**Aruba PEC S.p.A.**

# Manuale di Conservazione

**Versione**: 2.0
**Data aggiornamen** 6
**Approvato da:** Andre
**Classificazione documento**: pubblico

Sassetti Andrea 15.06.2026 10:07:12 UTC

| Versione | Data | Changelog |
|---|---|---|
| 2.0 | 10/06/2026 | Revisione completa del documento (modifiche in tutti i paragrafi). |
| 1.9 | 16/03/2022 | Sommario: rivista la numerazione di alcuni paragrafi<br>Par. 4.1: modificato il responsabile della sicurezza per il servizio di conservazione<br>Par. 12.3.1: Aggiunto il capitolo |

| | | |
|---|---|---|
| 1.8 | 22/12/2021 | Par. 1: Aggiornamento Scopo e ambito del documento<br>Par. 2: Revisione del Glossario<br>Par. 3 Aggiornamento della normativa di riferimento e degli Standard di riferimento<br>Par. 4: Revisione dei Ruoli e responsabilità<br>Par. 5: Aggiornamento delle strutture organizzative<br>Par. 6.3: Revisione dei formati attualmente gestiti<br>Par. 7.1: Correzioni alle modalità di acquisizione dei pacchetti di versamento per la loro presa in carico.<br>Par. 7.7.2: Rivisitazioni relative alla produzione di copie<br>Par. 7.8.2: Aggiunta di dettagli relativamente allo scarto dei pacchetti di archiviazione<br>Par. 7.11: Aggiunta di dettagli relativamente alla produzione degli audit log<br>Par. 9.2.2: Correzioni al mantenimento della firma per il periodo di conservazione<br>Par. 10.1.1: Correzioni alla nomina di Aruba quale responsabile del servizio di conservazione e del trattamento dei dati |
| 1.7 | 19/06/2020 | Par.4.1: Aggiornati Ruoli e Responsabilità |
| 1.6 | 17/04/2019 | Nuovo Template<br>Cap.1: Aggiornato Rappresentante Legale<br>Par.4.1: Aggiornati Ruoli e Responsabilità |
| 1.5 | 11/10/2018 | Aggiornamenti Terminologia, Normativa e Standard di Riferimento<br>Par.4.1: Aggiornati Ruoli e Reponsabilità<br>Par.6.4: Precisazione su inserimento delle c.d. extrainfo nell' IdC.<br>Par. 7.1: Aggiornamento modalità di acquisizione dei PdV.<br>Inserito par. 7.5.3 Rettifica dei pacchetti di archiviazione<br>Par.12.5: Rimosso riferimento a protocollo SSL<br>Par. 12.6: Rivisti dettagli gestione dei backup del sistema<br>Tutto il documento: aggiornamenti riferimenti a normativa trattamento dati personali |
| 1.4 | 11/12/2017 | Tutto il documento: inseriti testi alternativi per le immagini e verificata accessibilità<br>Par. 1.1: Specificata denominazione societaria del Conservatore Accreditato e inseriti dati identificativi della società<br>Par. 2.1: Uniformata terminologia relativa a IdC, IPdA e IPdV<br>Par. 6.3.2: Aggiornata tabella formati consigliati<br>Par 6.6.1: Aggiornati riferimenti alle specifiche specifiche del Pacchetto di Versamento<br>Par. 6.7.1: Aggiornata terminologia relativa a IdC<br>Par.7.5.2: Inserito paragrafo relativo a gestione PdA incompleti o non validi<br>Par. 7.6.1: Aggiornato paragrafo e corretto refuso di terminologia sul secondo punto<br>Par. 7.8.3: Descritta procedura per scarto immediato<br>Par.9.2: Modificato titolo paragrafo<br>Par. 9.2.1: Rivista descrizione delle attività di verifica dell'integrità degli archvi<br>Par 10.1.2: Aggiornati i contenuti della Scheda di Conservazione<br>Cap. 11: Rivisti ed aggiornati livelli di servizio (SLA) |

| | | |
|---|---|---|
| 1.3 | 20/09/2017 | Par.3.1: aggiornata normativa di riferimento<br>Par.4.1: aggiornati Responsabili del Servizio e date di nomina<br>Par.6.3: rimosso<br>Par.7.6: modificata terminologia (da “materiali” a documenti”);<br>Inserimento Par.7.7.3: Produzione copie o duplicati su supporti rimuovibili<br>Par. 7.11: inserito paragrafo “audit log”<br>Par.8.6: migliorata descrizione della soluzione di conservazione<br>Par.8.6.1: migliorata descrizione change management e inserito riferimento test di Quality Assurance<br>Par.9.2.: modificata cadenza verifica periodica dell’integrità degli archivi. Modificata descrizione procedura leggibilità archivi.<br>Par.9.2.1 modificata frequenza verifica integrità degli archivi Cap.11: Cambiata descrizione specifiche tecniche per “invio in conservazione del PdA”<br>Par.12.7: ridefinite modalità di isolamento delle componenti critiche<br>Par.12.8.3: migliorata descrizione della sicurezza organizzativa e aggiornati riferimenti normativi<br>12.8.4: aggiornate regole password utente<br>Tutto il documento: aggiornati riferimenti a documenti interni e procedure di sistema |
| 1.2 | 04/04/2016 | Modifiche su terminologie utilizzate |
| 1.1 | 02/02/2016 | Revisione del manuale a seguito della pubblicazione del nuovo schema sul sito istituzionale dell’Agid |
| 1.0 | 26/11/2014 | Prima versione documento |

# Sommario

# 1 Introduzione

## 1.1 Scopo e ambito del documento

Il presente documento costituisce il Manuale del sistema di conservazione del Conservatore Aruba PEC S.p.A. (di seguito "Aruba PEC" o "il Conservatore") ed è parte integrante della documentazione di riferimento del servizio. Il Manuale descrive l'organizzazione complessiva della conservazione, individuando i soggetti coinvolti e i rispettivi ruoli, responsabilità, obblighi e ambiti di competenza, incluse le eventuali attività affidate a terzi e le relative modalità di presidio. Sono inoltre riportati i dati dei soggetti che, nel tempo, hanno assunto la responsabilità del servizio e le funzioni assegnate nell'ambito del processo di conservazione.

Il Manuale illustra il modello di funzionamento e i principali processi operativi, con particolare riferimento alle modalità di presa in carico dei pacchetti di versamento e alla gestione del rapporto di versamento, ai controlli effettuati sui contenuti conferiti e ai criteri di trattamento e archiviazione dei pacchetti di conservazione. Vengono dettagliate le tipologie di documenti informatici ammesse al servizio, i formati gestiti, i metadati associabili alle diverse classi documentali e le eventuali eccezioni, nonché le regole per la produzione di duplicati o copie e per l'eventuale scarto/cancellazione secondo i tempi previsti per ciascuna tipologia documentale. Il documento disciplina anche le modalità di esibizione e di esportazione dal sistema, tramite produzione del pacchetto di distribuzione, nonché le condizioni e i casi in cui può essere richiesta la presenza di un pubblico ufficiale.

Il Manuale è redatto in conformità alla normativa vigente e recepisce le disposizioni del D.Lgs. 7 marzo 2005, n. 82 e s.m.i. (Codice dell'Amministrazione Digitale – CAD), oltre alle indicazioni contenute nei provvedimenti normativi e di prassi e nei riferimenti tecnici richiamati nelle sezioni dedicate. Il Cliente è tenuto a leggere con la massima attenzione il presente Manuale predisposto da Aruba PEC e, in qualità di unico Responsabile della conservazione, approva e fa propri i contenuti qui descritti, assicurandone l'applicazione per quanto di propria competenza e garantendo la corretta trasmissione delle informazioni agli utenti autorizzati.

## 1.2 Versione del Manuale e organizzazione responsabile

Questo documento è la versione 2.0 del Manuale del Conservatore di Aruba PEC S.p.A. e viene redatto, pubblicato ed aggiornato da Aruba PEC S.p.A.

Il soggetto responsabile del presente manuale operativo all'interno di Aruba PEC è:

**Andrea Sassetti**

Responsabile del Servizio

Aruba PEC S.p.A.

### *1.2.1 Soggetti approvatori*

Questo Manuale è approvato dalla Responsabile del Servizio, previa verifica da parte delle funzioni aziendali interessate.

### *1.2.2 Procedura di approvazione*

La redazione e approvazione del Manual segue le procedure previste dal Sistema di Gestione Qualità aziendale.

## 1.3 Documenti collegati

Il presente Manuale è integrato da una serie di documenti aziendali relativi a specifici aspetti connessi al Servizio di Conservazione Aruba PEC.

Di seguito è riportato l'elenco dei documenti disponibili per la consultazione, ove di natura pubblica.

| Nome | Nota di riservatezza |
|---|---|
| Appendice – Manuale di Conservazione | Documento pubblico |
| Addendum al Manuale di Conservazione Aruba PEC | Documento pubblico |

# 2 Terminologia

Secondo la normativa vigente e ai fini dell'interpretazione del presente Manuale, i termini e le espressioni sotto elencate avranno il significato descritto nelle definizioni in esso riportate. Qualora le definizioni adottate dalla normativa di riferimento non fossero riportate nell'elenco che segue, si rimanda ai testi in vigore per la loro consultazione.

I termini e le espressioni non definiti avranno il significato loro attribuito all'interno del paragrafo o sezione che li contiene.

Ai fini della fruizione del Servizio di conservazione digitale dei documenti informatici descritto nel presente Manuale, valgono ad ogni effetto anche le definizioni contenute nel Contratto, da intendersi, pertanto, qui interamente riportate e trascritte, nonché le seguenti:

## 2.1 Termini, acronimi e definizioni

| Termine | Definizione |
|---|---|
| ***Agenzia per l'Italia Digitale (AgID)*** | Ente pubblico non economico, con competenza nel settore delle tecnologie dell'informazione e della comunicazione nell'ambito della pubblica amministrazione. L'Ente, opera secondo le direttive per l'attuazione delle politiche e sotto la vigilanza del Ministro per la pubblica amministrazione e l'innovazione, con autonomia tecnica e funzionale, amministrativa, contabile, finanziaria e patrimoniale. |
| ***Accesso*** | Operazione che consente a chi ne ha diritto di prendere visione dei documenti informatici conservati. |
| ***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. |
| ***Agente di alterazione*** | Qualsiasi codice contenuto in un documento informatico potenzialmente idoneo a modificare la rappresentazione dell'informazione senza alterarne il contenuto binario (in via meramente esplicativa e non esaustiva: macro, codici eseguibili nascosti, formule di foglio di lavoro occulte in tutto o in parte, sequenze di caratteri occultate all'interno dei documenti informatici). |
| ***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, intestato dal Cliente al/i Titolare/i e di cui il/i medesimo/i è/sono giuridicamente responsabile/i. |

| | |
|---|---|
| ***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. |
| ***ASP - Application Service Provider*** | Fornitore di Servizi Applicativi. |
| ***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. |
| ***Base di dati*** | Collezione di dati registrati e correlati tra loro. |
| ***Certification Authority (CA)*** | prestatore di servizi fiduciari che rilascia certificati di firma e di sigillo. |
| ***Certificazione*** | Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi. |
| ***Ciclo di gestione*** | Arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo. |
| ***Chiusura del Pacchetto di Archiviazione*** | Operazione consistente nella sottoscrizione del Pacchetto di Archiviazione con firma digitale apposta da un Firmatario Delegato di Aruba PEC e apposizione di una validazione temporale con marca temporale alla relativa impronta. |
| ***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. |
| ***Codice eseguibile*** | Insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici. |
| ***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. |
| ***Contrassegno a stampa*** | Contrassegno generato elettronicamente, apposto a stampa sulla copia analogica di un documento amministrativo informatico per verificarne provenienza e conformità all'originale. |
| ***Contratto di servizio di conservazione dei documenti (CSCD)*** | Contratto di servizio di conservazione dei documenti, ove sono esplicitate chiaramente l'ambito dell'affidamento conferito, le specifiche funzioni, le attività e le responsabilità affidate dal Cliente ad Aruba PEC. |

| | |
|---|---|
| ***Coordinatore della Gestione Documentale*** | 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 e s.m.i. nei casi di amministrazioni che abbiano istituito più Aree Organizzative Omogenee. |
| ***Copia informatica di documento analogico*** | Il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto. |
| ***Copia per immagine su supporto informatico di documento analogico*** | Il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto. |
| ***Copia informatica di documento informatico*** | Il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari. |
| ***Copia di sicurezza*** | Copia di backup degli archivi del sistema di conservazione. |
| ***Descrittore evidenze*** | Vedi pacchetto informativo. |
| ***Destinatario*** | Identifica il soggetto/sistema al quale il documento informatico è indirizzato. |
| ***DIRT*** | Documenti informatici rilevanti ai fini delle disposizioni tributarie. |
| ***Domain Name System (DNS)*** | Sistema di gestione dei nomi simbolici associati ad indirizzi di siti e domini Internet. Quando un messaggio di posta elettronica (e-mail), o un applicativo di consultazione di siti internet (browser) punta ad un dominio, il DNS traduce il nome inserito sotto forma di URL (es. http//www.....it)/ in un indirizzo costituito da una sequenza numerica convenzionale (es. 123.123.23.3). |
| ***Documento analogico*** | La rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti. |
| ***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 analogico originale*** | Documento analogico che può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi. |
| ***Documento originale unico*** | E' quel documento analogico il cui contenuto non può essere desunto da altre scritture o documenti di cui sia obbligatoria la tenuta, anche presso terzi e che non soddisfa, dunque, alcuna delle condizioni elencate nella definizione di "Documento analogico originale". |
| ***Documento informatico*** | La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. |
| ***Duplicato informatico*** | Il documento informatico ottenuto mediante la memorizzazione, sullo stesso supporto o su supporti diversi, della medesima sequenza di valori binari del documento originario. |
| ***Duplicazione dei documenti informatici*** | Produzione di duplicati informatici. |
| ***Elenco Persone*** | Elenco delle persone designate dal Cliente ad operare in suo nome, conto e interesse con Aruba PEC per l'esecuzione del contratto. |

| | |
|---|---|
| ***Esibizione*** | Operazione che consente di visualizzare un documento conservato e di ottenerne copia; |
| ***Estratto per riassunto*** | Documento nel quale si attestano in maniera sintetica ma esaustiva fatti, stati o qualità desunti da dati o documenti in possesso di soggetti pubblici |
| ***Evidenza informatica*** | Una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica. |
| ***Fascicolo informatico*** | Raccolta, individuata con identificativo univoco, di atti, documenti e dati informatici, da chiunque formati, del procedimento amministrativo, nell'ambito della pubblica amministrazione. Per i soggetti privati è da considerarsi fascicolo informatico ogni aggregazione documentale, comunque formata, funzionale all'erogazione di uno specifico servizio o prestazione. |
| ***Firma digitale*** | Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici. |
| ***Fruibilità di un dato*** | La possibilità di utilizzare il dato anche trasferendolo nei sistemi informativi automatizzati di un'altra amministrazione. |
| ***Firmatario delegato*** | Responsabile del servizio di conservazione o Persona formalmente delegata ad apporre la propria firma digitale sui Pacchetto di Archiviazione per conto di Aruba PEC; questa persona può essere interna o esterna ad Aruba PEC, laddove è giuridicamente possibile. |
| ***Formato*** | Modalità di rappresentazione del documento informatico mediante codifica binaria; comunemente è identificato attraverso l'estensione del file e/o il tipo MIME. |
| ***Fornitore esterno*** | Organizzazione che fornisce ad Aruba PEC servizi relativi al suo sistema di conservazione dei documenti. |
| ***Funzionalità aggiuntive*** | Le ulteriori componenti del sistema di protocollo informatico necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni. |
| ***Funzionalità interoperative*** | Le componenti del sistema di protocollo informatico finalizzate a rispondere almeno ai requisiti di interconnessione di cui all'articolo 60 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i. |
| ***Funzionalità minime*** | La componente del sistema di protocollo informatico che rispetta i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i. |
| ***Funzione di hash*** | Una funzione matematica che genera, a partire da una evidenza informatica, una sequenza di bit (impronta) in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti. |
| ***Generazione automatica di documento informatico*** | Formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni. |
| ***Hardware Security Module (HSM)*** | Dispositivi hardware dedicati per la sicurezza crittografica e la gestione delle chiavi in grado di garantire un elevato livello di protezione. |

| | |
|---|---|
| ***Hypertext Transfer Protocol (HTTP)*** | Protocollo di trasmissione, che permette lo scambio di file (testi, immagini grafiche, suoni, video e altri documenti multimediali) su World Wide Web. |
| ***Information and Communication Technology (ICT)*** | Tecnologia dell'Informazione e delle Telecomunicazioni. Il dipartimento che gestisce i sistemi informatici e telematici; |
| ***Identificativo univoco*** | Sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione. |
| ***Indice di Conservazione (IdC)*** | L'Indice del Pacchetto di Archiviazione (IPdA) |
| ***Indice del Pacchetto di Archiviazione (IPdA)*** | Indice che contiene le informazioni relative al Pacchetto di Archiviazione in formato xml, anche indicato nello standard SInCRO come IdC (Indice di Conservazione) |
| ***Indice del Pacchetto di Versamento (IPdV)*** | Indice che contiene le informazioni relative al pacchetto di versamento in formato xml. |
| ***Immodificabilità*** | Caratteristica che rende la rappresentazione del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso. |
| ***Impronta*** | La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash. |
| ***Insieme minimo di metadati del documento informatico*** | Complesso dei metadati da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta. |
| ***Integrità*** | Insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato. |
| ***Interoperabilità*** | Capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi. |
| ***Leggibilità*** | Insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti. |
| ***Linee Guida*** | Linee Guida sulla formazione, gestione e conservazione dei documenti informatici emanate da AgID. |
| ***Log di sistema*** | Registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati. |
| **Manuale del sistema di conservazione** | Il presente documento, per brevità indicato anche come il "Manuale". |
| ***Manuale di gestione*** | Strumento che descrive il sistema di gestione informatica dei documenti. |
| ***Memorizzazione*** | Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici. |

| | |
|---|---|
| ***Marca temporale*** | Evidenza informatica che consente di rendere opponibile a terzi un riferimento temporale; la marca temporale prova l'esistenza in un certo momento di una determinata informazione, sotto forma di struttura dati firmata da una Time Stamping Authority. |
| ***Metadati*** | Insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione. |
| ***Normativa regolante la conservazione digitale di documenti informatici*** | Si intende: il D.lgs. 7 marzo 2005, n. 82 e s.m.i. (Codice dell'amministrazione Digitale "CAD") e i relativi decreti attuativi, le regole tecniche e aggiungendo, per il documento informatico a rilevanza tributaria, le disposizioni di cui al DMEF 17 giugno 2014 e s.m.i., il DPR 26 ottobre 1972 n. 633 e s.m.i., il DPR 29 settembre 1973 n. 600 e s.m.i., i provvedimenti interpretativi emessi dagli organi competenti. |
| ***Network Time Protocol (NTP)*** | Protocollo per la sincronizzazione del tempo. |
| ***Object IDentifier (OID)*** | Sequenza numerica univoca che identifica un oggetto (struttura, algoritmo, parametro, sistema) nell'ambito di una gerarchia generale definita dall'ISO. |
| ***Originali non unici*** | I documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi. |
| ***Pacchetto di Archiviazione*** | Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche e 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. |
| ***Pacchetto di invio documenti*** | Pacchetto informativo utilizzato per inviare i documenti fisici al sistema di conservazione a seguito dell'avvenuta accettazione di un pacchetto di versamento. |
| ***Pacchetto di versamento*** | Pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel Manuale di conservazione; |
| ***Pacchetto informativo*** | Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, documenti amministrativi informatici, documenti informatici rilevanti ai fini tributari, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare. |
| ***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 nell'ambito dell'organizzazione di appartenenza. |
| ***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 nell'ambito dell'organizzazione di appartenenza. |
| ***Piano di conservazione*** | Strumento, integrato con il sistema di classificazione per la definizione dei 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 e s.m.i. |

| | |
|---|---|
| ***Personal Identification Number (PIN)*** | Codice di sicurezza riservato che permette l'identificazione del soggetto abbinato ad un dispositivo fisico. Permette ad esempio l'attivazione delle funzioni del dispositivo di firma; |
| ***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; |
| ***Processo di conservazione*** | Insieme delle attività finalizzate alla conservazione dei documenti informatici; |
| ***Processo/servizio di marcatura temporale*** | E' il processo/servizio che associa in modo affidabile un'informazione e un particolare momento, al fine di stabilire prove attendibili che indicano il momento in cui l'informazione esisteva. |
| ***Produttore*** | E' il Cliente, di norma diverso dal Titolare, che in proprio o attraverso le persone fisiche da egli stesso incaricate produce il Pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione; nel caso di Pubblica Amministrazione è identificato nella figura del responsabile della gestione documentale. |
| ***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. |
| ***Registrazione informatica*** | Insieme delle informazioni risultanti da transazioni informatiche o dalla presentazione in via telematica di dati attraverso moduli o formulari resi disponibili in vario modo all'utente. |
| ***Registro particolare*** | Registro informatico specializzato per tipologia o per oggetto; nell'ambito della pubblica amministrazione è previsto ai sensi dell'articolo 53, comma 5 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.; |
| ***Registro di protocollo*** | Registro informatico della corrispondenza in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti. |
| ***Referente/i del Cliente*** | E'/sono le persone fisiche che il Cliente indica ad Aruba PEC quali punti di riferimento tecnico ed organizzativo per gli aspetti che riguardano le comunicazioni relative all'erogazione del servizio di conservazione. |
| ***Repertorio informatico*** | Registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche che trattano il procedimento, ordinati secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica. |
| ***Responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi*** | Dirigente o funzionario, comunque 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. |
| ***Responsabile della sicurezza*** | Soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza. |
| ***Riferimento temporale*** | Informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento. |

| | |
|---|---|
| ***Scarto*** | Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse culturale. |
| ***Scheda/e di conservazione*** | Elenco dei documenti informatici che il Cliente sottopone a conservazione con il Contratto. |
| ***Sistema di classificazione*** | Strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata. |
| ***Sistema di conservazione*** | Insieme di hardware, software, politiche, procedure, linee guida, regolamenti interni, infrastrutture fisiche e organizzative, volto ad assicurare la conservazione elettronica dei documenti del Cliente per il periodo di tempo specificato nel Contratto. Detto sistema tratta i documenti informatici in conservazione in pacchetti informativi che si distinguono in pacchetti di versamento, pacchetti di archiviazione e pacchetti di distribuzione; |
| ***Sistema di gestione informatica dei documenti*** | Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.; per i privati è il sistema che consente la tenuta di un documento informatico. |
| ***SSL – Secure Socket Layer*** | Protocollo standard per la gestione di transazioni sicure su Internet, basato sull'utilizzo di algoritmi crittografici a chiave pubblica. |
| ***Staticità*** | Caratteristica che indica l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione; |
| ***Transazione informatica*** | Particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche della base di dati. |
| ***Testo unico*** | Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni. |
| ***Titolare/i*** | La/e persona/e fisica/che o giuridica/che o altro tipo di società o ente che è/sono giuridicamente responsabili/e della formazione dei documenti da conservare formati in proprio ovvero formati da terzi in suo/loro nome, conto e interesse. |
| ***Titolare dell'oggetto della conservazione*** | Soggetto produttore degli oggetti di conservazione. |
| ***Time Stamping Authority (TSA)*** | Trust Service Provider che fornisce servizi di marcatura temporale. |
| ***Time Stamping Service (TSS)*** | servizio fiduciario consistente nella creazione di marcature temporali elettroniche. |
| ***Ufficio utente*** | Riferito ad un area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico. |
| ***Uniform Resource Locator (URL)*** | Sistema standard di nomenclatura specificante un sito, dominio o altro oggetto (file, gruppo di discussione, ecc.) su Internet. La prima parte dell'URL (http , ftp, file, telnet, news) specifica il protocollo di accesso all'oggetto; |

| | |
|---|---|
| ***Utente*** | 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. |
| ***Validazione temporale*** | Il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi. |
| ***Versamento agli archivi di stato*** | Operazione con cui il responsabile della conservazione di un'amministrazione statale effettua l'invio 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. |

# 3 Normativa e standard di riferimento

## 3.1 Normativa di riferimento

Il sistema di conservazione digitale di Aruba PEC, è stato realizzato in conformità alla normativa vigente in materia di conservazione dei documenti informatici. Alla data l'elenco dei principali riferimenti normativi italiani in materia è costituito da:

- Agenzia per l'Italia Digitale (AgID), **Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici** (Determinazione n. 407/2020 del 9 settembre 2020 e s.m.i.;);
- Agenzia per l'Italia Digitale (AgID) **Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici**. (Determinazioni AgID n. 455/2021 e s.m.i.;)
- **Regolamento (UE) N. 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
- **Regolamento (UE) 2024/1183** del Parlamento europeo e del Consiglio, dell'11 aprile 2024, che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale;
- **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.
- **Decreto Legislativo 30 giugno 2003, n. 196** e s.m.i. – Codice in materia di protezione dei dati personali;
- **Decreto Legislativo 22 gennaio 2004, n. 42** e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- **Decreto Legislativo 7 marzo 2005 n. 82** e s.m.i. – Codice dell'amministrazione digitale (CAD);
- **Decreto del Presidente della Repubblica 28 dicembre 2000**, **n. 445** e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- **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 s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- **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;
- **D.M. 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. 82/2005;
- **Il DPR nr. 1409 del 30 settembre 1963 -** (Legge archivistica) all'art. 30 prevede che le cartelle cliniche siano conservate illimitatamente. Secondo le norme vigenti, inoltre, gli originali cartacei delle cartelle cliniche in quanto originali unici, non possono essere distrutti;
- **Circolare Ministero della Sanità 19 dicembre 1986, n. 61 -** Circolare avente per oggetto il periodo di conservazione della documentazione sanitaria presso le istituzioni sanitarie pubbliche e private di ricovero e cura
- **DM 14.2.1997 -** Norma di attuazione del D.lgs n.230/95, "Determinazione delle modalità affinché i documenti radiologici e di medicina nucleare e i resoconti esistenti siano resi tempestivamente disponibili per successive esigenze mediche, ai sensi dell'art. 111, comma 10, del decreto legislativo 17 marzo 1995, n. 230"
- **D.lgs 26 maggio 2000, n. 187 -** Attuazione della direttiva 97/43/Euratom in materia di protezione sanitaria delle persone contro i pericoli delle radiazioni ionizzanti connesse ad esposizioni mediche
- **Prontuario di selezione per gli archivi delle aziende sanitarie locali e delle aziende ospedaliere, 2005**
  Atto di indirizzo che reca indicazioni sui tempi di conservazione dei documenti generati e/o custodita Aziende Sanitarie pubbliche ed accreditate, redatto dal Ministero per i Beni e la Attività Culturali
  **Consiglio dei Ministri – Conferenza Stato Regioni 02 Marzo 2012 -** Linee Guida per la dematerializzazione della documentazione clinica in diagnostica per immagini. Normativa e prassi.

## 3.2 Standard di riferimento

Dove non sono indicate una versione e/o una data specifica, si intende fare riferimento alla più recente versione disponibile del documento citato:

- **ISO 14721:2025 OAIS** (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- **ISO 16363:2025** Space data and information transfer systems — Audit and certification of trustworthy digital repositories
- **ISO/IEC 27001:2017** – "Information technology – Security techniques – Information security management systems – Requirements";
- **ISO/IEC 27001:2022** – Information security, cybersecurity and privacy protection — Information security management systems — Requirements;
- **ISO/IEC 27002:2022** – "Information technology — Security techniques — Code of practice for information security controls";
- **ISO/IEC 27005:2011** – "Information technology — Security techniques — Information security risk management);
- **ISO 9001:2015** – Quality management systems – Requirements;
- **ISO 37001:2025 -** Anti-bribery management systems — Requirements with guidance for use;
- **ISO 22301:2019** Security and resilience — Business continuity management systems — Requirements
- **UNI 11386:2020 Standard SInCRO** - Supporto all'interoperabilità nella conservazione e recupero degli oggetti digitali
- **ISO 15836:2009** Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.
- **Dicom 3.0** (Digital Imaging and Communications in Medicine, immagini e comunicazione digitali in medicina)
- **Health Level 7 (HL7)** versione 2.3.1 e 2.5
- Integrating the Healthcare Enterprise (IHE)
- **UNI ISO 15489-1: 2006** Information and documentation -- Records management -- Part 1: General
- **UNI ISO 15489-2: 2007** Information and documentation—Records management. Part 2: Guidelines
- **ETSI EN 319 401 V3.1.1 (2024-06)** Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- **ETSI TS 119 511 V1.2.1 (2025-10)** Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques.

# 4 Struttura organizzativa per il servizio di conservazione

## 4.1 Profilo aziendale

**Aruba PEC S.p.A.** (www.pec.it), società interamente controllata da Aruba S.p.A., è la società del Gruppo Aruba specializzata nell'erogazione di servizi digitali a valore legale, servizi fiduciari e soluzioni per la gestione dei processi documentali e delle comunicazioni elettroniche. Costituita nel 2006, la società ha progressivamente consolidato il proprio ruolo nel mercato italiano ed europeo, ampliando il perimetro della propria offerta dalla Posta Elettronica Certificata ai servizi di firma digitale, marcatura temporale, identità digitale e conservazione dei documenti informatici.

Aruba PEC è **Gestore di Posta Elettronica Certificata** accreditato presso AgID e iscritto nel relativo elenco pubblico. Il servizio PEC, nelle sue declinazioni consumer e business, è erogato in conformità al quadro normativo nazionale di riferimento, tra cui il DPR 11 febbraio 2005, n. 68, il Decreto Ministeriale 2 novembre 2005 e l'articolo 48 del Codice dell'Amministrazione Digitale, che attribuisce alla trasmissione tramite PEC valore legale equivalente, nei casi previsti, a quello della raccomandata con avviso di ricevimento.

Dal 2007 la società è inoltre accreditata come **Certification Authority** e presta servizi di firma elettronica qualificata, anche in modalità remota, nonché servizi di validazione temporale. Tali servizi rientrano nel perimetro dei servizi fiduciari disciplinati dal Regolamento (UE) n. 910/2014, eIDAS, e sono erogati in coerenza con il Codice dell'Amministrazione Digitale, le relative regole tecniche e le Linee Guida emanate da AgID.

Aruba PEC è altresì **Identity Provider SPID** tramite il servizio Aruba ID, realizzato in conformità al DPCM 24 ottobre 2014 e agli atti attuativi di AgID, che regolano il Sistema Pubblico di Identità Digitale e ne definiscono i requisiti di sicurezza, affidabilità e interoperabilità per l'accesso ai servizi online della Pubblica Amministrazione e dei soggetti privati aderenti.

Nell'ambito della gestione documentale, Aruba PEC fornisce servizi di **conservazione digitale a norma**, inclusa la conservazione dei messaggi PEC e dei documenti aziendali, anche attraverso piattaforme dedicate quali DocFly. I servizi di conservazione sono progettati ed erogati nel rispetto delle disposizioni del Codice dell'Amministrazione Digitale e delle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici, al fine di garantire nel tempo autenticità, integrità, affidabilità, leggibilità e reperibilità dei documenti conservati.

In particolare, per il Servizio di Conservazione:

- a partire dal 14/02/2022, Aruba PEC risulta iscritta al **Marketplace dei conservatori AgID**, a norma del Regolamento sui criteri per la fornitura dei servizi di conservazione AgID https://conservatoriqualificati.agid.gov.it/?page_id=276 ;
- a partire dal 7 agosto 2024, il servizio Docfly – Conservazione Digitale a Norma risulta **qualificato nel Marketplace ACN** secondo quanto disposto nel Decreto direttoriale prot. N. 29 del 02/01/2023, come modificato dal Decreto prot. N. 20610 in data 28/07/2023 https://www.acn.gov.it/portale/w/sa-3158 .

Aruba PEC S.p.A. possiede un articolato set di **certificazioni ISO** che attestano la maturità dei propri sistemi di gestione e l'affidabilità dei servizi erogati. In particolare, è certificata **ISO/IEC 27001** per il Sistema di Gestione della Sicurezza delle Informazioni, con estensioni **ISO/IEC 27017** e **27018** a tutela della sicurezza dei servizi cloud e della protezione dei dati personali. È inoltre conforme alla **ISO 9001** per la gestione della qualità dei processi aziendali e alla **ISO/IEC 20000-1** per la gestione dei servizi IT. A completamento del quadro, Aruba PEC ha conseguito anche la **ISO 22301**, relativa alla Business Continuity, a garanzia della continuità operativa dei servizi critici. Tali certificazioni supportano il posizionamento della società come prestatore affidabile di servizi digitali e fiduciari regolamentati.

## 4.2 Dati identificativi del Conservatore

Il servizio di Conservazione viene erogato dalla società Aruba PEC della quale riportiamo nel seguito tutte le informazioni identificative.

| Dati identificativi del Conservatore | |
|---|---|
| **Ragione Sociale:** | Aruba PEC S.p.A. |
| **Sede Legale:** | Via San Clemente, 53<br>24036 – Ponte San Pietro (BG)<br>Tel.: +39 0575 0500<br>Fax: +39 0575 862020 |
| **Partita IVA:** | 01879020517 |
| **Iscrizione registro delle imprese:** | Iscritta al registro delle imprese di Bergamo con numero 01879020517 |
| **REA:** | 445886 |
| **Capitale sociale:** | € 6.500.000 (interamente versati) |
| **Siti web:** | www.pec.it |
| **PEC:** | servizifiduciari@arubapec.it |

*Tabella 1 - Dati del Conservatore*

In questo capitolo sono indicate le strutture organizzative coinvolte nel servizio di conservazione comprese le responsabilità, che intervengono nelle principali funzioni che riguardano il servizio di conservazione.

## 4.3 Ruoli e responsabilità

Nel sistema di conservazione si individuano i seguenti ruoli principali:

| Ruolo | Organizzazione di appartenenza |
|---|---|
| Titolare dell'oggetto della conservazione | Cliente |
| Produttore dei PdV | Cliente |
| Responsabile della conservazione | Cliente |
| Referenti del Cliente | Cliente |
| Conservatore | Aruba PEC |
| Utente | Cliente/Terzi autorizzati |

Aruba PEC, nel suo ruolo di Conservatore, agisce nei limiti dell'affidamento conferito e nell'osservanza degli obblighi ivi previsti nonché nel rispetto della normativa regolante la conservazione digitale di documenti informatici e delle presenti prescrizioni; in particolare, essa agirà attraverso persone fisiche dalla stessa formalmente incaricate.

L'attività di Aruba PEC riguarda la sola conservazione digitale dei documenti informatici del Cliente, senza alcuna responsabilità e possibilità di intervento ed accesso al contenuto degli stessi.

A carico del Responsabile del servizio di conservazione, non è posto alcun obbligo/dovere di elaborare i documenti informatici versati in conservazione al fine di estrarre i relativi metadati che, pertanto, dovranno essere forniti e associati ai rispettivi documenti a cura e carico del Cliente.

Il Responsabile del servizio di conservazione opera altresì nell'osservanza di quanto stabilito nel presente *Manuale*, al quale, se necessario, è sin da ora autorizzato ad apportare le modifiche, le integrazioni e gli aggiornamenti ritenuti necessari e/o conseguenti al mutato contesto tecnico-giuridico della normativa in materia. Tutto il personale di Aruba PEC è stato assunto nel rispetto di politiche rigorose volte ad accertarne, tra l'altro, l'alto grado di professionalità nonché i requisiti morali e di onorabilità.

**L'utente** è il soggetto che richiede al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge. Tali informazioni vengono fornite dal sistema di conservazione secondo le modalità previste nel presente *Manuale*.

Come già anticipato, il processo di conservazione impone al Cliente l'istituzione di una struttura ed una organizzazione interna, coerente con le proprie politiche di efficienza gestionale, che garantisca la piena osservanza alle disposizioni normative di riferimento e di quanto previsto dal presente *Manuale,* dal *Contratto* e dai rispettivi allegati.

A tale scopo, in base alle specifiche necessità, il Cliente deve, sia dal punto di vista dell'impostazione operativa delle attività propedeutiche alla conservazione digitale dei propri documenti informatici sia dal punto di vista della scelta delle risorse coinvolte nel processo, organizzare il lavoro all'interno della propria organizzazione affinché esso venga svolto secondo i principi stabiliti dalla normativa in materia nonché dalle specifiche regole tecniche.

## 4.4 Ruoli all'interno della struttura organizzativa del Conservatore

Qui di seguito si dà conto della struttura organizzativa del processo di conservazione adottato evidenziando, nel contempo, le funzioni, le responsabilità e gli obblighi dei diversi soggetti che intervengono nel suddetto processo. Il processo di conservazione prevede una serie di attività che implicano il concorso di numerosi soggetti, a differenti livelli e con diverse responsabilità.

Qui di seguito vengono dettagliate per singola attività i diversi compiti e responsabilità delle figure preposte alla gestione

e controllo del sistema di conservazione.

Il processo di conservazione, prevede, le seguenti **figure responsabili**:

1. Responsabile del servizio di conservazione;
2. Responsabile della funzione archivistica di conservazione;
3. Responsabile del trattamento dei dati personali, ora Responsabile della protezione dei dati personali (DPO)
4. Responsabile della sicurezza dei sistemi per la conservazione;
5. Responsabile dei sistemi informativi per la conservazione;
6. Responsabile dello sviluppo e della manutenzione del sistema di conservazione

Ciascuno dei responsabili sopra elencati può avvalersi, per lo svolgimento delle attività al medesimo attribuite, di addetti ed operatori formalmente incaricati.

## 4.5 Nomine presso Aruba PEC

Nella tabella riportata di seguito sono indicate le figure che attualmente ricoprono gli incarichi indicati al precedente paragrafo, nonché lo storico dei responsabili che nel tempo hanno assunto i medesimi ruoli.

Per ciascun ruolo sono altresì descritte le specifiche funzioni.

| Ruoli e responsabilità | | | | | |
|---|---|---|---|---|---|
| **Ruolo** | **Cognome** | **Nome** | **Responsabilità** | **Data nomina** | **Data cessazione** |
| **Responsabile del servizio di conservazione** | Sassetti | Andrea | 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 al Cliente; 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. | 04/01/2019 | |
| | *Braccagni* | *Simone* | *Come sopra* | *01/09/2014* | *03/01/2019* |
| **Responsabile della funzione archivistica di conservazione** | Boschi | Serena | Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte del Cliente, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici; monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione; collaborazione col Cliente 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. | 01/09/2014 | |

| | | | | | |
|---|---|---|---|---|---|
| **Responsabile del trattamento dei dati personali, ora Responsabile della protezione dei dati personali (DPO)** | Giommoni | Roberta | 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. In particolare tenuto a:<br>a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento UE 2016/679 nonché da altre disposizioni relative alla protezione dei dati;<br>b) sorvegliare l'osservanza del Regolamento UE 2016/679, di altre disposizioni relative alla protezione dei dati nonché delle politiche del titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;<br>c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del Regolamento UE 2016/679;<br>d) cooperare con l'autorità di controllo; e<br>e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento UE 2016/679, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.<br>Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. | 24/05/2018 | |
| **Responsabile del trattamento dei dati personali** | *Braccagni* | *Simone* | *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.* | *01/09/2014* | *23/05/2018* |
| **Responsabile della sicurezza dei sistemi per la conservazione** | David | Neumarker | 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. | 28/02/2022 | |
| | *Tacconi* | *Nicola* | *Come sopra* | *13/05/2020* | *28/02/2022* |
| | *Corsi* | *Matteo* | *Come sopra* | *06/09/2017* | *13/05/2020* |

| | | | | | |
|---|---|---|---|---|---|
| | *Santoni* | *Adriano* | *Come sopra* | *01/09/2014* | *05/09/2017* |
| **Responsabile dei sistemi informativi per la conservazione** | Gaverini | Angelo | Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione; monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con il fornitore; 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. | 06/09/2017 | |
| | *Ravazza* | *Roberto* | *Come sopra* | *01/09/2014* | *05/09/2017* |
| **Responsabile dello sviluppo e della manutenzione del sistema di conservazione** | Mauro | Manetti | Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione; pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione; monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione; interfaccia col Cliente 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; gestione dello sviluppo di siti web e portali connessi al servizio di conservazione. | 06/09/2017 | |
| | *Pulvirenti* | *Salvatore* | *Come sopra* | *01/09/2014* | *05/09/2017* |

## 4.6 Responsabilità e funzioni nel processo di conservazione

Di seguito sono indicati i compiti, le responsabilità e le funzioni di firma in relazione alle diverse fasi del processo di conservazione digitale.

| Fasi del processo | Descrizione delle fasi del processo di conservazione | | COMPITI | RESPONSABILITA' | FIRMA |
|---|---|---|---|---|---|
| **FASE 1** | **Acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico** | | | | |
| | **Descrizione sintetica** | Il sistema di conservazione riceve il pacchetto di versamento comprensivo dei metadati contenente le informazioni sugli oggetti digitali che saranno inviati in conservazione; tali informazioni saranno usate per generare l'indice del pacchetto di versamento. | **SC** | **RMGO** | **==** |
| **FASE 2** | **Verifica che il pacchetto di versamento e gli oggetti contenuti siano coerenti con le modalità previste nel presente Manuale di conservazione e con i formati di conservazione** | | | | |
| | **Descrizione sintetica** | Viene verificato che il PdV ricevuto sia corretto in particolare che il file dei metadati sia in linea con lo standard DocFly. Viene verificato che il PdV è versato nei termini contrattuali e di servizio stabiliti col produttore.<br>Per ognuno dei documenti inviati viene verificato che l'hash del documento informatico sia corrispondente all'hash dichiarato all'interno del medesimo indice del pacchetto al fine di avere garanzia che la trasmissione del pacchetto sia avvenuta correttamente e che l'integrità del documento informatico ricevuto sia assicurata. Vengono inoltre effettuati controlli di leggibilità, integrità. | **SC** | **RMGO** | **==** |
| **FASE 3** | **Eventuale rifiuto del pacchetto di versamento, nel caso in cui le verifiche di cui alla FASE 2 abbiano evidenziato anomalie e/o non conformità** | | | | |
| | **Descrizione sintetica** | Il sistema scarta l'intero pacchetto e invia notifica in automatico | **SC** | **RMGO** | **==** |
| **FASE 4** | **Generazione automatica del rapporto di versamento relativo a ciascun pacchetto 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 di seguito descritte** | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | **Descrizione sintetica** | Il sistema genera in automatico il rapporto di versamento per ognuno dei PdV che ha superato i controlli qualitativi. | **SC** | **RMGO** | **==** |
| **FASE 5** | **Sottoscrizione del rapporto di versamento con firma digitale apposta da Aruba PEC** | | | | |
| | **Descrizione sintetica** | Il sistema provvede in automatico alla sottoscrizione digitale del rapporto di versamento con certificato del RSC e alla marcatura temporale del rapporto. | **SC** | **RMGO** | **RSC** |
| **FASE 6** | **Preparazione e gestione del Pacchetto di Archiviazione (c.d. Pacchetto di Archiviazione)** | | | | |
| | **Descrizione sintetica** | Il sistema genera il Pacchetto di Archiviazione secondo le modalità descritte al cap. 6. | **SC** | **RMGO** | **==** |
| **FASE 7** | **Sottoscrizione del Pacchetto di Archiviazione con firma digitale apposta da Aruba PEC e apposizione di una validazione temporale con marca temporale alla relativa impronta. Tale operazione viene in breve chiamata anche "Chiusura del Pacchetto di Archiviazione"** | | | | |
| | **Descrizione sintetica** | Come previsto da normativa l'Indice di Conservazione, viene sottoscritto digitalmente dal RSC, una volta passato nello stato "conservato". | **SC** | **RMGO** | **RSC** |
| **FASE 8** | **Preparazione e sottoscrizione con firma digitale del Responsabile del servizio di conservazione del Pacchetto di Distribuzione ai fini dell'esibizione richiesta dall'utente** | | | | |
| | **Descrizione sintetica** | Come previsto da normativa il PdD viene sottoscritto digitalmente dal RSC | **SC** | **RER** | **RSC** |
| **FASE 9** | **Produzione di duplicati informatici o di copie informatiche effettuati su richiesta del Cliente in conformità a quanto previsto dalle regole tecniche in materia di formazione del documento informatico** | | | | |
| | **Descrizione sintetica** | Richieste di duplicati o copie informatiche vengono sottoscritte digitalmente dal RSC in modo da attestarne l'autenticità rispetto al documento sorgente | **SC** | **RER** | **RSC** |
| **FASE 10** | **Eventuale scarto del Pacchetto di Archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dal contratto di servizio, dandone preventiva informativa al Cliente al fine di raccoglierne il consenso** | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | **Descrizione sintetica** | Una volta scaduti i termini di conservazione previsti dal contratto, il sistema provvede a inviare una mail di notifica al client, il quale potrà decidere in autonomia se cancellarli dal sistema. | **SC** | **RCD**<br>**DPO** | **==** |

Legenda:

- **RMGO** - responsabile del monitoraggio della gestione ordinaria del sistema e dei processi di base di conservazione
- **RER** - responsabile dell'esibizione/restituzione dei documenti informatici conservati
- **RIS** - responsabile dell'infrastruttura sistemistica, del piano di Disaster Recovery / Piano di continuità operativa (Business Continuity Plan) e della sicurezza
- **RCD** - responsabile della cancellazione dei documenti e dei dati digitali
- **DPO** - responsabile della protezione dei dati personali
- **RSC** - responsabile del servizio di conservazione
- **SC** - Sistema di conservazione

# 5 Oggetti sottoposti a conservazione

## 5.1 Descrizione delle tipologie dei documenti sottoposti a conservazione

Come chiaramente esplicitato nel Contratto, il servizio di conservazione digitale dei documenti informatici non ha ad oggetto la gestione e conservazione di supporti fisici o cartacei (analogici). Il sistema è predisposto esclusivamente per la conservazione di documenti in formato informatico, ivi incluse le copie informatiche e le copie per immagine di documenti originariamente analogici, conformemente agli articoli 22 e 23 del CAD.

Per ogni formato definito viene individuato anche il **software necessario per la visualizzazione** del documento informatico.

Il cliente in autonomia configura tramite l'applicazione web utente le classi di documenti, specificando i formati dei documenti che dovranno essere accettati per ogni classe documentale. Si raccomanda l'utilizzo di formati standardizzati per la conservazione a lungo termine, al fine di garantire nel tempo l'integrità, l'autenticità e l'interoperabilità dei file, in conformità alle Linee Guida AgID.

Ogni variazione di formato di documento oppure dei dati utilizzati per l'indicizzazione può essere eseguita in autonomia dal cliente tramite l'applicazione web utente.

Il sistema di conservazione digitale è impostato per accettare le seguenti tipologie di documento:

- **documenti informatici:** intesi, ai sensi dell'art. 1, comma 1, lett. p) del CAD, come "il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti";
- **documenti amministrativi** comprendenti ogni rappresentazione del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, formati o detenuti da soggetti pubblici o privati nell'ambito di attività di pubblico interesse, ai sensi dell'art. 22 della Legge n. 241/1990;
- **documenti rilevanti ai fini tributari** come stabilito nel DM del MEF del 17 giugno 2014;
- **documenti clinici** che possono contenere informazioni su osservazioni cliniche dirette, quali rivelazioni di anamnesi, segni vitali o sintomi, osservazioni indirette, derivanti, ad esempio da diagnostica strumentale, esami di laboratorio o rappresentazione iconografica di resoconti radiologici, oppure opinioni mediche quali valutazioni di osservazioni cliniche, consulti e consulenze, obiettivi da raggiungere o piani diagnostico terapeutici, azioni di natura clinico-sanitaria atte a generare osservazioni cliniche ed opinioni mediche;
- **altri documenti in genere.**

Le diverse tipologie di documenti sono prodotte/formate/emesse a cura e sotto l'esclusiva responsabilità del Cliente mediante una delle seguenti principali modalità dalle regole tecniche vigenti:

a) redazione tramite l'utilizzo di appositi strumenti software;

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) registrazione informatica 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 basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

Al fine di garantire l'immodificabilità del documento informatico, questo deve essere formato in modo che forma e contenuto non siano alterabili durante le fasi di tenuta e accesso, garantendone la staticità nella successiva fase di conservazione.

Al fine di garantire l'identificazione certa del soggetto che ha formato il documento, i documenti informatici posti in conservazione sono in genere sottoscritti con firma digitale del Cliente e dovranno essere identificati in modo univoco e persistente.

È prevista, in ogni caso, la possibilità di depositare in conservazione documenti informatici non sottoscritti.

## 5.2 Copie informatiche di documenti analogici originali unici

Come noto, l'art. 22 del CAD disciplina l'efficacia probatoria delle copie informatiche di documenti analogici, distinguendo principalmente due scenari:

a) (Art. 22, comma 2, CAD) Le copie per immagine su supporto informatico di documenti originali analogici hanno la stessa efficacia probatoria degli originali se la loro conformità è attestata da un notaio o da altro pubblico ufficiale a ciò autorizzato, secondo le disposizioni delle Linee Guida emanate ai sensi dell'art. 71 del CAD.

b) (Art. 22, comma 3, CAD) Le copie per immagine su supporto informatico di documenti originali analogici, prodotte nel rispetto delle Linee Guida, hanno la stessa efficacia probatoria degli originali da cui sono tratte, a condizione che la loro conformità all'originale non sia espressamente disconosciuta.

Pertanto, qualora intendesse depositare in conservazione copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico, il Cliente è tenuto, a propria cura e spese, a predisporre quanto necessario per ottemperare alle richiamate disposizioni, scegliendo una delle seguenti procedure.

In via preliminare, sarà sempre cura e onere del Cliente:

1. Produrre la copia per immagine su supporto informatico del documento analogico mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, come previsto dall'art. 22, comma 1-bis, del CAD

Successivamente, per garantire l'efficacia probatoria della copia, il Cliente dovrà alternativamente:

Opzione A (Efficacia fino a disconoscimento - Art. 22, co. 3, CAD): per avvalersi dell'efficacia probatoria subordinata al mancato disconoscimento, la copia per immagine, prodotta come sopra indicato, deve essere realizzata in conformità alle Linee Guida. A tal fine, per garantire l'integrità, l'immodificabilità e la riconducibilità della copia, è necessario che il Cliente apponga sulla stessa una firma elettronica qualificata o digitale.

Oppure

Opzione B (Piena efficacia probatoria - Art. 22, co. 2, CAD): per attribuire alla copia per immagine la stessa efficacia probatoria dell'originale, il Cliente dovrà richiedere l'attestazione di conformità da parte di un notaio o di altro pubblico ufficiale a ciò autorizzato. Tale attestazione può essere formalizzata in due modi:

- Attestazione integrata nel documento: l'attestazione di conformità viene inserita direttamente nel documento informatico contenente la copia per immagine. Il documento così formato deve essere sottoscritto con firma digitale o elettronica qualificata dal pubblico ufficiale che rilascia l'attestazione. In questo caso, il Cliente dovrà depositare in conservazione il singolo file contenente sia la copia sia l'attestazione firmata digitalmente dal pubblico ufficiale.
- Attestazione come documento separato: l'attestazione di conformità viene prodotta come un documento informatico separato, il quale deve contenere un riferimento temporale e l'impronta informatica (hash) di ogni copia per immagine a cui si riferisce. Anche questo documento separato deve essere sottoscritto con firma digitale o elettronica qualificata dal pubblico ufficiale. In questo caso, il Cliente dovrà depositare in conservazione sia i file delle copie per immagine, sia il file dell'attestazione separata.

Resta fermo che, nei casi in cui la normativa applicabile preveda la conservazione dell'originale analogico o specifiche modalità di autenticazione della conformità all'originale, il Cliente dovrà assicurare il rispetto di tali ulteriori prescrizioni prima del deposito in conservazione.

## 5.3 Formati gestiti

Come noto, la leggibilità di un documento informatico dipende dalla possibilità e dalla capacità di interpretare ed elaborare correttamente i dati binari che costituiscono il documento, secondo le regole stabilite dal formato con cui esso è stato rappresentato. Il formato di un documento informatico è la convenzione usata per rappresentare il contenuto informativo mediante una sequenza di byte.

Il sistema di conservazione Aruba PEC garantisce la conservazione dei documenti prodotti nei formati previsti dall'allegato 2 "Formati di File e Riversamento" delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici.

I formati ammessi sono definiti in fase di configurazione delle classi documentali, attività svolta dal Cliente in autonomia. Tali formati sono successivamente recepiti e riepilogati nelle Schede di Conservazione, che costituiscono parte integrante della documentazione contrattuale. La configurazione delle classi documentali è propedeutica all'attivazione del servizio.

### *5.3.1 Caratteristiche generali dei formati*

I formati scelti devono essere, puntualmente richiamati nell'apposito allegato al *Contratto.* Aruba PEC, comunque raccomanda un insieme di formati che sono stati dalla stessa valutati in funzione di alcune caratteristiche quali:

| CARATTERISTICA | | DESCRIZIONE DELLA CARATTERISTICA |
|---|---|---|
| 1 | **APERTURA** | Un formato si dice "aperto" quando è conforme a specifiche pubbliche, cioè disponibili a chiunque abbia interesse ad utilizzare quel formato. La disponibilità delle specifiche del formato rende sempre possibile la decodifica dei documenti rappresentati in conformità con dette specifiche, anche in assenza di prodotti che effettuino tale operazione automaticamente.<br>Questa condizione si verifica sia quando il formato è documentato e pubblicato da un produttore o da un consorzio al fine di promuoverne l'adozione, sia quando il documento è conforme a formati definiti da organismi di standardizzazione riconosciuti. In quest'ultimo caso tuttavia si confida che quest'ultimi garantiscono l'adeguatezza e la completezza delle specifiche stesse.<br>In relazione a questo aspetto, Aruba PEC ha privilegiato formati già approvati dagli Organismi di standardizzazione internazionali quali ISO e OASIS. |
| 2 | **SICUREZZA** | La sicurezza di un formato dipende da due elementi:<br>- il grado di modificabilità del contenuto del file;<br>- la capacità di essere immune dall'inserimento di codice maligno. |
| 3 | **PORTABILITÀ** | Per portabilità si intende la facilità con cui i formati possano essere usati su piattaforme diverse, sia dal punto di vista dell'hardware che del software, inteso come sistema operativo. Di fatto si ottiene mediante l'impiego fedele di standard documentati e accessibili e dalla loro diffusione sul mercato. |
| 4 | **FUNZIONALITÀ** | Per funzionalità si intende la possibilità da parte di un formato di essere gestito da prodotti informatici, che prevedono una varietà di funzioni messe a disposizione del Cliente per la formazione e gestione del documento informatico. |
| 5 | **SUPPORTO ALLO SVILUPPO** | Il supporto allo sviluppo è la modalità con cui si mettono a disposizione le risorse necessarie alla manutenzione e sviluppo del formato e i prodotti informatici che lo gestiscono (organismi preposti alla definizione di specifiche tecniche e standard, società, comunità di sviluppatori, ecc.). |
| 6 | **DIFFUSIONE** | La diffusione è l'estensione dell'impiego di uno specifico formato per la formazione e la gestione dei documenti informatici. Questo elemento influisce sulla probabilità che esso venga supportato nel tempo, attraverso la disponibilità di più prodotti informatici idonei alla sua gestione e visualizzazione. |

### *5.3.2 Formati consigliati per la conservazione*

Di seguito si fornisce un elenco non esaustivo dei formati consigliati per la conservazione:

| Formato | Estensione |
|---|---|
| PDF, PDF/A | .pdf |
| TIFF, TIFF/IT, TIFF/EP | tif , .tiff |
| JPG, JPG2000 | .jpg, .jpeg, .jfi, .jfif, .jif, .jpe |
| OOXML | .docx, .xlsx, .pptx |
| OPENDOCUMENT | .ods, .odp, .odg, .odb, .odf |
| XML | .xml, .xsl |
| TXT | .txt |
| ZIP | .zip |
| XFIR | .xfir |
| P7M | .p7m |
| TDS | .tds |
| Formati messaggi di posta elettronica | .eml ,.mht, .mbox |
| OPEN DOCUMENT | .ods, .odp, .odg, .odb, .odf |
| EXCEL® 2007 | .xls |

Tutti i formati gestiti dal Conservatore Aruba PEC vengono elencati all'interno di un apposito elenco, costantemente aggiornato.

### *5.3.3 Identificazione*

L'associazione del documento informatico al relativo formato avviene tramite la libreria Apache Tika, che rileva il formato effettivo del file inviato in conservazione. Successivamente, viene verificato che il formato riconosciuto sia stato configurato nella classe documentale indicata dal cliente in fase di versamento. Per identificare il formato dei files posti in conservazione il sistema procede con l'analisi di ogni singolo documento informatico contenuto all'interno dei pacchetti di versamento. Il Conservatore procede come segue:

| | | |
|---|---|---|
| **1** | **Fase di RICEZIONE** | Fase di ricezione del PdV. Il sistema di Aruba PEC riceve in un'unica soluzione sia i documenti che il file di metadati ad essi associati; esegue la verifica sugli hash dei documenti indicati e ne verifica la corrispondenza. |
| **2** | **Fase di VALIDAZIONE** | Viene fatto il controllo sul formato. Viene verificato che sia stato censito nella classe documentale configurata dal cliente in cui i documenti sono stati versati. |

## 5.4 Metadati da associare alle diverse tipologie di documenti

Con il termine "metadati" si indicano tutte le informazioni significative associate al documento informatico, escluse quelle che costituiscono il contenuto del documento stesso. I metadati riguardano principalmente, ma non esclusivamente, i

modi, i tempi ed i soggetti coinvolti nel processo della formazione del documento informatico, della sua gestione e della sua conservazione.

Metadati sono anche le informazioni riguardanti gli autori, gli eventuali sottoscrittori e le modalità di sottoscrizione e la classificazione del documento. I metadati devono essere associati al documento dal Cliente prima del versamento in conservazione e per tale ragione vengono esplicitati all'interno di uno specifico allegato, facente parte del Contratto di servizio stipulato con il Conservatore (come specificato al par. 10.1.2).

I metadati forniti dal Cliente restano di proprietà del Cliente medesimo.

I metadati, seppur chiaramente associati al documento informatico, possono essere gestiti indipendentemente dallo stesso. In relazione ai diversi tipi di documenti informatici posti in conservazione, è previsto un "**set minimo"** di metadati.

Oltre al set minimo di metadati, il Cliente potrà decidere di associare al documento informatico eventuali ulteriori metadati c.d. "*extrainfo*". Le extra info verranno inserite, al pari degli altri metadati, nell'indice di conservazione. I metadati *extrainfo* possono essere inseriti in fase di configurazione della classe documentale.

## 5.5 Modalità di assolvimento dell'imposta di bollo sui documenti posti in conservazione

Il Cliente è tenuto al pagamento dell'imposta di bollo eventualmente dovuta sui documenti depositati in conservazione.

Pertanto, il versamento dell'imposta dovuta dovrà essere effettuato dal Cliente nei termini previsti dall'art. 6 del DMEF 17 giugno 2014 e nei modi di cui all'art. 17 del D.Lgs. 9 luglio 1997, n. 241 e loro successive modificazioni e/o integrazioni.

Tutti i relativi e conseguenti obblighi, adempimenti e formalità per l'assolvimento dell'imposta di bollo sui documenti informatici posti in conservazione sono ad esclusivo onere e carico del Cliente, il quale dovrà attenersi alle disposizioni di legge ed ai documenti di prassi emanati ed emanandi.

Allo stesso modo, sono ad esclusivo onere e carico del Cliente tutte le comunicazioni da presentare al competente Ufficio delle entrate in forza di quanto stabilito dalla normativa regolante la conservazione digitale di documenti informatici.

## 5.6 Pacchetto di versamento

In questo paragrafo sono fornite le tipologie di pacchetto di versamento gestite e per ciascuna di esse descritta la struttura dati.

Sul sistema di Aruba PEC la creazione dell'indice di versamento IPdV (in formato xml) è generata in automatico dal sistema stesso basandosi sia sui parametri dichiarati durante la fase di versamento che sui metadati compilati dal cliente (apposito file se versamento via WS o tramite Front End nella modalità di versamento manuale, recuperati dall'interfaccia web in caso di versamento guidato).

Lo standard del Conservatore prevede l'indice di un pacchetto di versamento che si caratterizza per le seguenti parti:

- area di identificazione del PDV
- area di identificazione dei documenti costituenti il pacchetto e composta dai seguenti elementi:
  - metadato obbligatori
  - metadati extra-info

Nella prima parte il dato importante è il *pdvid* ovvero l'identificativo del PDV. Esso viene generato in automatico dal sistema e deve essere univoco all'interno dello spazio gestito dal produttore, quindi indipendentemente dall'archivio.

La seconda parte prevede una lista di elementi, uno per ogni documento da versare. Ogni singolo file deve essere per prima cosa identificato. A questo scopo sono necessari i seguenti dati:

- nome file
- algoritmo di hashing per la generazione dell'impronta
- impronta del documento

Inoltre, poiché il sistema deve controllare la tipologia di documento per valutarne l'aderenza alle configurazioni della classe su cui avviene il versamento, deve essere indicato il MIME type del documento.
Per rimanere poi aderenti alla norma vigente devono essere passati anche un id unico dei singoli documenti del pacchetto

e la data di chiusura degli stessi.

L'ultima parte dell'Indice contiene un insieme di metadati come indicato in fase di configurazione dal Produttore.

## 5.7 Pacchetto di Archiviazione

In questo paragrafo viene resa la struttura del Pacchetto di Archiviazione nonché il trattamento dei pacchetti di archiviazione.

### *5.7.1 Specifiche Pacchetto di Archiviazione*

Il Pacchetto di Archiviazione è costituito da una cartella, a sua volta composta da:

- Una sotto cartella contenente l'insieme degli elementi (documenti e/o altri PdA) che compongono il pacchetto comprese alcune evidenze di conservazione (IPdV e RdV);
- l'Indice del Pacchetto di Archiviazione (IPdA) che elenca tutti gli elementi del pacchetto.
  Il formato dell'indice è aderente allo standard UNI SInCRO (nel quale è indicato come IdC/PIndex – Indice di Conservazione) ed è marcato temporalmente e firmato elettronicamente con certificato del Responsabile del Sistema di Conservazione;
- L'RdC cioè la ricevuta di conservazione del PdA.

## 5.8 Pacchetto di Distribuzione

Il Pacchetto di Distribuzione contiene l'insieme degli elementi (documenti e/o PdA) precedentemente ricercati e selezionati dall'utente.

Viene offerto sotto forma di un archivio .zip che per ogni elemento contiene:

- Indice del pacchetto di distribuzione (IPDD) firmato e marcato contenente l'elenco dei PdA oggetto della distribuzione e i relativi documenti in essi contenuti;
- una cartella per ognuno dei PdA oggetto dell'esibizione. Nel caso di un documento il documento stesso, nel caso di un PdA l'intero PdA, ovvero tutti gli elementi di cui è costituito.

# 6 Il processo di conservazione

In questo capitolo sono riportate tutte le fasi inerenti il processo di conservazione dei documenti informatici

## 6.1 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico

Come già anticipato in altre parti del presente *Manuale*, unico responsabile del contenuto del pacchetto di versamento è il Cliente (Produttore), che deve formarlo, sottoscriverlo con firma digitale (ove previsto) e trasmetterlo al sistema di conservazione secondo le modalità operative di versamento definite nel presente *Manuale,* nel *Contratto* e nei rispettivi allegati.

L'operazione di versamento consiste nella trasmissione dei documenti da conservare e dei metadati che li specializzano, così come già accennato precedentemente.

L'operazione di versamento consiste nella trasmissione dei documenti da conservare e dei metadati che li specializzano, così come già accennato precedentemente.

La ricezione e presa in carico di un pacchetto di versamento segue uno schema logico di funzionamento che si articola in due fasi distinte:

1. ricezione del file di metadati (usato dal sistema per creare l'Indice del Pacchetto di Versamento IPdV) e ricezione dei documenti che fanno parte del Pacchetto di Versamento (PdV).
2. Validazione del PdV

L'uno e gli altri possono essere trasmessi al sistema di conservazione attraverso canali diversi. Alternativamente essi possono essere:

- interfaccia web
- invocazione di metodi tramite web service REST ~~(per i soli Produttori DF Premium)~~

Ogni canale messo a disposizione è provvisto di opportuni accorgimenti per la trasmissione dei dati in modalità sicura:

- l'interfaccia web viaggia su protocollo HTTPS
- il web service REST è contattabile tramite protocollo HTTPS
- la PEC nativamente garantisce autenticità della provenienza e notifica di consegna in modalità sicura

Per il versamento delle operazioni di conservazione di un PdV è necessario scegliere esclusivamente uno dei canali sopra citati.

Il sistema di conservazione prende in carico un PdV solo dopo aver superato con esito positivo i relativi controlli.

Tale operazione viene ufficialmente sancita dalla produzione del cosiddetto Rapporto di Versamento (RdV) che viene consegnato al cliente.

Poiché la produzione del RdV rappresenta formalmente la presa in carico del PdV da parte del sistema di conservazione, il RdV viene marcato temporalmente e firmato digitalmente direttamente o via delega dal Responsabile del servizio di Conservazione.

### *6.1.1 Versamento del file di metadati: creazione dell'indice del pacchetto di versamento*

L'IPdV è un'evidenza informatica, ovvero un file, che descrive il versamento stesso e i documenti che ne fanno parte attraverso l'uso di metadati. Questi sono di carattere diverso a seconda che descrivano proprietà e qualità del pacchetto in genere o dei singoli documenti.

È bene sottolineare che ogni PdV può contenere esclusivamente documenti della stessa tipologia, ovvero della stessa Classe Documentale. In questo senso l'elenco dei metadati dei singoli documenti è in qualche modo omogeneo.

Per consentire l'elaborazione automatica dei metadati il sistema di conservazione Aruba PEC richiede l'incapsulamento degli stessi in un determinato formato (JSON o csv) che di fatto concorre alla costruzione dell'IPdV da parte del sistema; tale IPdV sarà corredato anche da altre informazioni fornite tramite parametri della chiamata all'API (se il versamento è eseguito con WS) o dai valori immessi durante la fase di versamento da interfaccia Web (se il versamento avviene appunto

in maniera manuale o guidata da interfaccia grafica).

In tale file sono contenute sezioni diverse che identificano la qualità dei metadati. Essi infatti possono essere caratteristici del PdV e del soggetto versante, rappresentare direttive speciali di elaborazione per la conservazione, descrittivi dei singoli documenti che si vogliono conservare, a loro volta distinti in standard, come indicato nel paragrafo 12.4, o definiti insieme al Cliente in fase di stipula del contratto e infine caratteristici del formato del documento.

La funzione di ricezione dei documenti e relativi metadati dei pacchetti di versamento nel sistema di conservazione effettua, per ogni PdV, i seguenti controlli:

- abilitazione alla conservazione da parte del sistema di gestione documentale versante e in particolare dell'utente che effettua il versamento. In caso di esito negativo il sistema rifiuta il tentativo di versamento;
- controllo formale del file dei metadati. In particolare viene verificato che sia un formato JSON/csv valido per una delle Classi Documentali registrate a sistema. In caso di esito negativo il sistema rifiuta il tentativo di versamento;
- controllo sulla completezza e correttezza formale dei metadati, in relazione alla Classe Documentale rilevata. In caso di esito negativo il sistema rifiuta il tentativo di versamento;
- controllo sulla tipologia di documenti che si vuole versare. Ogni documento deve appartenere ad almeno uno dei formati ammessi dalla tipologia di Classe Documentale. In caso di esito negativo il sistema rifiuta il tentativo di versamento;
- eventuali controlli supplementari definiti insieme al Cliente. La gestione degli esiti negativi va formalizzato in sede contrattuale.

### *6.1.2 Ricezione documenti associati ad un pacchetto di versamento*

La ricezione dei documenti è contestuale all'invio del file dei metadati (JSON/csv) per cui il sistema di conservazione di verifica gli hash che sono dichiarati nel file JSON/csv.

Relativamente al singolo documento tra i metadati indicati sono di particolare importanza quelli utili all'identificazione dello stesso. Essi sono principalmente due: un hash del file stesso, ovvero una stringa di caratteri che normalizza con un particolare algoritmo in maniera univoca il documento stesso.

In particolare l'hash, che per il sistema di conservazione Aruba PEC deve essere in formato SHA256 o SHA512 base64, garantisce la riconoscibilità e incorruttibilità del documento in forma automatica e univoca.

Nel momento in cui un documento viene ricevuto da uno qualsiasi dei canali esposti precedentemente, ne viene calcolato l'hash in SHA265 e base64. Se il risultato è tra quelli precedentemente comunicati (tramite file JSON/csv) allora il file viene accettato.

Successivamente la funzione di ricezione dei documenti informatici nel sistema di conservazione effettua una serie di controlli atti a verificare formalmente leggibilità, integrità e la corrispondenza del documento alle regolamentazioni stabilite per la Classe Documentale di appartenenza. Per operare ciò il sistema determina il formato dello stesso sulla base di quanto esposto in precedenza (estensione e mimetype).

La mancata identificazione del formato del file causa il rifiuto dello stesso con conseguente restituzione di un errore.

Una volta individuato il formato del documento viene controllato che questo sia tra i formati ammessi per la Classe Documentale di appartenenza. Nel caso di esito negativo il PdV viene rifiutato e viene restituito un errore. Superati i primi controlli, ne vengono operati degli altri relativamente alla qualità dello stesso.

In relazione a ciascun documento informatico infine viene verificato che il salvataggio avvenga correttamente all'interno del sistema di conservazione.

Tutti i documenti informatici che non superano anche uno solo dei precedenti controlli **vengono rifiutati**. In questo caso non viene salvata alcuna informazione sul sistema di conservazione ed il pacchetto intero risulterà non conforme e quindi viene immediatamente eliminato.

**Quando tutti i documenti di un pacchetto di versamento vengono validati correttamente viene reso disponibile il rapporto di versamento sottoscritto con firma digitale dal Responsabile del servizio di Conservazione.**

Tale rapporto viene anche inviato via email da un indirizzo PEO all'indirizzo PEO del Responsabile di conservazione fornito dal cliente in fase contrattuale.

## 6.2 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti

Le funzionalità attivate nel processo di versamento/acquisizione del pacchetto di versamento prevedono dei controlli sia per i documenti versati che per i metadati ad essi associati (file che verrà utilizzato per la creazione automatica dell'indice del PdV) . La tabella riportata in basso elenca le diverse tipologie di controlli effettuati e per ognuna di esse indica l'azione prevista da sistema. Quest'ultima può tradursi in una operazione di rifiuto o notifica di un warning.

Il deposito di un pacchetto di versamento è distinto per ciascun pacchetto di documenti informatici omogenei (documenti omogenei, ossia aventi la stessa classe documentale). Pertanto, a classi documentali diverse corrispondono diversi PdV e versamenti, uno per ogni classe.

### Controlli nella fase di ricezione del PdV

| ID | Oggetto del controllo | Azione in caso di check negativo |
|---|---|---|
| **Verifica Autorizzazioni** | | |
| **1.01** | viene verificato che l'utente che effettua il versamento sia abilitato all'invio dei Pdv | Il sistema rifiuta l'intero pacchetto |
| **Verifica formale file metadata del PdV** | | |
| **2.01** | viene verificato che l'oggetto ricevuto sia formalmente un formato JSON o csv in linea con lo standard DocFly | Il sistema rifiuta l'intero pacchetto |
| **Verifica presenza dati-documenti nel file metadata del PdV** | | |
| **3.01** | viene effettuato un controllo semantico sui metadati presenti nell'indice del PdV | Il sistema rifiuta il PdV poiché uno o più metadati non rispettano il formato condiviso nel contratto di servizio |
| **3.02** | viene controllato che per ciascun documento dichiarato e descritto all'interno del file metadata del Pdv:<br>a. tutti i metadati minimi obbligatori siano presenti e nel formato corretto;<br>b. il formato del documento è un formato ammesso<br>c. l'estensione del documento sia tra quelle ammesse per il tipo documento;<br>d. il formato dichiarato sia corrispondente all'estensione del nome file | Il sistema rifiuta il PdV perché le verifiche formali sui documenti inviati e censiti nel file dei metadati hanno avuto esito negativo |

### Controlli sui documenti (files)

| ID | Oggetto del controllo | Azione in caso di check negativo |
|---|---|---|
| **Controllo ricezione documenti** | | |

| | | |
|---|---|---|
| **1.01** | Viene verificato, se richiesto dal cliente, che siano presenti firme digitali sul documento; | Il sistema rifiuta il PdV perché le verifiche sulla presenza di firme hanno avuto esito negativo |
| **1.02** | in caso di file firmati viene verificata la validità della firma apposta su ogni singolo documento:<br>• Controllo di conformità.<br>• Controllo Crittografico.<br>• Controllo Catena Trusted.<br>• Controllo Certificato.<br>• Controllo CRL | Il sistema rifiuta il pacchetto qualora il certificato di firma del documento non sia valido solo nel caso in cui sia stata richiesta la verifica della validità della firma stessa |
| **1.03** | viene verificato che il documento sia integro | Il sistema rifiuta il pacchetto nel caso l'hash del documento non sia corrispondente a quello dichiarato nel file metadata.json (o .csv) |
| **1.04** | viene verificato che il formato del documento informatico sia effettivamente valido e corrispondente a quanto dichiarato nel pacchetto di versamento. In tal caso i controlli eseguiti variano in funzione del formato atteso per ciascuno specifico documento. | Il sistema rifiuta il pacchetto poiché il formato del documento non è quello atteso |

## 6.3 Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico

Il sistema di conservazione predispone, per ciascun pacchetto di versamento, un **rapporto di versamento** che viene firmato dal Responsabile del Sistema di Conservazione. Lo schema del rapporto di versamento è illustrato nel paragrafo successivo (par. 6.3.1).

In particolare il rapporto di versamento contiene, tra l'altro, le seguenti informazioni:

- identificativo unico del PdV fornito dal sistema di conservazione;
- data di ricezione del PdV.
- per ogni documento viene indicato:
  - id univoco fornito dal sistema di conservazione;
  - hash;
  - data di ricezione;
  - esito della ricezione (accettato o warning);
  - Nome documento;
  - Hash;
  - Formato.

### 6.3.1 Specifiche rapporto di versamento

Il Rapporto di Versamento è basilare nel processo di conservazione, in quanto è documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.

Esso viene prodotto nel momento in cui tutti gli elementi utili per la conservazione del pacchetto di versamento sono stati consegnati al sistema e validati.

In esso sono presenti sempre i seguenti dati:

- id del Pacchetto di Versamento;
- id del Rapporto di Versamento;
- riferimento temporale (UTC) di generazione del Rapporto di Versamento;
- lista dei documenti afferenti al pacchetto. Per ognuno di essi sono distinguibili:
    - id come indicato nell'Indice del PdV;
    - id assegnato dal sistema;
    - impronta del documento;
    - nome del documento;
    - formato del documento;
    - data di ricezione del file;
    - esito controllo firma digitale (ove previsto);
    - esito controllo marca temporale (ove previsto).

Il Rapporto di Versamento viene sempre firmato digitalmente con certificato del Responsabile di Conservazione. In questo modo viene reso non modificabile.

## 6.4 Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie

Per la gestione dei rifiuti dei pacchetti di versamento e modalità di comunicazione delle anomalie si rimanda al par. 6.2.

## 6.5 Preparazione e gestione del Pacchetto di Archiviazione

Il Pacchetto di Archiviazione (PdA) è quello conservato dal sistema di conservazione e possiede un insieme completo di metadati utili alla conservazione a lungo termine.

Il Pacchetto di Archiviazione viene realizzato secondo lo standard di riferimento SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2020), che rappresenta lo standard nazionale riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione.

Uno o più pacchetti di versamento vengono trasformati in un Pacchetto di Archiviazione (PdA) in base alle regole tecniche standard del sistema di conservazione. Tali regole vengono definite entro gli accordi contrattuali alla configurazione della classe afferente agli stessi.

Il sistema di conservazione a lungo termine ha, fra le altre, la prerogativa di conservare l'autenticità dei documenti in esso contenuti.

La preservazione della suddetta autenticità non può però basarsi tout court sulla firma digitale in quanto quest'ultima:

- ha una validità slegata dall'architettura e dalla struttura del sistema di conservazione;
- ha una validità limitata nel tempo e pari al certificato emesso dalla CA;
- vede la propria sicurezza legata ad algoritmi soggetti ad obsolescenza tecnologica.

È pertanto fondamentale che il sistema di conservazione a lungo termine verifichi la validità ed il valore delle firme digitali apposte dal Cliente sui documenti informatici oggetto di conservazione.

A tale fine, il Cliente dovrà accertarsi che le firme digitali apposte sui documenti informatici inviati in conservazione:

a) siano valide al momento di sottoscrizione del documento informatico;

b) e mantengano piena validità sino al termine ultimo convenuto con il Conservatoreper la "chiusura" del Pacchetto di Archiviazione.

**Con la sottoscrizione dei pacchetti di archiviazione il Conservatore non sottoscrive il contenuto e la semantica dei documenti conservati ma asserisce solamente che il processo di conservazione è stato eseguito correttamente, nel rispetto della normativa regolante la conservazione digitale di documenti informatici**

### *6.5.1 Rettifica dei pacchetti di archiviazione*

Il sistema di conservazione prevede la possibilità di eseguire la rettifica del pacchetto di archiviazione in due distinte modalità:

1. Rettifica documentale
2. Rettifica dei metadati

In particolare la "rettifica documentale" avviene inviando un documento successivo rispetto a quello inviato in precedenza in conservazione. Tale operazione, riservata solamente al produttore o titolare con diritti di scrittura sulla classe documentale relativa, permette al cliente di sostituire un documento inviato in conservazione con un nuovo documento dello stesso tipo, lasciandone invariati i metadati.

Il cliente, una volta indicato il PDA sul quale applicare la rettifica, potrà procedere alla sostituzione di uno o più documenti ed inserire la motivazione relativa all'operazione. Il documento sarà sottoposto ai medesimi controlli di verifica previsti dal processo di conservazione sui documenti originariamente inviati al servizio di conservazione. Una volta sostituiti i documenti, il sistema mostrerà a video l'esito della rettifica: in caso di errori riscontrati, verrà indicato per ciascun documento la tipologia di errore, permettendo al cliente di apportare le modifiche necessarie per concludere l'operazione, altrimenti sarà confermato l'esito positivo della rettifica.

Il PDA rettificato conterrà l'IPDV ed i documenti modificati, mentre il PDA originale rimarrà a disposizione sul sistema di conservazione nel PDD e consultabile dal cliente in qualsiasi momento.

La "rettifica dei metadati" avviene in maniera simile alla precedente ma permette di mantenere i documenti già conservati andando a creare un PdA con le sole evidenze di conservazione in cui saranno riportati i valori modificati dal Produttore.

Le operazioni di rettifica verranno registrate nei log di sistema.

## 6.6 Preparazione e gestione del Pacchetto di Distribuzione ai fini dell'esibizione

Nel modello OAIS e in linea con la normativa vigente, il Pacchetto di Distribuzione è strutturato nel modello dati come il Pacchetto di Archiviazione. La differenza sta nella sua destinazione in quanto esso viene concepito per essere fruito ed utilizzato dall'utente finale (esibizione).

In questo caso, un PdD può anche non coincidere con il Pacchetto di Archiviazione originale conservato: anzi, molto spesso, ragioni di opportunità inducono a distribuire pacchetti informativi che sono un'estrazione del contenuto informativo di un PdA. Può anche verificarsi il caso di Pacchetto di Distribuzione che sono il frutto di più PdA che vengono "spacchettati" e reimpacchettati per un più fruibile utilizzo da parte dell'utente.

Un utente autorizzato da un soggetto produttore, quindi, è in grado di interrogare il sistema per ricevere in uscita uno specifico Pacchetto di Distribuzione. L'utente utilizzerà le funzionalità di richiesta di esibizione di un documento o di un insieme di documenti, per ottenerne una replica esatta secondo i fini previsti dalla norma.

In risposta alla richiesta iniziale di esibizione, da parte dell'utente, il sistema di conservazione risponderà restituendo un PdD che nel caso più completo conterrà:

- I file/documenti richiesti così come sono stati archiviati dal sistema al momento della messa in conservazione
- Indici dei Pacchetti di Archiviazione, marcati temporalmente e firmati come all'origine, con cui sono stati conservati i documenti richiesti. Al loro interno sono contenuti tutti i metadati di tutti i documenti messi in conservazione nello stesso PdA

A fronte di una richiesta di produzione del Pacchetto di Distribuzione, il sistema effettua delle verifiche di coerenza e correttezza del pacchetto e dei documenti in esso contenuti. A tal proposito, il sistema di conservazione verifica che le impronte dei documenti restituiti nel PdD corrispondano a quelle presenti nel relativo indice del Pacchetto di Archiviazione; in modo da garantire che i documenti stessi non abbiano subito alterazioni o modifiche nei contenuti.

La richiesta di produzione di un PdD implica l'invio di una comunicazione via PEC al Responsabile della Conservazione e

al Responsabile Produttore (Produttore dei PdV).

La richiesta di esibizione può avvenire da due tra i canali messi a disposizione: interfaccia web e web service.

In entrambi i casi il flusso di selezione dei documenti da esibire è il medesimo:

1. ricerca dei documenti attraverso opportuni filtri
2. selezione dei documenti/PdA individuati
3. richiesta di esibizione a partire dai documenti/PdA
4. produzione del link di download da cui scaricare il Pacchetto di Distribuzione

La ricerca dei documenti avviene tramite la selezione di filtri sui metadati. Una volta individuata la classe documentale di interesse l'utente può effettuare le ricerche inserendo i valori su cui filtrare per uno o più metadati di riferimento.

La ricerca contemporanea su più metadati implica un filtro più forte, ovvero una restrizione del numero dei documenti risultanti.

Inoltre è possibile effettuare una ricerca tra documenti di classi documentali differenti ma che sono accomunati per un particolare metadato.

Se ad esempio si volessero cercare tutti i documenti afferenti a un determinato numero pratica, dotando classi documentali di tipo differente dello stesso metadato “numero pratica” è possibile effettuare una ricerca di questo tipo.

Tutti i documenti di interesse risultanti dalle ricerche vengono quindi spostati in un'area di lavoro. Finita l'operazione di selezione l'utente può ulteriormente chiedere di esibire solo una parte dei documenti messi nell'area di lavoro.

Il Pacchetto di Distribuzione risultante dalla richiesta di esibizione contiene:

- i documenti da esibire
- gli indici dei PdA, marcati temporalmente e firmati elettronicamente così come al momento della conservazione, del flusso di conservazione relativo ai documenti scelti

Nel caso in cui tra i documenti figurino interi PdA, il Pacchetto di Distribuzione contiene tutti i documenti che lo compongono.

### *6.6.1 Attività conseguenti alla cessazione del contratto*

In tutti i casi di cessazione del rapporto contrattuale, il Conservatore consente al Cliente, nei termini previsti dalle Condizioni di fornitura, il recupero dei propri documenti.

Non incombe su Aruba PEC alcun obbligo di provvedere alla materiale restituzione dei documenti informatici conservati, dal momento che l’attività di recupero dovrà essere effettuata dal Cliente entro i 90 giorni dalla scadenza del contratto.

Il cliente ha la possibilità di recuperare il conservato in autonomia attraverso:

- interfaccia web;
- ove previsto, invocazione di metodi tramite web service REST.

Il sistema rende disponibile i PDD, che possono essere scaricati dal cliente, in maniera asincrona secondo quanto riportato nei termini del contratto.

## 6.7 Produzione di duplicati e copie informatiche

Nei successivi paragrafi vengono descritte le procedure adottate per la produzione di duplicati o copie.

### *6.7.1 Produzione di duplicati*

La produzione di duplicati informatici dei documenti conservati può avvenire a seguito di una richiesta proveniente dal dipartimento tecnico oppure da una richiesta effettuata direttamente all’interno del sistema di conservazione.

Individuato il documento informatico di interesse, una apposita funzione consente di estrarne un duplicato informatico, ai sensi dell'art. 1, comma 1, lett. i-quinquies) del D.Lgs. 82/2005. Il processo assicura che il documento ottenuto contenga la medesima sequenza di bit del documento informatico di origine conservato nel sistema. Tale duplicato, in conformità all'art. 23-bis, comma 1, del D.Lgs. 82/2005, ha il medesimo valore giuridico dell'originale e non richiede attestazione di

conformità.

### 6.7.2 Produzione di copie

La produzione di copie informatiche di documenti informatici, ai sensi dell'art. 1, comma 1, lett. i-quater) del D.Lgs. 82/2005, si rende necessaria in tutti i casi in cui venga generato un documento con contenuto identico all'originale conservato, ma con una diversa sequenza di valori binari. Ciò include, a titolo esemplificativo:

- la conversione del documento in un formato differente (procedura di riversamento).
- l'estrazione del documento per l'inserimento in supporti di memorizzazione che includono software aggiuntivi o sistemi di crittografia.
- la generazione di una versione del documento con metadati differenti o aggiuntivi.

Ai sensi dell'art. 23-bis, comma 2, del D.Lgs. 82/2005, tali copie hanno la stessa efficacia probatoria dell'originale se la loro conformità è attestata da un pubblico ufficiale o se non viene espressamente disconosciuta.

Il sistema di conservazione non consente l'invio dello stesso PdV per più di una volta. Una volta conclusa la fase di presa in carico del PdV e la conseguente creazione del RdV, come descritto nei successivi capitoli, non è possibile effettuare alcuna modifica e/o cancellazione.

In tale contesto il Conservatore, previo perfezionamento di specifico accordo scritto (in cui sono concordati ruoli, modalità, tempi e corrispettivi), provvede ad effettuare, in collaborazione col Cliente, le operazioni necessarie a produrre le copie informatiche dei documenti informatici depositati in conservazione secondo quanto stabilito dalla normativa e dalla regolamentazione tecnica vigenti.

### 6.7.3 Produzione di copie su supporti rimuovibili

In caso di richiesta di produzione di copie o duplicati su supporto rimuovibile, viene prodotto un insieme di DVD (o altro supporto), ognuno autoconsistente, consegnato al Responsabile della conservazione che ne ha fatto richiesta.

Il processo prevede l'uso di un apposito applicativo che permette la generazione di immagini complete o parziali degli archivi di conservazione che poi vengono riversate su supporto ottico da un operatore. Il software richiede in input l'identificativo dell'archivio di conservazione, le classi documentali desiderate e il periodo temporale coinvolto. L'output generato è dato dal contenuto selezionato dagli archivi di conservazione, lottizzato in pacchetti di dimensione compatibile alla capienza del supporto ottico.

I supporti creati vengono etichettati con una codifica generata automaticamente che in nessun modo riporta informazioni sul contenuto. In ogni singolo pacchetto sono presenti i documenti protetti con crittografia e il software di ricerca e accesso. Il software di ricerca e accesso permette, previo inserimento di una password da parte dell'utente, di poter visionare l'indice di quanto contenuto nei pacchetti prodotti, eseguire ricerche su metadati e decrittare e visionare i singoli documenti. Qualora il cliente desiderasse anche l'evidenza della conservazione, verrà consentito lo scarico, ovviamente decrittando in linea, del documento con il relativo Indice di Conservazione e tutte le evidenze necessarie.

La protezione dei documenti è quindi ottenuta tramite crittografia con un certificato pubblico, generato allo scopo. La decrittazione è eseguita tramite la chiave privata, abbinata al certificato, rilasciata col software di ricerca e accesso, e un PIN che viene recapitato a mezzo telematico al responsabile della conservazione. Insieme al PIN viene anche recapitata una descrizione del contenuto di ogni supporto: codice del supporto, evidente sull'etichetta dello stesso, archivio, classi documentali data conservazione primo Pacchetto di Archiviazione, data conservazione ultimo Pacchetto di Conservazione.

### 6.7.4 Intervento del Pubblico Ufficiale

In conformità al quadro normativo delineato dal D.Lgs. 82/2005 (CAD), la presenza del Pubblico Ufficiale (ad esempio, un notaio o altro soggetto a ciò autorizzato) si rende necessaria qualora sia richiesta l'attestazione di conformità di una copia informatica all'originale informatico conservato nel sistema (art. 23-bis, comma 2, CAD), ovvero qualora si debba produrre una copia su supporto analogico (cartaceo) conforme al documento informatico d'origine (art. 23, comma 1, CAD).

L'attestazione del pubblico ufficiale conferisce a tali copie la medesima efficacia probatoria dell'originale, prevenendo i rischi connessi a un eventuale disconoscimento esplicito della conformità da parte di terzi. L'intervento del pubblico

ufficiale non è invece legalmente richiesto per la produzione di duplicati informatici (estratti in conformità alle Linee Guida AgID), i quali mantengono per legge lo stesso valore giuridico dell'originale ad ogni effetto di legge in quanto presentano la medesima sequenza di bit dell'originale.

Il Conservatore richiede la presenza di un pubblico ufficiale nei casi in cui sia previsto il suo intervento, assicurando allo stesso l'assistenza tecnica necessaria per l'espletamento delle attività al medesimo attribuite.

Ogni risorsa, comprese quelle di natura economica, necessaria per l'espletamento delle attività attribuite al pubblico ufficiale dovrà essere garantita e sostenuta dal Cliente; pertanto, qualora il Cliente non se ne sia fatto carico direttamente, Aruba PEC è sin da ora autorizzata ad addebitare al Cliente tutti i costi e le spese, compresi gli onorari inerenti le attività prestate dal Pubblico Ufficiale, qualora la normativa o le esigenze di certezza probatoria del Cliente ne richiedano obbligatoriamente la presenza..

## 6.8 Scarto dei pacchetti di archiviazione

### *6.8.1 Trasferimento dei documenti informatici in conservazione*

Nella scheda di conservazione, parte integrante del contratto di servizio e sottoscritta dal cliente, sono indicati i tempi entro i quali le diverse tipologie di documenti devono essere trasferite in conservazione, ove, nel caso delle pubbliche amministrazioni, non già presenti nel Manuale di gestione.

### *6.8.2 Scarto dei documenti informatici conservati*

Relativamente alla possibilità di scarto, ossia di eliminare legalmente i documenti informatici conservati digitalmente a norma di legge, occorre distinguere preliminarmente la tipologia dei soggetti (Clienti) produttori, pubblici o privati.

Va preliminarmente osservato che in ambito privato, con l'eccezione degli archivi "dichiarati di notevole interesse storico", che divengono archivi specificatamente disciplinati, l'obbligo di conservazione dei documenti è disciplinato dall'ordinamento vigente e, in particolare, dai termini prescrittivi del codice civile nonché, per le scritture contabili, le fatture, le lettere e i telegrammi ricevuti e le copie delle fatture, delle lettere e dei telegrammi spediti, segnatamente dall'art. 2220 del c.c., il quale stabilisce l'obbligo di conservazione di dieci anni dalla data dell'ultima registrazione.

Il processo di scarto è composto di queste fasi:

1. l'elenco dei pacchetti di archiviazione contenenti i documenti destinati allo scarto è generato da Aruba PEC e trasmesso al responsabile della conservazione;
2. il responsabile della conservazione, verificato il rispetto dei termini temporali stabiliti dal piano di conservazione, lo comunica al responsabile della gestione documentale o al coordinatore della gestione documentale;
3. 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 ad Aruba PEC;
4. Aruba PEC provvede alla distruzione dei pacchetti di archiviazione.

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.

In ambito pubblico, oltre alle prescrizioni civilistiche, si rendono applicabili una serie di altre disposizioni specifiche, una su tutte, il Codice dei beni culturali e ambientali, emanato con il D.Lgs. 10 gennaio 2004, n. 42.

Inoltre, con riferimento agli archivi pubblici o privati, che rivestono interesse storico-artistico particolarmente importante, lo scarto del Pacchetto di Archiviazione avviene previa autorizzazione del Ministero per i beni e le attività culturali rilasciata al produttore secondo quanto previsto dalla normativa vigente in materia.

Al termine delle operazioni di distruzione dal sistema di conservazione dei pacchetti di archiviazione scartati, il Titolare dell'oggetto di conservazione deve notificare 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.

### 6.8.3 Richiesta di scarto immediato

I clienti possono richiedere al Conservatore lo scarto di alcuni Pacchetti di Archiviazione dal sistema di conservazione. Fermo quanto definito nel precedente paragrafo, riguardante il rispetto della normativa vigente in materia, il Responsabile della Conservazione potrà, previa compilazione della modulistica messa a disposizione da Aruba PEC, richiedere lo scarto di uno o più PdA.

Il richiedente dovrà indicare nel modulo i riferimenti all'archivio ed ai pacchetti di archiviazione che intende scartare, unitamente alle motivazioni dello scarto ed alla conferma di disporre di tutte le autorizzazioni necessarie per l'operazione.

Il modulo dovrà essere accompagnato da firma valida ed inviato tramite email all'indirizzo pec scarto@docfly.it.

Le operazioni di scarto verranno registrate nei log di sistema.

## 6.9 Garanzie di integrità, interoperabilità e trasferibilità

Al fine di garantire la piena interoperabilità e la trasferibilità dei dati nei processi di migrazione verso altri sistemi di conservazione, la struttura dell'Indice del Pacchetto di Archiviazione (IPdA) è realizzata da Aruba PEC in conformità con lo standard nazionale "Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali" (c.d. SInCRO), definito dalla norma UNI 11386.

I Pacchetti di Archiviazione (PdA) generati dal sistema di conservazione sono elaborati al fine esclusivo di garantire la conservazione digitale a lungo termine dei documenti informatici e dei relativi metadati associati, nonché di consentire la generazione dei Pacchetti di Distribuzione (PdD) necessari per l'esibizione e la consultazione.

Il processo di conservazione a norma impone che i Pacchetti di Archiviazione (PdA) siano "sigillati" mediante l'apposizione di una firma digitale o di un sigillo elettronico qualificato da parte del Responsabile della Conservazione (ovvero dal Responsabile del Servizio di Conservazione, se formalmente delegato) e associati a una validazione temporale opponibile a terzi, idonea a garantire l'attestazione della data certa e la validità giuridica del pacchetto nel tempo.

La produzione dei Pacchetti di Distribuzione (PdD) finalizzata all'esibizione non comporta la duplicazione binaria dei corrispondenti Pacchetti di Archiviazione (PdA); essa consiste nell'estrazione dei documenti conservati e dei relativi metadati di riferimento, i quali vengono organizzati in un formato idoneo a garantirne la leggibilità, l'autenticità, la provenienza e la conformità legale agli originali memorizzati nel sistema.

Una volta completato il processo di versamento e archiviazione, il Pacchetto di Archiviazione (PdA) memorizzato all'interno del sistema assume caratteristiche di assoluta immodificabilità e integrità, non potendo subire alcuna alterazione o modifica successiva all'apposizione della firma digitale (o del sigillo) e della validazione temporale.

Al fine di garantire continuità operativa, portabilità e trasferibilità del patrimonio documentale conservato, il sistema assicura l'esportazione e la messa a disposizione dei documenti informatici, dei relativi metadati e delle evidenze del processo di conservazione in modalità idonee a consentirne il riversamento o il subentro da parte di altro conservatore, nel rispetto dei requisiti di autenticità, integrità, leggibilità, reperibilità e conformità alle Linee guida vigenti. Restano in ogni caso garantiti l'accesso automatizzato all'archivio informatico, nonché la possibilità che i documenti conservati e i certificati qualificati siano trasferibili su altro supporto informatico, così da assicurare l'effettiva interoperabilità del sistema anche in caso di migrazione o cessazione del rapporto con il conservatore originario.

## 6.10 Tabella riepilogativa delle fasi del processo di conservazione

Il processo di conservazione si articola nelle seguenti fasi:

| | | |
|---|---|---|
| **FASE 1** | **Acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico** | |
| | **Descrizione sintetica** | Consiste nella ricezione dei documenti e del file contenenti i relativi metadati |
| **FASE 2** | **Verifica che il pacchetto di versamento e gli oggetti contenuti siano coerenti con le modalità previste nel presente Manuale di conservazione e con i formati di conservazione** | |
| | **Descrizione sintetica** | In questa fase vengono condotti i controlli sui metadati e vengono condotti i controlli specifici del documento ricevuto |
| **FASE 3** | **Eventuale rifiuto del pacchetto di versamento, nel caso in cui le verifiche di cui alla FASE 2 abbiano** | |

| | | |
|---|---|---|
| | **evidenziato anomalie e/o non conformità** | |
| | **Descrizione sintetica** | Viene restituito al sistema versante l'indicazione di eventuali anomalie. In tale caso il versamento viene rifiutato |
| **FASE 4** | **Generazione automatica del rapporto di versamento relativo al pacchetto 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 di seguito descritte** | |
| | **Descrizione sintetica** | Una volta processati i file ricevuti viene generato l'IPdV e di conseguenza il PdV stesso |
| **FASE 5** | **Sottoscrizione del rapporto di versamento con firma digitale apposta da Aruba PEC** | |
| | **Descrizione sintetica** | Il RdV viene firmato digitalmente dal Responsabile del servizio di Conservazione o da un suo delegato. Infine il RdV viene inviato al Cliente. In questa fase Aruba prende in carico il versamento ufficialmente |
| **FASE 6** | **Preparazione e gestione del Pacchetto di Archiviazione (c.d. Pacchetto di Archiviazione)** | |
| | **Descrizione sintetica** | Il Pacchetto di Archiviazione è un insieme di metadati in grado di fornire prova dell'integrità dell'insieme dei documenti, ad esso correlati la cui conservazione decorre da una data determinata, la cui prova di integrità è fornita tramite una firma elettronica qualificata, corroborata da una marca temporale.<br>La struttura del Pacchetto di Archiviazione è costruita sulla base delle specifiche della struttura dati (UNI 11386:2020) contenute nell'allegato 4 alle regole tecniche e secondo le modalità riportate nel manuale della conservazione |
| **FASE 7** | **Sottoscrizione del Pacchetto di Archiviazione con firma digitale apposta da Aruba PEC e apposizione di una validazione temporale con marca temporale alla relativa impronta. Tale operazione viene in breve chiamata anche "Chiusura del Pacchetto di Archiviazione"** | |
| | **Descrizione sintetica** | Il Pacchetto di Archiviazione (PdA), che viene costruito in automatico dal sistema e comprende uno o più PdV. I PdV vengono aggregati in base alle regole definite per la classe su cui i pacchetti afferiscono. La chiusura viene sancita dall'apposizione di opportuna marca temporale, per stabilirne l'istante di creazione, e firma digitale del Responsabile del servizio di Conservazione o di un suo delegato, per garantirne l'immodificabilità. Con la suddetta firma apposta in calce al Pacchetto di Archiviazione e la suddetta dichiarazione il conservatore NON SOTTOSCRIVE il contenuto e la semantica dei documenti conservati ma asserisce solamente che il processo di conservazione è stato eseguito correttamente, nel rispetto delle norme giuridiche e delle indicazioni contrattuali di servizio. |
| **FASE 8** | **Preparazione e sottoscrizione con firma digitale di Aruba PEC del Pacchetto di Distribuzione ai fini dell'esibizione richiesta dall'utente** | |
| | **Descrizione sintetica** | Il Pacchetto di Distribuzione (PdD) è definito in base alle esigenze del richiedente e può contenere anche un set parziale di metadati. È generato a partire dai pacchetti di archiviazione.<br>Nel caso più semplice il PdD contiene dei duplicati del PdA. In alternativa esso può essere costituito da una scelta di documenti conservati selezionati attraverso una o più interrogazioni. |
| **FASE 9** | **Produzione di duplicati informatici effettuati su richiesta del Cliente in conformità a quanto previsto dalle regole tecniche in materia di formazione del documento informatico** | |
| | **Descrizione sintetica** | Per duplicato informatico 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. I duplicati informatici hanno il medesimo valore giuridico, ad ogni effetto di legge, del documento informatico da cui sono tratti, se prodotti in conformità alle regole tecniche in materia di formazione del documento informatico, ovvero se contiene la stessa sequenza di bit del documento informatico di origine. |
| **FASE 10** | **Eventuale scarto del Pacchetto di Archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dal *Contratto* di servizio, dandone preventiva informativa al Cliente al fine di raccoglierne il consenso** | |
| | **Descrizione sintetica** | Alla scadenza dei termini di conservazione, il cliente in autonomia può decidere di cancellare i PdA in conservazione. |

## 6.11 Audit Log

Il sistema di conservazione registra per ogni evento rilevante a quanto definito nella normativa relativa al processo di conservazione.

In particolare sono gestiti i seguenti eventi:

- Creazione PDA;
- Conservazione PDA;
- Invio Rapporto di Versamento;
- Invio Rapporto di Conservazione;
- Esibizione PDD;
- Download Documento
- Scarto PDA;
- Verifica Integrità PDA;
- Rettifica Documentale e dei metadati.

Il log di audit è consultabile tramite applicativo e/o altre procedure comunicate dal produttore e attraverso il sistema di back office a chi gestisce il servizio o a pubblico ufficiale che ne faccia richiesta.

Il log viene salvato in apposito database e rimane disponibile nel tempo per consultazione. Oltre al log di audit sono presenti altri log di servizio relativi ad altri eventi generati dal sistema durante il processo di conservazione.

Il Rapporto di Conservazione è l'attestazione di avvenuta conservazione da parte del Conservatore del/i PdV ricevuti e della loro effettiva conservazione nel sistema. Le evidenze del Rapporto di Conservazione vengono inviate via mail ordinaria.

# 7 Il sistema di conservazione

## 7.1 Infrastruttura e componenti del sistema

Il Sistema di Conservazione è erogato in conformità alle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici e alle disposizioni dell'Agenzia per la Cybersicurezza Nazionale (ACN), mediante infrastrutture localizzate sul territorio nazionale e gestite dal Gruppo Aruba. I servizi sono ospitati presso Data Center di proprietà, progettati e gestiti secondo i requisiti della norma ISO/IEC 27001 e integrati nel perimetro dei Sistemi di Gestione certificati dell'Organizzazione. L'architettura complessiva del Sistema di Conservazione è finalizzata a garantire i requisiti di riservatezza, integrità, disponibilità, autenticità, immodificabilità, reperibilità e tracciabilità dei documenti informatici conservati, nonché la continuità operativa del servizio.

In relazione alle **componenti logiche**, l'architettura del Sistema di Conservazione è basata su un modello multi-tier, articolato nei livelli di presentazione, logica applicativa e archiviazione, in coerenza con i principi di separazione funzionale e controllo dei flussi informativi previsti dalle Linee Guida AgID. Il livello di presentazione gestisce le interfacce utente e applicative ed è progettato per garantire scalabilità e bilanciamento del carico. Il livello di logica applicativa governa i processi di conservazione, consultazione e ricerca dei documenti, assicurando la corretta esecuzione delle funzioni di backend e la disponibilità dei servizi. Il livello di archiviazione gestisce i dati e i metadati associati ai documenti conservati, garantendo coerenza, ridondanza e accessibilità controllata delle informazioni.

Il Sistema di Conservazione si avvale di **componenti tecnologiche** di classe enterprise, integrate in modo sinergico per garantire affidabilità, sicurezza e prestazioni. Le principali tecnologie includono sistemi documentali per la gestione dei contenuti, basi di dati per la conservazione dei metadati e delle informazioni di sistema, servizi di autenticazione e autorizzazione per il controllo degli accessi, web server e servizi applicativi per l'erogazione delle interfacce, sistemi di messaggistica per la gestione dei flussi documentali e motori di ricerca e audit per la tracciabilità delle operazioni. Tutte le componenti tecnologiche sono configurate in coerenza con le misure di sicurezza previste dal Sistema di Gestione della Sicurezza delle Informazioni certificato ISO/IEC 27001.

Quanto alle **componenti fisiche**, l'infrastruttura fisica del Sistema di Conservazione è costituita da due siti distinti e interconnessi: un sito primario, completamente ridondato e configurato in alta affidabilità, e un sito secondario predisposto per la replica dei dati e la continuità del servizio. I Data Center sono collegati tramite collegamenti dedicati e sono dotati di misure di sicurezza fisica, ambientale e impiantistica adeguate ai requisiti di resilienza e disponibilità previsti dalla normativa di riferimento. Tutte le componenti fisiche impiegate sono di tipologia enterprise e fornite da produttori leader di mercato, in conformità agli standard adottati dal Gruppo Aruba.

Per la descrizione dettagliata delle componenti logiche, tecnologiche e fisiche del Sistema di Conservazione, nonché delle specifiche misure di sicurezza adottate, si rimanda al Piano della Sicurezza.

## 7.2 Procedure operative

Nell'ambito dell'erogazione del Servizio di conservazione disciplinato dal presente Manuale Operativo, l'Organizzazione applica tutte le procedure, i controlli e le misure previste dai Sistemi di Gestione certificati ISO 9001 (Sistema di Gestione per la Qualità) e ISO 27001 (Sistema di Gestione della Sicurezza delle Informazioni), in quanto il Servizio rientra nel campo di applicazione dei certificati Aruba PEC.

Tali sistemi regolano le modalità operative adottate per garantire la sicurezza dei sistemi e dei dati trattati, con particolare riferimento alla gestione degli utenti e delle credenziali, assicurando i requisiti di Riservatezza, Integrità e Disponibilità.

La gestione tecnica dell'infrastruttura e delle componenti applicative del Servizio è effettuata in conformità alle procedure di Gruppo per la Gestione del Sistema Informativo Aruba, comprensive, a titolo esemplificativo, delle attività di backup, monitoraggio dei sistemi e gestione dei log, tutte ricomprese nel perimetro della certificazione ISO 27001 e descritte nel Piano di Sicurezza.

# 8 Monitoraggio e controlli

In questo capitolo si riporta 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.

## 8.1 Procedure di monitoraggio

Aruba PEC assicura la verifica periodica del funzionamento, nel tempo, del sistema di conservazione.

Il controllo della buona funzionalità del sistema di conservazione avviene tramite apposite funzionalità di monitoraggio del software. Esse mostrano l'esito delle operazioni automatiche eseguite sul sistema di conservazione come la generazione dei pacchetti di archiviazione, la chiusura dei pacchetti di archiviazione e la verifica dell'integrità degli archivi.

Unitamente all'esito delle predette operazioni vengono controllati anche i log delle operazioni medesime al fine di avere maggiore certezza di quanto effettivamente eseguito dal sistema di conservazione. Tutte queste informazioni sono controllate per ciascun singolo cliente.

Il monitoraggio avviene inoltre anche a livello di processi di elaborazione sul sistema di conservazione. Questo permette di individuare eventuali casi di processi bloccati che potrebbero inficiare il funzionamento del sistema stesso.

Un ultimo controllo del buon funzionamento del sistema può avvenire tramite il monitoraggio delle tracciature che vengono effettuate a livello di database. Tutte le operazioni eseguite determinano infatti la creazione di apposite revisioni che registrano tutte le modifiche intervenute sul sistema permettendo eventualmente di ripristinare i dati a seguito di situazioni anomale.

## 8.2 Verifiche sugli archivi

Aruba PEC assicura la verifica periodica, con cadenza non superiore ai 5 anni, dell'integrità degli archivi e della leggibilità degli stessi; assicura, inoltre, agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza.

Il sistema di conservazione esegue periodicamente ed automaticamente le operazioni di controllo dell'integrità degli archivi.

Il controllo eseguito è di due tipologie:

- **controllo di leggibilità:** consiste nel rendere disponibile attraverso una macchina virtuale un viewer per la visualizzazione dei documenti conservati. Il viewer specifico viene fornito sulla base dell'estensione del documento (mime type) e della versione del formato associato. Il dettaglio di tutte. La lista delle tipologie supportate è definita nella procedura "Registro dei formati supportati da DocFly2". Per ogni formato presente nel registro è individuato il relativo programma che ne permette la corretta visualizzazione (viewer). Il registro viene tenuto aggiornato sulla base dei nuovi formati o di quelli che diventano obsoleti. Conseguentemente sono aggiornati i viewer presenti sulla macchina virtuale per la corretta leggibilità dei documenti conservati.
- **controllo di integrità:** consiste nel ricalcolare l'hash di ciascun oggetto e verificare che corrisponda all'hash memorizzato nel sistema. Questo fornisce una ragionevole certezza dell'integrità degli oggetti dato che la funzione di hash restituisce un valore differente anche a seguito della modifica di un solo bit dell'oggetto.

La combinazione dei due tipi di controllo descritti non fornisce però garanzia di poter visualizzare correttamente il documento e che lo stesso sia effettivamente intellegibile dall'uomo.

Infatti questa garanzia non può essere fornita senza entrare nel merito del documento stesso. La garanzia della corretta visualizzazione del documento è d'altro canto garantita dalla scelta del formato PDF/A per i documenti conservati. Questo formato possiede infatti la caratteristica intrinseca di fornire leggibilità a lungo termine oltre all'ulteriore garanzia di essere basato su specifiche pubbliche (ISO 19005).

### 8.2.1 Pianificazione delle verifiche periodiche da effettuare

La verifica dell'integrità degli archivi viene effettuata sui filesystems in cui i documenti sono replicati, controllando tutti i file presenti in nei PdA conservati.

Viene verificato che i file distribuiti nei filesystems siano identici mediante:

- controllo del nome e della dimensione dei file presenti sui filesystems;
- calcolo dell'hash di ogni singolo file. Il valore viene confrontato con l'hash del corrispondente file censito nell'IPdV del PdA.

Il controllo su ciascun PdA conservato viene effettuato a intervalli temporali. La prima dell'integrità del PdA verifica viene effettuata entro 5 anni dalla conservazione del PdA. Le successive verifiche vengono effettuate entro i successivi 5 anni dalla conclusione dell'ultima verifica effettuata.

### 8.2.2 Mantenimento della firma per il periodo di conservazione

Il sistema di conservazione si avvale di un fornitore terzo per le attività di firma digitale e di marcatura temporale. Questo fornitore garantisce che gli elaboratori che offrono il servizio di marcatura temporale e di firma digitale sono protetti da livelli di protezione logica estremamente elevati. La medesima collocazione fisica del sistema garantisce gli elaboratori dalla possibilità di compromissioni fisiche grazie agli accorgimenti tecnici atti ad impedire accessi non autorizzati da persone e danneggiamenti da eventi accidentali. Non è infatti consentito l'accesso e la permanenza di una sola persona. I locali ove si svolgono le procedure di firma e marca sono dotati di sofisticati impianti di allarme, telecamere, microfoni, rilevatori di movimento (che si attivano soltanto quando nessuna persona vi è presente), al fine di controllare ogni movimento all'interno degli stessi.

## 8.3 Soluzioni adottate in caso di anomalie

In caso di anomalie riscontrate a seguito del monitoraggio delle funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi, sono presenti apposite procedure di emergenza (contingency) e piani di Business Continuity da applicare in attesa del ripristino del servizio (così come descritto dal Disaster Recovery Plan del Gruppo Aruba).

# 9 Sicurezza del sistema di conservazione

Aruba PEC S.p.A. è in possesso della certificazione ISO/IEC 27001 per il Sistema di Gestione della Sicurezza delle Informazioni, con perimetro comprendente il servizio di conservazione digitale. Tale certificazione attesta l'adozione di un approccio strutturato e sistematico alla gestione dei rischi per la sicurezza delle informazioni, volto a garantire riservatezza, integrità e disponibilità dei dati e dei documenti conservati, nonché la continuità e l'affidabilità del servizio nel tempo.

Nell'ambito di tale sistema, Aruba PEC ha definito e mantiene uno specifico Piano della Sicurezza relativo al servizio di conservazione, documento a carattere riservato nel quale sono descritte in modo dettagliato le misure organizzative, procedurali e tecnologiche adottate per la protezione delle informazioni e delle infrastrutture. Tale Piano costituisce un documento di tipo confidenziale e, per tale ragione, è destinato a consultazione esclusivamente interna o da parte delle autorità.

A livello di riferimento generale, le indicazioni di carattere complessivo sul framework di sicurezza applicato sono riportate nell'Appendice al Manuale, che fornisce una visione d'insieme delle politiche, dei controlli e dei principi di sicurezza adottati a supporto del servizio di conservazione.

## 9.1 Privacy e requisiti di sicurezza dei dati

Aruba PEC tutela la riservatezza dei dati personali e garantisce ad essi la protezione necessaria da ogni evento che possa metterli a rischio di violazione, trattandoli secondo le specifiche previsioni della vigente normativa in materia.

Come previsto dal Regolamento dell'Unione Europea n. 2016/679 ("GDPR"), ed in particolare all'art. 13, sono fornite all'utente ("Interessato") tutte le informazioni richieste dalla normativa relative al trattamento dei propri dati personali mediante apposita, specifica e preventiva informativa, resa altresì sempre disponibile all'interno del proprio sito istituzionale. Con specifico riferimento ai compiti affidati con la nomina a Responsabile del trattamento dei dati personali,

Aruba PEC comunica di ottemperare a quanto previsto dalla normativa vigente in materia ed alle prescrizioni di cui all'art. 28 del Regolamento (UE) 2016/679.

In conformità con le proprie politiche di sicurezza delle informazioni e del suo sistema di gestione ISO 27001, Aruba PEC s'impegna a non divulgare, comunicare o diffondere le informazioni e i dati dei quali verrà a conoscenza durante l'espletamento delle attività. Inoltre si impegna a rispettare, nello svolgimento delle attività oggetto del servizio di conservazione, tutti i principi, contenuti nelle disposizioni normative vigenti, relativi al trattamento dei dati personali e in particolare quelli contenuti nel Regolamento (UE) 2016/679 e garantisce che le informazioni personali, patrimoniali, statistiche, anagrafiche, e/o di qualunque altro genere, di cui verrà a conoscenza in conseguenza dei servizi resi, in qualsiasi modo acquisite, vengano considerati riservati e come tali trattati. Si impegnerà infine a dare istruzioni al proprio personale affinché tutti i dati e le informazioni vengano trattati nel rispetto della normativa di riferimento.

## 9.2 Analisi dei Rischi

Il Gruppo Aruba ha svolto un'analisi dei rischi sul Sistema di Conservazione estesa agli aspetti di sicurezza fisica, logica ed organizzativa, incluso il coinvolgimento di enti esterni (fornitori); l'analisi è riportata nel relativo **Piano della Sicurezza**.

# 10 Specifiche contrattuali

I documenti costituenti l'impianto contrattuale del servizio di conservazione a norma sono riportati nelle condizioni/accordo di fornitura.

Aruba PEC, in linea con la normativa vigente, garantisce contratti o accordi scritti che specificano e disciplinano diritti e responsabilità delle Parti, versamento e acquisizione, mantenimento, accesso, ritiro, deposito, diritti e responsabilità di conservazione sui i documenti che tratta, natura economica e di servizio

Ai fini dell'attivazione ed erogazione del servizio di conservazione il Cliente sottoscrive e perfeziona il relativo Contratto. SI tratta del contratto con il quale il Cliente affida ad Aruba PEC la conservazione digitale dei documenti informatici di cui è titolare nonché dei documenti informatici di titolarità di terzi soggetti dallo stesso prodotti, sottoscritti digitalmente e versati in conservazione in virtù di specifico affidamento a tal fine sottoscritto dai suddetti terzi in favore del Cliente.

### *10.1.1 Nomina di Aruba quale responsabile del servizio di conservazione e del trattamento dei dati*

Ai fini dell'erogazione del servizio di conservazione digitale a norma, il Cliente nomina e affida ad Aruba PEC quale Responsabile del Servizio di Conservazione e Responsabile esterno del trattamento dei dati come previsto dalla vigente normativa in materia di protezione dei dati personali (Regolamento (UE) 2016/679 e D.Lgs. 196/2003 e s.m.i.) e indicato all'art 3.9 delle Linee Guida. Pertanto, i ruoli di Responsabile della conservazione e di Titolare del trattamento sono ricoperti dal Cliente, mentre i ruoli di Responsabile del servizio di conservazione e di Responsabile del trattamento dei dati saranno ricoperti da Aruba PEC.

### *10.1.2 Scheda di conservazione*

Il documento denominato "Scheda di conservazione" costituisce parte integrante e sostanziale del Contratto.

Il Produttore condivide con il Conservatore le caratteristiche, le modalità ed i termini di versamento dei documenti informatici da sottoporre a conservazione digitale, approvando espressamente quanto indicato nella scheda conservazione.

Il contenuto della Scheda di conservazione è volto a precisare:

- le tipologie di documenti da conservare;
- i metadati minimi riferiti ad ogni classe/tipo documento
- eventuali (metadati) extrainfo riferiti ad ogni classe/tipo documento sui quali effettuare specifici controlli;
- i formati da adottare per ogni classe/tipo documento.

### *10.1.3 Elenco Persone*

Ai fini dell'affidamento del servizio di conservazione digitale di documenti informatici, il Cliente comunica l'identità delle persone fisiche e/ o giuridiche dallo stesso ufficialmente incaricate di mantenere i rapporti con Aruba PEC e titolate ad operare in nome e per conto del Produttore medesimo, precisandone funzione e ruolo.

## 10.2 Modello di funzionamento del servizio

L'obiettivo ed il compito di Aruba PEC è quello di conservare i documenti informatici del Cliente con sistemi coerenti alla normativa regolante la conservazione digitale dei documenti informatici.

In particolare, il servizio di conservazione digitale di Aruba PEC soddisfa le seguenti funzioni d'uso:

- salvaguardia dell'integrità dei documenti informatici conservati mediante apposizione della firma digitale al Pacchetto di Archiviazione. Nel suddetto Pacchetto di Archiviazione è presente, fra l'altro, l'impronta di ogni singolo documento sottoposto a conservazione;
- prolungamento della validità del documento mediante apposizione della marca temporale al Pacchetto di Archiviazione;
- accesso diretto tramite interfaccia Web ai documenti informatici conservati;
- semplicità di invio e versamento dei documenti informatici da sottoporre a conservazione;
- totale sicurezza nella trasmissione dei documenti informatici da sottoporre a conservazione.

Il sistema di conservazione opera secondo un modello organizzativo che garantisce la sua distinzione logica dal sistema di gestione documentale, qualora esistente presso il Cliente.

In particolare, la conservazione è svolta affidando ad Aruba PEC il ruolo ed i compiti fissati nell'Atto di Affidamento.

A tal fine, Aruba PEC ed il Cliente hanno adottato il presente *Manuale* ove sono illustrati dettagliatamente l'organizzazione, i soggetti coinvolti ed i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione dei processi, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate ed ogni altra informazione utile alla gestione ed alla verifica del funzionamento, nel tempo, del sistema di conservazione.

Pertanto, al fine di attivare il servizio di conservazione digitale dei documenti informatici è necessario che il Cliente abbia sottoscritto il *Contratto* e gli allegati ad esso relativi, all'interno dei quali vengono, fra l'altro, specificati:

a) i contenuti e le caratteristiche generali del Servizio di conservazione digitale;
b) i termini di decorrenza e la durata del Servizio di conservazione digitale;
c) gli eventuali Servizi Estesi erogati su richiesta del Cliente;
d) le responsabilità e gli obblighi del Cliente;
e) le responsabilità e gli obblighi di Aruba PEC;
f) le modalità di produzione/formazione/emissione/sottoscrizione dei documenti informatici;
g) la descrizione delle tipologie e delle classi dei documenti informatici da sottoporre a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di documenti e delle eventuali eccezioni;
h) la definizione dell'intervallo di conservazione ossia dell'intervallo di tempo intercorrente tra la presa in carico del pacchetto di versamento e la chiusura del Pacchetto di Archiviazione.
i) Le modalità di distribuzione/esibizione dei documenti informatici conservati;

### *10.2.1 Obblighi del Cliente*

Il processo di conservazione impone al Cliente l'istituzione di un'organizzazione interna idonea, che garantisca la piena osservanza delle disposizioni normative in tema di gestione documentale[1] e delle procedure da osservare per la corretta produzione/formazione/emissione e sottoscrizione dei documenti informatici destinati alla conservazione digitale in

[1] Si veda, a puro titolo di esempio, il DPR 28.12.2000, n. 445, il DPCM 3.12.2013 sul protocollo informatico, ove applicabili;

conformità alle regole tecniche di cui all'art. 71 del CAD ed a quanto stabilito dal presente *Manuale* e dal *Contratto*.

A tale scopo, in base alle specifiche necessità, il Cliente deve, sia dal punto di vista dell'impostazione operativa delle attività propedeutiche alla conservazione digitale dei documenti informatici che dal punto di vista della scelta delle risorse coinvolte nel processo, organizzare il lavoro affinché esso venga svolto secondo i principi stabiliti dalla normativa regolante la conservazione digitale dei documenti informatici.

Il Cliente, quindi, all'interno della propria struttura organizzativa, dovrà aver definito:

a) le procedure propedeutiche alla conservazione digitale a lungo termine dei documenti informatici;

b) le funzioni e le attività affidate, con particolare attenzione alla verifica della congruità e continuità dei processi di produzione/formazione/emissione dei documenti informatici destinati alla conservazione digitale a lungo termine;

c) la gestione delle responsabilità derivanti dalle funzioni ed attività affidate;

d) la documentazione delle deleghe ed il relativo mantenimento;

e) le misure organizzative e tecniche idonee ad evitare danno ad altri.

Il Cliente deve attenersi scrupolosamente alle regole previste dal presente *Manuale*, alle prescrizioni previste nel *Contratto* e negli allegati ad esso relativi.

Il Cliente deve altresì prendere visione del presente *Manuale* prima di inoltrare i pacchetti di versamento e/o qualsiasi altra richiesta a Aruba PEC.

### *10.2.2 Obblighi del Conservatore*

Aruba PEC, come analiticamente descritto nel *Contratto*, limitatamente alle attività ad essa affidate, è responsabile verso il Cliente per l'adempimento degli obblighi discendenti dall'espletamento delle attività previste dalla normativa vigente in materia di conservazione digitale di documenti informatici.

In particolare, Aruba PEC, ai fini dell'erogazione del Servizio oggetto del *Contratto*, svolge le attività ad essa affidate dal Cliente come in dettaglio riportate nel documento "*Atto di Affidamento*", nei modi e nei termini specificati nel presente *Manuale* e negli allegati ad esso relativi.

Pertanto è obbligo di Aruba PEC conservare digitalmente i documenti informatici del Cliente allo scopo di assicurare, dalla presa in carico e fino all'eventuale cancellazione, la loro conservazione a norma, garantendone, tramite l'adozione di regole, procedure e tecnologie, le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità.

Il Sistema di conservazione di Aruba PEC è in grado di esibire tutti i documenti informatici in esso conservati in qualsiasi momento del periodo di conservazione; a tal fine, Aruba PEC ha in essere procedure adeguate a soddisfare, senza indebiti ritardi, le richieste di accesso, esibizione o consegna dei documenti conservati, effettuate dai soggetti debitamente autorizzati.

Oltre alla restituzione dei documenti informatici trasferiti e conservati presso Aruba PEC, viene garantita anche la restituzione delle relative evidenze informatiche che comprovano la corretta conservazione degli stessi, fornendo gli elementi necessari per valutare la loro autenticità e validità giuridica.

**Non rientra fra i Servizi offerti da Aruba PEC la conservazione di documenti analogici.**

### *10.2.3 Compiti organizzativi*

Aruba PEC provvede alla realizzazione di una base di dati relativa ai documenti informatici che il Cliente versa in conservazione, gestita secondo i principi di sicurezza illustrati nel presente *Manuale* e nel *Contratto* attuati adottando procedure di tracciabilità tali da garantire la corretta conservazione, l'accessibilità a ogni singolo documento e la sua esibizione.

Aruba PEC si occupa altresì di definire:

a) le caratteristiche ed i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare e organizzare gli stessi in modo da garantire la corretta conservazione e la sicurezza dei dati, anche al fine di poterli prontamente produrre, ove necessario;

b) le procedure di sicurezza e tracciabilità che consentano di risalire in ogni momento alle attività effettuate durante l'esecuzione operativa di conservazione.

c) le procedure informatiche ed organizzative per la corretta tenuta dei supporti su cui vengono memorizzati i documenti informatici oggetto di conservazione.

d) le procedure informatiche ed organizzative atte ad esibire la documentazione conservata, in caso di richieste formulate da chi ne abbia titolo.

Aruba PEC si occupa di redigere e sottoporre a revisione il presente *Manuale*. Il Cliente si dovrà dotare di un proprio Manuale della Conservazione costituito dalla descrizione di componenti, processi ed organizzazione propri, integrato e completato, se ritenuto necessario, dal presente *Manuale*.

### *10.2.4 Compiti di manutenzione e controllo*

Aruba PEC provvede a:

- mantenere un registro cronologico del software dei programmi in uso nelle eventuali diverse versioni succedute nel tempo ed un registro cronologico degli eventi di gestione del sistema di conservazione comprensivo delle risoluzioni adottate per rimuovere eventuali anomalie;
- implementare specifici controlli di sistema per individuare e prevenire l'azione di software che possano alterare i programmi ed i dati;
- verificare la corretta funzionalità del sistema e dei programmi in gestione;
- analizzare e valutare periodicamente la registrazione degli eventi rilevanti ai fini della sicurezza (analisi del log di sistema);
- definire e documentare le procedure di sicurezza da rispettare per l'apposizione del riferimento temporale;
- mantenere e gestire i dispositivi di firma in conformità con le procedure stabilite dal certificatore qualificato che ha rilasciato i relativi certificati;
- verificare la validità delle marche temporali utilizzate dal sistema di conservazione;
- verificare il buon funzionamento del file system

### *10.2.5 Compiti operativi*

Aruba PEC effettua le seguenti attività:

- supervisione dell'intero sistema di conservazione digitale, verificando accuratamente i processi di apposizione delle firme digitali, dei riferimenti temporali e delle marche temporali, in modo che la procedura rispetti la normativa, assicurandosi che tutto il processo si realizzi secondo le procedure descritte nel presente *Manuale*;
- sincronizzazione dell'ora di sistema di tutti i sistemi utilizzati, verifica e controllo della sincronizzazione del clock di sistema per consentire registrazioni accurate e comparabili tra loro;
- mantenimento della documentazione descrittiva del processo di conservazione aggiornata nel corso del tempo.

### *10.2.6 Fasi del processo di conservazione e responsabilità*

Il servizio di conservazione digitale dei documenti informatici è erogato e sviluppato per rispondere alle esigenze di qualsiasi soggetto che abbia l'esigenza di conservare documenti informatici come imprese, professionisti, associazioni, Pubblica Amministrazione centrale e locale. Il servizio permette di conservare i documenti informatici del Cliente, garantendone l'integrità e la validità legale nel tempo nonché la loro "esibizione a norma".

Come già fatto osservare, il sistema di conservazione opera secondo i modelli organizzativi esplicitamente concordati con il Cliente e formalizzati nel Contratto e negli allegati ad esso relativi che garantiscono la sua distinzione logica dal sistema di gestione documentale del Cliente, qualora esistente.

Pertanto, la conservazione non viene svolta all'interno della struttura organizzativa del Cliente (soggetto titolare dei documenti informatici da conservare), ma è affidata ad Aruba PEC, che espleterà le attività per le quali ha ricevuto formale affidamento, nei limiti della stessa e per le quali opera in modo autonomo e ne è responsabile.

La sequenza di attività che vanno dalla fase propedeutica alla formazione dei documenti informatici alla fase di conservazione degli stessi è di seguito schematicamente rappresentata:

| SISTEMI | FASE | DESCRIZIONE E MACRO FASI DEL PROCESSO DI CONSERVAZIONE | ATTIVITÀ A CARICO DI: | |
|---|---|---|---|---|
| | | | CLIENTE | Aruba PEC |
| Sistema di gestione documentale del Cliente | 1 | Produzione/formazione/emissione a norma dei documenti informatici e contestuale generazione dei relativi metadati | X | |
| | 2 | Produzione del pacchetto di versamento | X | |
| | 3 | Deposito in conservazione del pacchetto di versamento e dei relativi documenti informatici completi di metadati | X | |
| Servizio di Fatturazione Elettronica e PEC | 1a | Produzione/formazione/emissione a norma dei documenti informatici e contestuale generazione dei relativi metadati | | X |
| | 2a | Produzione del pacchetto di versamento | | X |
| | 3a | Deposito in conservazione del pacchetto di versamento e dei relativi documenti informatici completi di metadati | | X |
| Sistema di Firma Digitale | 4 | Servizio di Firma Automatica e di eventuale apposizione marca temporale, da effettuare sui documenti tributari prima dell'invio al sistema di conservazione. | X | X |
| Sistema di conservazione digitale dei documenti informatici | 5 | Acquisizione da parte del sistema di conservazione del pacchetto di versamento prodotto dal Cliente per la sua presa in carico | | X |
| | 6 | Verifica che il pacchetto di versamento ed i documenti informatici in esso descritti siano coerenti e conformi alle prescrizioni stabilite dal Contratto di servizio | | X |
| | 7 | Eventuale rifiuto del pacchetto di versamento o dei documenti informatici, nel caso in cui le verifiche di cui alla fase 6 abbiano evidenziato delle anomalie | | X |
| | 8 | Generazione, in modo automatico, del rapporto di versamento relativo a ciascun pacchetto di versamento | | X |
| | 9 | Invio al Cliente del rapporto di versamento | | X |
| | 10 | Preparazione e gestione del Pacchetto di Archiviazione | | X |
| | 11 | "Chiusura" del Pacchetto di Archiviazione mediante sottoscrizione con firma digitale di Aruba PEC e apposizione di marca temporale | | X |
| | 12 | Richieste di esibizione dei documenti informatici conservati | X | |
| | 13 | Preparazione del Pacchetto di Distribuzione ai fini dell'esibizione richiesta dall'utente con tutti gli elementi necessari a garantire l'integrità e l'autenticità degli | | X |

| | | | | |
|---|---|---|---|---|
| | | stessi | | |
| | 14 | Richiesta del Cliente di duplicati informatici | X | |
| | 15 | Produzione di duplicati informatici su richiesta del Cliente | | X |

Dal prospetto di cui sopra emerge chiaramente come ogni singola fase del processo è propedeutica alle altre.

In ogni caso, prima di dare corso al processo di conservazione, il Cliente e Aruba PEC dovranno definire, attraverso il perfezionamento del Contratto e degli allegati ad esso relativi, come configurare il servizio in base alle specifiche esigenze del Cliente concordando le modalità di gestione e fruizione oltre alla quantità e tipologia di documenti da conservare.

# 11 Livelli di servizio (SLA)

I livelli di servizio relativi all'offerta standard, sono riportati nella tabella in basso e rappresentano le metriche di servizio che devono essere rispettate dal conservatore Aruba PEC nei confronti dei propri clienti/utenti.

| **CARATTERISTICHE GENERALI DEL SERVIZIO** | **SPECIFICHE TECNICHE** |
|---|---|
| **Disponibilità complessiva del servizio** | 99,95% |
| **Assistenza** | Sistema di ticketing e canale telefonico |
| **Periodo di fatturazione** | Annuale |
| **Durata minima contratto** | Un anno (eventuali upgrade richiesti in seguito alla stipula del contratto vanno ad allinearsi alla scadenza riportata sul contratto stesso) |
| **Datacenter su cui è attivabile il servizio** | DC1-IT (http://datacenter.aruba.it) |
| **FASI ELABORAZIONE PACCHETTI DI VERSAMENTO** | **SPECIFICHE TECNICHE** |
| **Presa in carico del PdV (Generazione del Rapporto di versamento)** | Entro 48h dal ricevimento dell'ultimo documento contenuto nel pacchetto di versamento |
| **Invio in conservazione del PdA** | Entro 72h[2] dalla presa in carico dell'ultimo PdV valido e completo contenuto nel PdA, nel caso in cui tutti i PdV contenuti nel PdA siano validi e completi |
| **RICHIESTA DI ESIBIZIONE** | **SPECIFICHE TECNICHE** |
| **Produzione del Pacchetto di Distribuzione** | Entro 24h dalla richiesta di produzione del PdD |

# 12 Disposizioni finali

## 12.1 Nullità o inapplicabilità di clausole

Se una qualsivoglia disposizione del presente Manuale, o relativa applicazione, risulti per qualsiasi motivo o in qualunque misura nulla o inapplicabile, il resto del presente Manuale (così come l'applicazione della disposizione invalida o

[2] A condizione che le regole di conservazione siano appropriate e sostenibili ai fini della garanzia del rispetto di tale tempistica.

inapplicabile ad altre persone o in altre circostanze) rimarrà valido e la disposizione nulla o inapplicabile sarà interpretata nel modo più vicino possibile agli intenti delle parti.

## 12.2 Interpretazione

Salvo disposizioni diverse, questo Manuale dovrà essere interpretato in conformità alla correttezza, buona fede ed a quanto ragionevole anche in virtù degli usi commerciali nazionali.

## 12.3 Nessuna rinuncia

In nessun caso eventuali inadempimenti e/o comportamenti del Cliente difformi rispetto al Manuale potranno essere considerati quali deroghe al medesimo o tacita accettazione degli stessi, anche se non contestati da Aruba PEC. L'eventuale inerzia di Aruba PEC nell'esercitare o far valere un qualsiasi diritto, clausola o disposizione del Manuale, non costituisce rinuncia a tali diritti o clausole.

## 12.4 Comunicazioni

Qualora Aruba PEC o il Cliente desiderino o siano tenuti ad effettuare delle comunicazioni, domande o richieste in relazione al presente Manuale, tali comunicazioni dovranno avvenire nelle modalità ed ai riferimenti indicati nel Contratto.

## 12.5 Intestazioni e Appendici e Allegati del presente Manuale Operativo

Le intestazioni, sottotitoli e altri titoli del presente Manuale sono utilizzati solo per comodità e riferimento, e non saranno utilizzati nell'interpretazione o applicazione di qualsiasi disposizione ivi contenuta.

Le appendici, gli allegati, comprese le definizioni del presente Manuale, sono parte integrante e vincolante del presente Manuale a tutti gli effetti.

## 12.6 Modifiche del Manuale di conservazione

Aruba PEC si riserva il diritto di aggiornare periodicamente il presente Manuale in modo estensibile al futuro e non retroattivo. Le modifiche sostituiranno qualsiasi disposizione in conflitto con la versione di riferimento del Manuale di conservazione.

## 12.7 Violazioni e altri danni materiali

Il Cliente rappresenta e garantisce che i documenti oggetto di conservazione e le informazioni in essi contenute non interferiscano, danneggino e/o violino diritti di una qualsiasi terza parte di qualunque giurisdizione.

## 12.8 Norme Applicabili

Le attività di conservazione contenute nel presente Manuale sono assoggettate alle leggi dell'ordinamento italiano.

Il presente documento informatico è formato nel rispetto delle regole tecniche di cui all'art. 71 del D.Lgs. 7 marzo 2005 n. 82 e s.m.i. (Codice dell'amministrazione digitale) e sottoscritto con firma digitale del Responsabile del Servizio Andrea Sassetti.