Ministero dell'Istruzione, dell'Università e della Ricerca

N.4 - FEDERIGO TOZZI - SIENA

Manuale di Gestione

Del Protocollo Informatico – sezione a)

Art. 5 DPMC 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 - Pubblicato in Gazzetta Ufficiale n. 59 del 12 marzo 2014 - supplemento ordinario

1. Principi generali

1.1 PREMESSA

Il decreto del Presidente del Consiglio dei Ministri del 31 ottobre 2000 concernente le "Regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica del 20 ottobre 1998 n. 428", all'art. 3, comma 1, lettera c) – come confermato dal decreto del Presidente del Consiglio dei Ministri del 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" – prevede per tutte le amministrazioni di cui all'art. 2 del decreto legislativo 30 marzo 2001, n. 165, l'adozione del Manuale di gestione del Protocollo.

Quest'ultimo, disciplinato dal successivo art. 5, comma 1, "descrive il sistema di gestione e di conservazione dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio".

In questo ambito è previsto che ogni amministrazione pubblica individui una o più Aree Organizzative Omogenee, all'interno delle quali sia nominato un responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'art. 50, comma 4 del Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa decreto – del Presidente della Repubblica n. 445 del 20 dicembre 2000 (già art.12 del citato DPR n. 428 del 20 ottobre 1998).

Obiettivo del Manuale di gestione è descrivere sia il sistema di gestione documentale a partire dalla fase di protocollazione della corrispondenza in ingresso e in uscita e di quella interna, sia le funzionalità disponibili agli addetti al servizio e ai soggetti esterni che a diverso titolo interagiscono con l'amministrazione.

Il protocollo informatico, anche con le sue funzionalità minime, costituisce l'infrastruttura di base tecnico-funzionale su cui avviare il processo di ammodernamento e di trasparenza dell'amministrazione.

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.

Il presente documento pertanto si rivolge non solo agli operatori di protocollo ma, in generale, a tutti i dipendenti e ai soggetti esterni che si relazionano con l'amministrazione.

Esso disciplina:

- la migrazione dei flussi cartacei verso quelli digitali, ovvero in via transitoria, i flussi cartacei in rapporto al protocollo informatico;
- i livelli di esecuzione, le responsabilità ed i metodi di controllo dei processi e delle azioni amministrative;
- l'uso del titolario di classificazione e del massimario di selezione e di scarto;
- le modalità di accesso alle informazioni da parte di coloro che ne hanno titolo ed interesse, in attuazione del principio di trasparenza dell'azione amministrativa.

Il Manuale è articolato in due parti, nella prima vengono indicati l'ambito di applicazione, le definizioni usate e i principi generali del sistema, nella seconda sono descritte analiticamente le procedure di gestione dei documenti e dei flussi documentali.

1.2 AMBITO DI APPLICAZIONE DEL MANUALE

Il presente Manuale di gestione del protocollo, dei documenti e degli archivi è adottato ai sensi dell'art. 3, comma c) del decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000 e successive modificazioni ed integrazioni, recante le regole tecniche per il protocollo informatico.

Esso descrive le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione

dei documenti, oltre che la gestione dei flussi documentali ed archivistici in relazione ai procedimenti amministrativi dell'amministrazione.
Attraverso l'integrazione con le procedure di gestione dei procedimenti amministrativi, di accesso agli atti ed alle informazioni e di archiviazione dei documenti, il protocollo informatico realizza le condizioni operative per una più efficiente gestione del flusso informativo e documentale interno dell'amministrazione anche ai fini dello snellimento delle procedure e della trasparenza dell'azione amministrativa.
Il protocollo fa fede, anche con effetto giuridico, dell'effettivo ricevimento e spedizione di un documento.

1.3 DEFINIZIONI E NORME DI RIFERIMENTO

Ai fini del presente Manuale si intende:

- per "amministrazione", N.4 - FEDERIGO TOZZI - SIENA;
- per "Testo Unico", il decreto del Presidente della Repubblica 20 dicembre 2000 n. 445 Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- per Regole tecniche, il 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.
- per Codice, il decreto legislativo 7 marzo 2005 n. 82 – Codice dell'amministrazione digitale – come integrato e corretto nel decreto legislativo 235/2010

Si riportano, di seguito, gli acronimi utilizzati più frequentemente:

- **AOO** Area Organizzativa Omogenea;
- **MdG** Manuale di Gestione del protocollo informatico e gestione documentale e degli archivi;
- **RPA** Responsabile del Procedimento Amministrativo il dipendente che ha la responsabilità dell'esecuzione degli adempimenti amministrativi relativi ad un affare;
- **RSP** Responsabile del Servizio per la tenuta del Protocollo informatico, la gestione dei flussi documentali e degli archivi;
- **PdP** Prodotto di Protocollo informatico – l'applicativo sviluppato o acquisito all'amministrazione /AOO per implementare il servizio di protocollo informatico;
- **UOP** Unità Organizzative di registrazione di Protocollo – rappresentano gli uffici che svolgono attività di registrazione di protocollo;
- **UOR** Uffici Organizzativi di Riferimento – un 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;
- **UU** Ufficio Utente – un ufficio dell'AOO che utilizza i servizi messi a disposizione dal sistema di protocollo informatico; ovvero il soggetto destinatario del documento, così come risulta dalla segnatura di protocollo nei campi opzionali.

Per le Norme ed i Regolamenti di riferimento vedasi l'elenco riportato in *Normativa di riferimento*, nell'allegato al presente MdG

1.4 AREE ORGANIZZATIVE OMOGENEE E MODELLI ORGANIZZATIVI

Per la gestione dei documenti, l'amministrazione individua un'unica Area Organizzativa Omogenea (AOO), composta dall'insieme di tutti gli UOP/UOR/UU articolati come riportato in *area organizzativa omogena e modello organizzativo*, allegato al presente MdG.
All'interno della AOO il sistema di protocollazione è unico.
Nell'unica AOO è istituito un servizio per la tenuta del protocollo informatico, la gestione dei flussi

documentali e degli archivi.
Nel medesimo allegato sono riportati la denominazione, il codice identificativo della AOO e l'insieme degli UOR che la compongono con la loro articolazione in UU.
All'interno della AOO il sistema di protocollazione è totalmente distribuito per la corrispondenza in entrata e in uscita; pertanto ogni UOR svolge anche i compiti di UOP.
L'allegato *area organizzativa omogena e modello organizzativo* è suscettibile di modifica in caso di inserimento di nuove UOP/UOR/UU o di riorganizzazione delle medesime.
Le modifiche sono proposte ai vertici dell'amministrazione dal RSP d'intesa con il responsabile del sistema informativo e con il responsabile della tutela dei dati personali. L'amministrazione si riserva la facoltà di autorizzare, in via transitoria e del tutto eccezionale, altri UOR allo svolgimento dell'attività di protocollazione.
Tale "decentramento" da un punto di vista operativo segue le indicazioni stabilite nel presente Manuale e sarà sottoposto al controllo del responsabile del protocollo informatico. Nelle UOR sarà utilizzato il medesimo sistema di numerazione di protocollo e l'operatore incaricato dell'attività di protocollazione dovrà essere abilitato dal RSP che ha anche il compito di vigilare sulla corretta esecuzione delle attività.

1.5 SERVIZIO PER LA GESTIONE INFORMATICA DEL PROTOCOLLO

In ogni AOO precedentemente individuata è istituito un servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi.
Alla guida del suddetto servizio è posto il Responsabile del Servizio di Protocollo informatico, della gestione dei flussi documentali e degli archivi (di seguito RSP).
Egli è funzionalmente individuato, e nominato con atto riportato nell'allegato del MdG *Nomina del Responsabile del Servizio per la tenuta del Protocollo informatico, della gestione dei flussi documentali e degli archivi e del suo Vicario.*
Al servizio è preposto un dirigente ovvero un funzionario, 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.
L'atto che istituisce il servizio e individua il responsabile per ciascuna AOO è riportato nell'allegato indicato, unitamente:

- alla denominazione del servizio;
- al nominativo del RSP;
- alla descrizione dei compiti assegnati al RSP;
- al nominativo del vicario del RSP nei casi di vacanza, assenza o impedimento di questi.

È compito del servizio:

- predisporre lo schema del Manuale di gestione del protocollo informatico con la descrizione dei criteri e delle modalità di revisione del medesimo;
- provvedere alla pubblicazione del Manuale (eventualmente anche sul sito Internet dell'amministrazione);
- proporre i tempi, le modalità e le misure organizzative e tecniche finalizzate alla eliminazione dei protocolli di settore e di reparto, dei protocolli multipli, dei protocolli di telefax e, più in generale, dei protocolli diversi dal protocollo informatico;
- predisporre il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici;
- abilitare gli addetti dell'amministrazione all'utilizzo del PdP e definire per ciascuno di essi il tipo di funzioni disponibili (ad esempio consultazione, modifica ecc.);
- garantire il rispetto delle disposizioni normative durante le operazioni di registrazione e di segnatura

di protocollo;

- garantire la corretta produzione e conservazione del registro giornaliero di protocollo;
- garantire la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti dalla AOO attraverso l'adozione dei formati standard previsti dalla normativa vigente;
- curare le funzionalità del sistema affinché, in caso di guasti o anomalie, siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
- garantire il buon funzionamento degli strumenti e il rispetto delle procedure concernenti le attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso dall'esterno e le attività di gestione degli archivi;
- autorizzare le operazioni di annullamento della registrazione di protocollo;
- aprire e chiudere il registro di protocollazione di emergenza.

1.6 CONSERVAZIONE DEI DOCUMENTI

Nell'ambito del servizio di gestione informatica del protocollo, al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro informatico di protocollo, entro la giornata lavorativa successiva, come previsto dal DPCM del 3 dicembre 2013 viene inviato al conservatore accreditato incaricato del servizio.
Le procedure di riversamento, predisposte dal RSP, sono illustrate nel piano di sicurezza del MdG.

1.7 FIRMA DIGITALE

Per l'espletamento delle attività istituzionali e per quelle connesse all'attuazione delle norme di gestione del protocollo informatico, di gestione documentale e di archivistica, l'amministrazione fornisce la firma digitale o elettronica qualificata ai soggetti da essa delegati a rappresentarla.
Nell'allegato *Elenco delle persone titolari di firma digitale* viene riportato l'elenco delle persone titolari di firma digitale e delle deleghe ricevute per la sottoscrizione di documenti digitali dell'amministrazione.

1.8 TUTELA DEI DATI PERSONALI

L'amministrazione titolare dei dati di protocollo e dei dati personali comuni, sensibili e/o giudiziari contenuti nella documentazione amministrativa di propria pertinenza dà attuazione al dettato del decreto legislativo 30 giugno 2003 n. 196 con atti formali aventi rilevanza interna ed esterna.

- Relativamente agli adempimenti interni specifici, gli addetti autorizzati ad accedere al sistema di protocollo informatico e a trattare i dati di protocollo veri e propri, sono stati incaricati dal titolare dei dati e, se nominato, dal responsabile.
- Relativamente agli adempimenti esterni, l'amministrazione si è organizzata per garantire che i certificati ed i documenti trasmessi ad altre pubbliche amministrazioni riportino le sole informazioni relative a stati, fatti e qualità personali previste da leggi e regolamenti e strettamente necessarie per il perseguimento delle finalità per le quali vengono acquisite; inoltre l'amministrazione certificante, in caso di accesso diretto ai propri archivi, rilascia all'amministrazione procedente apposita autorizzazione in cui vengono indicati i limiti e le condizioni di accesso volti ad assicurare la riservatezza dei dati personali ai sensi della normativa vigente.

Le regole e le modalità operative stabilite dall'amministrazione sono riportate nel piano di sicurezza di cui al successivo capitolo 3.
In relazione alla protezione dei dati personali trattati al proprio interno l'amministrazione dichiara di aver ottemperato a quanto previsto dal decreto legislativo 30 giugno 2003, n. 196, con particolare riferimento:

- al principio di necessità nel trattamento dei dati;
- al diritto di accesso ai dati personali da parte dell'interessato;
- alle modalità del trattamento e ai requisiti dei dati;

- all'informativa fornita agli interessati ed al relativo consenso quando dovuto;
- alla nomina degli incaricati del trattamento, per gruppo o individualmente;
- alle misure minime di sicurezza.

1.9 CASELLE DI POSTA ELETTRONICA

L'AOO si dota di una casella di Posta Elettronica Certificata istituzionale per la corrispondenza, sia in ingresso che in uscita, pubblicata sull'Indice delle Pubbliche Amministrazioni (IPA) e di due caselle di Posta Elettronica Ordinaria. Tali caselle costituiscono l'indirizzo virtuale della AOO e di tutti gli uffici (UOR) che ad essa fanno riferimento.

1.10 SISTEMA DI CLASSIFICAZIONE DEI DOCUMENTI

Con l'inizio della attività operativa del protocollo unico viene adottato un unico titolario di classificazione per l'archivio centrale unico dell'amministrazione valido per tutte le AOO in cui è articolata l'amministrazione.

Si tratta di un sistema logico astratto che organizza i documenti secondo una struttura ad albero definita sulla base della organizzazione funzionale dell'AOO, permettendo di organizzare in maniera omogenea e coerente i documenti che si riferiscono ai medesimi affari o ai medesimi procedimenti amministrativi.

La definizione del sistema di classificazione è stata effettuata prima dell'avvio del sistema di protocollo informatico. Il contenuto della classificazione è dettagliatamente illustrato nel successivo capitolo 9.

1.11 FORMAZIONE

Nell'ambito dei piani formativi richiesti a tutte le amministrazioni dalla direttiva del Ministro per la semplificazione e la pubblica amministrazione sulla formazione e la valorizzazione del personale delle pubbliche amministrazioni, l'amministrazione provvederà eventualmente a stabilire percorsi formativi specifici e generali che coinvolgono tutte le figure professionali.

1.12 PROCEDURE INTEGRATIVE DI CONSERVAZIONE SOSTITUTIVA

Per l'esecuzione del processo di conservazione sostitutiva dei documenti l'amministrazione si uniforma alle modalità previste dai DPCM 3/12/2013 e 13/11/2014. Prima di adottare eventuali accorgimenti e procedure integrative, anche successivamente all'avvio del processo di conservazione sostitutiva dei documenti, l'amministrazione comunica all'AGID le procedure integrative che intende adottare ai sensi dell'art. 7 della deliberazione CNIPA n. 11/2004.

2. Eliminazione dei protocolli diversi dal protocollo informatico

Il presente capitolo riporta la pianificazione, le modalità e le misure organizzative e tecniche finalizzate alla eliminazione dei protocolli diversi dal protocollo informatico.

2.1 PIANO DI ATTUAZIONE

In coerenza con quanto previsto e disciplinato, tutti i documenti inviati e ricevuti dall'amministrazione sono registrati all'interno del registro di protocollo informatico. Pertanto tutti i registri particolari di protocollo sono aboliti ed eliminati.

Il piano di attuazione del protocollo informatico prevede l'eliminazione dei diversi protocolli di settore, di reparto e multipli. A tal fine sono state svolte le seguenti attività:

- censimento preliminare dei diversi protocolli esistenti;

- analisi dei livelli di automazione;
- definizione degli interventi organizzativi, procedurali e tecnici da effettuare per adottare il protocollo informatico;
- valutazione dei tempi di sostituzione;
- stima dei costi derivanti.

Le informazioni raccolte ed il piano di azione che ne è derivato, riportato nell'allegato *Piano di eliminazione dei protocolli diversi dal protocollo informatico*, tengono conto della realtà organizzativa dell'AOO e della necessità di gestire la fase transitoria connessa con l'esaurimento delle pratiche in essere, protocollate e gestite anteriormente all'avvio del sistema di protocollo informatico e gestione documentale di cui al presente Manuale.
Il RSP esegue comunque, periodicamente, dei controlli a campione sulla corretta esecuzione del piano e sull'utilizzo regolare di un unico registro di protocollo, verificando, attraverso controlli ed ispezioni mirate nelle varie UOP/UOR/UU, la validità dei criteri di classificazione utilizzati.

3. 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.

3.1 OBIETTIVI DEL PIANO DI SICUREZZA

Il piano di sicurezza garantisce che:

- i documenti e le informazioni trattati dall'amministrazione 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.

3.2 GENERALITÀ

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* e le successive modifiche e integrazioni, 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.
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 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 quadrimestrale durante la fase di esercizio;
- piano di continuità del servizio con particolare riferimento sia alla esecuzione del versamento dei dati in conservazione sostitutiva, sia alla capacità di ripristino del sistema informatico entro sette giorni in caso di disastro;
- conservazione, a cura di Aruba Posta Elettronica Certificata SPA, dei dati e dei documenti secondo le norme stabilite dal decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 e le successive modifiche e integrazioni;
- 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;
- uso di codici identificativi 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. Tali operazioni possono essere delegate a operatori esterni autorizzati o essere automatizzati dal PdP.

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.

3.3 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 di riferimento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- 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.

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.
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 ai DPCM 13 gennaio 2004, 3 dicembre 2013, 13 novembre 2014 e le successive integrazioni. L'esecuzione del processo di marcatura temporale avviene utilizzando le procedure previste dal certificatore accreditato, con le prescritte garanzie di sicurezza.

3.4 GESTIONE DEI DOCUMENTI INFORMATICI

Il sistema operativo del PdP utilizzato dall'amministrazione, 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;
- 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 sistema di gestione informatica dei documenti:

- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
- garantisce la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
- fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
- 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.

3.4.1 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 di sicurezza, dal punto di vista organizzativo, sono state individuate le seguenti funzioni specifiche:

Ogni utente viene riconosciuto nel sistema informatico in base a delle credenziali e viene garantito l'accesso alle sezioni del PdP tramite una profilatura multilivellare, che permette di assegnare ad ogni utente l'accesso e la visualizzazione solo dei documenti permessi, come previsto dall'art. 7 del 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.*

In relazione alla componente fisica della sicurezza si segnala che i documenti fisici sono salvati in serverfarm esterne, la cui protezione è affidata al gestore del servizio.

3.4.2 Gestione delle registrazioni di protocollo e di sicurezza

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;
- dalle registrazioni del PdP.

Le registrazioni di sicurezza sono soggette alle seguenti misure:

- Backup giornaliero dei log degli accessi e delle operazioni
- Creazione del registro protocollo giornaliero

In questa sede viene espressamente richiamato quanto indicato nell'ultimo capoverso del paragrafo 3.2 del presente Manuale.

3.5 TRASMISSIONE E 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 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 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.

3.5.1 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 AGID del 23 gennaio 2013, n. 60.

3.5.2 All'interno della AOO

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.

3.6 ACCESSO AI DOCUMENTI INFORMATICI

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. Queste, in sintesi, sono: la consultazione, l'inserimento, la modifica, l'annullamento e l'eliminazione del documento.
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.

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.

3.6.1 Utenti interni alla 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.
La gestione delle utenze rispetta i seguenti criteri operativi:
Il RSP ha il permesso di creare, modificare e associare agli utenti dei profili di sicurezza a livello di sotto area, garantendone quindi la visualizzazione o la modifica secondo i criteri stabiliti dal RSP stesso.

3.6.2 Accesso al registro di protocollo per utenti interni alla AOO

L'autorizzazione all'accesso ai registri di protocollo è regolata tramite i seguenti strumenti:

- verifica delle credenziali all'accesso al PdP.
- controllo dei profili ad ogni azione dell'utente.

La visibilità completa sul registro di protocollo è consentita solo agli utenti con il permesso di Gestione completa e profilati per la visualizzazione dei documenti riservati. Questi utenti hanno il permesso di operare al di sopra di tutte le aree e posso assegnare i documenti agli UOP.
L'utente assegnatario dei documenti protocollati è invece abilitato alla visualizzazione e all'archiviazione del documento.

Nel caso in cui sia effettuata la registrazione di un documento sul protocollo particolare, la visibilità completa del documento stesso è possibile solo a coloro il cui accesso garantisce la visualizzazione dei documenti riservati.
Tutti gli altri utenti possono accedere solo ai dati di registrazione e non possono accedere alla visione del documento.

3.6.3 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 i 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.

3.7 CONSERVAZIONE DEI DOCUMENTI INFORMATICI

La conservazione dei documenti informatici avviene con le modalità e con le tecniche specificate nel decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 e le successive integrazioni.

3.7.1 Servizio di conservazione sostitutiva

Il responsabile della conservazione sostitutiva 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.
Il responsabile della conservazione digitale:

- adotta le misure necessarie per garantire la sicurezza fisica e logica del sistema preposto al processo di conservazione, 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;

3.8 POLITICHE DI SICUREZZA ADOTTATE DALLA AOO

Le politiche di sicurezza, riportate nell'allegato omonimo, stabiliscono sia le misure preventive per la tutela e l'accesso al patrimonio informatico, 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 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 dall'AGID o a seguito dei risultati delle attività di *audit*.
In ogni caso, tale attività è svolta almeno con cadenza annuale.

4.Modalità di utilizzo di strumenti informatici per lo scambio di documenti

Il presente capitolo fornisce indicazioni sulle modalità di utilizzo di strumenti informatici per lo scambio di documenti all'interno ed all'esterno dell'AOO.
Prima di entrare nel merito, occorre caratterizzare l'oggetto di scambio: il documento amministrativo.
Nell'ambito del processo di gestione documentale, il documento amministrativo, in termini operativi, è classificabile in:

- ricevuto;
- inviato;
- interno formale;
- interno informale.

Il documento amministrativo, in termini tecnologici, è classificabile in:

- informatico;
- analogico.

Secondo quanto previsto dall'art. 40 del decreto legislativo n. 82/2005 "1. Le pubbliche amministrazioni che dispongono di idonee risorse tecnologiche formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'articolo 71" e che "2. Fermo restando quanto previsto dal comma 1, la redazione di documenti originali su supporto cartaceo, nonché la copia di documenti informatici sul medesimo supporto è consentita solo ove risulti necessaria e comunque nel rispetto del principio dell'economicità".
Pertanto soprattutto nella fase transitoria di migrazione verso l'adozione integrale delle tecnologie digitali da parte dell'amministrazione, il documento amministrativo può essere disponibile anche nella forma analogica.

4.1 DOCUMENTO RICEVUTO

La corrispondenza in ingresso può essere acquisita dalla AOO con diversi mezzi e modalità in base alla tecnologia di trasporto utilizzata dal mittente.
Un documento informatico può essere recapitato:

1. a mezzo posta elettronica convenzionale o certificata;
2. tramite intranet
3. su supporto rimovibile quale, ad esempio, *CD ROM, DVD, floppy disk, tape, pen drive*, etc, consegnato direttamente alla UOP o inviato per posta convenzionale o corriere.

Un documento analogico può essere recapitato:

1. a mezzo posta convenzionale o corriere;
2. a mezzo posta raccomandata;
3. per telefax o telegramma;
4. con consegna diretta da parte dell'interessato o consegnato tramite una persona dallo stesso delegata alle UOP e/o agli UOR aperti al pubblico.

4.2 DOCUMENTO INVIATO

I documenti informatici, compresi di eventuali allegati, anch'essi informatici, sono inviati, di norma, per mezzo della posta elettronica convenzionale o certificata se la dimensione del documento non supera la dimensione massima prevista dal sistema di posta utilizzato dall'AOO.
In caso contrario, il documento informatico viene riversato, su supporto digitale rimovibile non modificabile e trasmesso con altri mezzi di trasposto al destinatario.

4.3 DOCUMENTO INTERNO FORMALE

I documenti interni sono formati con tecnologie informatiche e sottoposti a protocollazione ed archiviazione

4.4 DOCUMENTO INTERNO INFORMALE

Per questa tipologia di corrispondenza vale quanto illustrato nel paragrafo precedente ad eccezione della obbligatorietà dell'operazione di sottoscrizione e di protocollazione.
Per la formazione, la gestione e la sottoscrizione di documenti informatici aventi rilevanza esclusivamente interna ciascuna AOO può adottare, nella propria autonomia organizzativa, regole diverse da quelle contenute nelle regole tecniche vigenti. In questa eventualità, le diverse regole adottate saranno pubblicate nel presente MdG.

4.5 IL DOCUMENTO INFORMATICO

Il documento informatico è la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti; l'art. 20 del decreto legislativo del 30 dicembre 2010, n. 235, recante "Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69." prevede che:

"1. Il documento informatico da chiunque formato, la memorizzazione su supporto informatico e la trasmissione con strumenti telematici conformi alle regole tecniche di cui all'articolo 71 sono validi e rilevanti a tutti gli effetti di legge, ai sensi delle disposizioni del presente codice.
1-bis. L'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dall'articolo 21.

2 [abrogato]

3. Le regole tecniche per la trasmissione, la conservazione, la copia, la duplicazione, la riproduzione e la validazione temporale dei documenti informatici, nonché quelle in materia di generazione, apposizione e verifica di qualsiasi tipo di firma elettronica avanzata, sono stabilite ai sensi dell'articolo 71. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle regole tecniche sulla validazione temporale.

4. Con le medesime regole tecniche sono definite le misure tecniche, organizzative e gestionali volte a garantire l'integrità, la disponibilità e la riservatezza delle informazioni contenute nel documento informatico".

4.6 IL DOCUMENTO ANALOGICO CARTACEO

Per documento analogico si intende un documento amministrativo "*formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta (esempio: documenti cartacei), come le immagini su film (esempio: pellicole mediche, microfiches, microfilm), come le magnetizzazioni su nastro (esempio: cassette e nastri magnetici audio e video) su supporto non digitale*". Di seguito faremo riferimento ad un documento amministrativo cartaceo che può essere prodotto sia in maniera tradizionale (come, ad esempio, una lettera scritta a mano o a macchina), sia con strumenti informatici (ad esempio, una lettera prodotta tramite un sistema di videoscrittura o text editor) e poi stampato.
In quest'ultimo caso 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 destinatario, stampato su carta intestata e dotato di firma autografa.
Un documento analogico può essere convertito in documento informatico tramite opportune procedure di conservazione sostitutiva, descritte nel seguito del Manuale.

4.7 FORMAZIONE DEI DOCUMENTI – ASPETTI OPERATIVI

I documenti dell'amministrazione sono prodotti con sistemi informatici come previsto dalla vigente normativa.
Ogni documento formato per essere inoltrato all'esterno o all'interno in modo formale:

- tratta un unico argomento indicato in maniera sintetica ma esaustiva a cura dell'autore nello spazio riservato all'oggetto;
- è riferito ad un solo protocollo;
- può far riferimento a più fascicoli.

Le regole per la determinazione dei contenuti e della struttura dei documenti informatici sono definite dai responsabili dei singoli UOR.
Il documento deve consentire l'identificazione dell'amministrazione mittente attraverso le seguenti informazioni:

- la denominazione e il logo dell'amministrazione;
- l'indicazione completa della AOO e dell'UOR che ha prodotto il documento;
- l'indirizzo completo dell'amministrazione (via, numero, CAP, città, provincia);
- il numero di telefono della UOR;
- il codice fiscale dell'amministrazione.

Il documento deve inoltre recare almeno le seguenti informazioni:

- luogo di redazione del documento;
- la data, (giorno, mese, anno);
- il numero di protocollo;
- il numero degli allegati, se presenti;
- l'oggetto del documento;
- e trattasi di documento digitale, firma elettronica avanzata o qualificata da parte dell'istruttore del documento e sottoscrizione digitale del RPA e/o del responsabile del provvedimento finale;
- se trattasi di documento cartaceo, sigla autografa dell'istruttore e sottoscrizione autografa del Responsabile del Procedimento Amministrativo (RPA) e/o del responsabile del provvedimento finale.

Per agevolare il processo di formazione dei documenti informatici e consentire, al tempo stesso, la trattazione automatica dei dati in essi contenuti, l'AOO rende disponibili per via telematica moduli e formulari elettronici validi ad ogni effetto di legge.

4.8 SOTTOSCRIZIONE DI DOCUMENTI INFORMATICI

La sottoscrizione dei documenti informatici, quando prescritta, è ottenuta con un processo di firma digitale conforme alle disposizioni dettate dalla normativa vigente. L'amministrazione, quando non si configura come autorità di certificazione, si avvale dei servizi di una autorità di certificazione accreditata, iscritta nell'elenco pubblico dei certificatori accreditati tenuto dall'AGID.
I documenti informatici prodotti dall'amministrazione, indipendentemente dal software utilizzato per la loro redazione, prima della sottoscrizione con firma digitale, sono convertiti in uno dei formati standard previsti dalla normativa vigente in materia di archiviazione al fine di garantirne l'immodificabilità (vedi art. 3 comma 3 del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004).

4.9 REQUISITI DEGLI STRUMENTI INFORMATICI DI SCAMBIO

Scopo degli strumenti informatici di scambio e degli standard di composizione dei messaggi è garantire sia l'interoperabilità, sia i requisiti minimi di sicurezza di seguito richiamati:

- l'integrità del messaggio;
- la riservatezza del messaggio;
- il non ripudio dei messaggi;
- l'automazione dei processi di protocollazione e smistamento dei messaggi all'interno delle AOO;
- l'interconnessione tra AOO, ovvero l'interconnessione tra le UOP/UOR e UU di una stessa AOO nel caso di documenti interni formali;
- la certificazione dell'avvenuto inoltro e ricezione;
- l'interoperabilità dei sistemi informativi pubblici.

4.10 FIRMA DIGITALE

Lo strumento che soddisfa i primi tre requisiti di cui al precedente paragrafo 4.9 è la firma digitale utilizzata per inviare e ricevere documenti da e per l'AOO e per sottoscrivere documenti, compresa la copia giornaliera del registro di protocollo e di riversamento, o qualsiasi altro "file" digitale con valenza giuridico-probatoria.
I messaggi ricevuti, sottoscritti con firma digitale, sono sottoposti a verifica di validità. Tale processo si realizza in modo conforme a quanto prescritto dalla normativa vigente (si vedano le norme pubblicate sul sito w ww.agid.gov.it).

4.11 USO DELLA POSTA ELETTRONICA CERTIFICATA

Lo scambio dei documenti soggetti alla registrazione di protocollo è effettuato mediante messaggi, codificati in formato XML, conformi ai sistemi di posta elettronica compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche RFC 821-822, RFC 2045-2049 e successive modificazioni o integrazioni.
Il rispetto degli standard di protocollazione, di controllo dei medesimi e di scambio dei messaggi garantisce l'interoperabilità dei sistemi di protocollo (cfr. par. 3.5 Trasmissione e interscambio dei documenti informatici).
Allo scopo di effettuare la trasmissione di un documento da una AOO a un'altra utilizzando l'interoperabilità dei sistemi di protocollo, è necessario eseguire le seguenti operazioni:

- redigere il documento con un sistema di videoscrittura;
- inserire i dati del destinatario (almeno denominazione, indirizzo, casella di posta elettronica);
- firmare il documento (e eventualmente associare il riferimento temporale al documento firmato) e inviare il messaggio contenente il documento firmato digitalmente alla casella interna del protocollo;
- assegnare il numero di protocollo in uscita al documento firmato digitalmente;
- inviare il messaggio contenente il documento firmato e protocollato in uscita alla casella di posta istituzionale del destinatario.

L'utilizzo della Posta Elettronica Certificata (PEC) consente di:

- firmare elettronicamente il messaggio;
- conoscere in modo inequivocabile la data e l'ora di trasmissione;
- garantire l'avvenuta consegna all'indirizzo di posta elettronica dichiarato dal destinatario;
- interoperare e cooperare dal punto di vista applicativo con altre AOO appartenenti alla stessa e ad altre amministrazioni.

Gli automatismi sopra descritti consentono, in prima istanza, la generazione e l'invio in automatico di "ricevute di ritorno" costituite da messaggi di posta elettronica generati dal sistema di protocollazione della AOO ricevente. Ciascun messaggio di ritorno si riferisce ad un solo messaggio protocollato.
I messaggi di ritorno, che sono classificati in:

- conferma di ricezione;

- notifica di eccezione;
- aggiornamento di conferma;
- annullamento di protocollazione;

sono scambiati in base allo stesso standard SMTP previsto per i messaggi di posta elettronica protocollati in uscita da una AOO e sono codificati secondo lo stesso standard MIME.
Il servizio di Posta Elettronica Certificata è strettamente correlato all'Indice della Pubblica Amministrazione, dove sono pubblicati gli indirizzi istituzionali di posta certificata associati alle AOO.
Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato. La data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico, redatto in conformità alla normativa vigente e alle relative regole tecniche sono opponibili ai terzi. La trasmissione del documento informatico per via telematica, con una modalità che assicuri l'avvenuta consegna, equivale alla notificazione per mezzo della posta nei casi consentiti dalla legge.

5. Descrizione del flusso di lavorazione dei documenti

Il presente capitolo descrive il flusso di lavorazione dei documenti ricevuti, spediti o interni, incluse le regole di registrazione per i documenti pervenuti secondo particolari modalità di trasmissione.

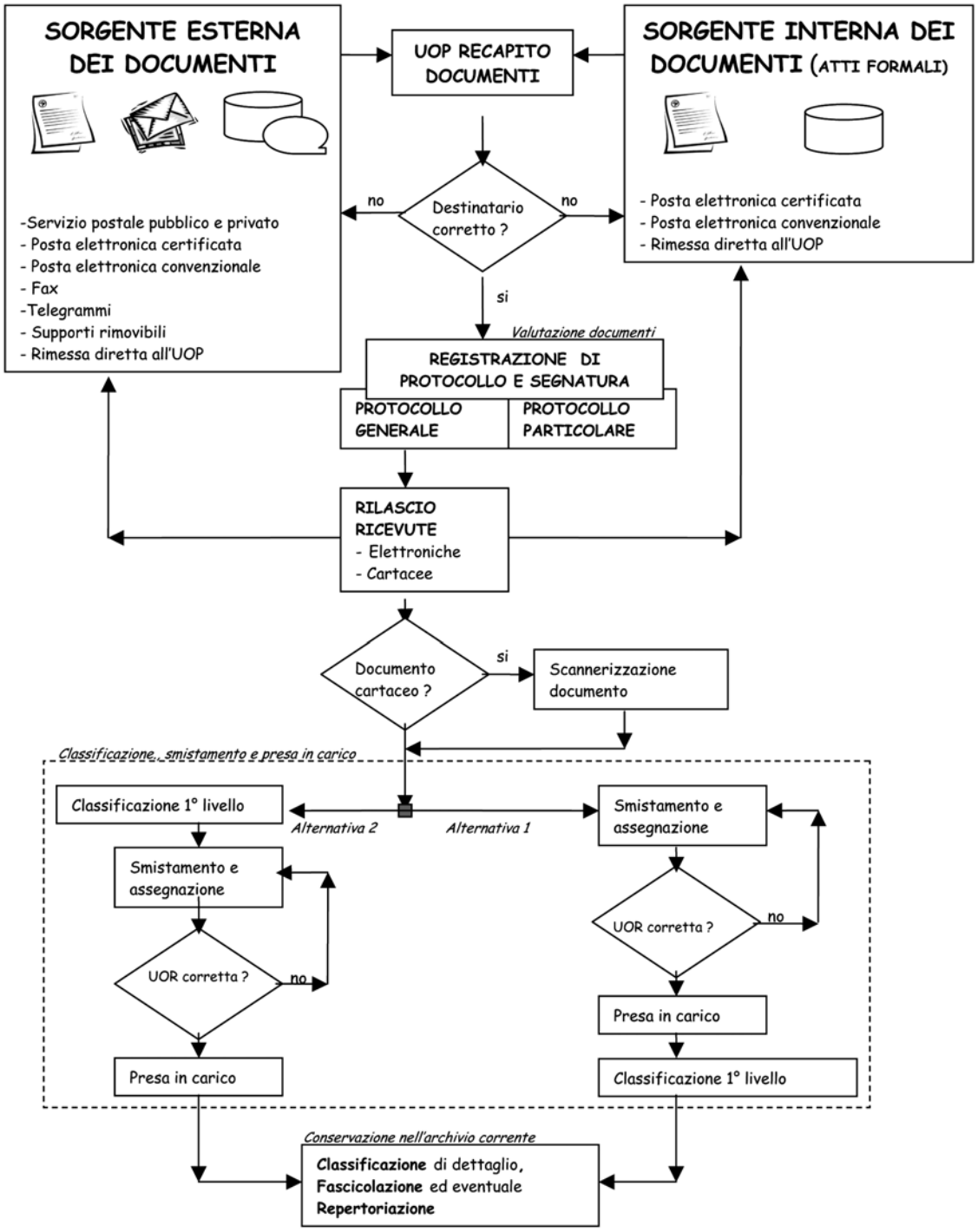
5.1 GENERALITÀ

Per descrivere i flussi di lavorazione dei documenti all'interno della AOO si fa riferimento ai diagrammi di flussi riportati nelle pagine seguenti.
Essi si riferiscono ai documenti:

- ricevuti dalla AOO, *dall'esterno o anche dall'interno se destinati ad essere ritrasmessi in modo formale in seno alla AOO*;
- inviati dalla AOO, *all'esterno o anche all'interno della AOO in modo formale*.

I flussi gestiti all'interno del sistema archivistico dell'amministrazione/AOO dalla sezione di deposito e storica dell'archivio sono sviluppati, per omogeneità e completezza di trattazione, nel successivo capitolo 9.
Come previsto dalla normativa vigente i flussi di seguito descritti sono il risultato del processo di censimento, di descrizione e di reingegnerizzazione dei processi dell'AOO, quale fase propedeutica ad un efficace ed efficiente impiego del sistema di protocollazione informatica e gestione documentale all'interno della AOO medesima.
I flussi relativi alla gestione dei documenti all'interno dell'AOO sono descritti graficamente nel paragrafo seguente prendendo in esame quelli che possono avere rilevanza giuridico-probatoria.
Per comunicazione informale tra uffici si intende lo scambio di informazioni, con o senza documenti allegati, delle quali è facoltativa la conservazione. Questo genere di comunicazioni sono ricevute e trasmesse per posta elettronica interna e non interessano il sistema di protocollo.
I flussi dei documenti interni di tipo informale trasmessi e ricevuti vengono descritti nell'allegato *descrizione dei flussi dei documenti all'interno dell'AOO*.

5.2 FLUSSO DEI DOCUMENTI RICEVUTI DALLA AOO



5.2.1 PROVENIENZA ESTERNA DEI DOCUMENTI

I documenti che sono trasmessi da soggetti esterni all'amministrazione sono, oltre quelli richiamati nel capitolo precedente, i telefax, i telegrammi e i supporti digitali rimovibili. Questi documenti sono recapitati alla/e UOP designata/e.

I documenti che transitano attraverso il servizio postale sono ritirati quotidianamente secondo le regole stabilite dal RSP riportate nell'allegato *Regole di raccolta e consegna della corrispondenza convenzionale al servizio postale nazionale*.

5.2.2 PROVENIENZA DI DOCUMENTI INTERNI FORMALI

Per sorgente interna dei documenti si intende qualunque RPA che invia formalmente la propria corrispondenza alla UOP della AOO per essere a sua volta nuovamente trasmessa, nelle forme opportune, ad altro UOR o UU della stessa AOO.

Il documento è di tipo informatico secondo i formati standard illustrati nel precedente capitolo.

I mezzi di recapito della corrispondenza considerati sono la posta elettronica convenzionale o certificata.
Nel caso di trasmissione interna, se al documento sono associati allegati che superano la dimensione della casella di posta elettronica della AOO, si procede ad un riversamento (nelle forme dovute), su supporto rimovibile da consegnare al destinatario del documento.

5.2.3 Ricezione di documenti informatici sulla casella di posta istituzionale

Di norma la ricezione dei documenti informatici è assicurata tramite la casella di posta elettronica certificata istituzionale che è accessibile solo alla/e UOP in cui si è organizzata l'AOO. Quando i documenti informatici pervengono alle UOP, la stessa unità, previa verifica della validità della firma apposta e della leggibilità del documento procede alla registrazione di protocollo.
Nel caso in cui venga recapitato per errore un documento indirizzato ad altro destinatario lo stesso è restituito al mittente con le modalità che saranno successivamente illustrate. L'operazione di ricezione dei documenti informatici avviene con le modalità previste dalle regole tecniche vigenti recanti standard del formato dei documenti, modalità di trasmissione, definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le AOO e associate ai documenti protocollati.
Essa comprende anche i processi di verifica dell'autenticità, della provenienza e dell'integrità dei documenti stessi.
Qualora i messaggi di posta elettronica non siano conformi agli standard indicati dalla normativa vigente ovvero non siano dotati di firma elettronica e si renda necessario attribuire agli stessi efficacia probatoria, il messaggio è inserito nel sistema di gestione documentale con il formato di origine apponendo la dicitura "Documento ricevuto via posta elettronica" e successivamente protocollato, smistato, assegnato e gestito. La valenza giuridico-probatoria di un messaggio così ricevuto è assimilabile a quella di una missiva non sottoscritta e comunque valutabile dal responsabile del procedimento amministrativo (RPA);
Il responsabile dello smistamento controlla quotidianamente i messaggi pervenuti nella casella di posta istituzionale e verifica se sono da protocollare.

5.2.4 Ricezione di documenti informatici sulla casella di posta elettronica non istituzionale

Nel caso in cui il messaggio viene ricevuto su una casella di posta elettronica non istituzionale o comunque non destinata al servizio di protocollazione, il messaggio viene inoltrato alla casella di posta istituzionale e inviando un messaggio, per conoscenza, al mittente con l'indicazione della casella di posta corretta. I controlli effettuati sul messaggio sono quelli sopra richiamati.

5.2.5 Ricezione di documenti informatici su supporti rimovibili

I documenti digitali possono essere recapitati anche per vie diverse dalla posta elettronica. Considerata l'assenza di standard tecnologici e formali in materia di registrazione di file digitali, la AOO si riserva la facoltà acquisire e trattare tutti i documenti informatici ricevuti su supporto rimovibile che riesce a decodificare e interpretare con le tecnologie a sua disposizione.
Superata questa fase il documento viene inserito nel flusso di lavorazione e sottoposto a tutti i controlli e gli adempimenti del caso.

5.2.6 Ricezione di documenti cartacei a mezzo posta convenzionale

I documenti pervenuti a mezzo posta o ritirati dal personale della UOP dagli uffici postali sono consegnati alla UOP.
Le buste o contenitori sono inizialmente esaminati per una preliminare verifica dell'indirizzo e del destinatario sugli stessi apposti.
La corrispondenza relativa a bandi di gara è registrata e successivamente consegnata chiusa all'ufficio responsabile della gara.
La corrispondenza personale non deve essere aperta, né protocollata ma deve essere consegnata al destinatario che ne valuterà il contenuto ed eventualmente, nel caso dovesse riguardare l'istituzione, provvederà a inoltrarla all'ufficio protocollo per la registrazione. La corrispondenza ricevuta via telegramma

o via telefax o le ricevute di ritorno della posta raccomandata, per ciò che concerne la registrazione di protocollo, sono trattate come un documento cartaceo con le modalità descritte nel successivo capitolo 10.
Quando la corrispondenza non rientra nelle categorie da ultimo indicate, si procede all'apertura delle buste e si eseguono gli ulteriori controlli preliminari alla registrazione.
La corrispondenza in arrivo è aperta il giorno lavorativo in cui è pervenuta e contestualmente protocollata. La busta si allega al documento per la parte relativa ai timbri postali.

5.2.7 Documenti cartacei ricevuti a mezzo posta convenzionale e tutela dei dati personali

Qualora una AOO sia organizzata per ricevere documenti su carta attraverso qualsiasi UOR aperta al pubblico, oltre, ovviamente alle UOP istituzionali, ovvero se per errore la corrispondenza viene recapitata ad un UOR quest'ultimo, a tutela dei dati personali eventualmente contenuti nella missiva, non apre le buste o i contenitori ricevuti ma rilascia ricevuta al mittente nelle forme stabilite dal RSP, e invia, nella stessa giornata, prima della chiusura del protocollo, la posta a una delle UOP abilitate e "incaricate" dell'apertura della corrispondenza e della protocollazione.
Il personale preposto alla apertura della corrispondenza è stato regolarmente autorizzato al trattamento dei dati personali.
In ogni caso i documenti così ricevuti devono essere inviati a cura dell'UOR/UU in busta chiusa, nella stessa giornata, prima della chiusura del servizio di protocollo, a una delle UOP autorizzata all'apertura della corrispondenza.

5.2.8 Errata ricezione di documenti digitali

Nel caso in cui pervengano sulla casella di posta istituzionale dell'AOO (certificata o meno) o in una casella non istituzionale messaggi dal cui contenuto si rileva che sono stati erroneamente ricevuti, l'operatore di protocollo rispedisce il messaggio al mittente con la dicitura "Messaggio pervenuto per errore non di competenza di questa AOO".

5.2.9 Errata ricezione di documenti cartacei

Nel caso in cui pervengano erroneamente alla UOP dell'amministrazione documenti indirizzati ad altri soggetti. Possono verificarsi le seguenti possibilità:

- busta indirizzata ad altra AOO della stessa amministrazione:

a) si invia alla AOO corretta;
b) se la busta viene aperta per errore, il documento è protocollato in entrata e in uscita inserendo nel campo oggetto una nota del tipo "documento pervenuto per errore" e si invia alla AOO destinataria apponendo sulla busta la dicitura "Pervenuta ed aperta per errore";

- busta indirizzata ad altra amministrazione:

a) si restituisce alla posta;
b) se la busta viene aperta per errore, il documento è protocollato in entrata e in uscita inserendo nel campo oggetto una nota del tipo "documento pervenuto per errore" e si invia al mittente apponendo sulla busta la dicitura "Pervenuta ed aperta per errore".

5.2.10 Attività di protocollazione dei documenti

Superati tutti i controlli precedenti, i documenti, digitali o analogici, sono protocollati e "segnati" nel protocollo generale o particolare (riservato) secondo gli standard e le modalità dettagliate nel capitolo 10.

5.2.11 Rilascio di ricevute attestanti la ricezione di documenti informatici

La ricezione di documenti 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 per via telematica, la notifica al mittente dell'avvenuto recapito del messaggio è assicurata dal servizio di posta elettronica certificata utilizzato dall'AOO con gli

standard specifici.
Il sistema di protocollazione informatica dei documenti, in conformità alle disposizioni vigenti, provvede alla formazione e all'invio al mittente di uno dei seguenti messaggi:

- *messaggio di conferma di protocollazione*: un messaggio che contiene la conferma dell'avvenuta protocollazione in ingresso di un documento ricevuto. Si differenzia da altre forme di ricevute di recapito generate dal servizio di posta elettronica dell'AOO in quanto segnala l'avvenuta protocollazione del documento, e quindi l'effettiva presa in carico;
- *messaggio di notifica di eccezione*: un messaggio che notifica la rilevazione di una anomalia in un messaggio ricevuto;
- *messaggio di annullamento di protocollazione*: un messaggio che contiene una comunicazione di annullamento di una protocollazione in ingresso di un documento ricevuto in precedenza;
- *messaggio di aggiornamento di protocollazione*: un messaggio che contiene una comunicazione di aggiornamento riguardante un documento protocollato ricevuto in precedenza.

5.2.12 Rilascio di ricevute attestanti la ricezione di documenti cartacei

Gli addetti alle UOP non possono rilasciare ricevute per i documenti che non sono soggetti a regolare protocollazione.
La semplice apposizione del timbro datario dell'UOP per la tenuta del protocollo sulla copia, non ha alcun valore giuridico e non comporta alcuna responsabilità del personale dell'UOP in merito alla ricezione ed all'assegnazione del documento.
Quando il documento cartaceo è consegnato direttamente dal mittente o da altra persona incaricata ad una UOP di protocollo ed è richiesto il rilascio di una ricevuta attestante l'avvenuta consegna, la UOP che lo riceve è autorizzata a:

- fotocopiare gratuitamente la prima pagina del documento;
- apporre sulla copia così realizzata il timbro dell'amministrazione con la data e l'ora d'arrivo e la sigla dell'operatore.

5.2.13 Conservazione dei documenti informatici

I documenti informatici sono archiviati su supporti di memorizzazione, in modo non modificabile, contestualmente alle operazioni di registrazione e segnatura di protocollo.
I documenti ricevuti per via telematica sono resi disponibili agli UU, attraverso la rete interna dell'amministrazione/AOO, subito dopo l'operazione di smistamento e di assegnazione.

5.2.14 Conservazione delle rappresentazioni digitali di documenti cartacei

I documenti ricevuti su supporto cartaceo, dopo le operazioni di registrazione e segnatura, sono acquisiti in formato immagine attraverso un processo di scansione.
Il processo di scansione avviene in diverse fasi:

- acquisizione delle immagini in modo tale che ad ogni documento, anche se composto da più pagine, corrisponda un unico file;
- verifica della leggibilità e della qualità delle immagini acquisite;
- collegamento delle immagini alle rispettive registrazioni di protocollo in modo non modificabile;
- memorizzazione delle immagini su supporto informatico, in modo non modificabile.

Le rappresentazioni digitali dei documenti cartacei sono archiviate secondo le regole vigenti, in modo non modificabile al termine del processo di scansione.
I documenti cartacei dopo l'operazione di riproduzione in formato immagine e conservazione sostitutiva ai sensi della delibera CNIPA 19 febbraio 2004 n.11 vengono inviati agli UOR/UU/RPA destinatari per le operazioni di fascicolazione e conservazione.

I documenti con più destinatari, sono riprodotti in formato immagine ed inviati solo in formato elettronico.
La riproduzione dei documenti cartacei in formato immagine viene eseguita sulla base dei seguenti criteri:

- se il documento ricevuto in formato A4 o A3 non supera le xx pagine viene acquisito direttamente con le risorse, umane e strumentali, interne all'AOO;
- se il documento ha una consistenza maggiore o formati diversi dai precedenti, viene acquisito in formato immagine solo se esplicitamente richiesto dagli UOR/UU/RPA di competenza, avvalendosi eventualmente dei servizi di una struttura esterna specializzata. In questo caso il RSP, insieme al RPA, individua i documenti da sottoporre al processo di scansione e ne fissa i tempi, diversi da quelli ordinari, e le modalità esecutive.
- In ogni caso non vengono riprodotti in formato immagine i seguenti documenti:

– i certificati medici contenenti la diagnosi

– certificati di invalidità

– certificati contenenti dati sensibili;

5.2.15 Classificazione, assegnazione e presa in carico dei documenti

Gli addetti alla UOP provvedono ad inviare il documento all'ufficio smistamento che identifica l'UOR di destinazione. Quest'ultimo:

- esegue una verifica di congruità in base alle proprie competenze;
- in caso di errore rinvia il documento all'ufficio smistamento di origine;
- in caso di verifica positiva, esegue l'operazione di presa in carico smistandola al proprio interno ad UU o direttamente al RPA;
- esegue la prima classificazione (o classificazione di primo livello) del documento sulla base del titolario di classificazione in essere presso l'amministrazione.

5.2.16 Conservazione dei documenti nell'archivio corrente

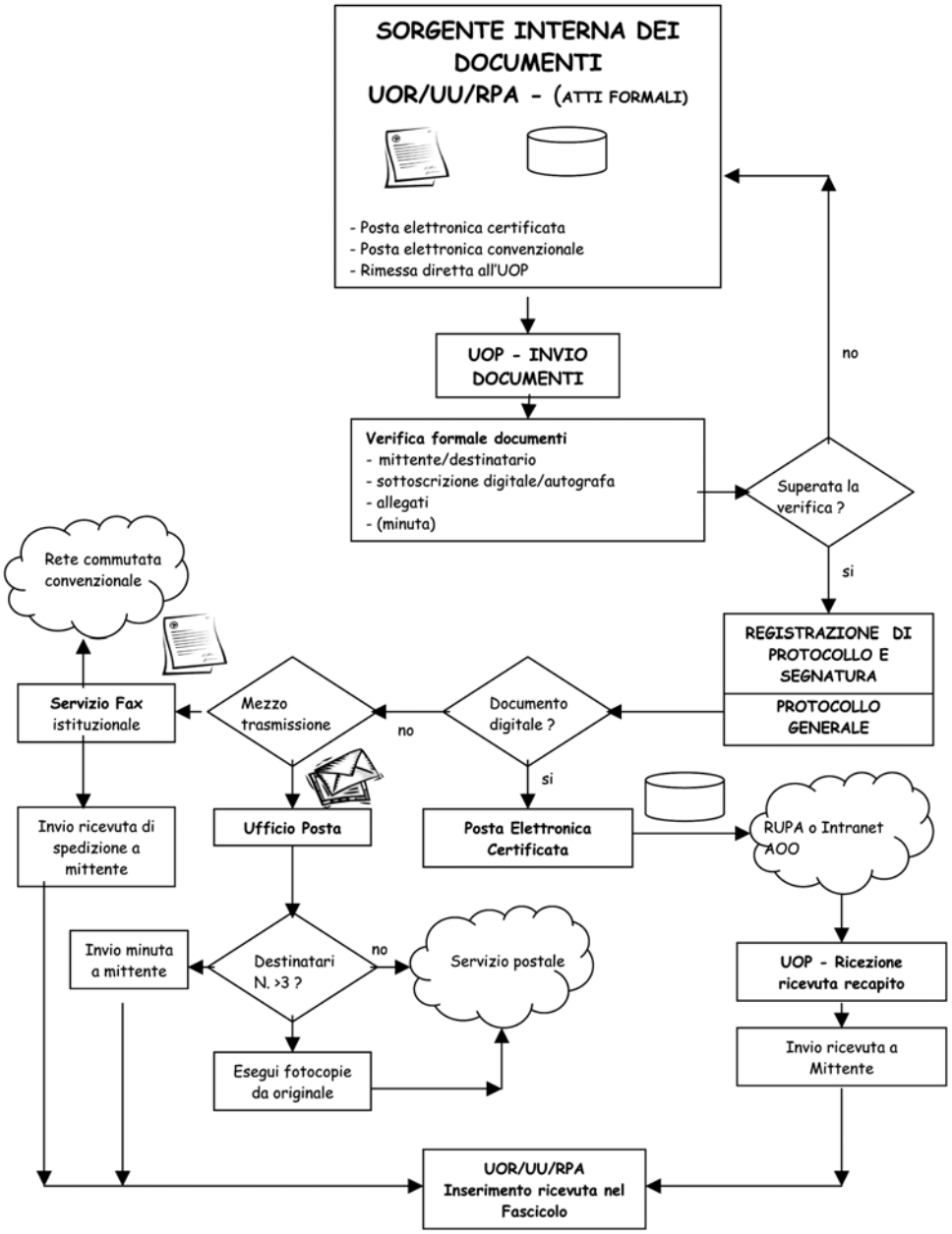
Durante l'ultima fase del flusso di lavorazione della corrispondenza in ingresso vengono svolte le seguenti attività:

1. classificazione di livello superiore sulla base del titolario di classificazione adottato dall'AOO;
2. fascicolazione del documento secondo le procedure previste dall'AOO
3. inserimento del fascicolo nel repertorio dei fascicoli nel caso di apertura di un nuovo fascicolo.

5.2.17 Conservazione dei documenti e dei fascicoli nella fase corrente

All'interno di ciascun ufficio utente di ciascun UOR della AOO sono stati individuati e formalmente incaricati gli addetti alla organizzazione e tenuta dei fascicoli "attivi" (e chiusi in attesa di riversamento nell'archivio di deposito) e alla conservazione dei documenti al loro interno. Generalmente i responsabili della conservazione dei documenti e dei fascicoli nella fase corrente sono gli stessi RPA.

5.3 FLUSSO DEI DOCUMENTI INVIATI DALLA AOO



5.3.1 SORGENTE INTERNA DEI DOCUMENTI

Nel grafico di cui al paragrafo 5.3 per sorgente interna (all'AOO) dei documenti si intende l'unità organizzativa mittente interna all'AOO che invia, tramite il RPA, la corrispondenza alla UOP della AOO stessa affinché sia trasmessa, nelle forme e nelle modalità più opportune, ad altra amministrazione o altra AOO della stessa amministrazione, ovvero ad altro ufficio (UU o UOR) della stessa AOO.

Per documenti in partenza s'intendono quelli prodotti dal personale degli uffici dell'AOO nell'esercizio delle proprie funzioni avente rilevanza giuridico-probatoria e destinati ad essere trasmessi ad altra amministrazione o altra AOO della stessa amministrazione, ovvero ad altro ufficio (UU o UOR) della stessa AOO.

Il documento è in formato digitale formato secondo gli standard illustrati nei precedenti capitoli.

I mezzi di recapito della corrispondenza considerati sono quelli stessi richiamati nell'articolo 35 Posta Elettronica Certificata.

Nel caso di trasmissione interna di allegati al documento di cui sopra che possono superare la capienza della casella di posta elettronica si procede ad un riversamento (con le modalità previste dalla normativa

vigente), su supporto rimovibile da consegnare al destinatario contestualmente al documento principale.
I documenti in partenza contengono l'invito al destinatario a riportare i riferimenti della registrazione di protocollo della lettera alla quale si da riscontro.
Durante la fase transitoria di migrazione verso l'utilizzo di un sistema di gestione documentale interamente digitale, il documento può essere in formato analogico. I mezzi di recapito della corrispondenza in quest'ultimo è il servizio postale.

5.3.2 Verifica formale dei documenti

Ogni UOR è autorizzata dall'AOO per il tramite del RSP, a svolgere attività di registrazione di protocollo e apposizione della segnatura per la corrispondenza in uscita.
Di conseguenza tutti i documenti originali da spedire, siano essi informatici o analogici, sono direttamente protocollati e spediti dagli UOR.
Gli UOR provvedono ad eseguire al loro interno le verifiche di conformità della documentazione predisposta per essere trasmessa con le stesse modalità descritte nel capitolo precedente.
Se la verifica da esito positivo, il documento viene registrato nel registro di protocollo generale o particolare; in caso contrario è restituito al mittente UU/RPA con le osservazioni del caso.

5.3.3 Registrazione di protocollo e segnatura

La protocollazione e la segnatura della corrispondenza in partenza, sia essa in formato digitale che in formato analogico, è effettuata direttamente dai singoli RPA/UU/UOR abilitati in quanto collegati al sistema di protocollo informatico della AOO a cui appartengono.
Le attività di registrazione degli elementi obbligatori e degli elementi accessori del protocollo e la relativa segnatura della missiva da inviare sono effettuate dal RPA. Il documento registrato presso il protocollo riservato è contrassegnato anteponendo al numero della segnatura una sigla (ad es. "RIS").

5.3.4 Trasmissione di documenti informatici

Le modalità di composizione e di scambio dei messaggi, il formato della codifica e le misure di sicurezza sono conformi alla circolare AGID 23 gennaio 2013, n. 60.
I documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari, ovvero abilitato alla ricezione della posta per via telematica (il destinatario può essere anche interno alla AOO).
Per la spedizione dei documenti informatici l'AOO si avvale dei servizi di autenticazione e marcatura temporale offerti da un certificatore accreditato iscritto nell'elenco pubblico tenuto dall'AGID.
Per la spedizione dei documenti informatici, l'AOO si avvale di un servizio di "Posta Elettronica Certificata", conforme al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, che può essere offerto da un soggetto esterno in grado di assicurare la sicurezza del canale di comunicazione, di dare certezza sulla data di spedizione e di consegna dei documenti attraverso una procedura di rilascio di ricevute di ritorno elettroniche.
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, dell'esistenza o del contenuto della corrispondenza, delle comunicazioni o dei 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.

5.3.5 Trasmissione di documenti cartacei a mezzo posta

La UOR provvede direttamente alla trasmissione "fisica" del documento in partenza e alla spedizione del documento, di norma il giorno lavorativo in cui è stato protocollato.

5.3.6 Affrancatura dei documenti in partenza

L'UOP *(o in alternativa l'ufficio addetto allo smistamento della posta)* provvede alle operazioni necessarie per l'invio della corrispondenza in partenza (ad es.: pesatura e affrancatura delle lettere ordinarie, affrancatura delle lettere fuori formato, pesatura, timbratura ed affrancatura posta prioritaria, ricezione e verifica delle distinte di raccomandate compilate ed etichettate dagli uffici, pesatura, affrancatura e registrazioni delle raccomandate estere ecc.).
Al fine di consentire il regolare svolgimento di tali operazioni, la corrispondenza in partenza deve essere consegnata alla UOP *(o in alternativa all'ufficio posta)* secondo le regole richiamate nell'allegato *Regole di raccolta e consegna della corrispondenza convenzionale al servizio postale nazionale.*

5.3.7 Conteggi spedizione corrispondenza

L'UOP *(o in alternativa l'ufficio posta)* effettua i conteggi relativi alle spese giornaliere e mensili sostenute per le operazioni di invio della corrispondenza.

5.3.8 Documenti in partenza per posta convenzionale con più destinatari

Qualora i destinatari siano più di uno, e comunque in numero maggiore di tre, può essere autorizzata la spedizione di copie dell'originale. L'elenco dei destinatari, in formato cartaceo, è allegato alla minuta.

5.3.9 Inserimento delle ricevute di trasmissione nel fascicolo

La minuta del documento cartaceo spedito, ovvero le ricevute dei messaggi telefax, ovvero le ricevute digitali del sistema di posta certificata utilizzata per lo scambio dei documenti digitali, sono conservate all'interno del relativo fascicolo.
Gli UOR che effettuano la spedizione di documenti informatici o cartacei direttamente curano anche l'archiviazione delle ricevute di ritorno.

6. Regole di smistamento ed assegnazione dei documenti ricevuti

Il presente capitolo riporta le regole di smistamento ed assegnazione dei documenti ricevuti.

6.1 REGOLE DISPONIBILI CON IL PDP

Le AOO che fruiscono del servizio di protocollo con il proprio PdP eseguono lo smistamento e l'assegnazione dei documenti protocollati e segnati adottando le funzionalità di seguito illustrate:

L'attività di smistamento consiste nell'operazione di inviare un documento da protocollare e segnare all'UOR competente in base alla classificazione di primo livello del titolario, e/o all'oggetto del documento.

Con l'assegnazione si provvede al conferimento della responsabilità del procedimento amministrativo ad un soggetto fisico e alla trasmissione del materiale documentario oggetto di lavorazione.

Effettuato lo smistamento e l'assegnazione, il RPA provvede alla presa in carico del documento allo stesso assegnato e provvede alla registrazione del documento nel protocollo.

L'UOR competente è incaricato della gestione del procedimento a cui il documento si riferisce e prende in carico il documento.

I documenti che sono immediatamente riconducibili ad una specifica UOR e/o materia, vengono inoltrati direttamente dalla UOP.

I termini per la definizione del procedimento amministrativo che prende avvio dal documento, decorrono comunque dalla data di protocollazione.

Il sistema di gestione informatica dei documenti memorizza tutti i passaggi, conservando, per ciascuno di essi, l'identificativo dell'utente che effettua l'operazione, la data e l'ora di esecuzione.

La traccia risultante definisce, ai fini normativi e regolamentari, i tempi del procedimento amministrativo ed i conseguenti riflessi sotto il profilo della responsabilità.

Nell'allegato *area organizzativa omogena e modello organizzativo* sono riportati gli UOR destinatari dello smistamento e autorizzati all'assegnazione dei documenti ricevuti dall'AOO e protocollati dagli UOP.

Lo smistamento iniziale eseguito dalla/e UOP recapita ai dirigenti di ciascuna UOR, attraverso funzioni specifiche del sistema di protocollo informatico, i documenti indirizzati all'UOR medesimo.

Quest'ultimi, dopo averne preso visione, provvedono ad accettarli e ad assegnarli ai propri UU/RPA, oppure in caso di errore, ad informare il mittente (UOP) e a smistare la notifica ad altro UOR.

L'UOR del procedimento amministrativo indica, sul documento in arrivo, il nominativo del RPA. Qualora non sia diversamente specificato il RPA coincide con il dirigente dell'UOR.

6.2 CORRISPONDENZA DI PARTICOLARE RILEVANZA

Quando un documento pervenuto appare di particolare rilevanza, indipendentemente dal supporto utilizzato, è preventivamente inviato in visione al dirigente, che provvede ad individuare l'UOR competente a trattare il documento fornendo eventuali indicazioni per l'espletamento della pratica.

6.3 ASSEGNAZIONE DEI DOCUMENTI RICEVUTI IN FORMATO DIGITALE

I documenti ricevuti dall'AOO per via telematica, o comunque disponibili in formato digitale, sono assegnati all'UOR competente attraverso i canali telematici dell'AOO al termine delle operazioni di registrazione e smistamento.
Il responsabile dell'UOR può protocollare il documento, applicare la segnatura di protocollo, visualizzare i documenti, attraverso l'utilizzo dell'applicazione di protocollo informatico e in base alle abilitazioni previste potrà:

- visualizzare gli estremi del documento;
- visualizzare il contenuto del documento;
- individuare come assegnatario il RPA competente per la materia a cui si riferisce il documento.

La "presa in carico" dei documenti informatici viene registrata dal PdP in modo automatico e la data di ingresso dei documenti negli UOR competenti coincide con la data di assegnazione degli stessi.
I destinatari del documento per "competenza" lo ricevono esclusivamente in formato digitale.

6.4 ASSEGNAZIONE DEI DOCUMENTI RICEVUTI IN FORMATO CARTACEO

I documenti ricevuti dall'amministrazione in formato cartaceo, *se successivamente acquisiti in formato immagine con l'ausilio di scanner*, una volta concluse le operazioni di registrazione, di segnatura e di assegnazione, sono fatti pervenire al RPA di competenza per via informatica attraverso la rete interna dell'amministrazione/AOO. L'originale cartaceo può essere successivamente trasmesso al RPA oppure essere conservato dalla UOP.

La "presa in carico" dei documenti informatici viene registrata dal sistema in modo automatico e la data di ingresso dei documenti negli UOR di competenza coincide con la data di assegnazione degli stessi.

I documenti cartacei gestiti dalla UOP sono di norma smistati entro le xxx ore dal momento in cui sono pervenuti, salvo che vi siano, entro detto lasso di tempo, uno o più giorni non lavorativi, nel qual caso l'operazione di smistamento viene assicurata entro le 24 ore dall'inizio del primo giorno lavorativo successivo.

6.5 MODIFICA DELLE ASSEGNAZIONI

Nel caso di assegnazione errata, l'UOR/UU che riceve il documento, se è abilitato all'operazione di smistamento, provvede a trasmettere l'atto all'UOR competente, in caso contrario comunica l'errore alla UOP che ha erroneamente assegnato il documento, che procederà ad una nuova assegnazione.
Nel caso in cui un documento assegnato erroneamente ad un UU afferisca a competenze attribuite ad altro UU dello stesso UOR, l'abilitazione al relativo cambio di assegnazione è attribuita al dirigente della UOR medesima o a persona da questi incaricata.
Il sistema di gestione informatica del protocollo tiene traccia di tutti i passaggi memorizzando l'identificativo dell'utente che effettua l'operazione con la data e l'ora di esecuzione.

7. UO responsabili delle attività di registrazione di protocollo, di organizzazione e di tenuta dei documenti

Il presente capitolo individua le unità organizzative responsabili delle attività di registrazione di protocollo, di organizzazione e di tenuta dei documenti all'interno della AOO
In base al modello organizzativo adottato dall'Amministrazione/AOO (si veda il par. 1.4 del presente MdG), nell'allegato *area organizzativa omogena e modello organizzativo* è riportato, per ciascuna AOO, l'elenco delle unità organizzative responsabili delle attività di registrazione del protocollo (UOP). Relativamente alla organizzazione e alla tenuta dei documenti dell'amministrazione all'interno di ciascuna AOO (o della AOO se unica), sono istituiti il servizio archivistico e eventualmente il servizio per la conservazione sostitutiva e sono definite le strutture dedicate alla conservazione dei documenti.
I servizi in argomento sono stati identificati e formalizzati prima di rendere operativo il servizio di gestione informatica del protocollo, dei documenti e degli archivi.

7.1 SERVIZIO ARCHIVISTICO

L'amministrazione ha istituito il servizio archivistico denominato Aruba Posta Elettronica Certificata SPA nell'ambito dell'unica AOO in cui è organizzato il servizio di protocollo e gestione documentale.
Il servizio archivistico è funzionalmente e strutturalmente integrato nel suddetto servizio per la tenuta del protocollo informatico. Alla guida del servizio archivistico è preposto .

7.2. SERVIZIO DELLA CONSERVAZIONE SOSTITUTIVA DEI DOCUMENTI

Il servizio in parola è realizzato al fine di trasferire su supporto informatico rimovibile le informazioni:

- del protocollo informatico;
- della gestione dei documenti:
- relative ai fascicoli che fanno riferimento a procedimenti conclusi;

Il responsabile delle procedure di conservazione sostitutiva, può delegare, in tutto o in parte, lo svolgimento delle proprie attività ad una o più persone dell'AOO che, per competenza ed esperienza, garantiscano la corretta esecuzione di tali operazioni. L'amministrazione si riserva la facoltà di affidare, in tutto o in parte, ad altri soggetti, pubblici o privati, il procedimento di conservazione e di riversamento;

questi sono tenuti ad osservare quanto previsto dalle norme vigenti in materia di protocollo e protezione dei dati personali (integrate, all'occorrenza, da specifici richiami contrattuali).
Nel caso di affidamento a "soggetto esterno", l'amministrazione provvede ad incaricare formalmente tale soggetto (ad esempio Società di servizi, Consulente, ecc) delle attività di conservazione e riversamento e nel contempo lo diffida dal comunicare o diffondere, anche accidentalmente, gli eventuali dati personali comuni, sensibili e/o giudiziari presenti nei supporti oggetto di copia e di riversamento.

8. Elenco dei documenti esclusi dalla protocollazione e dei documenti soggetti a registrazione particolare

8.1 DOCUMENTI ESCLUSI

Sono esclusi dalla registrazione di protocollo, le tipologie di documenti riportati nell'allegato *elenco dei documenti esclusi dalla registrazione del protocollo*.
Sono inoltre esclusi dalla registrazione di protocollo tutti i documenti di cui all'art. 53 comma 5 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

8.2 DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE

Sono esclusi dalla registrazione di protocollo generale e sono soggetti a registrazione particolare le tipologie di documenti riportati in *elenco dei documenti soggetti a registrazione particolare* allegato al presente MdG.
Tale tipo di registrazione consente comunque di eseguire su tali documenti tutte le operazioni previste nell'ambito della gestione dei documenti, in particolare la classificazione, la fascicolazione, la repertoriazione.
Questi documenti costituiscono comunque delle serie di interesse archivistico, ciascuna delle quali deve essere corredata da un repertorio contenente le seguenti informazioni:

- dati identificativi di ciascun atto (persona fisica o giuridica che adotta il documento, data di adozione, oggetto….);
- numero di repertorio, un numero progressivo;
- dati di classificazione e di fascicolazione.