previste dalla normativa vigente in materia, evidenziandone le differenze e l'efficacia probatoria del documento informatico su cui vengono apposte.

Firmato digitalmente da ROBERTO FRACCIA

- **Protocollo informatico** (cfr. cap. 5. "*Il protocollo informatico*"): vengono fornite specifiche indicazioni relative alla registrazione di protocollo e istruzioni operative per gestire le relative attività (es. protocollabilità di un documento, gestione degli allegati, scrittura dei dati di protocollo, informazioni minime della segnatura di protocollo, differimento della registrazione, rilascio della ricevuta di avvenuta protocollazione), nonché informazioni in merito alla gestione di avvenimenti particolari legati alla protocollazione (es. ricorso al registro di emergenza nel caso di interruzione o malfunzionamento del sistema di protocollo informatico, annullamento delle registrazioni di protocollo), o a fattispecie particolari di documenti (es. documentazione soggetta a registrazione particolare).

- **Gestione delle copie dei documenti** (cfr. par. 5.10. "*Modalità di svolgimento del processo di scansione*"): vengono fornite specifiche indicazioni in merito alle modalità di svolgimento del processo di scansione di documentazione cartacea, nonché in merito alle modalità di attestazione della conformità della copia per immagine su supporto informatico di un documento analogico.

- **Tutela dei dati personali e misure di sicurezza** (cfr. par. 6.1. "*Tutela dei dati personali e misure di sicurezza*"): vengono dettagliate le diverse iniziative che devono essere intraprese dall'Istituzione scolastica al fine di ottemperare a quanto previsto dalla normativa vigente in materia di protezione dei dati personali (Regolamento UE 679/2016) e, al tempo stesso, vengono fornite istruzioni in merito alle misure tecniche e organizzative necessarie al fine di garantire un livello di sicurezza adeguato del sistema di gestione informatica dei documenti al rischio in materia di protezione dei dati personali.

- **Diritto di accesso agli atti** (cfr. par. 6.2. "*Diritto di accesso agli atti*"): vengono approfondite le tematiche del diritto di accesso documentale e del diritto all'accesso civico generalizzato, dettagliando i soggetti coinvolti, le modalità di gestione delle richieste e la tipologia di documenti che possono essere visionati, anche alla luce del tema della *privacy*.

Focus su procedure operative

Nel *format* di manuale vengono fornite indicazioni in merito ad alcune procedure operative, fermo restando la possibilità per la singola scuola di definire autonomamente le modalità di attuazione in base alle specifiche esigenze e peculiarità in cui opera, a titolo esemplificativo:

- **Acquisizione di un documento:** sono state evidenziate le diverse modalità da attuare, differenziate sulla base delle scelte effettuate dalla singola Scuola in merito al modello organizzativo (accentrato / parzialmente accentrato) e alla modalità di conservazione (ibrida / sostitutiva) (cfr. par. 3.1.1. "*Processo di produzione e gestione - Acquisizione*").

- **Gestione di documenti pervenuti erroneamente all'Istituzione scolastica:** è stata definita una procedura *standard* che può essere adottata dalle Istituzioni scolastiche per la gestione di tale casistica (cfr. par. 3.1.1. "*Processo di produzione e gestione - Acquisizione*").

- **Gestione di documenti di cui non sia identificabile l'autore, ovvero pervenuti all'Istituzione scolastica privi di firma**: è stata definita una procedura *standard* che può essere adottata dalle Istituzioni scolastiche per la gestione di tale casistica (cfr. par. 4.1. "*Documento ricevuto*").

- **Utilizzo di formati di *file* specifici**: è stato suggerito alle Istituzioni scolastiche, sulla base di valutazioni di interoperabilità e tenuto conto dei requisiti di non alterabilità ed immutabilità dettati dalla normativa vigente, l'utilizzo dei formati PDF, XML e TIFF per la redazione dei documenti (cfr. par. 3.1.2. "*Processo di produzione e gestione - Creazione*").

- **Assegnazione del documento acquisito**: è stata suggerito alle Istituzioni scolastiche di prevedere la possibilità di revoca dell'assegnazione da parte del Responsabile di gestione documentale ovvero del suo vicario (cfr. par. 3.1.1. "*Processo di produzione e gestione - Acquisizione*").

Firmato digitalmente da ROBERTO FRACCIA

- **Creazione del documento**: è stata definita una procedura *standard* che può essere adottata dalle Istituzioni scolastiche per lo svolgimento delle attività attinenti alla fase di creazione del documento (cfr. par. 3.1.2. "*Processo di produzione e gestione - Creazione*").
- **Versamento in archivio di deposito**: sono state fornite alle Istituzioni scolastiche indicazioni di massima in merito a possibili tempistiche per effettuare l'operazione di verifica della presenza di pratiche chiuse nell'archivio corrente (cfr. par. 3.1.5. "*Processo di gestione - Archiviazione*").
- **Verifica della validità della firma digitale**: sono state fornite indicazioni in merito alla necessità di verificare la validità della firma digitale di un documento ricevuto tramite apposita funzione del sistema di protocollo, prima di procedere con la protocollazione (cfr. par. 4.6.1. "*Le firme elettroniche*").
- **Modalità di scrittura dei dati di protocollo**: sono state definite specifiche regole per la redazione dei dati nell'ambito del sistema di protocollo informatico, fermo restando la facoltà delle scuole di integrare le regole definite con ulteriori indicazioni (cfr. par. 5.2. "*Scrittura di dati di protocollo*").
- **Ricevuta di avvenuta protocollazione**: è stata definita una modalità *standard* che può essere adottata dalle Istituzioni scolastiche per effettuare tale attività (cfr. par. 5.5. "*Ricevuta di avvenuta protocollazione*").
- **Gestione del registro di emergenza**: è stata suggerita alle Istituzioni scolastiche l'adozione dei Moduli di Registrazione di Emergenza nel caso si renda necessario l'utilizzo del registro di emergenza a causa di interruzioni del funzionamento del sistema di protocollo informatico (cfr. par. 5.7. "*Registro di emergenza*").
- **Registri particolari**: è stata lasciata la facoltà alle Istituzioni scolastiche di decidere quali documenti sono soggetti a questo specifico regime, definendone al contempo le modalità di gestione (cfr. par. 5.8. "*Registri particolari*").
- **Annullamento delle registrazioni di protocollo**: è stata definita una procedura *standard* che può essere adottata dalle Istituzioni scolastiche per lo svolgimento di tale attività (cfr. par. 5.9. "*Annullamento delle registrazioni di protocollo*").

3.2 TITOLARIO UNICO DI CLASSIFICAZIONE PER LE ISTITUZIONI SCOLASTICHE

Il **titolario di classificazione delle Istituzioni scolastiche** (Allegato 2) supporta le Istituzioni scolastiche nella classificazione dei documenti, descrivendone l'organizzazione in settori e categorie e facilitandone dunque una schematizzazione logica.

Il titolario rappresenta uno strumento essenziale per la corretta formazione e gestione degli archivi delle scuole, nonché funzionale alla conservazione dei documenti, in quanto garantisce l'applicazione di procedure uniformi di registrazione e classificazione degli atti tra le Istituzioni scolastiche.

Il titolario è articolato su due livelli:

1. il primo livello (**Titolo**) definisce i titoli di classificazione dei documenti;
2. il secondo livello (**Classe**) elenca le specifiche classi incluse all'interno di ciascun titolo.

Per ulteriori informazioni in merito alle modalità di classificazione e aggregazione dei documenti, si veda l'Appendice "***Focus sulle aggregazioni documentali delle Istituzioni scolastiche***".

3.3 MASSIMARIO DI CONSERVAZIONE E SCARTO PER LE ISTITUZIONI SCOLASTICHE

Il **massimario di conservazione e scarto** (Allegato 3) supporta le Istituzioni scolastiche nello svolgimento delle operazioni di scarto. Esso descrive le informazioni relative ai tempi, ai criteri e alle regole per la

Firmato digitalmente da ROBERTO FRACCIA

conservazione, selezione e scarto della documentazione archiviata. In particolare, fornisce indicazioni riguardo ai documenti da conservare illimitatamente o che possono essere proposti per lo scarto dopo un periodo di tempo stabilito.

Il massimario è articolato su quattro livelli:

Per il IV livello "libero" è concesso alle Scuole di aggiungere delle voci su una struttura non predefinita.

3.4 Firma Elettronica Avanzata

Oltre agli strumenti sopra elencati, che vengono allegati alle presenti Linee guida, il Ministero dell'Istruzione mette a disposizione delle Istituzioni scolastiche **Sigillo**, un applicativo per l'apposizione della **Firma Elettronica Avanzata**, che rappresenta uno strumento fondamentale per consentire una transizione da un sistema di tipo analogico e cartaceo ad un sistema esclusivamente digitale e «*paperless*».

L'applicativo consente alle Istituzioni scolastiche di far sottoscrivere i propri documenti informatici, tramite Firma Elettronica Avanzata, a tutti i soggetti tenuti ad apporre la firma sugli stessi, senza la necessità di utilizzare un certificato di firma digitale emesso da una *Certification Authority*.

Sigillo rappresenta uno strumento sicuro e affidabile in quanto – oltre a garantire l'immodificabilità del documento dopo l'apposizione della firma – abbina indissolubilmente l'oggetto della sottoscrizione con il processo di autenticazione SPID e, dunque, con l'identità del firmatario.

Per ulteriori informazioni in merito alle modalità di funzionamento di tale applicativo, è possibile consultare il materiale di supporto (manuali utente e *video tutorial*) messo a disposizione delle Istituzioni scolastiche.

Firmato digitalmente da ROBERTO FRACCIA

APPENDICE

FOCUS SULLE AGGREGAZIONI DOCUMENTALI DELLE ISTITUZIONI SCOLASTICHE

L'obiettivo del presente *focus* è quello di fornire alle Istituzioni scolastiche un quadro unitario sulle modalità di inserimento dei documenti nelle aggregazioni documentali, nel perimetro dell'autonomia riconosciuta in tale ambito dal Testo Unico sulla Documentazione Amministrativa (D.P.R. 445/2000)[4].

A tal fine, il *focus* è strutturato come segue:

- **Assunzioni di partenza**, in cui si riportano le definizioni adottate per la presente trattazione di alcuni termini chiave nel contesto della classificazione e fascicolazione dei documenti;
- **Principi-guida di organizzazione delle aggregazioni documentali**, in cui si delineano dei "principi-guida" per l'organizzazione delle aggregazioni documentali quanto più rispondenti alle esigenze di funzionamento delle scuole. Ogni principio è corredato da un esempio concreto di applicazione.

Assunzioni di partenza

Documento: qualsiasi atto, in forma analogica o informatica, che fa parte dell'archivio di una Istituzione scolastica[5]. I documenti sono classificati sulla base del titolario e possono essere inseriti all'interno di aggregazioni documentali.

Titolario (anche conosciuto come piano di classificazione): struttura logica che permette di organizzare i documenti secondo uno schema desunto dalle funzioni e dalle attività della scuola[6]. Esso si articola su due livelli: titoli (indicati con numeri romani) e classi (indicati con numeri arabi).

Aggregazione documentale: insieme di documenti o insieme di fascicoli riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente[7]. Distinguiamo[8] tre tipi di aggregazioni documentali, di seguito descritte: i fascicoli, le serie documentali e le serie di fascicoli.

Fascicolo: aggregazione documentale strutturata e univocamente identificata[9]. Si possono costituire diverse tipologie di fascicoli[10] (per affare, per persona fisica o giuridica, per attività, per procedimento). I fascicoli sono aperti di norma al livello più basso del titolario di classificazione (nel caso delle scuole, quindi, nell'ambito di una delle classi, il secondo livello). Nel caso del fascicolo per persona fisica o giuridica il fascicolo può essere aperto anche al livello di titolo (primo livello), quindi esso potrà contenere documenti appartenenti a classi diverse[11].

Serie documentale: aggregazione di documenti con caratteristiche omogenee, raggruppati ad esempio in base alla tipologia documentaria (es. delibere, decreti, fatture) o alla provenienza (cioè se prodotti da un medesimo organo, come il Consiglio d'istituto o il Collegio dei docenti) o all'oggetto (es. documenti relativi ad un

[4] L'art. 64, comma 4, del TUDA stabilisce quanto segue: "*Le amministrazioni determinano autonomamente e in modo coordinato per le aree organizzative omogenee, le modalità di attribuzione dei documenti ai fascicoli che li contengono e ai relativi procedimenti, definendo adeguati piani di classificazione d'archivio per tutti i documenti, compresi quelli non soggetti a registrazione di protocollo.*"
[5] Definizione basata sul glossario dei termini archivistici della Direzione Generale Archivi del Ministero della Cultura.
[6] Definizione basata sull'Allegato 1 delle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*".
[7] Definizione basata sull'Allegato 1 delle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*".
[8] Tale distinzione delle aggregazioni documentali in tre diverse tipologie è basata sul paragrafo 4 dell'Allegato 5 delle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*".
[9] Definizione basata sull'Allegato 1 delle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*".
[10] Le tipologie di fascicoli identificate si basano sul paragrafo 4 dell'Allegato 5 delle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*".
[11] Per le indicazioni sulla classificazione dei fascicoli sulla base dei diversi livelli di titolario, ci si è basati sulla definizione di repertorio all'interno del glossario dei termini archivistici della Direzione Generale Archivi del Ministero della Cultura e sul Piano di classificazione per gli archivi dei Comuni.

Firmato digitalmente da ROBERTO FRACCIA

progetto PON)[12]. I documenti all'interno di una serie, non essendo aggregati utilizzando il titolario di classificazione come nel caso dei fascicoli, possono appartenere a titoli e classi differenti tra loro. La serie documentale stessa, quindi, non viene classificata, ma dev'essere comunque gestita dal sistema informatico, il cui *software* deve pertanto prevedere un'apposita funzione[13].

Serie di fascicoli: fascicoli accorpati per ragioni funzionali in base alla classe di riferimento (es. tutti i fascicoli aperti all'interno del titolo I classe 6 "Elezioni e nomine") o alla tipologia di fascicoli (es. tutti i fascicoli del personale)[14].

Principi-guida di organizzazione delle aggregazioni documentali

1. Classificazione dei documenti. Tutti i documenti gestiti dall'Istituzione scolastica devono essere classificati sulla base del titolario al momento della creazione o dell'acquisizione.

Esempio. La Scuola acquisisce una domanda di ferie da parte del docente Mario Rossi. Tale documento è classificato nel titolo VII "Personale", classe 4 "Assenze".

2. Classificazione dei fascicoli. I fascicoli sono tipicamente aperti al livello più basso del titolario di classificazione (in base al titolario, la classe o secondo livello). In alcuni casi, è possibile utilizzare anche il primo livello (titolo) come per i fascicoli di persona fisica.

Esempio A. (fascicolo al 1° livello)

Il fascicolo del docente Mario Rossi è aperto all'interno del titolo VII "Personale" (1° livello del titolario).

Esempio B. (fascicolo al 2° livello)

Il fascicolo delle azioni legali collettive del personale è aperto all'interno del titolo III "Attività giuridico-legale", classe 1 "Contenzioso" (2° livello del titolario).

3. Serie documentali (non classificate). Le serie documentali sono aggregazioni di documenti uguali per forma e/o provenienza, ma differenti per contenuto, ovvero incardinati in titoli diversi. Per tale motivo, le serie documentali non possono essere classificate in base alle partizioni del titolario.

Esempio A. *La serie documentale dei decreti del Dirigente Scolastico del 2021 contiene documenti con classificazione diversa sia per primo che secondo livello del titolario:*

- *Decreto di organizzazione degli uffici per il contenimento dell'epidemia da Covid-19 → classificato nel titolo VI "Finanzia e patrimonio", classe 9 "DVR e sicurezza"*
- *Decreto di costituzione del comitato per la valutazione dei docenti → classificato nel titolo I "Amministrazione", classe 6 "Elezioni e nomine"*

[12] Definizione basata sul paragrafo 4 dell'Allegato 5 delle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*".

[13] Per le indicazioni sulla (non) classificazione delle serie documentali, ci si è basati sull'approccio indicato nel Piano di classificazione per gli archivi dei Comuni con riferimento ai "repertori", che corrispondono a ciò che nella presente trattazione è chiamato "serie documentale". Si è scelto, infatti, di non impiegare il termine repertorio in quanto questo può generare ambiguità rispetto al concetto di repertorio di fascicoli.

[14] Definizione basata sul paragrafo 4 dell'Allegato 5 delle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*".

Firmato digitalmente da ROBERTO FRACCIA

***Esempio B**. La serie documentale di un progetto PON contiene documenti con classificazione diversa sia per primo che secondo livello del titolario.*

- *Descrizione del progetto e dei suoi obiettivi → classificato nel titolo IV "Didattica", classe 2 "Attività extra-curricolari";*
- *Contratto di incarico dell'esperto esterno → classificato nel titolo VII "Personale", classe 8 "Collaboratori esterni";*
- *Fattura per il pagamento dell'esperto esterno → classificato nel titolo VI "Finanzia e patrimonio", classe 2 "Uscite e piani di spesa".*

Ciascuno di questi documenti sarà ulteriormente inserito nel fascicolo di competenza, ad es. il contratto di incarico dell'esperto esterno sarà inserito nel fascicolo personale dell'esperto esterno.

4. Serie di fascicoli. Le serie di fascicoli possono essere utilizzate per aggregare fascicoli omogenei per oggetto o tipologia o comunque per ragioni funzionali all'organizzazione del lavoro.

Esempio. (serie di fascicoli del personale dipendente)

La Scuola può aggregare tutti i fascicoli del personale supplente per l'anno 2021 in una serie di fascicoli.

5. Associazione di documenti ad aggregazioni documentali. Un documento può essere associato a uno o più aggregazioni documentali in base alle esigenze di funzionamento dell'Istituzione scolastica.

Esempio A. (Inserimento documento in un fascicolo)

La scuola notifica al docente Mario Rossi una contestazione degli addebiti. Tale documento viene classificato all'interno del titolo VII "Personale", classe 6 "Obiettivi, incarichi, valutazione e disciplina". Inoltre, esso è inserito nel fascicolo personale di Mario Rossi (aperto nella classe VII "Personale").

Esempio B. (Inserimento documento in due fascicoli)

La scuola può inserire la domanda di ferie di Mario Rossi in due diversi fascicoli, entrambi necessariamente aperti all'interno del titolo VII "Personale", in cui il documento è classificato:

- *Nel fascicolo 2021-VII.0 "Mario Rossi", cioè il fascicolo del docente Mario Rossi, aperto nel 2021 all'interno del titolo VII "Personale";*
- *Nel fascicolo 2021-VII.4, cioè il fascicolo delle domande di ferie, aperto nel 2021 all'interno del titolo VII "Personale", classe 4 "Assenze".*

Esempio C. (Inserimento documento in un fascicolo e una serie documentale)

La scuola inserisce il verbale di approvazione del progetto extra-curricolare "Corso di teatro" in un fascicolo e in una serie documentale:

- *Nel **fascicolo** 2021-IV.2, cioè il fascicolo del progetto extra-curricolare "Corso di teatro", aperto nel 2021 all'interno del titolo IV "Didattica", classe 2 "Attività extra-curricolari";*
- *Nella **serie documentale** dei verbali di approvazione del progetto da parte del Consiglio d'istituto n. 15/2021, cioè la quindicesima serie documentale aperta nel 2021 dall'Istituzione scolastica.*

Firmato digitalmente da ROBERTO FRACCIA

ALLEGATI

ALLEGATO 1: *FORMAT* DI MANUALE PER LA GESTIONE DEI FLUSSI DOCUMENTALI DELLE ISTITUZIONI SCOLASTICHE

ALLEGATO 2: TITOLARIO UNICO DI CLASSIFICAZIONE PER LE ISTITUZIONI SCOLASTICHE

ALLEGATO 3: MASSIMARIO DI CONSERVAZIONE E SCARTO PER LE ISTITUZIONI SCOLASTICHE

Firmato digitalmente da ROBERTO FRACCIA

Ministero dell'Istruzione

Dipartimento per le risorse umane, finanziarie e strumentali
Direzione generale per i sistemi informativi e la statistica

Ministero della Cultura

Direzione Generale Archivi

Format di manuale per la gestione dei flussi documentali delle Istituzioni scolastiche

Firmato digitalmente da ROBERTO FRACCIA

Firmato digitalmente da ROBERTO FRACCIA

Firmato digitalmente da ROBERTO FRACCIA

PREMESSA

Le "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*", emanate dall'AgID, prevedono l'obbligo per le Pubbliche Amministrazioni di redigere con provvedimento formale e pubblicare sul proprio sito istituzionale il Manuale di gestione documentale.

Il presente Manuale di gestione documentale, adottato dall'Istituzione scolastica [*denominazione*] al fine di adeguarsi alle disposizioni di cui sopra, descrive il sistema di gestione dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Nel dettaglio, il Manuale descrive il modello organizzativo adottato dalla scuola per la gestione documentale e il processo di gestione del ciclo di vita del documento, oltre a fornire specifiche istruzioni in merito al documento amministrativo ed al documento informatico, al protocollo informatico e alle tematiche di accesso, trasparenza e *privacy*.

Il Manuale è destinato alla più ampia diffusione interna ed esterna, in quanto fornisce le istruzioni complete per eseguire correttamente le operazioni di formazione, registrazione, classificazione, fascicolazione e archiviazione dei documenti. Pertanto, il presente documento si rivolge non solo agli operatori di protocollo ma, in generale, a tutti i dipendenti e ai soggetti esterni che si relazionano con gli organi dell'Istituto.

GLOSSARIO

ACRONIMI

AgID	Agenzia per l'Italia Digitale
AOO	Area Organizzativa Omogenea
CAD	Codice dell'Amministrazione Digitale (D.Lgs. n. 82/2005 e ss.mm.ii.)
D.L.	Decreto-legge
D.Lgs.	Decreto Legislativo
DPCM	Decreto del Presidente del Consiglio dei Ministri
D.P.R.	Decreto del Presidente della Repubblica
DSGA	Direttore dei Servizi Generali e Amministrativi
GDPR	Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE
iPA	Indice delle Pubbliche Amministrazioni
PEC	Posta Elettronica Certificata
PEO	Posta Elettronica Ordinaria
RPD	Responsabile della protezione dei dati
RPCT	Responsabile per la prevenzione della corruzione e della trasparenza
RUP	Responsabile unico del procedimento
UOR	Unità Organizzativa Responsabile

Firmato digitalmente da ROBERTO FRACCIA

1. IL MANUALE DI GESTIONE DOCUMENTALE

Il presente manuale descrive il sistema di produzione e gestione dei documenti, anche ai fini della conservazione.

In coerenza con il quadro normativo di riferimento, il manuale è volto a disciplinare le attività di creazione, acquisizione, registrazione, classificazione, assegnazione, fascicolazione e archiviazione dei documenti informatici, oltre che la gestione dei flussi documentali e archivistici dell'Istituzione scolastica, nonché, seppur in via residuale, la gestione dei documenti non informatici. Tali attività sono finalizzate alla corretta identificazione e reperibilità dei documenti acquisiti e creati dalla scuola nell'ambito dell'esercizio delle proprie funzioni amministrative.

Il manuale, dunque, costituisce una guida dal punto di vista operativo per tutti coloro che gestiscono documenti all'interno dell'Istituzione scolastica, in modo tale da facilitare un corretto svolgimento delle operazioni di gestione documentale.

1.1 MODALITÀ DI APPROVAZIONE E AGGIORNAMENTO

Il Responsabile della gestione documentale[1] si occupa della predisposizione del manuale, che è adottato con provvedimento dal Dirigente Scolastico.

Il manuale deve essere aggiornato periodicamente effettuando il censimento delle attività/prassi in essere, la razionalizzazione delle stesse, l'individuazione e la definizione degli aspetti organizzativi e gestionali in termini di fasi, tempi e risorse umane impegnate nell'automazione dei flussi documentali nel rispetto della normativa.

Ogni evento suscettibile di incidere sull'operatività ed efficacia del manuale medesimo deve essere tempestivamente segnalato al Responsabile della gestione documentale, al fine di prendere gli opportuni provvedimenti in ordine all'eventuale modifica e/o integrazione della procedura stessa.

1.2 FORME DI PUBBLICITÀ E DIVULGAZIONE

In coerenza con quanto previsto nelle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*"[2] (a seguire, anche "Linee Guida"), adottate dall'AgID con Determinazione n. 407/2020 ed in seguito aggiornate con Determinazione n. 371/2021 (da attuare entro il 1° gennaio 2022), ovvero che il manuale sia reso pubblico mediante la pubblicazione sul sito istituzionale in una parte chiaramente identificabile dell'area "Amministrazione trasparente", prevista dall'art. 9 del D.Lgs. 33/2013,[3] il presente manuale è reso disponibile alla consultazione del pubblico mediante la diffusione sul sito istituzionale dell'Istituzione scolastica.

[1] Per ulteriori dettagli in merito a tale figura, si veda il par. "2.2. - Ruoli e responsabilità".
[2] Si ricorda che le Linee Guida AgID hanno carattere vincolante, come precisato dal Consiglio di Stato - nell'ambito del parere reso sullo schema di decreto legislativo del correttivo al D.Lgs. 82/2005 n. 2122/2017 del 10.10.2017. Ne deriva che, nella gerarchia delle fonti, anche le presenti Linee Guida sono inquadrate come un atto di regolamentazione, seppur di natura tecnica, con la conseguenza che esse sono pienamente azionabili davanti al giudice amministrativo in caso di violazione delle prescrizioni ivi contenute. Nelle ipotesi in cui la violazione sia posta in essere da parte dei soggetti di cui all'art. 2, comma 2, del citato D.Lgs. 82/2005, è altresì possibile presentare apposita segnalazione al difensore civico, ai sensi dell'art. 17 del medesimo Codice.
[3] L'art. 9, comma 1, del D.lgs. 33/2013, prevede che: "*Ai fini della piena accessibilità delle informazioni pubblicate, nella home page dei siti istituzionali è collocata un'apposita sezione denominata «Amministrazione trasparente», al cui interno sono contenuti i dati, le informazioni e i documenti pubblicati ai sensi della normativa vigente. Al fine di evitare eventuali duplicazioni, la suddetta pubblicazione può essere sostituita da un collegamento ipertestuale alla sezione del sito in cui sono presenti i relativi dati, informazioni o documenti, assicurando la qualità delle informazioni di cui all'articolo 6. Le amministrazioni non possono disporre filtri e altre soluzioni tecniche atte ad impedire ai motori di ricerca web di indicizzare ed effettuare ricerche all'interno della sezione «Amministrazione trasparente»*".

Firmato digitalmente da ROBERTO FRACCIA

2. IL MODELLO ORGANIZZATIVO

2.1. AREA ORGANIZZATIVA OMOGENEA

L'art. 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445 "*Testo unico delle disposizioni legislative e regolamentari in materia di regolamentazione amministrativa*" stabilisce che "*Ciascuna Amministrazione individua, nell'ambito del proprio ordinamento, gli uffici da considerare ai fini della gestione unica o coordinata dei documenti per grandi aree organizzative omogenee, assicurando criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna tra le aree stesse*".

L'Istituzione scolastica individua al proprio interno un'unica Area Organizzativa Omogenea (AOO), alla quale corrisponde un Registro unico di protocollo, denominato [*denominazione registro*].

L'AOO può essere sotto-articolata in Unità Organizzative Responsabili (UOR), ovvero l'insieme di uffici che, per tipologia di mandato istituzionale e di competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato.

L'articolazione delle UOR è riportata all'Allegato [*numero allegato*].

L'allegato di cui sopra è suscettibile di modifiche. L'inserimento/cancellazione/aggiornamento delle UOR deve essere formalizzato con provvedimento a firma del Responsabile della gestione documentale e recepito nel presente manuale.

2.2. RUOLI E RESPONSABILITÀ

L'Istituzione scolastica, allo scopo di assicurare un trattamento uniforme dei documenti, una puntuale applicazione delle disposizioni ed un periodico monitoraggio delle modalità d'uso degli strumenti di gestione documentale, deve prevedere al suo interno le seguenti figure:

- il **Responsabile della gestione documentale** ed il suo vicario[4];
- il **Responsabile della conservazione**;
- il **Responsabile per la prevenzione della corruzione e della trasparenza**;
- il **Responsabile della protezione dei dati**, ai sensi dell'art. 37 del Regolamento UE 679/2016.

Inoltre, in aggiunta alle figure sopra elencate, si evidenzia la rilevanza di individuare il **Referente per l'indice delle Pubbliche Amministrazioni** (iPA), soggetto a cui il Dirigente Scolastico affida il compito, sia organizzativo che operativo, di interagire con il gestore dell'iPA per l'inserimento e la modifica dei dati dell'Istituzione scolastica, nonché per ogni altra questione riguardante la presenza della stessa presso l'iPA[5].

Il **Responsabile della gestione documentale** è il soggetto in possesso di idonei requisiti professionali o di professionalità tecnico-archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'art. 61 del D.P.R. 28 dicembre 2000, n. 445, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione.

[4] Come definito nelle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" emanate dall'AgID "*Le Pubbliche Amministrazioni, nell'ambito del proprio ordinamento, provvedono a: […] nominare, in ciascuna delle AOO, il responsabile della gestione documentale e un suo vicario, in possesso di idonee competenze giuridiche, informatiche ed archivistiche*".
[5] Le *"Linee Guida dell'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi* (IPA)", adottate dall'AgID, al paragrafo 2.2, stabiliscono che "*Il Responsabile dell'Ente nell'istanza di accreditamento nomina un Referente IPA che ha il compito di interagire con il Gestore IPA per l'inserimento e la modifica dei dati, nonché per ogni altra questione riguardante la presenza dell'Ente nell'IPA*".

Firmato digitalmente da ROBERTO FRACCIA

Tenuto conto di quanto sopra, il Responsabile della gestione documentale è individuato, all'interno dell'Istituzione scolastica, nella persona del [*tipologia di soggetto (es. Dirigente Scolastico)*][6].

Il Responsabile della gestione documentale ed il suo vicario sono nominati con apposito provvedimento del Dirigente Scolastico.

Il **Responsabile della conservazione** è il soggetto in possesso di idonee competenze giuridiche, informatiche ed archivistiche, che opera secondo quanto previsto dall'art. 44, comma 1-*quater*, del D.Lgs. 82/2005 (di seguito anche "CAD")[7].

In particolare, il Responsabile della conservazione:

a) definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli *standard* internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;
b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
c) genera e sottoscrive il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
d) genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
f) effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;
g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità, adotta analoghe misure con riguardo all'obsolescenza dei formati;
h) provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
i) predispone le misure necessarie per la sicurezza fisica e logica del sistema di conservazione;
j) assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
l) provvede per le amministrazioni statali centrali e periferiche a versare i documenti informatici, le aggregazioni informatiche e gli archivi informatici, nonché gli strumenti che ne garantiscono la

[6] Si precisa che, anche nell'ipotesi in cui il Responsabile della gestione documentale venga individuato in una figura diversa dal Dirigente Scolastico, alcuni compiti e responsabilità restano in capo allo stesso Dirigente, nel rispetto delle previsioni contenute nell'art. 4, comma 2, e nell'art. 25 del D.Lgs. 165/2001.
[7] L'art. 44, comma 1-*quater*, del CAD prevede che: "*Il responsabile della conservazione, che opera d'intesa con il responsabile della sicurezza e con il responsabile dei sistemi informativi, può affidare, ai sensi dell'articolo 34, comma 1-bis, lettera b), la conservazione dei documenti informatici ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative, e tecnologiche e di protezione dei dati personali. Il responsabile della conservazione della pubblica amministrazione, che opera d'intesa, oltre che con i responsabili di cui al comma 1-bis, anche con il responsabile della gestione documentale, effettua la conservazione dei documenti informatici secondo quanto previsto all'articolo 34, comma 1-bis*".

Firmato digitalmente da ROBERTO FRACCIA

consultazione, rispettivamente all'Archivio centrale dello Stato e agli archivi di Stato territorialmente competenti, secondo le tempistiche fissate dall'art. 41, comma 1, del Codice dei beni culturali[8];

m) predispone il manuale di conservazione e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Nel caso in cui il servizio di conservazione venga affidato ad un conservatore, le attività suddette o alcune di esse, ad esclusione della lettera m), potranno essere affidate al responsabile del servizio di conservazione, rimanendo in ogni caso inteso che la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile, rimane in capo al Responsabile della conservazione, chiamato altresì a svolgere le necessarie attività di verifica e controllo in ossequio alle norme vigenti sui servizi affidati in *outsourcing* dalle Pubbliche Amministrazioni.

Il ruolo del Responsabile della conservazione può essere svolto dal Responsabile della gestione documentale o anche da altre figure. Tenuto conto di quanto sopra, il Responsabile della conservazione è individuato, all'interno dell'Istituzione scolastica, nella persona del [*tipologia di soggetto (es. Dirigente Scolastico)*].

Il Responsabile della conservazione è nominato con apposito decreto del Dirigente Scolastico.

Il **Responsabile per la prevenzione della corruzione e della trasparenza** (RPCT) è il soggetto al quale può essere presentata l'istanza di accesso civico, qualora la stessa abbia ad oggetto dati, informazioni o documenti oggetto di pubblicazione obbligatoria ai sensi del D.Lgs. 33/2013[9].

Il RPCT, oltre a segnalare i casi di inadempimento o di adempimento parziale degli obblighi in materia di pubblicazione previsti dalla normativa vigente, si occupa delle richieste di riesame dei richiedenti ai quali sia stato negato totalmente o parzialmente l'accesso civico generalizzato, ovvero che non abbiano avuto alcuna risposta entro il termine stabilito (si veda, per maggiori dettagli quanto specificato nel paragrafo 6.2.2).

Il **Responsabile della protezione dei dati** (RPD) è il soggetto nominato con apposito decreto del Dirigente Scolastico, che ha il compito di sorvegliare sull'osservanza della normativa in materia di protezione dei dati personali, ossia il Regolamento UE 679/2016 (di seguito, anche "GDPR") e il D.Lgs. 196/2003 (di seguito, anche "Codice *privacy*") come modificato dal D.Lgs. 101/2018.

Il Responsabile della protezione dei dati deve essere coinvolto in tutte le questioni che riguardano la gestione e la protezione dei dati personali e ha il compito sia di informare e sensibilizzare il personale della scuola riguardo agli obblighi derivanti dalla citata normativa sia di collaborare con il Titolare e il Responsabile del trattamento, laddove necessario, nello svolgimento della valutazione di impatto sulla protezione dei dati[10].

[8] L'art. 41, comma 1, del Codice dei beni culturali prevede che: "*Gli organi giudiziari e amministrativi dello Stato versano all'archivio centrale dello Stato e agli archivi di Stato i documenti relativi agli affari esauriti da oltre trent'anni, unitamente agli strumenti che ne garantiscono la consultazione. Le liste di leva e di estrazione sono versate settant'anni dopo l'anno di nascita della classe cui si riferiscono. Gli archivi notarili versano gli atti notarili ricevuti dai notai che cessarono l'esercizio professionale anteriormente all'ultimo centennio*".

[9] Art. 5, comma 3, lett. d), D.Lgs. 33/2013.

[10] La figura del Responsabile della protezione dei dati è disciplinata dal Considerando n. 97 e dagli artt. 37 – 39 del Regolamento UE 679/2016, nonché dalle Linee guida sui responsabili della protezione dei dati, già richiamate nel testo (*http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5930287*). Tale figura ha il compito di: valutare i rischi di ogni trattamento; collaborare con il Titolare/Responsabile del trattamento, laddove necessario, nel condurre una valutazione di impatto sulla protezione dei dati; informare e sensibilizzare il Titolare o il Responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal Regolamento e da altre disposizioni in materia di protezione dei dati; cooperare con il Garante e fungere da punto di contatto per il Garante su ogni questione connessa al trattamento; supportare il Titolare o il Responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un registro delle attività di trattamento. Il Responsabile della protezione dei dati è individuato tra i soggetti in possesso di specifici requisiti, competenze professionali e conoscenze specialistiche in materia di protezione dei dati, in linea con le funzioni che è chiamato a svolgere e che deve poter adempiere in piena indipendenza e in assenza di conflitti di interesse.

Firmato digitalmente da ROBERTO FRACCIA

Sul punto, le "*Linee Guida sui responsabili della protezione dei dati*", adottate dal WP29 il 13 dicembre 2016, emendate in data 5 aprile 2017, precisano che "*Assicurare il tempestivo e immediato coinvolgimento del RPD, tramite la sua informazione e consultazione fin dalle fasi iniziali, faciliterà l'osservanza del RGPD e promuoverà l'applicazione del principio di privacy (e protezione dati) fin dalla fase di progettazione; pertanto, questo dovrebbe rappresentare l'approccio standard all'interno della struttura del titolare/responsabile del trattamento. Inoltre, è importante che il RPD sia annoverato fra gli interlocutori all'interno della struttura suddetta, e che partecipi ai gruppi di lavoro che volta per volta si occupano delle attività di trattamento*".

Per ciò che concerne le modalità attraverso le quali il Responsabile della protezione dei dati si interfaccia con il Responsabile della gestione documentale e con il Responsabile della conservazione in merito all'adozione delle misure di sicurezza del sistema di gestione informatica dei documenti, si rimanda a quanto descritto nel dettaglio al paragrafo 6.1.

2.3. MODELLO ORGANIZZATIVO ADOTTATO

[Nel caso di adozione di un sistema accentrato]

Il sistema di protocollazione è unico per l'Istituzione scolastica e viene adottato un sistema "accentrato", per cui tutte le comunicazioni sono gestite, sia in ingresso che in uscita, da un'unica UOR che si occupa della loro protocollazione. In dettaglio:

- le **comunicazioni in ingresso**, indipendentemente dalla tipologia di comunicazione (via PEC, PEO o formato cartaceo) giungono presso il punto unico di accesso, dove vengono registrate a protocollo e smistate nelle diverse UOR a seconda della competenza;
- le **comunicazioni in uscita** sono trasmesse ad un'unica UOR, che si occupa della loro protocollazione e del loro invio.

[Nel caso di adozione di un sistema parzialmente accentrato]

Il sistema di protocollazione adottato dall'Istituzione scolastica è "parzialmente accentrato", per cui tutte le comunicazioni giungono al punto unico di accesso mentre possono essere trasmesse in uscita da tutte le UOR. In dettaglio:

- le **comunicazioni in ingresso**, indipendentemente dalla tipologia di comunicazione (via PEC, PEO o formato cartaceo) giungono presso il punto unico di accesso, dove vengono registrate a protocollo e smistate nelle diverse UOR a seconda della competenza;
- le **comunicazioni in uscita** sono trasmesse in uscita dalle singole UOR.

Le UOR e i soggetti abilitati per la ricezione, l'assegnazione, la consultazione, la protocollazione, la classificazione e l'archiviazione dei documenti sono individuati dal Responsabile della gestione documentale mediante atti organizzativi interni.

2.4. CASELLE DI POSTA ELETTRONICA

L'Istituzione scolastica è dotata di una casella di Posta Elettronica Certificata (PEC) istituzionale per la gestione del servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi. L'indirizzo PEC deve essere pubblicato sull'indice delle Pubbliche Amministrazioni.

La casella di cui sopra costituisce l'indirizzo virtuale della sede legale dell'AOO. Inoltre, l'Istituzione scolastica si avvale delle seguenti caselle PEC "di servizio" opportunamente autorizzate ed attivate, per le quali si descrivono i termini e le modalità d'uso: [*termini e modalità d'uso*]. *[A titolo esemplificativo, l'Istituzione scolastica può istituire una casella PEC per la gestione delle comunicazioni con il Dirigente relativamente a documenti soggetti a protocollo riservato]*.

Firmato digitalmente da ROBERTO FRACCIA

L'Istituzione scolastica è dotata anche di una casella di Posta Elettronica Ordinaria (PEO) istituzionale, utile a gestire i messaggi di posta elettronica con annessi documenti ed eventuali allegati, aventi rilevanza amministrativa.

Inoltre, l'Istituzione scolastica si avvale di caselle di Posta Elettronica Ordinaria interne ("di servizio") da affidare alla gestione di una UOR o del singolo operatore[11].

Le disposizioni vincolanti inerenti ai termini e modalità d'uso delle PEC e delle PEO sono pubblicati sul sito istituzionale dell'Istituzione scolastica.

3. IL CICLO DI VITA DEL DOCUMENTO

Il ciclo di vita del documento è articolato nei processi di produzione, gestione e conservazione:

- il **processo di produzione** del documento si sostanzia principalmente nell'acquisizione di documenti cartacei, informatici e/o telematici ovvero nella creazione degli stessi;
- il **processo di gestione** interessa tutte le attività a partire dalla registrazione del documento, alla classificazione, assegnazione e fascicolazione/archiviazione corrente;
- il **processo di conservazione** si sostanzia nel trasferimento dei documenti dall'archivio corrente all'archivio di deposito (dal quale possono eventualmente seguire l'attività di scarto e di delocalizzazione) e dall'archivio di deposito all'archivio storico.

Nei paragrafi successivi si riporta una panoramica dei processi suddivisi per:

- processo di produzione e gestione;
- processo di conservazione.

3.1. PROCESSO DI PRODUZIONE E GESTIONE

Il processo di produzione e gestione fornisce una sintesi delle attività da porre in essere con riferimento sia alla produzione del documento, sia alle fasi di gestione dello stesso. Il processo di produzione è suddiviso in "Processo di produzione - Acquisizione" e "Processo di produzione - Creazione", al fine di distinguere rispettivamente le attività relative ai documenti in entrata dalle attività relative ai documenti elaborati dall'Istituzione scolastica.

Con riferimento alla gestione del documento, si fornisce un dettaglio delle seguenti fasi: classificazione, fascicolazione, archiviazione.

[11] Ai sensi della Direttiva 27 novembre 2003 del Ministro per l'innovazione e le tecnologie, "*Appare, perciò, necessario che le pubbliche amministrazioni provvedano a dotare tutti i dipendenti di una casella di posta elettronica (anche quelli per i quali non sia prevista la dotazione di un personal computer) e ad attivare, inoltre, apposite caselle istituzionali affidate alla responsabilità delle strutture di competenza.*"

Firmato digitalmente da ROBERTO FRACCIA

3.1.1. PROCESSO DI PRODUZIONE E GESTIONE - ACQUISIZIONE

Il "Processo di produzione e gestione – Acquisizione" è descritto differenziando il caso in cui l'*input* sia un documento cartaceo dal caso in cui sia informatico, dato che i documenti provenienti dall'esterno possono essere di natura cartacea o di natura informatica.

Nel caso di **documento cartaceo in ingresso**, nella fase di acquisizione, l'Istituzione scolastica ricevente:

- rilascia una ricevuta timbrata, qualora il documento dovesse essere consegnato a mano[12];
- verifica la competenza del documento stesso.

Nel caso di documenti pervenuti erroneamente all'Istituzione scolastica ma indirizzati ad altri soggetti, il documento:

- si restituisce per posta;

oppure

- se la busta che lo contiene viene aperta per errore, è protocollato in entrata e in uscita, inserendo nel campo oggetto e nel campo di classificazione la nota "Documento pervenuto per errore", ed è rinviato al mittente apponendo sulla busta la dicitura "Pervenuta ed aperta per errore".

Se il documento è di competenza dell'Istituzione scolastica ricevente, segue la fase di registrazione in cui l'operatore addetto alla protocollazione:

- valuta se il documento è da protocollare (cfr. par. "4.8. - Protocollabilità di un documento");
- nel caso in cui il documento sia da protocollare procede alla scansione e alla successiva verifica di conformità all'originale della copia informatica (cfr. par. "5.10. - Modalità di svolgimento del processo di scansione");
- verifica la presenza di categorie particolari di dati personali, di cui all'articolo 9 del Regolamento UE 679/2016, ai fini dell'attuazione delle misure di sicurezza previste al paragrafo 6.1;
- provvede alla classificazione del documento sulla base del titolario di classificazione;
- provvede alla protocollazione in ingresso del documento;
- appone il timbro contenente i dati contenuti nella segnatura di protocollo tramite l'apposita funzionalità del servizio di protocollo informatico ovvero, solo in caso di impossibilità, procede manualmente.

Nella fase di assegnazione, l'operatore addetto alla protocollazione provvede all'assegnazione del documento al personale competente secondo le seguenti modalità e regole di assegnazione [*modalità e regole di assegnazione*]. Il Responsabile della gestione documentale, ovvero il vicario, può, in ogni caso, rettificare l'assegnatario del documento.

Successivamente alle fasi di registrazione, classificazione e assegnazione, è necessario procedere con la fase di fascicolazione/archiviazione del documento.

[Nel caso di conservazione ibrida]

Per i documenti cartacei, si provvede alla conservazione ibrida, in cui è prevista la conservazione sia del documento analogico originale sia della copia informatica. Pertanto, il Responsabile della gestione:

[12] Il servizio protocollo non rilascia, di regola, ricevute per i documenti che non sono soggetti a regolare protocollazione. La semplice apposizione del timbro datario sulla copia non ha alcun valore giuridico e non comporta alcuna responsabilità del personale amministrativo della scuola in merito alla ricezione ed all'assegnazione del documento.

Firmato digitalmente da ROBERTO FRACCIA

- inserisce il documento cartaceo in un nuovo fascicolo o in un fascicolo già esistente all'interno dell'archivio corrente cartaceo;
- inserisce il documento informatico in un nuovo fascicolo o in un fascicolo già esistente all'interno dell'archivio corrente elettronico.

[Nel caso di conservazione sostitutiva]

Per i documenti cartacei, si provvede alla conservazione sostitutiva, con la quale è garantita nel tempo la validità legale di un documento informatico, inteso come una rappresentazione di atti o fatti e dati su un supporto sia esso analogico o informatico. Pertanto, il Responsabile della gestione:

- attesta la conformità del documento informatico al documento cartaceo, ai sensi dell'art. 22, comma 2, del CAD;
- può distruggere il documento cartaceo;
- inserisce il documento informatico in un nuovo fascicolo o in un fascicolo già esistente all'interno dell'archivio corrente elettronico.

Si precisa che non possono essere distrutti i documenti elencati dal DPCM 21 marzo 2013[13], per i quali rimane l'obbligo della conservazione del cartaceo anche nel caso di conservazione sostitutiva.

[In entrambi i casi (conservazione ibrida e conservazione sostitutiva)]

Per tali attività, il Responsabile della gestione può disporre apposita delega all'assegnatario o ad altro personale appositamente individuato.

Di seguito si fornisce la rappresentazione grafica del processo sopra descritto.

[13] L'Allegato al DPCM 21 marzo 2013 avente ad oggetto "*Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni*", riporta tra i documenti analogici originali unici per i quali permane l'obbligo della conservazione dell'originale cartaceo, i seguenti:
a) atti contenuti nella Raccolta ufficiale degli atti normativi della Repubblica;
b) atti giudiziari, processuali e di polizia giudiziaria per i venti anni successivi;
c) opere d'arte;
d) documenti di valore storico – artistico, ivi compresi quelli in possesso delle forze armate;
e) documenti, ivi compresi quelli storico – demaniali, conservati negli archivi, nelle biblioteche e nelle discoteche di Stato, ivi compresi gli atti e documenti conservati nella biblioteca storica dell'ex Centro Studi Esperienze della Direzione Centrale per la prevenzione e la Sicurezza Tecnica del Dipartimento dei V.V.F., de soccorso pubblico e della difesa civile;
f) atti notarili;
g) atti conservati dai notai ai sensi della legge 16 febbraio 1913, n. 89, prima della loro consegna agli Archivi notarili;
h) atti conservati presso gli Archivi notarili.

Firmato digitalmente da ROBERTO FRACCIA

Nel caso di **documento informatico in ingresso**, nella fase di acquisizione, l'Istituzione scolastica ricevente verifica la competenza del documento.

Nel caso di documenti pervenuti erroneamente sulla casella PEC o PEO dell'Istituzione scolastica, l'operatore di protocollo rispedisce il messaggio al mittente con la dicitura "Messaggio pervenuto per errore – non di competenza di questa Amministrazione". Inoltre, se il documento è stato erroneamente protocollato, l'addetto al protocollo provvede ad annullare la registrazione, secondo le modalità descritte nel presente manuale, oppure a protocollare il documento in uscita indicando come oggetto "Protocollato per errore".

Se il documento è di competenza dell'Istituzione scolastica ricevente, segue la fase di registrazione in cui l'operatore addetto al protocollo:

- valuta se il documento è da protocollare (cfr. par. "4.8. - Protocollabilità di un documento");
- nel caso in cui il documento sia da protocollare procede alla verifica di validità della firma (se presente)[14];
- verifica la presenza di categorie particolari di dati personali, di cui all'articolo 9 del Regolamento UE 679/2016, ai fini dell'attuazione delle misure di sicurezza di cui al paragrafo 6.1;
- provvede alla classificazione del documento sulla base del titolario di classificazione[15];
- provvede alla protocollazione in ingresso.

Nella fase di assegnazione l'operatore addetto al protocollo provvede ad assegnare il documento al personale competente. Il Responsabile della gestione documentale può, in ogni caso, rettificare l'assegnatario del documento.

Qualora l'ordinamento giuridico preveda, per particolari categorie di documenti elettronici, degli obblighi relativamente all'uso di formati di file specifici ovvero di vincoli aggiuntivi su formati generici, le Istituzioni scolastiche, assolvendo tali obblighi, accettano i suddetti documenti elettronici solo se prodotti nei formati o con i vincoli aggiuntivi obbligatori.

Con la conservazione digitale si esegue la fase di fascicolazione/archiviazione corrente in cui gli utenti opportunamente abilitati provvedono all'inserimento del documento informatico o in un nuovo fascicolo o in un fascicolo già esistente all'interno dell'archivio corrente elettronico.

Di seguito si fornisce la rappresentazione grafica del processo sopra descritto.

3.1.2. PROCESSO DI PRODUZIONE E GESTIONE - CREAZIONE

Nel "Processo di produzione e gestione – Creazione", si considera come *input* del processo esclusivamente il documento di natura informatica (cfr. par. "4.6. - Documento informatico").

[14] Per ulteriori approfondimenti, si veda il cap. "4. - Il documento amministrativo".
[15] Nel caso di dubbi in merito alla voce del titolario da attribuire al documento, l'operatore addetto al protocollo si confronta con il Responsabile della gestione documentale in merito alla corretta classificazione.

Firmato digitalmente da ROBERTO FRACCIA

Nella fase di creazione, il documento:

- è elaborato dal personale competente ed inviato al Dirigente o altro personale responsabile (ad es. DSGA) per la revisione dello stesso, ovvero è elaborato dal Dirigente stesso;
- è successivamente approvato o dal Dirigente o da altro personale responsabile in base alla competenza.

Nella fase di elaborazione e revisione, è possibile fare circolare il documento tra i soggetti interessati registrandolo come "bozza".

I documenti informatici prodotti, indipendentemente dal *software* utilizzato per la loro creazione, prima della loro sottoscrizione con firma digitale, sono convertiti in uno dei formati *standard* previsti dalla normativa vigente[16], al fine di garantire la loro non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura.

È possibile utilizzare formati diversi da quelli elencati nell'Allegato 2 "*Formati di file e riversamento*" delle Linee Guida, effettuando una valutazione di interoperabilità, svolta in base alle indicazioni previste nel medesimo Allegato[17].

I formati utilizzati dall'Istituzione scolastica, secondo la valutazione di interoperabilità, sono: PDF, XML e TIFF.

Nella fase di registrazione l'operatore di protocollo provvede:

- alla verifica della presenza di categorie particolari di dati personali, di cui all'articolo 9 del Regolamento UE 679/2016;
- alla classificazione del documento sulla base del titolario di classificazione[18];
- alla registrazione di protocollo.

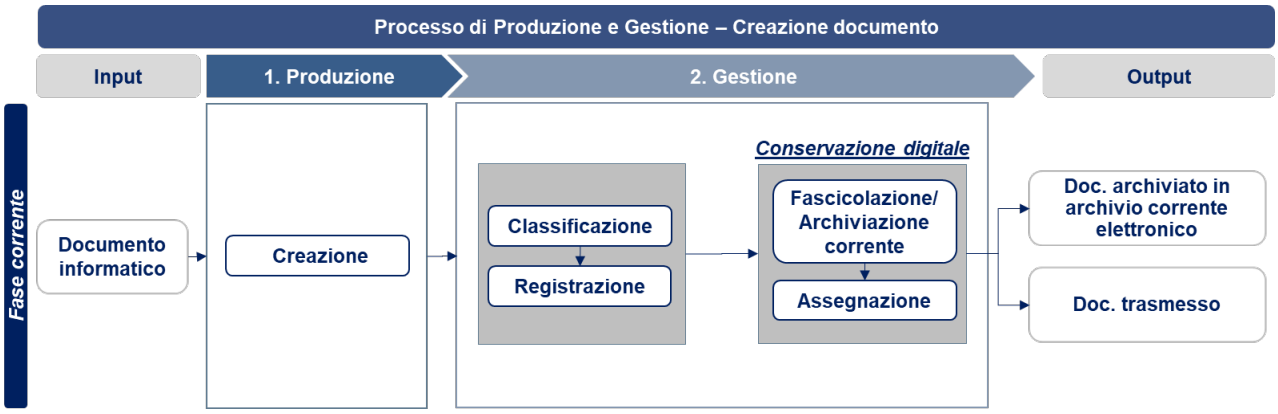
Nella fase di fascicolazione/archiviazione corrente l'operatore di protocollo provvede all'inserimento del documento informatico in un fascicolo già esistente o, nel caso in cui il fascicolo non sia presente, provvede a crearlo oppure a richiederne la creazione all'utente opportunamente abilitato.

Successivamente alla fase di fascicolazione/archiviazione, il documento può essere oggetto di una nuova assegnazione o di pubblicazione.

Di seguito si fornisce la rappresentazione grafica del processo sopra descritto.

[16] Allegato 2 alle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" emanate dall'AgID.
[17] La valutazione di interoperabilità, in quanto parte della gestione informatica dei documenti, viene effettuata periodicamente e, comunque, ogni anno, allo scopo di individuare tempestivamente cambiamenti delle condizioni espresse dai punti sopra elencati. Il manuale di gestione documentale contiene l'elenco dei formati utilizzati e la valutazione di interoperabilità.
[18] Nel caso di dubbi in merito alla voce del titolario da attribuire al documento, l'operatore addetto al protocollo si confronta con il Responsabile della gestione documentale in merito alla corretta classificazione.

Firmato digitalmente da ROBERTO FRACCIA



3.1.3. PROCESSO DI GESTIONE - CLASSIFICAZIONE

La classificazione è l'operazione obbligatoria che consente di organizzare i documenti, secondo un ordinamento logico, in relazione alle funzioni e alle competenze dell'Istituzione scolastica. Essa è eseguita a partire dal titolario di classificazione.

Il titolario, di cui all'Allegato [*numero allegato*], è l'insieme delle voci logiche gerarchicamente strutturate e articolate in gradi divisionali (titolo/classe/eventuale sottoclasse), stabilite sulla base delle funzioni dell'Amministrazione. Esso è definito con apposito decreto del Dirigente Scolastico ed è unico a livello di Istituzione scolastica.

Tutti i documenti ricevuti e prodotti dall'Istituzione scolastica, indipendentemente dal supporto sul quale vengono formati, sono classificati in base al titolario di classificazione; mediante tale operazione si assegna al documento, oltre al codice completo dell'indice di classificazione (titolo, classe e eventuale sottoclasse), anche il numero di repertorio del fascicolo. L'operazione suddetta è obbligatoria all'atto della registrazione di protocollo, ma è possibile effettuare delle successive modifiche.

La classificazione, necessaria e fondamentale, è prodromica all'inserzione di un documento all'interno di un determinato fascicolo.

3.1.4. PROCESSO DI GESTIONE - FASCICOLAZIONE

La fascicolazione è l'attività di riconduzione logica (e, nel caso di documenti cartacei, anche fisica) di un documento all'interno dell'unità archivistica che ne raccoglie i precedenti, al fine di mantenere vivo il vincolo archivistico che lega ogni singolo documento alla relativa pratica.

Ogni documento, dopo la sua classificazione, viene inserito nel fascicolo di riferimento. I documenti sono archiviati all'interno di ciascun fascicolo o, all'occorrenza sotto-fascicolo, secondo l'ordine cronologico di registrazione.

I fascicoli sono organizzati per[19]:

- **affare**, al cui interno vengono compresi documenti relativi a una competenza non proceduralizzata, ma che, nella consuetudine amministrativa, l'Istituzione scolastica deve concretamente portare a buon fine. Il fascicolo per affare ha una data di apertura e una durata circoscritta. Esso, infatti, viene chiuso alla chiusura dell'affare;
- **attività**, al cui interno vengono compresi i documenti prodotti nello svolgimento di un'attività amministrativa semplice che implica risposte obbligate o meri adempimenti, per la quale quindi non è prevista l'adozione di un provvedimento finale. Ha in genere durata annuale;

[19] Allegato 5 alle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" emanate dall'AgID.

Firmato digitalmente da ROBERTO FRACCIA

- **persona fisica**, al cui interno vengono compresi tutti i documenti, anche con classifiche diverse, che si riferiscono a una persona fisica. Quasi sempre i fascicoli intestati alle persone restano correnti per molti anni;
- **persona giuridica**, al cui interno vengono compresi tutti i documenti, anche con classifiche diverse, che si riferiscono a una persona giuridica. Quasi sempre i fascicoli intestati alle persone restano correnti per molti anni;
- **procedimento amministrativo**, al cui interno vengono conservati una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un provvedimento amministrativo. Il fascicolo viene chiuso al termine del procedimento amministrativo[20].

All'interno dei fascicoli è possibile creare dei sotto-fascicoli.

Ogni ufficio si fa carico di gestire le pratiche di propria competenza. Qualora un documento dia luogo all'avvio di un nuovo procedimento, il soggetto preposto provvede all'apertura di un nuovo fascicolo. Al fine di determinare la tipologia di aggregazione documentale (tipologia di serie e tipologia di fascicoli) da adottare, si fa riferimento al Piano di organizzazione delle aggregazioni documentali, riportato all'Allegato [*numero allegato*]. Un documento può essere assegnato anche a più fascicoli. La formazione di un nuovo fascicolo avviene attraverso l'operazione di "**apertura**" che comprende la registrazione di alcune informazioni essenziali. Il fascicolo informatico, infatti, reca l'indicazione[21]:

- dell'amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
- delle altre amministrazioni partecipanti;
- del responsabile del procedimento;
- dell'oggetto del procedimento;
- dell'elenco dei documenti contenuti;
- dell'identificativo del fascicolo medesimo.

Il fascicolo di norma viene aperto all'ultimo livello della struttura gerarchica del titolario. In alcuni casi, è possibile utilizzare anche il primo livello (titolo), come per i fascicoli di persona fisica.

In presenza di un documento da inserire in un fascicolo, i soggetti deputati alla fascicolazione stabiliscono, con l'ausilio delle funzioni di ricerca del sistema di protocollo informatico, se esso si colloca nell'ambito di un procedimento in corso, oppure se dà avvio ad un nuovo procedimento:

1. se si colloca nell'ambito di un procedimento in corso:
    - selezionano il relativo fascicolo;
    - collegano la registrazione di protocollo del documento al fascicolo selezionato (se si tratta di un documento su supporto cartaceo, assicurano l'inserimento fisico dello stesso nel relativo carteggio);
2. se dà avvio ad un nuovo procedimento:
    - eseguono l'operazione di apertura del fascicolo di cui al paragrafo precedente;
    - assegnano la pratica su indicazione del responsabile del procedimento;
    - collegano la registrazione di protocollo del documento al fascicolo aperto.

Il fascicolo viene chiuso al termine del procedimento. La data di chiusura si riferisce alla data dell'ultimo documento prodotto. Quando si verifica un errore nella assegnazione di un fascicolo, l'utente abilitato

[20] A norma dell'art. 41, comma 2, del CAD, "*La pubblica amministrazione titolare del procedimento raccoglie in un fascicolo informatico gli atti, i documenti e i dati del procedimento medesimo da chiunque formati;* […]".
[21] A norma dell'art. 41, comma 2-*ter*, del CAD.

Firmato digitalmente da ROBERTO FRACCIA

all'operazione di fascicolazione provvede a correggere le informazioni inserite nel sistema informatico e ad inviare il fascicolo all'UOR di competenza. Il sistema di gestione informatizzata dei documenti tiene traccia di questi passaggi, memorizzando per ciascuno di essi l'identificativo dell'operatore che effettua la modifica con la data e l'ora dell'operazione.

I fascicoli sono annotati nel repertorio dei fascicoli. Il repertorio dei fascicoli, ripartito per ciascun titolo del titolario, è lo strumento di gestione e di reperimento dei fascicoli. La struttura del repertorio rispecchia quella del titolario di classificazione e quindi varia in concomitanza con l'aggiornamento di quest'ultimo. Mentre il titolario rappresenta in astratto le funzioni e le competenze che la scuola può esercitare in base alla propria missione istituzionale, il repertorio dei fascicoli rappresenta in concreto le attività svolte e i documenti prodotti in relazione a queste attività. Nel repertorio sono indicati:

- la data di apertura;
- l'indice di classificazione completo (titolo, classe ed eventuale sottoclasse);
- il numero di fascicolo (ed altre eventuali partizioni in sotto-fascicoli e inserti);
- la data di chiusura;
- l'oggetto del fascicolo (ed eventualmente l'oggetto dei sotto-fascicoli e inserti);
- l'annotazione sullo stato della pratica a cui il fascicolo si riferisce (pratica in corso da inserire nell'archivio corrente, pratica chiusa da inviare all'archivio di deposito, pratica chiusa da inviare all'archivio di storico o da scartare).

Il repertorio dei fascicoli è costantemente aggiornato.

Oltre ad essere inserito in un fascicolo, un documento può essere inserito in una o più serie documentali, che rappresentano aggregazioni di documenti con caratteristiche omogenee, raggruppati ad esempio in base alla tipologia documentaria (es. delibere, decreti, fatture) o alla provenienza (cioè se prodotti da un medesimo organo, come il Consiglio d'istituto o il Collegio dei docenti) o all'oggetto (es. documenti relativi ad un progetto PON).[22] I documenti all'interno di una serie, non essendo aggregati utilizzando il titolario di classificazione come nel caso dei fascicoli, possono appartenere a titoli e classi differenti tra loro. La serie documentale stessa, quindi, non viene classificata in base alle partizioni del titolario.

Specifiche indicazioni in merito alle modalità di inserimento dei documenti nelle aggregazioni documentali, sono contenute nell'Appendice "*Focus sulle aggregazioni documentali delle Istituzioni scolastiche*" alle "Linee guida per la gestione documentale nelle Istituzioni scolastiche".

3.1.5. PROCESSO DI GESTIONE - ARCHIVIAZIONE

Le Istituzioni scolastiche definiscono nel proprio manuale la gestione degli archivi rifacendosi alla seguente articolazione archivistica[23]:

- **archivio corrente**: riguarda i documenti necessari alle attività correnti;
- **archivio di deposito**: riguarda i documenti ancora utili per finalità amministrative o giuridiche, ma non più indispensabili per la trattazione delle attività correnti;
- **archivio storico**: riguarda i documenti storici selezionati per la conservazione permanente.

L'archiviazione, per alcune fattispecie di documenti, può avvenire presso archivi gestiti a livello centrale dal Ministero dell'Istruzione. A titolo esemplificativo, le istanze che pervengono alla scuola mediante il Servizio Istanze OnLine, che permette di effettuare in modalità digitale la presentazione delle domande connesse ai

[22] Tale definizione di "serie documentale" è basata sul paragrafo 4 dell'Allegato 5 alle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" emanate dall'AgID.
[23] "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" emanate dall'AgID.

Firmato digitalmente da ROBERTO FRACCIA

principali procedimenti amministrativi dell'Amministrazione, sono protocollate in ingresso dalla AOO appositamente costituita presso il Ministero dell'Istruzione, e sono rese disponibili alle Istituzioni scolastiche.

Tenendo conto che l'archivio corrente è organizzato su base annuale e che il passaggio dall'archivio corrente all'archivio di deposito è possibile solo qualora il fascicolo contenga documenti afferenti a procedimenti conclusi, è necessario verificare quali fascicoli contengono documenti afferenti ad una pratica chiusa. Tale verifica può essere effettuata:

- ad ogni fine anno, in modo tale che i fascicoli delle pratiche non chiuse entro il dicembre precedente vengano "trascinati" nell'archivio corrente del nuovo anno e i fascicoli delle pratiche chiuse vengano "trascinati" nell'archivio di deposito;

oppure,

- in corso d'anno qualora la pratica sia chiusa.

Dato che sarebbe troppo oneroso e pressoché inutile conservare illimitatamente l'archivio nella sua totalità esso deve essere periodicamente sottoposto ad una selezione razionale, che va prevista fin dal momento della creazione dei documenti, e va disciplinata nel piano di conservazione[24] (Allegato [*numero allegato*]), a sua volta integrato con il sistema di classificazione. A tal fine si inserisce lo sfoltimento (attività eseguita nell'archivio corrente).

Lo sfoltimento è un'attività propedeutica ad una corretta conservazione documentale: al momento della chiusura del fascicolo, ad esempio, oppure prima del trasferimento dello stesso all'archivio di deposito, l'eventuale carteggio di carattere transitorio e strumentale deve essere selezionato ed estratto dal fascicolo da parte dell'operatore incaricato del trattamento della pratica. Si tratta, cioè, di estrarre dal fascicolo le copie e i documenti che hanno appunto carattere strumentale e transitorio, utilizzati dall'operatore incaricato o dal responsabile del procedimento, ma che esauriscono la loro funzione nel momento in cui viene emesso il provvedimento finale oppure non sono strettamente connessi al procedimento (ad es., appunti, promemoria, copie di normativa e documenti di carattere generale).

Nell'ambito dell'archivio di deposito avviene l'operazione di scarto che non deve essere applicato, salvo diverse indicazioni dettate dalla Soprintendenza archivistica, su documentazione facente parte dell'archivio storico le cui pratiche siano esaurite da oltre 40 anni, mentre può essere sempre effettuato sulla documentazione dell'archivio di deposito, che contiene tutte le pratiche chiuse che non abbiano maturato i 40 anni di conservazione.

La carenza di spazio negli archivi nonché la produzione smisurata e la conservazione di carte anche inutili non possono giustificare la distruzione non autorizzata di documenti e nemmeno la cancellazione di documenti elettronici[25], poiché lo scarto dei documenti dell'archivio della scuola è subordinato all'autorizzazione della Soprintendenza archivistica[26]. È una forma di scarto anche la cancellazione di documenti elettronici.

Fatto salvo quanto sopra, l'operazione di scarto è supportata dal massimario di conservazione e scarto, grazie al quale è prodotto annualmente l'elenco dei documenti e dei fascicoli per i quali è trascorso il periodo obbligatorio di conservazione e che quindi sono suscettibili di scarto archivistico. I documenti selezionati per la conservazione permanente sono depositati contestualmente agli strumenti che ne garantiscono l'accesso

[24] Art. 68, comma 1, del D.P.R. 445/2000.
[25] Art. 169, D.Lgs. 22 gennaio 2004, n. 42 "Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137".
[26] Art. 21, comma 1, D.Lgs. 22 gennaio 2004, n. 42 "Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137".

Firmato digitalmente da ROBERTO FRACCIA

nell'Archivio di Stato competente per territorio o trasferiti nella separata sezione di archivio, secondo quanto previsto dalle vigenti disposizioni in materia di tutela dei beni culturali.

3.2. PROCESSO DI CONSERVAZIONE

Il ciclo di gestione di un documento informatico termina con il suo versamento in un sistema di conservazione che è coerente con quanto disposto dal CAD e dalle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*". Il processo di conservazione prevede quattro fasi:

- versamento in archivio di deposito;
- scarto;
- versamento in archivio storico;
- delocalizzazione.

In questo contesto, si inserisce la figura del Responsabile della conservazione, i cui compiti sono stati descritti al precedente paragrafo 2.2.

Ai sensi dell'art. 34, comma 1-*bis*, del CAD, come modificato dall'art. 25, comma 1, lett. e), del D.L. 76/2020 (c.d. "Decreto Semplificazione"), convertito con Legge n. 120/2020, le Pubbliche Amministrazioni possono procedere alla conservazione dei documenti informatici:

a) all'interno della propria struttura organizzativa;
b) affidandola, in modo totale o parziale, nel rispetto della disciplina vigente, ad altri soggetti, pubblici o privati che possiedono i requisiti di qualità, di sicurezza e organizzazione individuati, nel rispetto della disciplina europea, nelle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" nonché in un regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici emanato da AgID[27], avuto riguardo all'esigenza di assicurare la conformità dei documenti conservati agli originali nonché la qualità e la sicurezza del sistema di conservazione.

Per la conservazione dei documenti informatici, l'Istituzione scolastica si avvale del seguente modello [*interno/esterno*].

Il sistema di conservazione garantisce l'accesso all'oggetto conservato per il periodo previsto dal piano di conservazione del titolare dell'oggetto della conservazione e dalla normativa vigente, o per un tempo superiore eventualmente concordato tra le parti, indipendentemente dall'evoluzione del contesto tecnologico.

Ai sensi dell'art. 44, comma 1-*ter*, del CAD, come da ultimo modificato dal D.L. 76/2020, "*In tutti i casi in cui la legge prescrive obblighi di conservazione, anche a carico di soggetti privati, il sistema di conservazione dei documenti informatici assicura, per quanto in esso conservato, caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità, secondo le modalità indicate nelle Linee guida*".

In ogni caso, i sistemi di conservazione devono consentire la possibilità di eliminare i documenti ove necessario (laddove previsto dalla normativa vigente).

Si tenga conto altresì del periodo di conservazione e di scarto dei documenti che contengono al loro interno dati personali. In base alla normativa vigente in materia di protezione dei dati personali, infatti, tale periodo di

[27] L'AgID ha adottato con Determinazione n. 455/2021 il "*Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici*" e i relativi allegati. L'allegato A, in particolare, fissa i requisiti per l'erogazione del servizio di conservazione per conto delle Pubbliche Amministrazioni. Il regolamento prevede, inoltre, l'istituzione di un *marketplace* per i servizi di conservazione quale sezione autonoma del *Cloud Marketplace* cui possono iscriversi i soggetti, pubblici e privati, che intendono erogare il servizio di conservazione dei documenti informatici per conto delle Pubbliche Amministrazioni. L'iscrizione al *marketplace* non è obbligatoria ma i conservatori che intendono partecipare a procedure di affidamento da parte delle Pubbliche Amministrazioni devono ugualmente possedere i requisiti previsti nel suddetto regolamento e sono sottoposti all'attività di vigilanza di AgID.

Firmato digitalmente da ROBERTO FRACCIA

tempo non deve essere superiore a quello necessario agli scopi per i quali i dati sono stati raccolti o successivamente trattati.

3.2.1. VERSAMENTO IN ARCHIVIO DI DEPOSITO

Nella fase di versamento in archivio di deposito[28] il responsabile per la tenuta degli archivi[29]:

- controlla periodicamente tutte le pratiche fascicolate presenti nell'archivio corrente, sia cartaceo che elettronico, al fine di identificare quelle per cui la lavorazione è già stata conclusa e compila una lista della documentazione presente nelle pratiche chiuse;
- provvede allo sfoltimento eliminando l'eventuale carteggio di carattere transitorio e strumentale presente nel fascicolo;
- provvede al versamento di tutta la documentazione, sia cartacea che elettronica, presente nella lista all'archivio di deposito;
- provvede al versamento nell'archivio corrente del nuovo anno della documentazione delle pratiche appartenenti alle pratiche presenti nell'archivio corrente (ancora in fase di lavorazione).

Di seguito, si fornisce la rappresentazione grafica del processo sopra descritto.

3.2.2. SCARTO

Nell'archivio di deposito si eseguono le attività relative alla fase di scarto in cui il responsabile per la tenuta degli archivi:

- verifica periodicamente la tipologia e i tempi di conservazione della documentazione, sia cartacea che elettronica, presente nell'archivio di deposito per individuare quella da scartare applicando le disposizioni del massimario di conservazione e scarto;
- procede con la compilazione di una lista della documentazione da scartare e da inviare alla Soprintendenza per l'approvazione e la comunica al Responsabile della gestione documentale;
- invia, in caso di documenti cartacei, la documentazione presente sulla lista al soggetto competente per la distruzione della carta;

[28] L'art. 67 del D.P.R. 445/2000 disciplina il trasferimento dei documenti all'archivio di deposito, prevedendo, nel dettaglio che "*1. Almeno una volta ogni anno il responsabile del servizio per la gestione dei flussi documentali e degli archivi provvede a trasferire fascicoli e serie documentarie relativi a procedimenti conclusi in un apposito archivio di deposito costituito presso ciascuna amministrazione. 2. Il trasferimento deve essere attuato rispettando l'organizzazione che i fascicoli e le serie avevano nell'archivio corrente. 3. Il responsabile del servizio per la gestione dei flussi documentali e degli archivi deve formare e conservare un elenco dei fascicoli e delle serie trasferite nell'archivio di deposito.*".

[29] Il responsabile per la tenuta degli archivi può essere il Dirigente Scolastico o altro personale in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'art. 61 del D.P.R. 28 dicembre 2000, n. 445.

Firmato digitalmente da ROBERTO FRACCIA

- provvede ad eliminare la documentazione elettronica presente nella lista approvata dalla Soprintendenza.

In caso di affidamento esterno del servizio di conservazione, l'elenco dei pacchetti di archiviazione contenenti i documenti destinati allo scarto è generato dal responsabile del servizio di conservazione e trasmesso al Responsabile della conservazione che, a sua volta, verificato il rispetto dei termini temporali stabiliti dal massimario di conservazione e scarto, lo comunica al Responsabile della gestione documentale.

3.2.3. VERSAMENTO IN ARCHIVIO STORICO

Nella fase di versamento in archivio storico[30], il responsabile per la tenuta degli archivi:

- verifica se nell'archivio di deposito esistono pratiche esaurite da oltre 40 anni, sia in forma cartacea che elettronica;
- provvede a preparare una lista contenente tutta la documentazione presente nelle pratiche stesse, qualora dovessero essere presenti pratiche esaurite da oltre 40 anni;
- provvede ad inviare la lista della documentazione da versare al personale competente, in caso di documentazione cartacea, che deve individuare un archivio storico con sufficiente spazio per dare seguito al versamento.

3.2.4. DELOCALIZZAZIONE

La fase di delocalizzazione è avviata nel caso in cui, dopo aver effettuato le operazioni di scarto e dopo aver effettuato l'eventuale versamento nell'archivio storico, dalla verifica del grado di saturazione dell'archivio di deposito cartaceo, risulta che l'archivio è saturo. Nel caso in cui l'archivio di deposito cartaceo dovesse essere saturo, il responsabile per la tenuta degli archivi:

- provvede ad individuare la documentazione da delocalizzare selezionandola tra quella più prossima alla data di scarto;
- provvede a stilare la lista dei documenti da delocalizzare.

L'addetto competente:

- analizza la documentazione ricevuta;
- provvede a identificare una struttura con sufficiente spazio negli archivi;
- autorizza la delocalizzazione della documentazione presso una struttura interna nel caso in cui questa sia disponibile.

Il responsabile per la tenuta degli archivi provvede ad inviare la richiesta di autorizzazione alla Soprintendenza competente. Una volta ricevuta l'approvazione dalla Soprintendenza competente, il responsabile per la tenuta degli archivi provvede ad inviare la documentazione da delocalizzare.

4. IL DOCUMENTO AMMINISTRATIVO

Per documento amministrativo, ai sensi dell'art. 1, comma 1, lett. a), del D.P.R. 28 dicembre 2000, n. 445, si intende "*ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa*".

[30] L'art. 69 del D.P.R. 445/2000, rubricato "Archivi storici", prevede che "*I documenti selezionati per la conservazione permanente sono trasferiti contestualmente agli strumenti che ne garantiscono l'accesso, negli Archivi di Stato competenti per territorio o nella separata sezione di archivio secondo quanto previsto dalle vigenti disposizioni in materia di tutela dei beni culturali*".

Firmato digitalmente da ROBERTO FRACCIA

Nell'ambito del processo di gestione documentale, il documento amministrativo dal punto di vista operativo è classificabile in documento:

- ricevuto;
- inviato;
- di rilevanza esterna;
- di rilevanza interna.

In base alla natura, invece, è classificabile in documento:

- analogico;
- informatico.

L'art. 40, comma 1, del CAD, come modificato da ultimo dall'art. 66, comma 1, del D.Lgs. 13 dicembre 2017, n. 217, stabilisce che "*Le pubbliche amministrazioni formano gli originali dei propri documenti, inclusi quelli inerenti ad albi, elenchi e pubblici registri, con mezzi informatici secondo le disposizioni di cui al presente codice e le Linee guida*".

Per ciò che concerne la trasmissione dei documenti tra Pubbliche Amministrazioni, ai sensi di quanto disposto dall'art. 47 del CAD, essa deve avvenire:

- attraverso l'utilizzo della posta elettronica[31]; *ovvero*
- in cooperazione applicativa.

Le suddette comunicazioni sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza. Il comma 2, del citato art. 47, stabilisce infatti che "*Ai fini della verifica della provenienza le comunicazioni sono valide se: a) sono sottoscritte con firma digitale o altro tipo di firma elettronica qualificata; b) ovvero sono dotate di segnatura di protocollo di cui all'articolo 55 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445; c) ovvero è comunque possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle Linee guida. È in ogni caso esclusa la trasmissione di documenti a mezzo fax; d) ovvero trasmesse attraverso sistemi di posta elettronica certificata di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68*".

Specifiche indicazioni in materia di scambio di documenti amministrativi protocollati tra AOO sono contenute nell'Allegato 6 alle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*".

4.1. DOCUMENTO RICEVUTO

La corrispondenza in ingresso può essere acquisita dall'Istituzione scolastica con diversi mezzi e modalità in base sia alla modalità di trasmissione scelta dal mittente sia alla natura del documento. Un documento informatico può essere recapitato[32]:

- a mezzo posta elettronica convenzionale (PEO);
- a mezzo posta elettronica certificata (PEC);
- mediante supporto removibile (ad es. CD, *pendrive*).

[31] Come riportato nell'Appendice C dell'Allegato 6 alle *Linee Guida per la formazione, gestione e conservazione dei documenti informatici*, l'utilizzo della posta elettronica è *"da intendersi quale modalità transitoria nelle more dell'applicazione delle comunicazioni tra AOO tramite cooperazione applicativa"*. Pertanto, la cooperazione applicativa viene identificata come l'unica modalità a tendere per le comunicazioni di documenti amministrativi protocollati tra AOO.
[32] Per ciò che riguarda la trasmissione dei documenti tra le Pubbliche Amministrazioni, specifiche indicazioni sono contenute all'interno dell'art. 47 del CAD.

Firmato digitalmente da ROBERTO FRACCIA

Un documento analogico, assunto che le principali tipologie di documenti analogici che pervengono alle Istituzioni scolastiche sono telegrammi, documenti per posta ordinaria e raccomandate, può essere recapitato:

- attraverso il servizio di posta tradizionale;
- *pro manibus*.

I documenti, analogici o digitali, di cui non sia identificabile l'autore sono regolarmente aperti e registrati al protocollo (con indicazione "Mittente anonimo"), salvo diversa valutazione del Dirigente Scolastico, che provvederà ad eventuali accertamenti.

I documenti ricevuti privi di firma ma il cui mittente è comunque chiaramente identificabile, vengono protocollati (con indicazione "Documento non sottoscritto") e inoltrati al responsabile del procedimento, che valuterà la necessità di acquisire la dovuta sottoscrizione per il perfezionamento degli atti.

La funzione notarile del protocollo (cioè della registratura) è quella di attestare data e provenienza certa di un documento senza interferire su di esso. Sarà poi compito del responsabile del procedimento valutare, caso per caso, ai fini della sua efficacia riguardo ad un affare o ad un determinato procedimento amministrativo, se il documento privo di firma possa essere ritenuto valido o meno[33].

4.2. Documento inviato

I documenti informatici sono inviati all'indirizzo elettronico dichiarato dai destinatari, abilitato alla ricezione della posta per via telematica.

4.3. Documento di rilevanza esterna

Per documento di rilevanza esterna si intende qualunque documento ricevuto/trasmesso da/a altro Ente o altra persona fisica o giuridica. La gestione è normata dal CAD.

4.4. Documento di rilevanza interna

Per documenti di rilevanza interna si intendono tutti quelli che a qualunque titolo sono scambiati tra UOR o persone dell'Istituzione scolastica stessa.

Possono distinguersi in:

- **comunicazioni informali tra UOR** (documenti di natura prevalentemente informativa): per comunicazioni informali tra unità si intendono gli scambi di informazioni che non hanno valenza giuridico probatoria, né rilevanza ai fini dell'azione amministrativa. Queste comunicazioni avvengono, di norma, tramite PEO e non sono soggette a protocollazione ed archiviazione;
- **scambio di documenti fra UOR** (documenti di natura prevalentemente giuridico-probatoria): per scambio di documenti fra unità si intendono le comunicazioni ufficiali di un certo rilievo ai fini dell'azione amministrativa e delle quali si deve tenere traccia. Le comunicazioni di questo genere devono comunque essere protocollate.

4.5. Documento analogico

Per documento analogico si intende "*la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti*"[34].

[33] Per approfondimenti in merito alle tipologie di sottoscrizione elettronica, si veda il par. "4.6.1 - Le firme elettroniche".
[34] Art. 1, comma 1, lett. p-*bis*), D.lgs. 7 marzo 2005, n. 82, CAD.

Firmato digitalmente da ROBERTO FRACCIA

Si definisce "originale" il documento cartaceo nella sua redazione definitiva, perfetta ed autentica negli elementi sostanziali e formali, comprendente tutti gli elementi di garanzia e di informazione del mittente e del destinatario, stampato su carta intestata e dotato di firma autografa[35].

La sottoscrizione di un documento determina:

- l'**identificazione dell'autore** del documento;
- la **paternità** del documento: con la sottoscrizione l'autore del documento si assume la paternità dello stesso, anche in relazione al suo contenuto. A questo proposito si parla di non ripudiabilità del documento sottoscritto;
- l'**integrità** del documento: il documento scritto e sottoscritto manualmente garantisce da alterazioni materiali da parte di persone diverse da quella che lo ha posto in essere.

4.6. DOCUMENTO INFORMATICO

Per documento informatico si intende "*il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*"[36]. Il documento informatico, come precisato nel paragrafo 2.1.1. delle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" emanate da AgID, è formato mediante una delle seguenti modalità:

"*a) creazione tramite l'utilizzo di strumenti software o servizi cloud qualificati che assicurino la produzione di documenti nei formati e nel rispetto delle regole di interoperabilità di cui all'allegato 2;*

b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;

c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;

d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica".

Il documento informatico è immodificabile se la sua memorizzazione su supporto informatico in formato digitale non può essere alterata nel suo accesso, gestione e conservazione.

A seconda che il documento informatico sia formato secondo una delle modalità sopra riportate, l'immodificabilità e l'integrità sono garantite da una o più delle operazioni indicate nelle citate Linee Guida, al paragrafo 2.1.1. (pag. 13).

Al momento della formazione del documento informatico immodificabile, devono essere generati e associati permanentemente ad esso i relativi metadati. L'insieme dei metadati associati dall'Istituzione scolastica ai documenti informatici e ai documenti amministrativi informatici corrispondono a quelli obbligatori previsti nell'Allegato 5 delle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*". Potranno essere individuati ulteriori metadati da associare a particolari tipologie di documenti informatici, come i documenti soggetti a registrazione particolare.

[35] Per approfondimenti in merito alla ricezione di documenti privi di firma, si veda il par. "4.1. – Documento ricevuto".
[36] Art. 1, comma 1, lett. p), D.lgs. 7 marzo 2005, n. 82, CAD. La definizione è altresì contenuta all'interno dell'art. 1, comma 1, lett. b), del D.P.R. 445/2000: "*b) DOCUMENTO INFORMATICO: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.*".

Firmato digitalmente da ROBERTO FRACCIA

[*In caso di determinazione di ulteriori metadati da associare a particolari tipologie di documenti informatici*]

Gli ulteriori metadati e le particolari tipologie di documenti informatici a cui devono essere associati vengono riportati nell'Allegato [*numero allegato*].

Un documento nativo informatico non può essere convertito in formato analogico prima della sua eventuale acquisizione a sistema di protocollo o archiviazione informatica. Nel caso di documenti soggetti a sottoscrizione, è possibile fare ricorso alla firma elettronica avanzata (FEA), messa a disposizione delle Istituzioni scolastiche dal Ministero. I Dirigenti Scolastici ed i Direttori dei Servizi Generali ed Amministrativi delle Istituzioni Scolastiche statali di ogni ordine e grado possono, inoltre, fare ricorso alla firma digitale, tramite l'apposita funzione presente sul SIDI. Le suddette modalità di firma vengono delineate ed analizzate nel paragrafo successivo.

4.6.1. LE FIRME ELETTRONICHE

La firma elettronica costituisce la modalità ordinaria di firma dei documenti informatici.

In particolare, la normativa vigente in materia individua diverse tipologie di sottoscrizione elettronica:

- firma elettronica, ovvero l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzata come metodo di autentificazione (art. 3, n. 10, Reg. UE n. 910/2014);
- firma elettronica avanzata, ovvero l'insieme dei dati allegati o connessi ad un documento informatico che consentono l'identificazione del firmatario e garantiscono la connessione univoca con quest'ultimo (art. 3, n. 11, Reg. UE n. 910/2014);
- firma elettronica qualificata, ovvero una firma elettronica avanzata che si basa su un certificato qualificato (art. 3, n. 12, Reg. UE n. 910/2014);
- firma digitale, ovvero una particolare firma elettronica qualificata che si basa su un certificato qualificato e su un sistema di chiavi crittografiche (art. 1, comma 1, lett. s), CAD).

In considerazione del tipo di tecnologia utilizzata, la firma digitale rappresenta la tipologia di firma più sicura. Essa è disciplinata dall'art. 24 del CAD il quale, ai commi 1, 2, 3 e 4, prevede che "*1. La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata. 2. L'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente. 3. Per la generazione della firma digitale deve adoperarsi un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso. 4. Attraverso il certificato qualificato si devono rilevare, secondo le Linee guida, la validità del certificato stesso, nonché gli elementi identificativi del titolare di firma digitale e del certificatore e gli eventuali limiti d'uso. Le linee guida definiscono altresì le modalità, anche temporali, di apposizione della firma*".

Si tenga conto, altresì, che secondo quanto stabilito dall'art. 24, comma 4-*bis*, del CAD, qualora ad un documento informatico sia apposta una firma digitale o un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso, il documento si ha come non sottoscritto, salvo che lo stato di sospensione sia stato annullato. Ad ogni modo, l'eventuale revoca o sospensione, comunque motivata, ha effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.

Si rappresenta, inoltre, che l'articolo 20, comma 1-*bis*, del CAD, come modificato dall'art. 20, comma 1, lett. a) del D.Lgs. 13 dicembre 2017, n. 217, stabilisce che "*Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi è apposta una firma*

Firmato digitalmente da ROBERTO FRACCIA

digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. In tutti gli altri casi, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida".

Ai sensi dell'art. 20, commi 1-*ter* e 1-*quater*, del CAD, introdotti dall'art. 20, comma 1, lett. b), del D.lgs. 13 dicembre 2017, n. 217: "(1-*ter*) *L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare di firma elettronica, salvo che questi dia prova contraria. (1-quater) Restano ferme le disposizioni concernenti il deposito degli atti e dei documenti in via telematica secondo la normativa, anche regolamentare, in materia di processo telematico*".

Dalle disposizioni sopra riportate, risulta possibile individuare quale sia l'efficacia probatoria del documento informatico, sulla base del tipo di firma apposta sullo stesso. Nel dettaglio:

- i **documenti sottoscritti con firma elettronica "semplice"** soddisfano il requisito della forma scritta e il loro valore probatorio è liberamente valutabile in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità della firma stessa;
- i **documenti sottoscritti con firma elettronica avanzata, firma elettronica qualificata e firma digitale** soddisfano il requisito della forma scritta e hanno l'efficacia prevista dall'art. 2702 c.c.[37], ovvero fanno piena prova fino a querela di falso;
- i **documenti sottoscritti con firma digitale con certificato revocato, scaduto o sospeso** fanno piena prova fino a disconoscimento, ai sensi di quanto disposto dall'art. 2712 c.c.[38].

Si rileva, inoltre, che l'art. 25 del CAD, rubricato "*Firma autenticata*", prevede che la firma elettronica o qualsiasi altro tipo di firma elettronica avanzata, autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato, si ha per riconosciuta ai sensi dell'art. 2703 c.c.[39].

Il CAD[40] stabilisce, altresì, che gli atti elencati ai numeri da 1 a 12 dell'art. 1350 c.c. debbano essere sottoscritti con firma elettronica qualificata o digitale, a pena di nullità. Gli atti di cui al n. 13, del citato art. 1350 c.c., invece, oltre ai tipi di firma sopra menzionati, possono essere sottoscritti anche con firma elettronica avanzata o devono essere formati con le ulteriori modalità di cui all'articolo 20, comma 1-*bis*, primo periodo.[41]

---

[37] L'art. 2702 c.c. stabilisce che "*La scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta*".

[38] L'art. 2712 c.c. stabilisce che "*Le riproduzioni fotografiche, informatiche o cinematografiche, le registrazioni fonografiche e, in genere, ogni altra rappresentazione meccanica di fatti e di cose formano piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime*".

[39] L'art. 2703 c.c. stabilisce che "*1. Si ha per riconosciuta la sottoscrizione autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato. 2. L'autenticazione consiste nell'attestazione da parte del pubblico ufficiale che la sottoscrizione è stata apposta in sua presenza. Il pubblico ufficiale deve previamente accertare l'identità della persona che sottoscrive*".

[40] Art. 21, comma 2-*bis*, del CAD.

[41] L'art. 1350 c.c. stabilisce che "*Devono farsi per atto pubblico o per scrittura privata, sotto pena di nullità: 1) i contratti che trasferiscono la proprietà di beni immobili; 2) i contratti che costituiscono, modificano o trasferiscono il diritto di usufrutto su beni immobili, il diritto di superficie, il diritto del concedente e dell'enfiteuta; 3) i contratti che costituiscono la comunione di diritti indicati dai numeri precedenti; 4) i contratti che costituiscono o modificano le servitù prediali, il diritto di uso su beni immobili e il diritto di abitazione; 5) gli atti di rinunzia ai diritti indicati dai numeri precedenti; 6) i contratti di affrancazione del fondo enfiteutico; 7) i contratti di anticresi; 8) i contratti di locazione di beni immobili per una durata superiore a nove anni; 9) i contratti di società o di associazione con i quali si conferisce il godimento di beni immobili o di altri diritti reali immobiliari per un tempo eccedente i nove anni o per un tempo indeterminato; 10) gli atti che costituiscono rendite perpetue o vitalizie, salve le disposizioni relative alle rendite dello Stato; 11) gli atti di divisione di beni immobili e di altri diritti reali immobiliari; 12) le transazioni che hanno per oggetto controversie relative ai rapporti giuridici menzionati nei numeri precedenti; 13) gli altri atti specialmente indicati dalla legge*".

Firmato digitalmente da ROBERTO FRACCIA

La registrazione di protocollo di un documento informatico sottoscritto con firma digitale è eseguita dopo che l'operatore di protocollo ha verificato la validità della firma digitale con apposita funzione sul sistema di protocollo.

Fatto salvo quanto sopra rappresentato, i documenti informatici possono essere anche senza firma e in tal caso si seguirà la disciplina contenuta al par. "4.1. – Documento ricevuto"[42].

Da ultimo, si rappresenta che, in tutti gli atti cartacei che provengono e che sono generati da sistemi automatizzati, la firma sul documento cartaceo del funzionario responsabile può essere sostituita dalla dicitura dalla "*Firma autografa sostituita a mezzo stampa, ai sensi dell'art. 3, comma 2, Legge 39/1993*".

4.7. CONTENUTI MINIMI DEI DOCUMENTI

Occorre che i documenti amministrativi, sia analogici che informatici, aventi rilevanza esterna, contengano le seguenti informazioni:

- denominazione e logo dell'amministrazione mittente;
- indirizzo completo dell'amministrazione (via, numero, CAP, città, provincia);
- indirizzo di posta elettronica certificata dell'Istituzione scolastica;
- indicazione dell'Istituzione scolastica e dell'UOR che ha prodotto il documento;
- il numero di telefono dell'UOR e del RUP (facoltativo, a piè di pagina se previsto);
- C.F., P.IVA, Codice iPA, Codice univoco per la F.E.

Inoltre, il documento deve recare almeno le seguenti informazioni:

- luogo e data (gg/mm/anno) di redazione del documento;
- numero di protocollo;
- oggetto del documento.

Esso non deve contenere il riferimento al numero di fax, coerentemente a quanto disposto dall'art. 14, comma 1-*bis*, del decreto-legge 21 giugno 2013, n. 69, così come modificato dalla legge 9 agosto 2013, n. 98, recante "*Misure per favorire la diffusione del domicilio digitale*", il quale stabilisce che, ai fini della verifica della provenienza delle comunicazioni, è in ogni caso esclusa la trasmissione di documenti a mezzo fax tra Pubbliche Amministrazioni. È facoltà del Responsabile della gestione documentale aggiungere a quelle fin qui esposte altre regole per la determinazione dei contenuti e per la definizione della struttura dei documenti informatici. Si evidenzia, altresì, che in tema di accesso ai documenti amministrativi[43], a ciascuna Istituzione scolastica spetta l'onere di specificare con precisione gli estremi di registrazione di un documento sui propri sistemi di protocollo.

L'indicazione di tali elementi (tra cui l'oggetto) deve essere rispondente agli *standard* indicati nel presente manuale[44]. Ciò perché prerequisito essenziale del pieno godimento del diritto all'accesso agli atti è la reperibilità di quest'ultimi che è assicurata da una corretta e standardizzata definizione/trascrizione dell'oggetto.

[42] Per approfondimenti in merito alla ricezione di documenti privi di firma, si veda il par. "4.1. – Documento ricevuto"
[43] Nell'ambito della disciplina di accesso, l'art. 1, comma 1, lett. d), della L. 241/1990 definisce il documento amministrativo come "*ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale*".
[44] Per ulteriori approfondimenti, si veda il par. "5.2. - Scrittura di dati di protocollo".

Firmato digitalmente da ROBERTO FRACCIA

4.8. PROTOCOLLABILITÀ DI UN DOCUMENTO

Sono oggetto di registrazione obbligatoria, ai sensi dell'art. 53, comma 5, del D.P.R. n. 445 del 2000, i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici[45].

Inoltre, l'art. 40-*bis* del CAD, come modificato dagli artt. 37, comma 1, e 66, comma 1, del D.lgs. 13 dicembre 2017, n. 217, prevede che formano oggetto di registrazione di protocollo ai sensi dell'articolo 53[46] del D.P.R. n. 445 del 2000, "*le comunicazioni che provengono da o sono inviate a domicili digitali eletti ai sensi di quanto previsto all'articolo 3-bis, nonché le istanze e le dichiarazioni di cui all'articolo 65 in conformità alle Linee guida*".

Sono invece esclusi dalla registrazione obbligatoria[47]:

- le gazzette ufficiali;
- i bollettini ufficiali e i notiziari della Pubblica Amministrazione;
- le note di ricezione delle circolari e altre disposizioni;
- i materiali statistici;
- gli atti preparatori interni;
- i giornali, le riviste;
- i libri;
- i materiali pubblicitari;
- gli inviti a manifestazioni;
- tutti i documenti già soggetti a registrazione particolare dell'Amministrazione.

Nel caso in cui sia necessario attribuire una data certa a un documento informatico non soggetto a protocollazione prodotto all'interno dell'Istituzione scolastica, si applicano le regole per la "validazione temporale" di cui al DPCM del 22 febbraio 2013 "*Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71*".

In particolare, la "validazione temporale" consente di stabilire il momento temporale in cui il documento informatico è stato formato ed è definita come il risultato di una procedura informatica in grado di offrire un riferimento temporale opponibile a terzi.

Lo strumento per ottenere questo risultato è la "marca temporale"[48], ovvero "*il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo*".

5. IL PROTOCOLLO INFORMATICO

5.1. PROTOCOLLAZIONE

Per protocollazione si intende l'attività di registrazione di protocollo mediante la quale è eseguita l'apposizione o l'associazione al documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso.

---

[45] Le *"Linee Guida sulla formazione, gestione e conservazione dei documenti informatici"*, emanate dall'AgID, prevedono che "*La registrazione informatica dei documenti è rappresentata dall'insieme di dati in forma elettronica allegati o connessi al documento informatico al fine dell'identificazione univoca di tutti i documenti prodotti e acquisiti. Per la Pubblica Amministrazione vale quanto disposto ai sensi dell'articolo 53, comma 5, del TUDA*".

[46] L'art. 53, comma 5, del D.P.R. 445/2000, al primo periodo prevede che "*Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici*".

[47] Art. 53, comma 5, del D.P.R.445/2000.

[48] Art. 1, comma 1, del DPCM 22 febbraio 2013.

Firmato digitalmente da ROBERTO FRACCIA

I documenti che devono essere registrati a protocollo sono indicati nel paragrafo "4.8. - Protocollabilità di un documento amministrativo".

Ogni numero di protocollo individua un unico documento e gli eventuali allegati allo stesso e, di conseguenza, ogni documento con i relativi allegati reca un solo numero di protocollo immodificabile. Quindi non è consentito:

- protocollare un documento già protocollato;
- apporre manualmente la segnatura di protocollo, salvo i casi in cui l'apposizione tramite l'applicativo possa deteriorare le informazioni fondamentali del documento (ad es. sovrapposizione del timbro in ingresso al timbro in uscita, presenza di etichetta adesiva plastificata che verrebbe annerita dalla stampante);
- in caso di spedizione ed arrivi massivi, apporre una segnatura del tipo es.: 1741/1, 1741/2, 1741/3, ecc. oppure attribuire ad essi lo stesso numero di protocollo;
- protocollare sul registro ufficiale atti di rilevanza interna senza utilizzare l'apposita modalità di protocollazione interna;
- selezionare un numero di protocollo alla data di ricezione del documento al fine di effettuare l'operazione di protocollazione in una data successiva;
- apporre la firma sul documento successivamente alla protocollazione;
- associare ad una precedente registrazione ulteriori allegati prodotti o ricevuti successivamente.

La protocollazione per ogni documento è effettuata mediante la memorizzazione dei seguenti elementi[49]:

- numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile;
- data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile;
- mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile;
- oggetto del documento, registrato in forma non modificabile;
- data e protocollo del documento ricevuto, se disponibili;
- l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari, in grado di identificarne univocamente il contenuto, registrata in forma non modificabile;
- informazioni inerenti all'assegnazione interna all'amministrazione e la eventuale classificazione[50].

L'operazione di protocollazione, così come appena descritta, deve essere effettuata solo **dopo** aver caricato sul sistema il documento principale e i suoi allegati (che devono riportare tutti il medesimo numero di protocollo).

5.2. SCRITTURA DI DATI DI PROTOCOLLO

La gestione informatizzata dei flussi documentali dell'Istituzione scolastica necessita una particolare attenzione alla qualità delle informazioni associate, in fase di protocollazione, ai documenti interessati, al fine di evitare che questi risultino non reperibili o difficilmente rintracciabili.

A tal fine, sono di seguito riportate le regole cui gli utilizzatori del sistema di protocollo informatico devono attenersi, per la redazione dei seguenti dati:

[49] Tali elementi sono definiti nell'art. 53, comma 1, del D.P.R. 445/2000.
[50] Tale elemento è previsto dalle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" emanate dall'AgID.

Firmato digitalmente da ROBERTO FRACCIA

TIPO DI DATI	REGOLE
Nomi di persona	- Prima il nome e poi il cognome - Tutto maiuscolo **Esempio**: MARIO ROSSI
Titoli professionali e/o istituzionali	Sempre omessi
Nomi di città e di stati	In lingua italiana, per esteso e senza puntare **Esempio**: San Vitaliano (Na) e non S. Vitaliano (Na)
Nomi di ditte e società	- Se riportano nomi di persona valgono le precedenti regole - Usare sigle, in maiuscolo e senza punti o, in alternativa, acronimi - La forma societaria senza punti **Esempio**: GIUSEPPE BIANCO, ACME SpA
Enti e associazioni in genere	Usare sigle in maiuscolo e senza punti, laddove disponibili
Ministeri	Usare la forma ridotta e puntata della sola parola Ministero, oppure l'acronimo **Esempio**: MIN. ISTRUZIONE, oppure MI
Enti di secondo livello	Usare la forma estesa o acronimi noti
Sigle in genere	In maiuscolo e senza punti **Esempio**: MI
Virgolette e apici	- Digitare il carattere direttamente dalla tastiera - Non eseguire la funzione copia e incolla di *Windows*
Date	Usare il seguente formato numerico: GG-MM-AAAA o GGMMAAAA **Esempio**: 20-07-2020 o 20072020 e non 20/07/2020

Oltre a quanto sopra rappresentato, l'Istituzione scolastica adotta le seguenti ulteriori regole per la redazione dei dati: [*elenco regole aggiuntive*].

5.3. SEGNATURA DI PROTOCOLLO

La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso. L'operazione di segnatura è effettuata dall'applicativo automaticamente e contemporaneamente all'operazione di registrazione di protocollo[51]. Essa consente di individuare ciascun documento in modo inequivocabile.

Le informazioni minime previste nella segnatura di protocollo sono[52]:

[51] Art. 55, comma 2, D.P.R. 445/2000 e "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*", emanate dall'AgID, pag. 20.
[52] Tali informazioni sono definite all'art. 55 del D.P.R. 445/2000.

Firmato digitalmente da ROBERTO FRACCIA

- il progressivo di protocollo[53];
- la data di protocollo;
- l'identificazione in forma sintetica dell'Amministrazione o dell'Area Organizzativa individuata.

L'operazione di segnatura di protocollo può includere ogni altra informazione utile o necessaria, qualora tali informazioni siano disponibili già al momento della registrazione di protocollo. Quando il documento è indirizzato ad altre Amministrazioni ed è formato e trasmesso con strumenti informatici, la segnatura di protocollo può includere tutte le informazioni di registrazione del documento.

La segnatura di protocollo dell'Istituzione scolastica, in ottemperanza alle regole tecniche precedentemente esposte, adotta il *set* di informazioni minime ed utilizza quale identificativo dell'Amministrazione il codice con cui l'Istituzione scolastica è univocamente identificata sull'indice delle Pubbliche Amministrazioni.

5.4. DIFFERIMENTO DELLA REGISTRAZIONE DI PROTOCOLLO

Le registrazioni di protocollo dei documenti pervenuti all'Istituzione scolastica sono effettuate nella giornata di arrivo e comunque non oltre tre giorni lavorativi dal ricevimento di detti documenti. Qualora nei tempi sopra indicati non possa essere effettuata la registrazione di protocollo, il Responsabile della gestione può autorizzare la registrazione in tempi successivi fissando comunque un limite di tempo e conferendo valore, nel caso di scadenze predeterminate, al timbro datario d'arrivo, esplicitandone l'autorizzazione attraverso apposite note interne. Il protocollo differito consiste nel differimento dei termini di registrazione e si applica ai documenti in arrivo.

5.5. RICEVUTA DI AVVENUTA PROTOCOLLAZIONE

La ricezione dei documenti via PEC comporta l'invio al mittente di due tipologie diverse di ricevute: una legata al servizio di posta certificata, una al servizio di protocollazione informatica. Nel caso di ricezione di documenti informatici mediante PEC, la notifica al mittente dell'avvenuto recapito del messaggio è assicurata dal servizio di posta elettronica certificata, utilizzato dall'Istituzione scolastica con gli *standard* specifici.

In caso di documenti pervenuti via PEO, è inviata una conferma di ricezione con relativa segnatura informatica in formato XML del documento attraverso apposita funzione ("Inoltro" o "Rispondi").

5.6. REGISTRO GIORNALIERO DI PROTOCOLLO

Il registro di protocollo è lo strumento attraverso cui è possibile identificare in modo univoco e certo i documenti ricevuti e spediti mediante la registrazione di determinati elementi che caratterizzano ogni singolo documento. Per tale motivo, il registro di protocollo svolge una fondamentale funzione giuridico probatoria, attestando l'esistenza di un determinato documento all'interno del sistema di gestione documentale e garantendone l'autenticità.

Dunque, in coerenza con la normativa vigente, il registro ufficiale di protocollo è unico, sia per la protocollazione in ingresso, che in uscita, che in modalità interna e la numerazione progressiva delle registrazioni di protocollo è unica indipendentemente dal modello organizzativo adottato. La numerazione si chiude al 31 dicembre e ricomincia il 1° gennaio successivo. Essa si aggiorna automaticamente e quotidianamente.

Deve essere prodotto automaticamente il registro giornaliero di protocollo costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno.

[53] Ai sensi dell'art. 57, comma 1, del D.P.R. 445/2000 44 "*Il numero di protocollo è progressivo e costituito da almeno sette cifre numeriche. La numerazione è rinnovata ogni anno solare.*".

Firmato digitalmente da ROBERTO FRACCIA

Esso deve essere inviato automaticamente dal sistema di protocollo, in formato tale da garantirne la non modificabilità. Al fine di garantire la non modificabilità delle operazioni di registrazione, il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione[54].

Si specifica che con riferimento alle protocollazioni effettuate esclusivamente sul Registro ufficiale di protocollo, l'operatore che gestisce lo smistamento dei documenti può definire "riservata" una registrazione di protocollo ed assegnarla per competenza ad un utente assegnatario.

Si ricorda che sono soggetti a protocollazione riservata i seguenti documenti:

- documenti relativi a vicende di persone o a fatti privati o particolari;
- documenti di carattere politico o di indirizzo che, se resi di pubblico dominio, possono ostacolare il raggiungimento degli obiettivi prefissati;
- documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa.

È possibile impostare una data di scadenza al carattere riservato del documento. Una volta scaduti i termini di riservatezza, il documento diventa visibile a chi è abilitato.

5.7. REGISTRO DI EMERGENZA

Nel caso di interruzioni del funzionamento del sistema di protocollo informatico per cause tecniche accidentali o programmate, ai sensi dell'art. 63 del Testo Unico, le registrazioni di protocollo vengono effettuate su un registro di emergenza[55].

Il Responsabile della gestione documentale autorizza con proprio provvedimento la predisposizione del registro di emergenza in forma cartacea oppure in forma digitale e, al ripristino della funzionalità del sistema di protocollo informatico, tutte le registrazioni effettuate vengono inserite a sistema, continuando la numerazione del protocollo generale raggiunta al momento dell'interruzione del servizio. A tale registrazione è associato anche il numero di protocollo e la data di registrazione riportati sul protocollo di emergenza, mantenendo una correlazione con il numero utilizzato in emergenza. Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione del funzionamento del sistema di protocollo. In questi casi, dovranno essere compilati in ogni loro parte e firmati, i Moduli di Registrazione di Emergenza.

Qualora l'interruzione del funzionamento del sistema di protocollo si prolunghi per più di ventiquattro ore, il Responsabile della gestione documentale, ai sensi della normativa vigente, autorizza l'uso del registro di emergenza per periodi successivi di non più di una settimana; in tali casi sul registro di emergenza, oltre alle informazioni di cui sopra, vengono riportati gli estremi del provvedimento di autorizzazione.

---

[54] "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*", emanate dall'AgID.

[55] L'art. 63 del D.P.R. 445/2000 prevede che "*1. Il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi autorizza lo svolgimento anche manuale delle operazioni di registrazione di protocollo su uno o più registri di emergenza, ogni qualvolta per cause tecniche non sia possibile utilizzare la normale procedura informatica. Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema. 2. Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre ventiquattro ore, per cause di eccezionale gravità, il responsabile per la tenuta del protocollo può autorizzare l'uso del registro di emergenza per periodi successivi di non più di una settimana. Sul registro di emergenza vanno riportati gli estremi del provvedimento di autorizzazione. 3. Per ogni giornata di registrazione di emergenza è riportato sul registro di emergenza il numero totale di operazioni registrate manualmente. 4. La sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'area organizzativa omogenea. 5. Le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico, utilizzando un'apposita funzione di recupero dei dati, senza ritardo al ripristino delle funzionalità del sistema. Durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, che provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza".*

Firmato digitalmente da ROBERTO FRACCIA

5.8. REGISTRI PARTICOLARI

All'interno dell'Istituzione scolastica sono istituiti registri particolari che possono essere sottratti alla consultazione da parte di chi non sia espressamente abilitato e per i quali possono essere previste particolari forme di riservatezza e di accesso. Su questi registri vanno caricati solo i documenti informatici o le immagini dei documenti cartacei secondo le istruzioni presenti sul decreto istitutivo del registro particolare in parola che deve essere integralmente riportato nel presente manuale.

I documenti che sono soggetti a particolare registrazione dell'Istituzione scolastica e che, ai sensi dell'art. 53, comma 5, del D.P.R. 445/2000, sono esclusi dalla protocollazione sono definiti nel presente manuale, con indicazione della modalità di gestione dei relativi registri.

Sono soggetti a registrazione particolare i seguenti documenti: [*tipologia documenti*].

[Nell'Istituzione scolastica possono essere sono soggetti a registrazione particolare, a titolo esemplificativo:

- *le delibere del Consiglio d'Istituto e del Collegio dei docenti;*
- *i verbali del Consiglio d'Istituto, della Giunta esecutiva, del Collegio dei docenti, dei Consigli di classe*
- *i decreti del Dirigente Scolastico;*
- *i diplomi;*
- *i certificati rilasciati dall'Istituzione scolastica (es. di iscrizione).]*

Per la gestione del trattamento delle registrazioni particolari informatiche vengono individuati i seguenti registri: [*denominazione registri*].

Di seguito si descrivono le modalità di gestione dei registri sopra elencati: [*modalità di gestione dei registri*].

5.9. ANNULLAMENTO DELLE REGISTRAZIONI DI PROTOCOLLO

La necessità di modificare anche un solo campo tra quelli obbligatori della registrazione di protocollo registrato in forma non modificabile, per correggere errori verificatisi in sede di immissione manuale di dati o attraverso l'interoperabilità dei sistemi di protocollo mittente e destinatario, comporta l'obbligo di annullare l'intera registrazione di protocollo.

Solo il Responsabile della gestione documentale è autorizzato ad annullare ovvero a dare disposizioni di annullamento delle registrazioni di protocollo. L'annullamento di una registrazione di protocollo deve essere richiesto con specifica e-mail, adeguatamente motivata, indirizzata al Responsabile della gestione documentale che, solo a seguito della valutazione della particolare questione, può autorizzare l'annullamento stesso.

Le informazioni annullate devono rimanere memorizzate nella base di dati per essere sottoposte alle elaborazioni previste dalla procedura. In tale ipotesi, la procedura per indicare l'annullamento riporta la dicitura "annullato" in posizione sempre visibile e tale, comunque, da consentire la lettura di tutte le informazioni originarie unitamente alla data, all'identificativo dell'operatore ed agli estremi del provvedimento d'autorizzazione. Il sistema registra l'avvenuta rettifica, la data e il soggetto che è intervenuto.

Al momento dell'annullamento di una registrazione di protocollo generale l'applicativo richiede la motivazione e gli estremi del provvedimento di annullamento.

5.10. MODALITÀ DI SVOLGIMENTO DEL PROCESSO DI SCANSIONE

Il processo di scansione si articola nelle seguenti fasi:

- acquisizione delle immagini in modo tale che ad ogni documento, anche composto da più pagine, corrisponda un unico *file* in un formato *standard* abilitato alla conservazione;

Firmato digitalmente da ROBERTO FRACCIA

- verifica della correttezza dell'acquisizione delle immagini e della esatta corrispondenza delle immagini ottenute con gli originali cartacei;
- collegamento delle immagini alla rispettiva registrazione di protocollo, in modo non modificabile;
- memorizzazione delle immagini, in modo non modificabile.

In linea con la certificazione di processo[56], l'operatore di protocollo, a valle del processo di scansione, attesta la conformità del documento scansionato al documento originale.

In breve, la conformità della copia per immagine su supporto informatico di un documento analogico è garantita mediante:[57]

- attestazione di un pubblico ufficiale;
- apposizione della firma digitale o firma elettronica qualificata o firma elettronica avanzata o altro tipo di firma ai sensi dell'art. 20, comma 1-*bis*, ovvero del sigillo elettronico qualificato o avanzato da parte di chi effettua il raffronto.

L'attestazione di conformità delle copie può essere inserita nel documento informatico contenente la copia per immagine o essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine.

Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o firma elettronica qualificata o avanzata del notaio o del pubblico ufficiale a ciò autorizzato.

In ogni caso non vengono riprodotti in formato immagine i documenti che per caratteristiche fisiche non possono essere sottoposti a scansione (formati non *standard* o particolarmente voluminosi).

Si precisa che qualora debbano essere protocollati documenti contenenti categorie particolari di dati personali di cui all'art. 9 del Regolamento UE 679/2016, l'operatore di protocollo, dotato delle necessarie abilitazioni, dovrà contrassegnare il documento come contenente dati riservati[58].

6. ACCESSO, TRASPARENZA E PRIVACY

6.1. TUTELA DEI DATI PERSONALI E MISURE DI SICUREZZA

Il sistema di gestione documentale dell'Istituzione scolastica deve adottare un meccanismo di *compliance* e rispetto della normativa in materia di protezione dei dati personali, ai sensi del Reg. UE 679/2016 e del D.Lgs. 196/2003, modificato dal D.Lgs. 101/2018[59].

L'Istituzione scolastica deve intraprendere iniziative volte ad ottemperare a quanto previsto dal Regolamento UE 679/2016, con particolare riferimento:

- al principio di liceità del trattamento dei dati;

[56] Si vedano, in merito, gli articoli 22, comma 1-*bis*, e 23-*ter*, comma 1-*bis*, del CAD e l'Allegato 3 alle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" emanate dall'AgID.
[57] Art. 22 del CAD.
[58] Per ulteriori approfondimenti, si veda il par. "6.1 – Tutela dei dati personali e misure di sicurezza".
[59] "*Le Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" emanate dall'AgID, stabiliscono che "[…] *il responsabile della gestione documentale ovvero, ove nominato, il coordinatore della gestione documentale, in accordo con il responsabile della conservazione di cui al paragrafo 4.6, con il responsabile per la transizione digitale e acquisito il parere del responsabile della protezione dei dati personali, predispone il piano della sicurezza del sistema di gestione informatica dei documenti, prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali, ai sensi dell'art. 32 del Regolamento UE 679/2016 (GDPR), anche in funzione delle tipologie di dati trattati, quali quelli riferibili alle categorie particolari di cui agli artt. 9-10 del Regolamento stesso.*".

Firmato digitalmente da ROBERTO FRACCIA

- al principio di minimizzazione del trattamento dei dati[60];
- all'esercizio dei diritti di cui agli artt. 15-22 del GDPR da parte degli interessati;
- alle modalità del trattamento e ai requisiti dei dati;
- all'informativa fornita agli interessati ed al relativo consenso quando dovuto;
- all'analisi dei rischi sui diritti e le libertà dei soggetti interessati;
- all'individuazione del Responsabile della protezione dei dati;
- all'individuazione dei Soggetti autorizzati al trattamento dei dati;
- all'analisi dei rischi sui diritti e le libertà dei soggetti interessati;
- alle misure di sicurezza[61].

Fatto salvo quanto sopra, particolare rilevanza assume il concetto di *accountability* e la capacità di adottare un processo efficace per la protezione dei dati, affinché si riduca al minimo il rischio di una loro possibile violazione.

A tal fine, il Responsabile della gestione documentale, in accordo con il Responsabile della conservazione, con il Responsabile per la transizione digitale, e acquisito il parere del Responsabile della protezione dei dati personali, predispone il piano della sicurezza del sistema di gestione informatica dei documenti, prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali, ai sensi dell'art. 32 del Reg. UE 679/2016, anche in funzione delle tipologie di dati trattati, quali quelli riferibili alle categorie particolari di cui agli artt. 9-10 del Regolamento stesso.

Sul punto, il Garante della *privacy* nel Parere sullo schema di "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" del 13 febbraio 2020, ha evidenziato che il mero rinvio alle misure di cui alla circolare AgID del 18 aprile 2017, n. 2/2017, nell'ambito dei requisiti di sicurezza cui sono tenuti i vari soggetti coinvolti nel trattamento, non è di per sé sufficiente ad assicurare l'adozione di misure di sicurezza del trattamento adeguate, in conformità al Regolamento, a norma del quale, occorre invece valutare, in concreto, i rischi che possono derivare, in particolare, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

L'Istituzione scolastica è tenuta ad adottare, pertanto, idonee e preventive misure di sicurezza, volte a custodire i dati personali trattati, in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

Nello specifico, le misure di carattere tecnico/organizzativo adottate dall'Istituzione scolastica sono le seguenti: [*elenco delle misure adottate*].

[Le misure di carattere tecnico/organizzativo possono comprendere, se del caso e a titolo esemplificativo:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

[60] Art. 5, comma 1, lett. c), del Regolamento UE 679/2016.
[61] Le misure di sicurezza devono "*garantire un livello di sicurezza adeguato al rischio*" del trattamento; in questo senso l'art. 32 par. 1 del Regolamento UE 679/2016 offre una lista aperta e non esaustiva.

Firmato digitalmente da ROBERTO FRACCIA

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.]

6.2. DIRITTO DI ACCESSO AGLI ATTI

6.2.1. ACCESSO DOCUMENTALE

Per diritto di accesso si intende, ai sensi dell'art. 22, comma 1, lett. a), della L. 241/1990, "*il diritto degli interessati di prendere visione e di estrarre copia di documenti amministrativi*".

Gli istanti devono essere portatori di un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento amministrativo e ai documenti connessi.

Gli interessati devono effettuare una richiesta di accesso motivata, essendo necessaria una valutazione oggettiva circa la posizione dell'istante per verificare l'esistenza di un nesso di strumentalità rispetto ad una situazione giuridicamente tutelata e collegata al documento al quale è richiesto l'accesso.

Il diritto di accesso è escluso per[62]:

- i documenti coperti dal segreto di Stato;
- i procedimenti tributari;
- l'attività della Pubblica Amministrazione diretta all'emanazione di atti normativi o amministrativi generali;
- i procedimenti selettivi contenenti informazioni di carattere psicoattitudinale.

Il diritto all'accesso ai documenti amministrativi è prioritario rispetto al diritto alla riservatezza in tutti quei casi in cui l'istanza ostensiva sia preordinata alla tutela e alla difesa dei propri interessi giuridici.

L'Istituzione scolastica deve effettuare una valutazione oggettiva circa la posizione dell'istante per verificare l'esistenza di un nesso di strumentalità rispetto ad una situazione giuridicamente tutelata e collegata al documento al quale è richiesto l'accesso, tenendo conto altresì di quanto previsto eventualmente nello specifico regolamento per l'accesso documentale, adottato dalla scuola, in conformità alle previsioni contenute nella delibera ANAC 1309/2016.

Per quanto afferisce ai profili *privacy*, il D.Lgs. 196/2003 all'art. 59, rubricato "*Accesso a documenti amministrativi e accesso civico*" prevede che "*1. Fatto salvo quanto previsto dall'articolo 60, i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990, n. 241, e successive modificazioni e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò che concerne i tipi di dati di cui agli articoli 9 e 10 del regolamento e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso.".*

In breve, si rileva che rispetto ai[63]*:*

- *Dati personali:* il diritto all'accesso ai documenti amministrativi può prevalere sull'interesse alla riservatezza, nel rispetto del principio di minimizzazione;
- *Dati cc.dd. sensibili e giudiziari:* il diritto all'accesso prevale solo laddove sia strettamente indispensabile;
- *Dati cc.dd. sensibilissimi (dati genetici e/o idonei a rivelare lo stato di salute e la vita sessuale):* il diritto di accesso prevale esclusivamente se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi consiste in un diritto della personalità o in un altro diritto o libertà fondamentale.

[62] Art. 24, L. 241/1990.
63 Art. 24, comma 7, D. Lgs. 241/1990; Art. 59 e 60, D. Lgs. 196/2003.

Firmato digitalmente da ROBERTO FRACCIA

A tal proposito, nella gestione degli accessi e consultazione dei documenti detenuti dall'Istituzione scolastica, da parte di terzi, il Responsabile della gestione è tenuto ad informare in modo costante ed aggiornato il Responsabile della protezione dei dati personali.

In ogni caso, nell'ipotesi di accesso diretto ai propri archivi, l'Amministrazione titolare dei dati, rilascia all'Amministrazione procedente apposita autorizzazione in cui vengono indicati eventuali limiti e condizioni di accesso, volti ad assicurare la riservatezza dei dati personali ai sensi della normativa vigente anche mediante la stipula di apposite convenzioni di servizio.

Allo stesso modo, nel caso in cui sia effettuata una protocollazione riservata (come indicato nel paragrafo 5.8.), la visibilità completa del documento è possibile solo all'utente assegnatario per competenza e agli operatori di protocollo che hanno il permesso applicativo di protocollazione riservata (permesso associato al ruolo). Tutti gli altri utenti (seppure inclusi nella giusta lista di competenza) possono accedere solo ai dati di registrazione (ad esempio, progressivo di protocollo, data di protocollazione), mentre sono oscurati i dati relativi al profilo del protocollo (ad esempio, classificazione).

I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio o di una ricerca *full text*.

6.2.2. ACCESSO CIVICO GENERALIZZATO (FOIA)

Il diritto all'accesso civico generalizzato (FOIA) riguarda la possibilità di accedere a dati, documenti e informazioni detenuti dalle Pubbliche Amministrazioni ulteriori rispetto a quelli oggetto di pubblicazione obbligatoria previsti dal D.Lgs. 33/2013[64].

Le istanze possono essere presentate da chiunque, a prescindere da particolari requisiti di qualificazione, e senza necessità di motivazione.

L'accesso civico generalizzato è volto a:

- assicurare a chiunque l'accesso indipendentemente dalla titolarità di situazioni giuridiche soggettive;
- promuovere la partecipazione al dibattito pubblico;
- favorire forme diffuse di controllo sul perseguimento delle finalità istituzionali e sull'utilizzo delle risorse pubbliche.

Le Istituzioni scolastiche, al fine di esaminare le istanze, dovrebbero adottare anche adeguate soluzioni organizzative, quali, ad esempio, *"la concentrazione della competenza a decidere sulle richieste di accesso in un unico ufficio (dotato di risorse professionali adeguate, che si specializzano nel tempo, accumulando know how ed esperienza), che, ai fini istruttori, dialoga con gli uffici che detengono i dati richiesti*", come indicato nella Deliberazione ANAC 1309/2016[65].

Fatto salvo quanto sopra, le scuole destinatarie dell'istanza, devono emettere un provvedimento espresso e motivato nei successivi trenta giorni.

[64] L'accesso civico generalizzato è previsto dall'art. 5, comma 2, del D.Lgs. 33/2013 e si differenzia dall'accesso civico semplice di cui al comma 1 del medesimo articolo, il quale stabilisce che "*L'obbligo previsto dalla normativa vigente in capo alle pubbliche amministrazioni di pubblicare documenti, informazioni o dati comporta il diritto di chiunque di richiedere i medesimi, nei casi in cui sia stata omessa la loro pubblicazione*". Come precedentemente evidenziato, l'istanza di accesso civico, qualora abbia a oggetto dati, informazioni o documenti oggetto di pubblicazione obbligatoria ai sensi del D.Lgs. 33/2013, è presentata al Responsabile per la prevenzione della corruzione e della trasparenza.

[65] La Deliberazione ANAC n. 1309 del 28 dicembre 2016, recante "*Linee Guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 c. 2 del D.Lgs. 33/2013*" è stata adottata ai sensi dell'art. 5-*bis*, comma 6, del D.Lgs. 33/2013 il quale stabilisce che "*Ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui al presente articolo, l'Autorità nazionale anticorruzione, d'intesa con il Garante per la protezione dei dati personali e sentita la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, adotta linee guida recanti indicazioni operative*".

Firmato digitalmente da ROBERTO FRACCIA

Si rappresenta che l'accesso civico generalizzato è limitato qualora sia pregiudicato un interesse pubblico, ovvero:

- la sicurezza pubblica e l'ordine pubblico;
- la sicurezza nazionale;
- la difesa e le questioni militari;
- le relazioni internazionali;
- la politica e la stabilità finanziaria ed economica dello Stato;
- la conduzione di indagini sui reati e il loro perseguimento;
- il regolare svolgimento di attività ispettive.

L'Istituzione scolastica deve, altresì, effettuare un'attività valutativa con la tecnica del bilanciamento, caso per caso, tra l'interesse pubblico alla *disclosure* generalizzata e la tutela di interessi considerati validi dall'ordinamento. Il diniego è necessario per evitare un pregiudizio concreto alla tutela di uno dei seguenti interessi privati:

- protezione dei dati personali;
- libertà e segretezza della corrispondenza;
- interessi economici e commerciali, inclusi la proprietà intellettuale, il diritto d'autore e i segreti commerciali[66].

Sulle richieste di riesame presentate dai richiedenti ai quali sia stato negato totalmente o parzialmente l'accesso o che non abbiano avuto risposta entro il termine stabilito, il Responsabile per la prevenzione della corruzione e della trasparenza decide con provvedimento motivato, entro il termine di venti giorni.

Qualora l'accesso sia stato negato o differito per esigenze di tutela della protezione dei dati personali, il Responsabile della prevenzione della corruzione e della trasparenza, fatto salvo il confronto con il RPD, deve provvedere, sentito il Garante per la protezione dei dati personali, il quale si pronuncia entro il termine di dieci giorni dalla richiesta.

Il termine per l'adozione del provvedimento da parte del RPCT è sospeso fino alla ricezione del parere del Garante e comunque per un periodo non superiore ai predetti dieci giorni[67].

Nei casi di risposta negativa o parzialmente negativa sopra elencati, l'Istituzione scolastica è tenuta, ad ogni modo, a una congrua e completa motivazione.

Specifiche indicazioni e raccomandazioni operative sul FOIA sono contenute nella Circolare del Ministro per la Semplificazione e la Pubblica Amministrazione n. 2/2017 avente ad oggetto "*Attuazione delle norme sull'accesso civico generalizzato (c.d. FOIA)*", in particolare:

- uffici competenti;
- tempi di decisione;
- controinteressati;
- rifiuti non consentiti;
- dialogo con i richiedenti;
- Registro degli accessi.

Il 28 giugno 2019 il Ministero della Pubblica Amministrazione ha adottato, inoltre, la circolare n. 1/2019 allo scopo di fornire alle Pubbliche Amministrazioni "*indirizzi e chiarimenti*" ulteriori rispetto alle

[66] Si vedano, sul punto, l'art. 5-*bis* del D.Lgs. 33/2013 e la Deliberazione ANAC 1309/2016.
[67] Art. 5, comma 7, del D.Lgs. 33/2013.

Firmato digitalmente da ROBERTO FRACCIA

"*raccomandazioni operative*" di cui alla circolare n. 2/2017 ed alle Linee Guida dell'ANAC adottate d'intesa con il Garante per la protezione dei dati personali nel 2016. I profili trattati riguardano:

- criteri applicativi di carattere generale;
- regime dei costi;
- notifica ai controinteressati;
- partecipazione dei controinteressati alla fase di riesame;
- termine per proporre l'istanza di riesame;
- strumenti tecnologici di supporto.

6.2.3. REGISTRO DEGLI ACCESSI

Il registro delle richieste di accesso presentate per tutte le tipologie di accesso è istituito presso l'Istituzione scolastica, in conformità a quanto stabilito dai già citati documenti, ovvero, la Deliberazione ANAC n. 1309/2016, nonché dalla Circolare del Ministro per la Pubblica Amministrazione n. 2/2017, e dalla successiva Circolare del Ministro per la Pubblica Amministrazione n. 1/2019.

Il registro è costituito attraverso la raccolta organizzata delle richieste con l'indicazione dell'oggetto, della data e del relativo esito (con data della decisione), il quale sarà pubblicato sul sito istituzionale dell'Istituzione scolastica con cadenza trimestrale. L'implementazione del registro avviene mediante l'utilizzo del sistema di protocollo informatico e dei flussi documentali di cui è dotata l'Istituzione scolastica ai sensi del D.P.R. n. 445 del 2000, del CAD e delle relative regole tecniche.

Firmato digitalmente da ROBERTO FRACCIA