MANUALE DEL SERVIZIO DI CONSERVAZIONE DI SOGEI S.P.A.

FG-75-CO-01

29 maggio 2026

Documento Pubblico

INDICE

1. ELENCO DELLE MODIFICHE APPORTATE AL DOCUMENTO

Versione	Data approvazione	Descrizione
1.0	04 febbraio 2014	Manuale della conservazione sostitutiva
2.0	25 maggio 2016	Adeguamento del manuale di conservazione alla struttura prevista da AGID. Adeguamento del Sistema di conservazione alle regole tecniche in materia - DPCM 3 dicembre 2013.
2.1	9 novembre 2016	Sostituzione del termine "data" con "data approvazione" nel registro delle versioni. Precisazioni sull'organizzazione del sistema di deleghe nel par. 7.5.
2.2	18 settembre 2017	Avvicendamento del Responsabile della funzione archivistica di conservazione. Modifica delle modalità di comunicazione delle anomalie nel rifiuto dei pacchetti di versamento par. 7.4.
2.3	23 marzo 2018	Nuovo assetto organizzativo di Sogei S.p.A. per l'erogazione del servizio di conservazione digitale, con decorrenza dal 2 marzo 2018. Designazione del DPO, in ottemperanza al Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (GDPR) e in coerenza con quanto stabilito dal Consiglio di Amministrazione del 19 marzo 2018, come da comunicazione organizzativa del 22 marzo 2018. Modifica del capitolo 4.2 RUOLI E RESPONSABILITÀ DI SOGEI S.P.A.
2.4	09 gennaio 2020	Inserimento riferimenti normativi eIDAS. Avvicendamento del Responsabile della funzione archivistica di conservazione. Aggiornamento elenco formati. Precisazioni su descrizione del servizio di Time Stamping Authority. Aggiornamento dei riferimenti normativi par. 3.1. Revisione del registro delle versioni.
2.5	31 maggio 2021	Adeguamento agli standard redazionali di Sogei S.p.A. Aggiornamento della struttura organizzativa per nuovo organigramma di Sogei (par. 4.2.) Revisione dei testi e della rappresentazione grafica relativamente alle componenti logiche (par. 8.1) e tecnologiche (par. 8.2).

Versione	Data approvazione	Descrizione
		Descrizione degli strumenti di supporto al monitoraggio operativo a seguito di razionalizzazione degli stessi (par. 9.1.2) Aggiornamenti rispetto alle Linee guida di AgID (ruolo del produttore del PDV, firma digitale dei pacchetti informativi, conservazione dello schema per i file di formato xml)
2.6	31 maggio 2022	Aggiornamento dei ruoli e responsabilità di Sogei S.p.A. (par. 4.2) Modifica denominazione del manuale in "manuale del servizio"
2.7	12 settembre 2022	Aggiornamento dei ruoli e responsabilità di Sogei S.p.A. (par. 4.2)
2.8	10 maggio 2023	Aggiornamento dei ruoli e responsabilità di Sogei S.p.A. (par. 4.2) con decorrenza dal 1° aprile 2023, Comunicazione organizzativa N. 2023.03.
2.9	09 giugno 2023	Aggiornamento dei ruoli e responsabilità di Sogei S.p.A. in base alla Comunicazione organizzativa N. 2023.05 e Aggiornamento delle deleghe (par. 4.2).
3.0	20 maggio 2024	Indicazione dei nuovi formati gestiti (par. 7.1), inserimento del nuovo schema del pacchetto di archiviazione. Adeguamento allo standard redazionale aziendale.
3.1	29 maggio 2025	Aggiornamento dell'architettura del sistema, capitolo 9. Aggiornamento del ruolo "Responsabile del trattamento dati personali".
3.2	24 aprile 2026	Aggiornamento glossario e paragrafo 7.1 con la misura di sicurezza cifratura dei file. Revisione generale del documento per refusi e integrazioni per migliorare la comprensione.
3.3	29 maggio 2026	Aggiornamento dei ruoli e responsabilità di Sogei S.p.A. a seguito della riorganizzazione aziendale (Ordini di servizio del 6 maggio 2026).

2. SCOPO E AMBITO DEL DOCUMENTO

La conservazione dei documenti digitali è un elemento determinante nel processo di evoluzione e potenziamento dell'intero sistema informativo della fiscalità.

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

- a) i documenti informatici e i documenti amministrativi informatici coni metadati ad essi associati;

- b) le aggregazioni documentali informatiche (fascicoli e serie) con i metadati ad esse associati contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che costituiscono le aggregazioni medesime, nel rispetto di quanto indicato per le Pubbliche Amministrazioni nell'articolo 67, comma 2, del DPR 445/200042 e art. 44, comma 1-bis, CAD;

- c) gli archivi informatici con i metadati associati.

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

Il presente manuale descrive il modello organizzativo della conservazione adottato e illustra nel dettaglio l'organizzazione della struttura che realizza il processo di conservazione, definendo i soggetti coinvolti e i ruoli svolti dagli stessi nel modello organizzativo di funzionamento dell'attività di conservazione.

Descrive inoltre il processo, le architetture e le infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.

Gli elementi illustrati e descritti sono validi e rilevanti per tutti gli enti per i quali Sogei svolge il servizio di conservazione e gestisce il processo di conservazione ai sensi della normativa in materia.

In particolare, il servizio di conservazione prevede quel complesso di attività che partendo dall'acquisizione degli oggetti da conservare passa attraverso la memorizzazione degli stessi su supporti ottici e termina con l'apposizione del

riferimento temporale e/o della firma digitale da parte del responsabile della conservazione, che attesta il corretto svolgimento del processo.

Torna al sommario

3. TERMINOLOGIA (GLOSSARIO E ACRONIMI)

Per quanto riguarda il servizio di conservazione è di riferimento il glossario allegato alle linee guida di AgID, di cui vengono riportate in tabella alcune definizioni integrate con termini specifici del contesto Sogei.

Termine	Definizione
Archiviazione elettronica	Processo di memorizzazione, su un qualsiasi idoneo supporto, di documenti informatici, anche sottoscritti, univocamente identificati mediante un codice di riferimento, antecedente all'eventuale processo di conservazione
CA	Certification Authority
Cifratura dei file	Processo di sicurezza informatica che consiste nel trasformare i dati contenuti in un file in una forma illeggibile, utilizzando un algoritmo e una chiave segreta. Solo chi possiede la chiave corretta può decifrare il file e riportarlo alla forma originale.
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
Delega alla firma dei pacchetti di archiviazione	è un documento generato e conservato nel sistema di conservazione che rappresenta per ciascuno dei tecnici della conservazione l'ambito della delega, il delegante e la validità temporale della stessa
Documento informatico	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Documento analogico	documento formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta (esempio: documenti cartacei), come le immagini su film (esempio: pellicole mediche, microfiche, microfilm),

Termine	Definizione
	come le magnetizzazioni su nastro (esempio: cassette e nastri magnetici audio e video). Si distingue in documento originale e copia
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 archiviato	documento informatico, anche sottoscritto, sottoposto al processo di archiviazione elettronica
Documento conservato	documento sottoposto al processo di conservazione
Documento informatico	la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Documenti in formato XML	XML (sigla di eXtensible Markup Language) è un linguaggio di markup, ovvero un linguaggio marcatore basato su un meccanismo sintattico che consente di definire e controllare il significato degli elementi contenuti in un documento o in un testo. Un XSD definisce il tipo di un documento XML in termini di elementi e attributi che possono apparire, in quale relazione reciproca, quale tipo di dati può contenere, ed altro. Può essere usata anche con un programma di validazione, al fine di accertare a quale tipo appartiene un determinato documento XML. XSLT (eXtensible Stylesheet Language Transformations) è il linguaggio di trasformazione dell'XML. Ha lo scopo di rendere possibile la trasformazione di un documento XML in un altro documento tramite un foglio di stile XSL, che fornisce la semantica per la trasformazione
Esibizione	operazione che consente di visualizzare un documento conservato
Evidenza informatica	Sequenza finita di *bit* che può essere elaborata da una procedura informatica
Firma digitale	così come definita all'articolo 1, comma 1, lettera n, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445. "...il risultato della procedura informatica (validazione) basata su un sistema di chiavi

Termine	Definizione
	asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore 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
FTP server	programma che permette di accettare connessioni in entrata e di comunicare con un Client attraverso il protocollo FTP
Funzione di HASH crittografica	funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o digest in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
Impronta crittografica o hash	sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di hash crittografica a un'evidenza informatica
Marca Temporale	una marca temporale (timestamp) è una sequenza di caratteri che rappresentano una data e/o un orario per accertare l'effettivo avvenimento di un certo evento
Memorizzazione	processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici, anche sottoscritti (Si intende sottoscrizione ai sensi dell'articolo 10, commi 2 e 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 così come modificato dall'articolo 6 del decreto legislativo 23 gennaio 2002, n. 10)
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
Pacchetto di archiviazione	pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel manuale di conservazione

Termine	Definizione
Pacchetto di distribuzione	pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione
Pacchetto di versamento	pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione
Presa in carico	accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione e, in caso di affidamento del servizio all'esterno, dagli accordi stipulati tra il titolare dell'oggetto di conservazione e il responsabile del servizio di conservazione
Produttore del pacchetto di versamento	persona fisica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con il responsabile della gestione documentale
Pubblico Ufficiale	nei casi in cui è prevista, il responsabile della conservazione assicura la presenza di un pubblico ufficiale secondo l'Art. 7 delle regole tecniche in materia di conservazione
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
Rapporto di conservazione	documento informatico che attesta l'avvenuta conservazione da parte del sistema di conservazione dei documenti inviati dal produttore
Registro del pacchetto di versamento	strutture documentali in cui sono memorizzati gli estremi dei pacchetti di versamento ed il loro stato durante tutto il processo di conservazione
Riferimento temporale	insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC)
Riversamento	procedura mediante la quale uno o più documenti informatici sono convertiti da un formato di file (ovvero di busta, ovvero di pacchetto di file) ad un altro, lasciandone invariato il contenuto per quanto

Termine	Definizione
	possibilmente permesso dalle caratteristiche tecniche del formato (ovvero dei formati) dei file e delle codifiche di destinazione
Sigillo elettronico	dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi
Titolare dell'oggetto di conservazione	Soggetto produttore degli oggetti di conservazione.
W.O.R.M. (write once read many)	l'acronimo indica la caratteristica di alcuni tipi di supporti (ottici o magnetici) che rende i dati registrati su di essi non-modificabili e non-cancellabili, ma solo accessibili in lettura ed in copia.

Torna al sommario

4. NORMATIVA E STANDARD DI RIFERIMENTO

Di seguito sono riportati la normativa e gli standard di riferimento.

4.1 NORMATIVA DI RIFERIMENTO

Alla data l'elenco dei principali riferimenti normativi italiani in materia, ordinati secondo il criterio della gerarchia delle fonti, è costituito da:

- 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 della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (GDPR)
- 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);
- DPCM 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Linee Guida sulla formazione gestione e conservazione dei documenti informatici del 10 settembre 2020 e s.m.i;
- DPCM 3 dicembre 2013, contenente "Regole tecniche per il protocollo informatico", a partire dalla data di applicazione delle presenti Linee guida sono abrogate tutte le disposizioni fatte salve le seguenti: •art. 2 comma 1 , Oggetto e ambito di applicazione; •art. 6 , Funzionalità; •art. 9 , Formato della segnatura di protocollo; •art. 18 commi 1 e 5, Modalità di registrazione dei

documenti informatici; •art. 20, Segnatura di protocollo dei documenti trasmessi; •art. 21, Informazioni da includere nella segnatura.

- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.
- Regolamento eIDAS (electronic IDentification Authentication and Signature) - Regolamento UE n° 910/2014 sull'identità digitale Regolamento eIDAS.
- Linee guida del 6 giugno 2019 contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate.
- Linee guida del 09/01/2020 sull'Accessibilità degli strumenti informatici.

Per quanto attiene alle normative in vigore nei luoghi dove sono conservati i documenti, si precisa che il Sistema di conservazione si trova nel Data Center Sogei, e che le normative di riferimento sono pubblicate sul sito internet di Sogei S.p.A.

Torna al sommario

4.2 STANDARD DI RIFERIMENTO

Si riportano di seguito i riferimenti dei principali standard elencati nell'allegato 4 "Standard e specifiche tecniche" delle linee guida relativamente alla conservazione digitale e sicurezza informatica.

Per la conservazione digitale:

- UNI 11386 - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.
- ISO 14721 - OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione.
- ISO 15836 - Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core
- ISO/TR 18492 - Long-term preservation of electronic document-based information.

Per la sicurezza informatica:

- ISO/IEC 27001 - Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);

- ISO/IEC 27017 - Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services;

- ETSI TS 101 533-1 V1.2.1 - Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;

- ETSI TR 101 533-2 V1.2.1 - Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.

Torna al sommario

5. RUOLI E RESPONSABILITÀ

L'ente o il soggetto diretto interessato è il titolare dell'oggetto della conservazione e, attraverso il proprio Responsabile della Conservazione, definisce e attua le politiche complessive del sistema di conservazione governandone la gestione con piena responsabilità ed autonomia. In relazione al modello organizzativo adottato affida a Sogei S.p.A. la gestione del servizio di conservazione secondo quanto previsto dalla normativa in materia.

Torna al sommario

5.1 RUOLI E RESPONSABILITÀ DEL CLIENTE

Il Responsabile della Conservazione svolge le seguenti attività:

a) definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;

b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;

c) genera e sottoscrive il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;

d) genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;

e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;

f) effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;

g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di

memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;

h) provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;

i) predispone le misure necessarie per la sicurezza fisica e logica del sistema di conservazione;

j) assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;

k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;

l) provvede per le amministrazioni statali centrali e periferiche a versare i documenti informatici, le aggregazioni informatiche e gli archivi informatici, nonché gli strumenti che ne garantiscono la consultazione, rispettivamente all'Archivio centrale dello Stato e agli archivi di Stato territorialmente competenti, secondo le tempistiche fissate dall'art. 41, comma 1, del Codice dei beni culturali;

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

Nel caso in cui il servizio di conservazione venga affidato ad un conservatore, le attività suddette o alcune di esse, ad esclusione della lettera m), potranno essere affidate al responsabile del servizio di conservazione

L'utente abilitato, ovvero il responsabile della conservazione o suo delegato, può richiedere al sistema di conservazione l'accesso ai documenti conservati per acquisire le informazioni di interesse nei limiti previsti dalla legge e nelle modalità previste dal manuale di conservazione.

Il produttore del pacchetto di versamento provvede a generare e trasmettere al sistema di conservazione i pacchetti di versamento nelle modalità e con i formati concordati con il conservatore secondo quanto descritto nel manuale di conservazione.

Provvede inoltre a verificare il buon esito della operazione di trasferimento al sistema di conservazione tramite la presa visione del rapporto di versamento prodotto dal sistema di conservazione stesso.

Torna al sommario

5.2 RUOLI E RESPONSABILITÀ DI SOGEI S.P.A.

Responsabile del Servizio di Conservazione

È la persona che nel rispetto del modello organizzativo adottato ed in accordo con il Responsabile della Conservazione, definisce ed attua le politiche complessive del sistema di conservazione.

È il riferimento aziendale per la definizione degli aspetti contrattuali, dei costi del servizio e della qualità del processo di conservazione e risulta, allo stesso tempo, l'unica interfaccia verso la struttura cliente e più in particolare verso il Responsabile della Conservazione.

Il Responsabile del servizio di conservazione assicura:

- la definizione, in accordo con il Responsabile della Conservazione, delle caratteristiche e dei requisiti del sistema di conservazione in funzione della tipologia dei documenti (analogici o informatici) e degli altri oggetti da conservare, della quale tiene evidenza;
- la definizione e la documentazione delle procedure da rispettare per l'apposizione del riferimento temporale ovvero, ove richiesto, della marca temporale; per tale attività si avvale del Responsabile della sicurezza dei sistemi per la conservazione;
- la definizione delle misure necessarie per la sicurezza fisica e logica del sistema preposto al Servizio di Conservazione e delle copie di sicurezza effettuate in base alle caratteristiche delle informazioni in termini di riservatezza, disponibilità, integrità; per tale attività si avvale del supporto del Responsabile della sicurezza dei sistemi per la conservazione;
- la verifica periodica dell'effettiva leggibilità dei formati conservati e provvede, se necessario, alla definizione delle procedure di riversamento diretto o sostitutivo; per tale attività si avvale del Responsabile dei sistemi informativi per la conservazione;
- l'assistenza e le risorse necessarie per l'espletamento delle attività del pubblico ufficiale, avvalendosi del Responsabile dei sistemi informativi per la conservazione.

Il Responsabile del servizio di conservazione inoltre:

- è responsabile dell'evoluzione del Servizio di Conservazione e della corretta erogazione del servizio di conservazione;
- rendiconta periodicamente al Responsabile della Conservazione le attività svolte e lo stato del sistema di conservazione;
- è responsabile dell'introduzione di nuovi formati di documento gestiti dal sistema di conservazione;
- presidia la normativa vigente in tema di conservazione.

Responsabile della funzione archivistica di conservazione

Si occupa della definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore. Supporta la definizione dei requisiti di acquisizione, della verifica di integrità ed effettua la descrizione archivistica dei documenti e degli altri oggetti trasferiti.

Il Responsabile della funzione archivistica di conservazione supporta la descrizione dei criteri per l'esibizione, l'accesso e la fruizione del patrimonio documentario e informativo conservato. Inoltre:

- supporta la definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici e degli altri oggetti da conservare;
- effettua il monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione;
- supporta l'ente produttore ai fini del trasferimento in conservazione;
- gestisce i rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.

Responsabile del trattamento dei dati personali

Effettua le seguenti attività:

- approva ed emana le policy e le linee strategiche in materia di sicurezza e privacy;
- compie gli adempimenti operativi spettanti alla Sogei ai sensi del Regolamento europeo in materia di protezione dei dati personali (UE) 2016/679.

Di seguito si riporta in sintesi l'organizzazione aziendale Sogei per la gestione del trattamento dei dati personali che prevede:

- il Responsabile della protezione dei dati personali (Data Protection Officer – DPO) a cui sono attribuiti i compiti di cui all'art. 39 del Regolamento generale europeo in

materia di protezione dei dati 2016/679, tra cui, in particolare, quello di informare e fornire consulenza sugli obblighi derivanti dal Regolamento e di sorvegliarne l'osservanza, fornire un parere sulla valutazione di impatto sulla protezione dei dati, cooperare con l'Autorità di controllo.

- il "Direttore Risorse Umane, Organizzazione, Privacy Comunicazione e Acquisti" di Sogei avente il compito di approvare ed emanare le policy e le linee strategiche in materia di sicurezza e privacy nonché di compiere gli adempimenti operativi spettanti alla Sogei ai sensi del Regolamento europeo in materia di protezione dei dati personali (UE) 2016/679.
- Inoltre, in Sogei, i ruoli e le responsabilità nel trattamento dei dati personali da parte del personale della stessa sono correlati alla specifica posizione ricoperta da ciascuno nell'ambito dell'organizzazione aziendale.

Responsabile della sicurezza dei sistemi per la conservazione

Effettua le seguenti attività:

- controlla il rispetto dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza;
- segnala eventuali difformità al Responsabile del servizio di conservazione e individua e pianifica le necessarie azioni correttive.

Il Responsabile della sicurezza dei sistemi per la conservazione ha inoltre il compito di:

- garantire la completa funzionalità dell'architettura anche sotto il profilo della sicurezza;
- garantire l'efficienza dell'architettura implementata, attraverso i ruoli di:
  - amministratore dei sistemi che ospitano il Servizio di Conservazione, rappresentati da:
    - servizi web di colloquio con gli utenti / applicazioni esterni rispetto al confine del sistema;
    - componenti di schedulazione / orchestrazione delle attività di conservazione;
    - componenti di processo e controllo;
  - amministratore delle basi dati che accolgono i metadati del Servizio di Conservazione;
  - amministratore del dispositivo di memorizzazione dei documenti digitali e altri oggetti, conforme ai requisiti in materia;

- amministratore della piattaforma, che implementa e rende disponibili i servizi "documentali".

Responsabile dello sviluppo e della manutenzione del sistema di conservazione

Si occupa dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione. Egli effettua:

- la pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione;
- il monitoraggio dei livelli di servizio (SLA) definiti per il sistema di conservazione;
- è l'interfaccia con l'ente produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche.

Responsabile dei sistemi informativi per la conservazione

È responsabile:

- della gestione dell'esercizio delle componenti HW e SW del sistema di conservazione;
- del monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore;
- della segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.

Il Responsabile dei sistemi informativi per la conservazione si avvale, mediante delega, della struttura "Architetture e Tecnologie Innovative" per la progettazione e l'implementazione dell'architettura del Servizio di Conservazione e delle eventuali evoluzioni e della struttura "Sistemi e Servizi per il Data Center", per la pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione.

Ha infine il compito di:

- archiviare e rendere disponibili, con l'impiego di procedure elaborative, relativamente ai pacchetti di archiviazione, le informazioni previste dalla normativa in materia;
- adottare le misure necessarie per la sicurezza fisica e logica del sistema preposto al Servizio di Conservazione e il necessario backup;

- assicurare l'apposizione della firma digitale e del riferimento temporale alla fine di ciascun processo di conservazione;
- assicurare la disponibilità dei supporti utilizzati e la gestione delle procedure di sicurezza e di tracciabilità che ne garantiscono la corretta conservazione, anche per consentire l'esibizione di ciascun documento conservato;
- effettuare il monitoraggio costante del regolare svolgimento del servizio;
- rendicontare periodicamente al Responsabile del servizio di conservazione le attività svolte e lo stato del sistema di conservazione.

Il Responsabile dei sistemi informativi per la conservazione può delegare, in tutto o in parte, lo svolgimento delle proprie attività a personale che per competenza e/o esperienza garantiscano la corretta esecuzione di quanto delegato.

Tecnico della conservazione

È la persona che in base alla catena delle deleghe effettua la firma dei pacchetti di archiviazione (PdA) tramite gli strumenti disponibili.

Ruolo	Nominativo	Periodo nel ruolo	Eventuali deleghe
Responsabile del servizio di conservazione	T. Bernardi - Responsabile dell'area "Soluzioni Gestionali, Documentali e AdeR"	Dal 29/05/2026	Nessuna.
Responsabile della funzione archivistica di conservazione	F. Quai "Soluzioni Documentali"	Dal 12/09/2022	Nessuna.
Responsabile della sicurezza dei sistemi per la conservazione	G. Ciminari - Responsabile dell'area "Cybersecurity"	Dal 31/03/2021	Nessuna.
Responsabile del trattamento dati personali	A. Trogu – Direttore della struttura "Legale, Privacy e Approvvigionamenti"	Dal 29/05/2025	Nessuna.
Responsabile dei sistemi informativi per la conservazione	G. Carlone - Responsabile dell'area "Presidio e Gestione Control Room"	Dal 29/05/2023	- Responsabile della struttura "Architetture e Tecnologie Innovative"

Ruolo	Nominativo	Periodo nel ruolo	Eventuali deleghe
			- Responsabile della struttura "Gestione Operazioni Data Center" - I tecnici di conservazione
Responsabile sviluppo e manutenzione del sistema di conservazione	C. Taddeo - Responsabile della linea operativa "Soluzioni Documentali"	Dal 29/05/2026	Nessuna.

Figura 1 - Organizzazione del servizio di conservazione

Torna al sommario

6. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

6.1 ORGANIGRAMMA

Gli attori principali sono il responsabile della conservazione dell'ente cliente e il responsabile del servizio di conservazione della Sogei S.p.A., che operano secondo gli accordi di servizio interni.

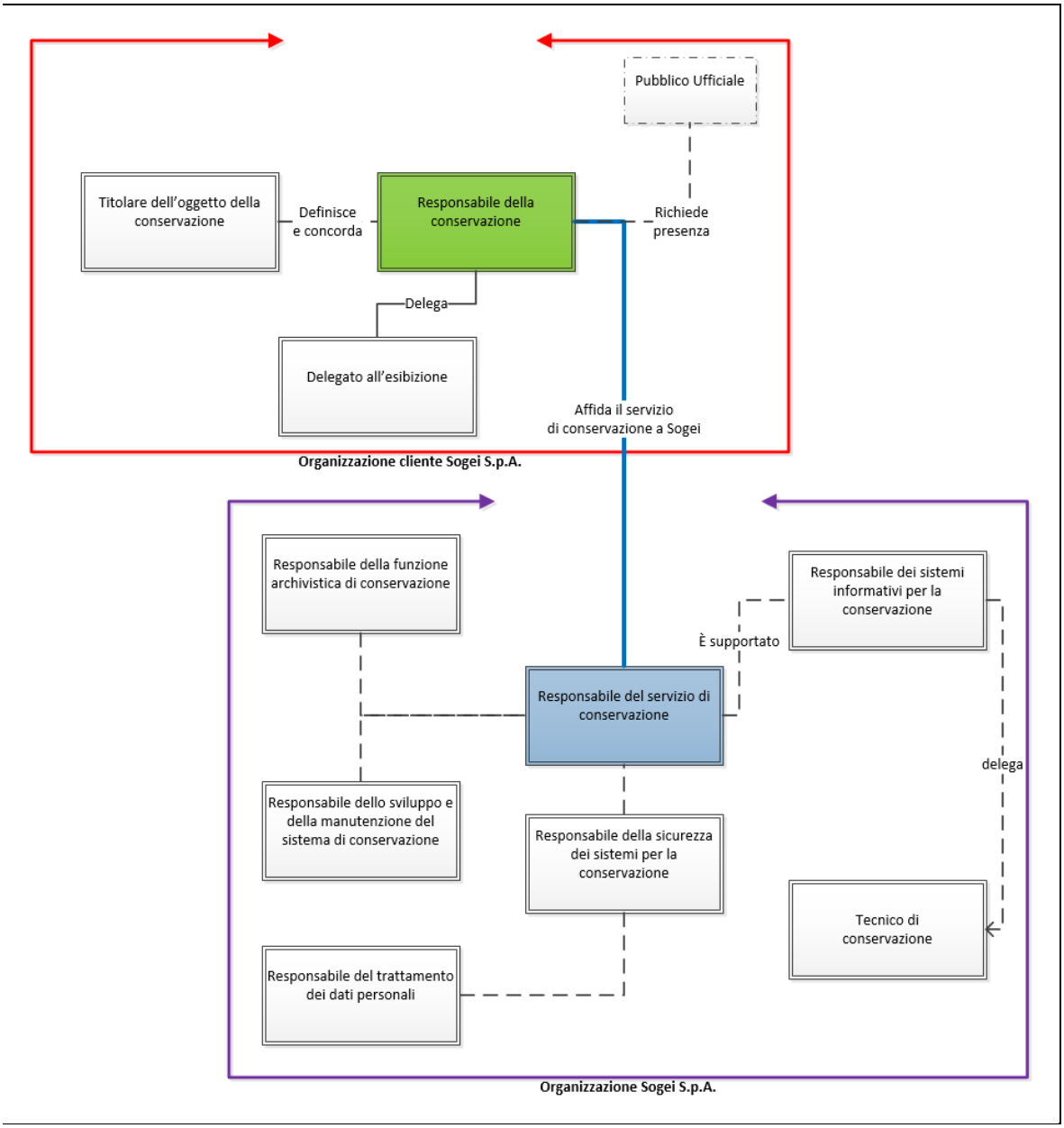

Figura 2 – Organigramma e relazioni tra i responsabili

Torna al sommario

6.2 STRUTTURE ORGANIZZATIVE

Sono di seguito descritte le strutture organizzative, comprese le responsabilità, che intervengono nelle principali funzioni che riguardano il servizio di conservazione.

Le attività proprie di ciascun contratto di servizio di conservazione sono svolte nella struttura organizzativa del Responsabile del servizio di conservazione, in particolare:

- l'attivazione del servizio di conservazione (a seguito della sottoscrizione di un contratto);
- la chiusura del servizio di conservazione (al termine di un contratto).

Tramite il "Sistema di conservazione dei documenti digitali", sono svolte le seguenti attività:

- acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento;
- preparazione e gestione del pacchetto di archiviazione;
- preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta;
- scarto dei pacchetti di archiviazione.

La struttura organizzativa del Responsabile dei sistemi informativi per la conservazione effettua le attività proprie di gestione dei sistemi informativi:

- conduzione e manutenzione del sistema di conservazione;
- monitoraggio del sistema di conservazione;
- change management;
- verifica periodica di conformità a normativa e standard di riferimento.

Torna al sommario

6.3 OSSERVATORIO TECNOLOGICO

Nell'organizzazione del responsabile del servizio di conservazione esiste un osservatorio tecnologico che a seguito di evoluzioni tecnologiche sui formati, effettua il riesame complessivo della progettazione del sistema ed indirizza le ulteriori attività degli esperti in materia, individuati nell'ambito delle singole strutture organizzative e

consultati relativamente agli argomenti di competenza. Qualora necessario possono essere coinvolti ulteriori referenti per tematiche specifiche.

Il gruppo di esperti, struttura organizzativa virtuale multidisciplinare in materia di formati e tecnologie, produce la documentazione tecnica, studia le normative, effettua le valutazioni di merito; effettua un monitoraggio periodico sui risultati relativi alla leggibilità dei documenti digitali e altri oggetti conservati provvedendo se necessario, per il riversamento digitale, a:

- definire i nuovi formati e il relativo software per l'esibizione;
- individuare/progettare il software di controllo del nuovo formato;
- individuare/progettare il software di conversione dei formati;
- progettare le elaborazioni per il riversamento.

Le risultanze di tale attività sono condivise con il responsabile del servizio di conservazione.

Le attività correlate con il riversamento digitale sono avviate e realizzate nel momento in cui si ravvisano le specifiche necessità. Le attività di riversamento digitale sono definite in base agli esiti del monitoraggio ed all'analisi dell'obsolescenza dei formati da parte dell'osservatorio tecnologico.

Torna al sommario

7. OGGETTI SOTTOPOSTI A CONSERVAZIONE

Di seguito sono descritti gli oggetti conservati e i pacchetti informativi gestiti dal sistema di conservazione.

Nel presente manuale si fa riferimento genericamente ai "documenti" anche se in tale definizione sono ricomprese tutte le tipologie descritte nel paragrafo seguente.

7.1 OGGETTI CONSERVATI

Di seguito l'elenco delle tipologie di documenti digitali e altri oggetti cui viene applicato il processo di conservazione:

- Documenti informatici / amministrativi informatici generati all'esterno della infrastruttura di Sogei e ricevuti tramite i servizi telematici dedicati ai clienti.
- Documenti informatici / amministrativi informatici generati dalle applicazioni interne alla infrastruttura di Sogei secondo quanto previsto dai flussi dei processi e/o procedimenti automatizzati.
- Fascicoli informatici chiusi.

Per gli oggetti documentali sono previste le seguenti specificità:

- Documenti firmati digitalmente;
- Documenti non firmati digitalmente;
- Documenti rilevanti ai fini tributari per i quali è apposta la marcatura temporale a livello di:
  - Singolo documento, se necessario certificare il momento della chiusura del documento;
  - Pacchetto di archiviazione, se necessario certificare il momento della conservazione del documento.
- Documenti con allegati.

Per i fascicoli informatici non sono definite particolari specificità.

Il sistema di conservazione gestisce tutti i formati di file previsti dalla normativa in materia, sottoponendo i documenti da conservare a due diverse modalità di validazione:

- la modalità rigorosa "strict-mode", tramite la verifica del rispetto dello standard ISO di riferimento, ovvero rispetto alle specifiche tecniche pubbliche o agli schemi di riferimento; tale modalità viene applicata nel caso particolare dei file PDF/A per i quali è prevista la conservazione illimitata nel tempo.

- la modalità non rigorosa "no-strict-mode", tramite la verifica delle caratteristiche dei file come l'estensione nel nome del file, un codice interno al file, come il *magic number*, la tipologia MIME; tale modalità viene applicata nei casi in cui è previsto un tempo di conservazione limitato nel tempo. L'applicazione di tale modalità deve essere concordata ed accettata dal Responsabile della conservazione.

Nella tabella seguente sono indicati i **formati di file** gestiti dal sistema di conservazione nella modalità rigorosa "strict-mode".

FORMATO	ESTENSIONE	MODALITÀ DI VALIDAZIONE
PDF/A 1-a	.pdf	Rispetto allo standard ISO di riferimento
PDF/A 1-b	.pdf	Rispetto allo standard ISO di riferimento
PDF	.pdf	Rispetto allo standard ISO di riferimento
TIFF	.tif .tiff	Rispetto alle specifiche tecniche pubbliche
POSTA ELETTRONICA	.eml	Rispetto alla codifica UTF-8
POSTA ELETTRONICA CERTIFICATA	.eml	Rispetto alla codifica UTF-8
XML NON STRUTTURATO (SENZA SCHEMA XSD)	.xml	Rispetto alla codifica UTF-8
TESTO	.txt	Rispetto alla codifica UTF-8
XML	.xml	Rispetto allo schema XSD di riferimento
Open Office XML	.docx	Rispetto allo standard ISO di riferimento

Figura 3 - Elenco dei formati gestiti

I **formati di firma** gestiti dal sistema di conservazione in fase di verifica dell'integrità dei documenti da conservare sono quelli previsti dagli standard europei che prevedono tre tipi di sottoscrizione digitale, identificati dagli acronimi CAdES, PAdES, XAdES.

In particolare:

- CAdES, in questo caso il file sottoscritto conserva il suo nome e la sua estensione originale, al quale viene aggiunta l'estensione ". p7m";

- XAdES, in questo caso il file sottoscritto è sempre un file di estensione .xml;
- PAdES, in questo caso il file sottoscritto è sempre un file di estensione .pdf.

Le tipologie di verifica della validità del certificato di firma attivabili sono le seguenti:

- nessuna verifica della validità del certificato di firma;
- verifica della validità del certificato di firma alla data corrente (data di sistema);
- verifica della validità del certificato di firma rispetto al riferimento temporale del documento, ovvero ad una data specifica fornita dal processo di business;
- verifica della validità del certificato di firma rispetto all'attributo signing time contenuto nel certificato di firma stesso.

È possibile attivare **misure di sicurezza** specifiche per documenti contenenti dati sensibili al fine di aumentare il livello di protezione delle informazioni nel sistema di conservazione. In particolare, è disponibile la cifratura dei file.

Quando viene attivata la cifratura, i file ricevuti in chiaro vengono cifrati e messi in sicurezza nell'archivio di conservazione; nel momento in cui vengono richiesti per l'esibizione vengono restituiti in chiaro.

Torna al sommario

7.2 PACCHETTO DI VERSAMENTO

Il pacchetto di versamento – nel seguito PDV – è un pacchetto informativo inviato dal produttore del PDV al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione.

Il produttore del PDV genera il pacchetto e ne assicura la trasmissione al sistema di conservazione, secondo le modalità operative definite nel manuale di conservazione.

Ogni PDV può contenere esclusivamente documenti della stessa tipologia, ovvero della stessa Classe Documentale. Pertanto, l'elenco dei metadati dei documenti contenuti nel PDV è omogeneo.

I metadati sono di carattere diverso a seconda che descrivano proprietà e qualità del pacchetto in genere o dei singoli documenti.

Per consentire l'elaborazione automatica dei metadati il sistema di conservazione richiede l'incapsulamento degli stessi in un determinato formato XML, che di fatto costituisce l'Indice del pacchetto di versamento – nel seguito IPdV.

L'IPdV è un'evidenza informatica, ovvero un file, che descrive il versamento e i documenti che ne fanno parte attraverso l'uso di metadati. È in formato XML.

Torna al sommario

7.3 PACCHETTO DI ARCHIVIAZIONE

Il pacchetto di archiviazione – nel seguito PDA – è un pacchetto informativo prodotto dalla trasformazione di uno o più pacchetti di versamento.

La struttura del PDA è costruita sulla base delle specifiche della struttura dati indicate dallo standard UNI 11386 e secondo le modalità riportate nel manuale di conservazione.

Il PDA viene generato automaticamente dal sistema di conservazione, tramite gli appositi processi.

Il PDA 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 (o digitale).

Nei casi in cui è necessario fornire data certa, rispetto al momento in cui è generato il PDA, oltre alla firma elettronica qualificata è apposta anche una marcatura temporale.

L'IPdA è un'evidenza informatica, ovvero un file, che descrive l'archiviazione e i documenti che ne fanno parte attraverso l'uso di metadati. È in formato XML.

La struttura dell'indice del pacchetto di archiviazione IPdA è di seguito schematizzata.

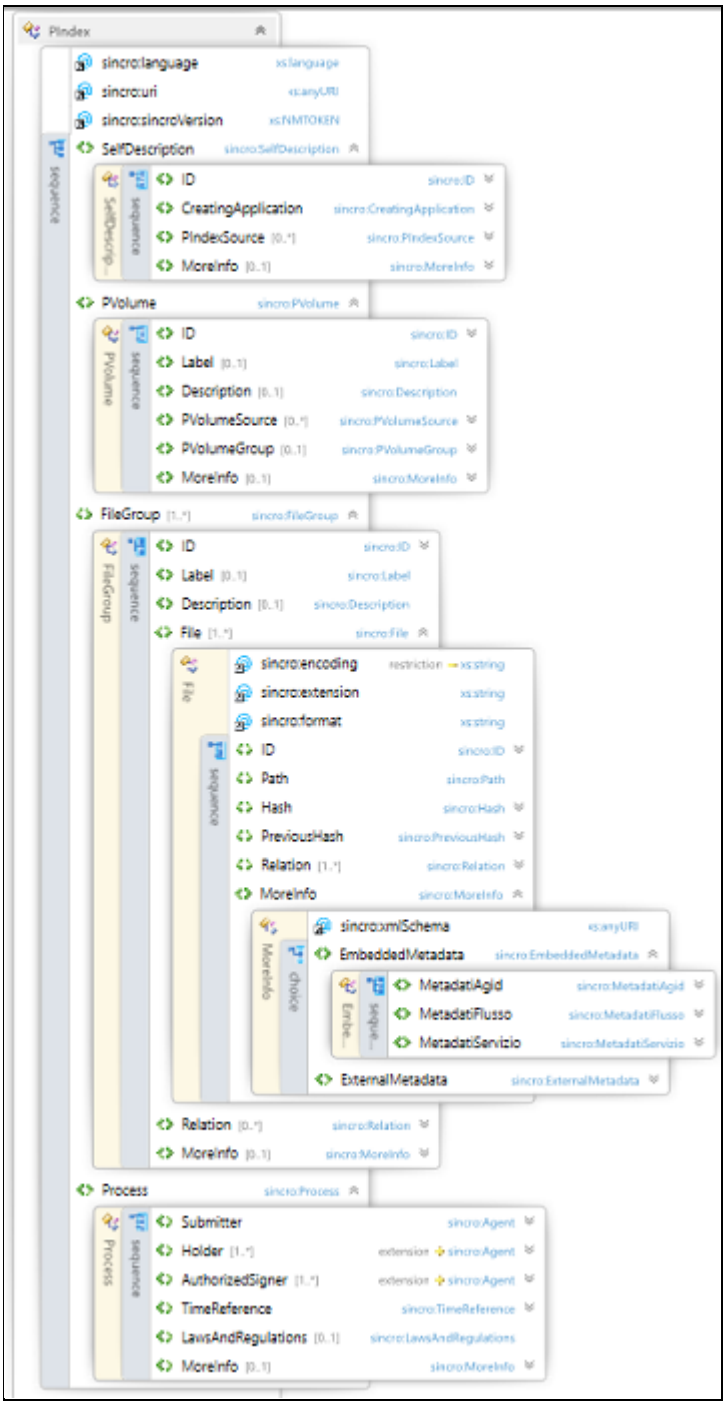

Figura 4 - Struttura IPdA

Torna al sommario

7.4 PACCHETTO DI DISTRIBUZIONE

Il pacchetto di distribuzione – nel seguito PDD – è un pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta.

Il PDD viene generato automaticamente dal sistema di conservazione, tramite gli appositi processi, a seguito di una richiesta da parte dell'utente.

Il PDD è un insieme di metadati e documenti corrispondenti alla richiesta di esibizione effettuata da un utente.

Il PDD è un archivio compresso in formato .zip che contiene i seguenti elementi:

- indice del pacchetto di distribuzione – IPdD;
- la copia dei file relativi ai documenti richiesti (in formato originale firmato o meno);
- il foglio di stile .xslt per i file di formato XML;
- il file firmato relativo al PDA del documento (uno o più in base ai documenti oggetto della richiesta di esibizione);
- il file firmato della delega del Tecnico della conservazione che ha firmato il PDA del documento (uno o più).

Il pacchetto di distribuzione è firmato con firma digitale dal sistema di conservazione.

L'IPdD è un'evidenza informatica, ovvero un file, che descrive la distribuzione e i documenti che ne fanno parte attraverso l'uso di metadati. È in formato XML.

Torna al sommario

7.5 DELEGA ALLA FIRMA DEI PDA

La delega alla firma dei PDA conferita nell'ambito della catena delle deleghe al Tecnico della conservazione che effettua l'operazione di firma del pacchetto di archiviazione è anch'essa un oggetto conservato nel sistema di conservazione. Viene generata una delega per ciascun cliente che affida il servizio di conservazione a Sogei.

La delega è un'evidenza informatica, ovvero un file, che descrive i dati della delega attraverso l'uso di metadati. È in formato XML.

Le informazioni che costituiscono la delega sono riportate di seguito:

- Cliente del servizio di conservazione;
- data definizione struttura di riferimento della delega, corrisponde alla data/versione della struttura di riferimento dell'xml;
- progressivo di identificazione univoco della delega, corrisponde ad un codice alfanumerico che identifica univocamente la delega e la versione di riferimento;
- data di autorizzazione alla firma del delegato, data di generazione della delega;
- dati del delegato, ruolo, nome, cognome, codice fiscale;
- ambito, di applicazione in base alle risorse assegnate al delegato:
  - oggetto: impostato con il "riferimento normativo in materia di firma digitale" - unico per tutte le deleghe;
  - servizio, Servizio di conservazione per il quale si è autorizzati alla firma;
  - dati del responsabile della conservazione, ruolo, nome cognome codice fiscale (delegante 1 livello);
  - dati del responsabile dei sistemi informativi per la conservazione, ruolo, denominazione (delegante 2 livello);
  - dati del delegante, ruolo nome cognome codice fiscale;
  - riferimento normativo, "in materia di conservazione" - unico per tutte le deleghe;
  - attributi, metadati specifici relativamente ai quali si è autorizzati alla firma.

Torna al sommario

8. IL PROCESSO DI CONSERVAZIONE

Il processo di conservazione si svolge secondo una serie di fasi schematizzate nella figura seguente.

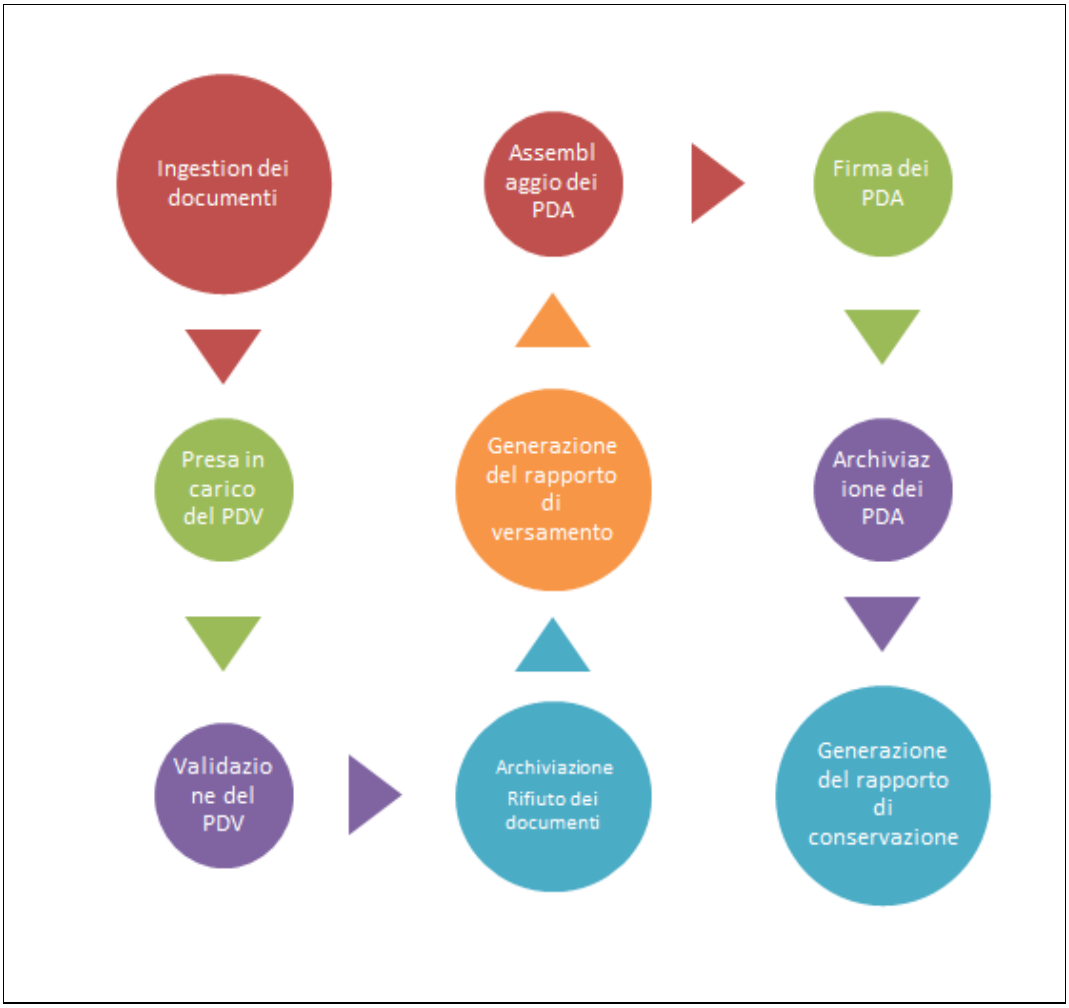

Figura 5 - Il processo di conservazione

- Ingestion dei documenti: rappresenta la fase di trasmissione del pacchetto di versamento da parte del produttore del PDV e la ricezione da parte del sistema di conservazione.
- Presa in carico del PDV: rappresenta la fase di presa in carico del pacchetto di versamento da parte del sistema di conservazione, l'esito positivo dei controlli formali è confermato da una ricevuta di presa in carico rilasciata al produttore del

PDV. In caso di esito negativo dei controlli formali il pacchetto di versamento non è preso in carico.

- Validazione del PDV: rappresenta la fase di elaborazione del pacchetto di versamento da parte del sistema di conservazione e si riferisce all'applicazione dei controlli di univocità, formato, integrità e autenticità sui singoli documenti da conservare.
- Archiviazione / rifiuto dei documenti: rappresenta la fase di archiviazione dell'oggetto della conservazione nel sistema di conservazione in caso di esito positivo della fase precedente ovvero il rifiuto.
- Generazione del rapporto di versamento: rappresenta la fase in cui il sistema di conservazione, per ogni pacchetto di versamento elaborato, genera il rapporto di versamento in cui per ciascun documento indica l'esito positivo o negativo dell'archiviazione con relativa motivazione della fase di controllo.
- Assemblaggio dei PDA: rappresenta la fase di assemblaggio dei documenti in pacchetti di archiviazione secondo le regole di archiviazione previste per ciascun servizio di conservazione.
- Firma dei PDA: rappresenta la fase di firma dei pacchetti di archiviazione assemblati. Sono previste due modalità di firma, la firma automatica remota massiva tramite HSM e in alternativa la firma manuale da parte dei Tecnici della conservazione.
- Archiviazione dei PDA: rappresenta la fase di conservazione dei pacchetti di archiviazione che è l'ultima fase del processo.
- Generazione del rapporto di conservazione: rappresenta la fase in cui il sistema di conservazione, per ciascun servizio di conservazione e per ogni giornata genera il rapporto di conservazione in cui per ciascun documento indica l'esito positivo e la data di conservazione.

Di seguito sono descritte nel dettaglio le modalità tramite le quali sono svolte le attività del processo di conservazione.

Torna al sommario

8.1 MODALITÀ DI ACQUISIZIONE DEI PACCHETTI DI VERSAMENTO PER LA LORO PRESA IN CARICO

L'operazione di versamento consiste nella trasmissione da parte del produttore del PDV degli oggetti da conservare e dei metadati che li identificano.

Il versamento prevede una unica modalità di trasmissione cioè il canale web tramite invocazione di appositi servizi di ingestion esposti dal sistema di conservazione e dettagliati nel capitolo che descrive il sistema di conservazione.

Il versamento è effettuato tramite i PDV.

L'invio dei PDV prevede i seguenti passi da parte del produttore:

- Predisposizione dei documenti da conservare in una destinazione nota e condivisa con il sistema di conservazione.
- Generazione dell'indice del PDV secondo la struttura predefinita.
- Richiamo dei servizi di ingestion del sistema di conservazione.

Il produttore nel momento in cui richiama i servizi di ingestion deve comunicare le seguenti informazioni:

- IPdV[1], stringa relativa al file xml secondo la struttura predefinita;
- Impronta dell'IPdV e algoritmo di calcolo.

Sono registrate le informazioni della ricezione del pacchetto di versamento nel registro dei pacchetti di versamento che prevede le seguenti informazioni:

- Nome dell'applicazione produttore del PDV
- Codice servizio di conservazione
- Identificativo del PDV
- Impronta del PDV
- Numero file contenuti nel PDV
- Stato del PDV, impostato con ricevuto
- Data ricezione del PDV.

Torna al sommario

[1] Nel IPdV sono contenuti i riferimenti dei documenti predisposti nella destinazione nota e condivisa con il sistema di conservazione.

8.2 VERIFICHE EFFETTUATE SUI PACCHETTI DI VERSAMENTO E SUGLI OGGETTI IN ESSI CONTENUTI

Il sistema di conservazione per ogni PDV inviato dal produttore del PDV effettua i seguenti controlli:

- Verifica abilitazione del produttore del PDV per l'invio del pacchetto tramite confronto tra l'utenza chiamante e l'utenza definita nel sistema di controllo accessi (par. 8.6) (identificazione certa del produttore).
- Confronto tra l'impronta (hash del PDV) dichiarata e quella calcolata dal sistema di conservazione in fase di ingestion.
- Verifica conformità struttura IPdV allo schema di riferimento.
- Verifica univocità riferimenti documentali all'interno del pacchetto.
- Verifica corrispondenza tra riferimento documentale dichiarato all'interno del pacchetto e quello presente nella destinazione nota e condivisa.
- Memorizzazione dei dati del pacchetto di versamento.

Nel caso in cui tutti i controlli hanno esito positivo, il sistema di conservazione:

- Conferma esito positivo della presa in carico nell'ambito della risposta al versamento.
- Genera la ricevuta di presa in carico.
- Appone la firma elettronica sulla ricevuta di presa in carico.
- Rende disponibile la ricevuta di presa in carico nella destinazione nota e condivisa per il recupero da parte del produttore del PDV.

Sono registrate le informazioni della acquisizione del pacchetto di versamento nel registro dei pacchetti di versamento che prevede le seguenti informazioni:

- Nome dell'applicazione produttore del PDV
- Codice servizio di conservazione
- Identificativo del PDV
- Impronta del PDV
- Numero file contenuti nel PDV
- Stato del PDV, impostato con acquisito
- Data acquisizione del PDV.

Il processo di conservazione continua per i soli PDV presi in carico dal sistema di conservazione.

I PDV presi in carico sono memorizzati negli archivi del sistema di conservazione per le successive verifiche preliminari alla conservazione.

In particolare, sono effettuate le seguenti verifiche:

- Validazione metadati: la prima verifica effettuata riguarda la correttezza dei metadati presenti nel IPdV; i metadati sono validati rispetto alle specifiche concordate in fase di configurazione del servizio di conservazione per le diverse tipologie documentali sia in termini di valori contenuti sia in termini di tipo di dato (data, stringa, lista valori ammessi).
- Verifica integrità: il sistema di conservazione, in relazione all'integrità dei documenti da conservare, effettua ove previsto la verifica della firma digitale e la validità del certificato di firma secondo gli accordi specifici descritti nel manuale di conservazione per ciascun documento referenziato dal IPdV.
- Validazione formato: il sistema di conservazione, in relazione al formato dei documenti da conservare comunicato tra i metadati del IPdV, effettua la verifica di formato per ciascun documento referenziato dal IPdV.

Il processo di conservazione continua per i documenti per i quali tutti i controlli hanno avuto esito positivo mentre si interrompe per i documenti per i quali almeno uno dei controlli ha dato esito negativo.

Torna al sommario

8.3 ACCETTAZIONE DEI PACCHETTI DI VERSAMENTO E GENERAZIONE DEL RAPPORTO DI VERSAMENTO DI PRESA IN CARICO

Il sistema di conservazione genera un rapporto di versamento per ciascuno dei PDV per i quali è stata completata la verifica di dettaglio e la verifica di tutti i documenti contenuti.

Nel rapporto di versamento sono indicati:

- I documenti versati per i quali tutti i controlli hanno avuto esito positivo e sono stati memorizzati nel dispositivo W.O.R.M. in attesa del completamento del processo di conservazione.
- I documenti versati per i quali almeno uno dei controlli ha avuto esito negativo e sono stati sottoposti al processo di rifiuto ed il processo di conservazione si è interrotto.

Nel rapporto di versamento sono indicati gli esiti per ciascuno dei documenti contenuti nel PDV, nel caso di esito negativo è indicata la motivazione del rifiuto.

Il sistema di conservazione effettua le seguenti attività:

- Genera il rapporto di versamento, secondo la schedulazione prevista per il processo automatico di generazione del documento.
- Valorizza il riferimento temporale presente nella struttura del rapporto di versamento con la data di sistema in formato timestamp e senza soluzione di continuità firma il rapporto di versamento, applicando una firma elettronica che contiene la data e l'ora della firma.
- Rende disponibile il rapporto di versamento nella destinazione nota e condivisa per il recupero da parte del produttore
- Memorizza il rapporto di versamento nei propri archivi per un periodo di tempo prestabilito per eventuali riscontri.

Sono registrate le informazioni della accettazione del pacchetto di versamento nel registro dei pacchetti di versamento che prevede le seguenti informazioni:

- Nome dell'applicazione produttore del PDV
- Codice servizio di conservazione
- Identificativo del PDV
- Impronta del PDV
- Numero file contenuti nel PDV
- Stato del PDV, impostato con elaborato
- Data elaborazione del PDV.

Torna al sommario

8.4 RIFIUTO DEI PACCHETTI DI VERSAMENTO E MODALITÀ DI COMUNICAZIONE DELLE ANOMALIE

Nel caso in cui almeno uno dei controlli descritti nel paragrafo 7.2 che il sistema di conservazione effettua sul PDV ha esito negativo, il sistema di conservazione:

- Rifiuta l'intero PDV.
- Comunica l'esito negativo e la relativa motivazione.

Il PDV, se rifiutato, non può essere nuovamente inviato al sistema di conservazione; in caso di errori, il produttore del PDV deve procedere alla generazione di un nuovo PDV.

Sono registrate le informazioni della acquisizione del pacchetto di versamento nel registro dei pacchetti di versamento e lo stato di errore nel caso specifico del rifiuto, che prevede le seguenti informazioni:

- Nome dell'applicazione produttore del PDV
- Codice servizio di conservazione
- Identificativo del PDV
- Impronta del PDV
- Numero file contenuti nel PDV
- Stato del PDV, impostato con stato errore
- Data acquisizione del PDV.

Nel caso in cui il pacchetto di versamento non è preso in carico dal sistema di conservazione in modo sincrono, cioè in tempo reale, è notificato al sistema chiamante un esito di errore da parte del medesimo servizio di ingestion. Il PDV non viene memorizzato nel sistema.

Inoltre, il sistema di conservazione:

- Genera la ricevuta di errore nella presa in carico.
- Firma elettronicamente la ricevuta di errore nella presa in carico.
- Rende disponibile la ricevuta di errore nella presa in carico nella destinazione nota e condivisa per il recupero da parte del produttore.

Torna al sommario

8.5 PREPARAZIONE E GESTIONE DEL PACCHETTO DI ARCHIVIAZIONE

Il sistema di conservazione genera i PDA applicando le regole di assemblaggio dei documenti secondo i seguenti criteri:

- Servizio di conservazione.
- Tipologia documentale.
- Specifici metadati se definiti.

I PDA sono riferiti ai documenti già acquisiti nel dispositivo W.O.R.M. in attesa di conservazione.

È da precisare che l'organizzazione dei documenti nei PDA può essere diversa dalla organizzazione dei documenti nei PDV poiché i criteri di assemblaggio sono specifici del sistema di conservazione e rispondono ai criteri di composizione dell'archivio di conservazione.

Tra i criteri di assemblaggio sono presenti anche il tempo e la dimensione, per consentire una gestione ottimizzata dell'archiviazione nel sistema di conservazione.

In tal senso i PDA vengono generati in base ad una specifica schedulazione temporale e conterranno un numero massimo di elementi concordato nel manuale di conservazione.

I PDA sono numerati progressivamente nel sistema di conservazione.

I PDA sono sottoposti alla firma digitale da parte dei tecnici della conservazione ovvero alla firma automatica remota massiva in base al flusso di conservazione.

Il Responsabile dei Sistemi Informativi per la conservazione delega la firma del PDA a specifico personale che ricopre il ruolo di "tecnico della conservazione" e l'elenco dei nominativi è riportato in una apposita comunicazione archiviata presso il delegante, nel caso della firma automatica remota massiva la firma viene apposta tramite un certificato intestato al Responsabile dei Sistemi Informativi per la conservazione.

La firma digitale del PDA è subordinata alla verifica dei poteri di firma tramite la verifica della presenza di una delega valida per il tecnico della conservazione ovvero della delega del Responsabile dei Sistemi Informativi per la conservazione.

Nei casi previsti contestualmente alla firma digitale del PDA è apposta in modalità automatica anche la marca temporale.

Il sistema di conservazione per ogni PDA firmato dal produttore effettua i seguenti controlli preliminari alla conservazione:

- Verifica integrità del PDA, tramite verifica della firma digitale e verifica validità del certificato alla data di firma.
- Verifica conformità struttura IPdA allo schema di riferimento.
- Verifica correttezza metadati e impronte.
- Verifica dei dati di firma presenti nella specifica sezione con le deleghe attive al momento della firma.
- Calcolo dell'hash del PDA.

Il processo di conservazione continua per i PDA per i quali tutti i controlli hanno avuto esito positivo mentre si interrompe per i PDA per i quali almeno uno dei controlli ha dato esito negativo; in tale caso i PDA sono posti in uno stato di errore per le successive verifiche.

Nel caso in cui siano riscontrati errori nei PDA, gli oggetti in essi referenziati vengono resi nuovamente disponibili per una nuova fase di assemblaggio ed i PDA in errore sono rimossi.

I PDA per i quali tutti i controlli hanno avuto esito positivo sono memorizzati nel dispositivo W.O.R.M. ed il processo di conservazione è completato.

Torna al sommario

8.6 PREPARAZIONE E GESTIONE DEL PACCHETTO DI DISTRIBUZIONE AI FINI DELL'ESIBIZIONE

Il sistema di conservazione prevede la predisposizione e gestione dei pacchetti di distribuzione ai fini dell'esibizione. In tal caso il PDD contiene i documenti richiesti e i riferimenti ad essi correlati anche se conservati con riferimento a PDA diversi.

Il sistema di conservazione genera il PDD su richiesta da parte dell'utente di una lista di documenti da esibire.

La lista dei documenti da esibire è costruita sulla base di criteri di ricerca finalizzati all'individuazione puntuale dei documenti di interesse.

Il sistema di conservazione accetta richieste di esibizione riferite a più documenti; tali richieste possono essere corredate da una motivazione da parte dell'utente che può essere un testo libero o predefinito.

Il PDD può contenere un numero limite di documenti impostato in base ad una soglia configurabile; pertanto, il sistema di conservazione suddivide i documenti nei pacchetti di distribuzione in base alla soglia di contenimento prevista.

È possibile quindi che a fronte di una richiesta di esibizione siano generati più PDD.

Il sistema di conservazione effettua le seguenti attività:

- Genera il PDD.
- Appone con meccanismi automatici la firma digitale del Responsabile del servizio di conservazione ovvero del Responsabile dei Sistemi Informativi per la conservazione sul PDD.

- Rende disponibile il PDD per la consultazione da parte dell'utente abilitato.
- Memorizza il PDD nei propri archivi per un periodo di tempo prestabilito per eventuali riscontri e poi lo rimuove.

Torna al sommario

8.7 PRODUZIONE DI DUPLICATI E COPIE INFORMATICHE E DESCRIZIONE DELL'EVENTUALE INTERVENTO DEL PUBBLICO UFFICIALE NEI CASI PREVISTI

Il sistema di conservazione produce i duplicati informatici dei documenti conservati nel momento in cui genera il pacchetto di distribuzione e li inserisce al suo interno.

Tra le informazioni inserite nell'indice del pacchetto di distribuzione è presente l'impronta del file del documento conservato e del pacchetto di archiviazione calcolata in fase di ricezione nel sistema di conservazione ed archiviazione nel dispositivo W.O.R.M ed il relativo algoritmo di calcolo.

Il sistema di conservazione rende disponibile una funzione per il prelievo dei PDD tramite il download dell'intero pacchetto.

L'utente abilitato che ne ha fatto richiesta può autonomamente confrontare l'impronta del file conservato duplicato ed inserito nel pacchetto di distribuzione con l'impronta inizialmente calcolata per accertarsi della correttezza.

Per quanto riguarda le copie informatiche e l'attestazione di conformità all'originale il sistema di conservazione non prevede funzionalità di supporto in quanto tale attività non è tra quelle delegate al Responsabile del servizio di conservazione; è un'attività effettuata dal Responsabile della conservazione cliente.

Nei casi in cui è prevista, il Responsabile della conservazione assicura la presenza di un pubblico ufficiale al fine di dichiarare la conformità della copia all'originale conservato.

Torna al sommario

8.8 SCARTO DEI PACCHETTI DI ARCHIVIAZIONE

Il sistema di conservazione prevede specifiche funzionalità per effettuare lo scarto dei pacchetti di archiviazione alla scadenza dei termini di conservazione previsti dalla norma o secondo quanto indicato dal piano di conservazione del Titolare dell'oggetto di conservazione.

Nel caso degli archivi pubblici o privati, che rivestono interesse storico particolarmente importante, l'eventuale scarto del pacchetto di archiviazione avviene previa autorizzazione da parte dell'autorità preposta, rilasciata al Titolare dell'oggetto della conservazione, secondo quanto previsto dalla normativa vigente in materia.

Tali funzionalità supportano le operazioni previste per l'eliminazione di quei contenuti dell'archivio per i quali sono decorsi i termini di conservazione. Lo scarto è effettuato rispetto ai pacchetti di archiviazione.

Le funzionalità disponibili permettono di effettuare le seguenti attività:

- Definire le strutture informative per memorizzare le operazioni di scarto;
- Analizzare l'archivio per individuare i pacchetti di archiviazione da scartare;
- Predisporre il report di scarto da sottoporre alla validazione del Titolare dell'oggetto della conservazione;
- Effettuazione dello scarto, ovvero la eliminazione fisica dei pacchetti di archiviazione e relativi documenti / fascicoli conservati. Contestualmente vengono eliminati fisicamente anche tutti i prodotti del processo di conservazione (ricevute di presa in carico, rapporti di versamento e conservazione, pacchetti di distribuzione).

Da un punto di vista concettuale, un documento transita nella fase di scarto quando si avvicina la conclusione del periodo di conservazione previsto per quella tipologia di documento.

I pacchetti di archiviazione sono omogenei per tipologia di documento, pertanto, sono individuati in base ai medesimi criteri temporali.

Una volta che il pacchetto di archiviazione / documento è scartato non è più visibile nell'archivio di conservazione.

Torna al sommario

8.9 PREDISPOSIZIONE DI MISURE A GARANZIA DELL'INTEROPERABILITÀ E TRASFERIBILITÀ AD ALTRI CONSERVATORI

Ai fini dell'interoperabilità tra i sistemi di conservazione sono stati adottati i seguenti criteri.

I formati adottati per gli oggetti documentali predisposti dal Sistema di conservazione e quelli ammessi per i documenti di cui è richiesta la conservazione da parte del titolare

dell'oggetto della conservazione, sono scelti secondo quanto previsto nell'allegato "Formati" delle linee guida, a garanzia dei principi dell'interoperabilità tra i sistemi di conservazione

I pacchetti di archiviazione sono realizzati secondo i requisiti previsti dallo standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali, che è lo standard riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione. In analogia allo standard SInCRO, la struttura utilizzata prevede una specifica articolazione per mezzo del linguaggio formale XML.

Sono previsti pacchetti di distribuzione coincidenti con i pacchetti di archiviazione in casi specifici, come ad esempio per l'esportazione massiva dal sistema di oggetti conservati.

Tutti gli ulteriori pacchetti informativi progettati e realizzati per il Sistema di conservazione nonché le ricevute prodotte dal sistema, sono derivate da tale struttura standard e personalizzate per gli utilizzi specifici nel rispetto delle medesime regole adottate per i pacchetti di archiviazione.

Torna al sommario

8.10 CONFIGURAZIONE DEI SERVIZI DI CONSERVAZIONE

Il Responsabile del servizio di conservazione dei documenti, in collaborazione con il Responsabile della conservazione, definisce le regole e le modalità di erogazione del servizio di conservazione che vengono descritte nel documento denominato "Specificità del contratto".

La definizione di tali regole prevede:

- la definizione dei profili da attribuire agli utenti delegati dal Responsabile della conservazione e le regole di visibilità degli oggetti conservati:
  - ogni utente è associato ad un insieme di risorse che consentono di operare nel sistema di conservazione per eseguire specifiche attività;
  - le risorse associate a ciascun profilo possono essere all'occorrenza disattivate o riattivate;
  - gli utenti sono delegati alle funzionalità di esibizione in relazione agli ambiti di competenza;
- la determinazione dei singoli servizi di conservazione caratterizzati da un insieme di tipologie documentali omogenee, in particolare devono essere definiti:

- la natura ed eventuali specificità dei documenti da conservare;
- i metadati dei documenti, obbligatori e opzionali;
- le regole di assemblaggio dei pacchetti di archiviazione.

Torna al sommario

8.11 LE RICEVUTE DEL SISTEMA DI CONSERVAZIONE

Nel presente capitolo sono descritte le ricevute prodotte dal sistema di conservazione.

Tali ricevute sono generate secondo strutture informative predefinite e condivise con i produttori dei PDV.

Sono generate, firmate e messe a disposizione dei produttori dei PDV per un periodo di tempo prestabilito in destinazione nota e condivisa con il sistema di conservazione.

Le ricevute sono cancellate dal sistema al decorrere dei termini previsti per ciascuna specifica tipologia e/o servizio di conservazione.

Torna al sommario

8.11.1 RICEVUTA DI PRESA IN CARICO

La ricevuta di presa in carico – nel seguito RPC - è un pacchetto informativo generato dal sistema di conservazione a fronte della corretta presa in carico di un pacchetto di versamento.

La RPC è generata automaticamente dal sistema di conservazione e sottoscritta con firma elettronica.

Ogni RPC si riferisce ad un pacchetto di versamento.

La RPC è un'evidenza informatica, ovvero un file, che descrive la presa in carico e i documenti che ne fanno parte attraverso l'uso di metadati. È in formato XML.

8.11.2 RICEVUTA DI ERRORE NELLA PRESA IN CARICO

La ricevuta di errore nella presa in carico – nel seguito RPC_E - è un pacchetto informativo generato dal sistema di conservazione a fronte di errori nella fase di presa in carico di un pacchetto di versamento.

La RPC_E è generata automaticamente dal sistema di conservazione e sottoscritta con firma elettronica.

Ogni RPC_E si riferisce ad un pacchetto di versamento.

La RPC_E è un'evidenza informatica, ovvero un file, che descrive l'errore nella presa in carico e i documenti che ne fanno parte attraverso l'uso di metadati. È in formato XML.

Torna al sommario

8.11.3 RAPPORTO DI VERSAMENTO

Il rapporto di versamento – nel seguito RDV - è un pacchetto informativo generato dal sistema di conservazione al termine dei controlli formali di integrità e formato effettuati dal sistema di conservazione sui singoli documenti contenuti in un pacchetto di versamento.

Il RDV è generato automaticamente dal sistema di conservazione e sottoscritto con firma elettronica. Viene reso disponibile al produttore del PDV in una destinazione nota e condivisa con il sistema di conservazione.

Ogni RDV si riferisce ad un pacchetto di versamento e riporta per ogni documento l'esito positivo o negativo delle verifiche effettuate, in questo ultimo caso riportando la motivazione dell'esito di rifiuto.

Il RDV è un'evidenza informatica, ovvero un file, che descrive l'esito delle verifiche effettuate sui documenti che ne fanno parte attraverso l'uso di metadati. È in formato XML.

Torna al sommario

8.11.4 RAPPORTO DI CONSERVAZIONE

Il rapporto di conservazione – nel seguito RDC - è un pacchetto informativo generato dal sistema di conservazione al termine della fase di conservazione dei documenti.

La RDC è generata automaticamente dal sistema di conservazione e sottoscritta con firma elettronica. Viene resa disponibile al produttore del PDV in una destinazione nota e condivisa con il sistema di conservazione.

Per ogni servizio di conservazione, la RDC si riferisce ai pacchetti di archiviazione ed ai documenti conservati in una certa data e riporta per ogni documento la data di conservazione.

Il RDC è un'evidenza informatica, ovvero un file, che descrive l'esito conservazione e comunica le relative date di conservazione dei documenti che ne fanno parte attraverso l'uso di metadati. È in formato XML.

Torna al sommario

8.12 IL SISTEMA DELLE DELEGHE

Le deleghe alla firma dei PDA sono generate tramite un processo automatico in base alle competenze attribuite tramite il sistema di autenticazione e autorizzazione utilizzato dal sistema di conservazione. Sono prodotte in formato XML e contengono le informazioni relative alla gerarchia dei deleganti/delegati nell'ambito delle risorse assegnate per i documenti afferenti a ciascun servizio di conservazione.

La delega è firmata dal sistema di conservazione con firma elettronica tramite un certificato elettronico, rilasciato al sistema di conservazione stesso, ed emesso dalla CA interna di Sogei, ad essa intestata.

La delega firmata e i suoi attributi sono memorizzati su W.O.R.M.

Le deleghe non vengono mai cancellate.

Qualora il responsabile dei sistemi informativi per la conservazione decida di revocare le autorizzazioni di firma, l'aggiornamento è tracciato nella base informativa e riportato su W.O.R.M.

In caso di modifica delle autorizzazioni alla firma, ovvero nel caso in cui l'ambito di applicazione sia variato, è generata una nuova versione della delega in sostituzione della precedente.

Analogamente una nuova versione della delega è creata al variare della gerarchia delle responsabilità tracciate nella delega stessa.

Il sistema mantiene memoria, per ogni servizio di conservazione, delle variazioni nel tempo della catena di responsabilità.

Torna al sommario

9. IL SISTEMA DI CONSERVAZIONE

Di seguito sono descritte le componenti del sistema di conservazione.

9.1 COMPONENTI LOGICHE

Di seguito è riportata la descrizione delle componenti logiche del sistema di conservazione rappresentata schematicamente nella figura seguente.

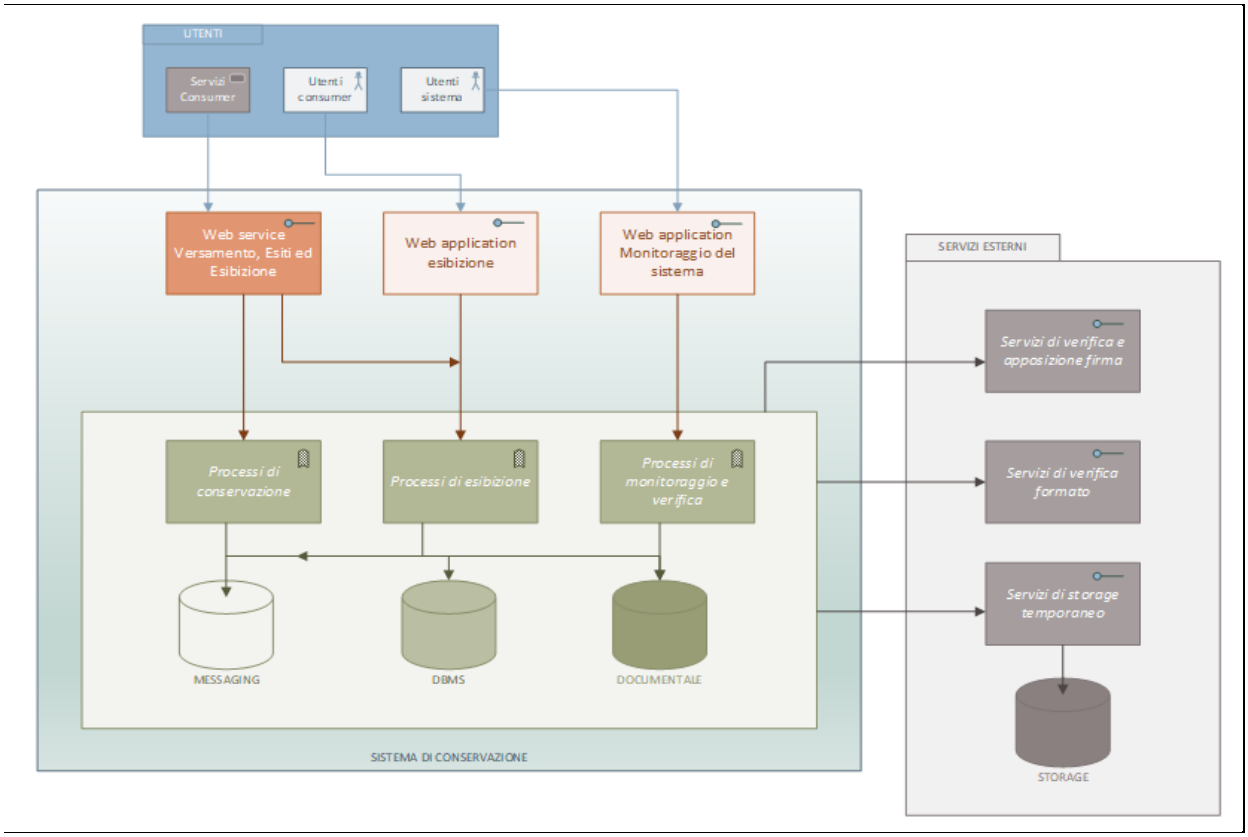

Figura 6 - Componenti logiche

- Utenti: gli utenti del sistema di conservazione sono rappresentati da:
  - I consumer ovvero le applicazioni del sistema informativo che producono e inviano in conservazione i documenti;
  - i responsabili della conservazione o loro delegati che possono richiedere l'esibizione dei documenti del loro ambito di pertinenza;
  - gli utenti che governano e monitorano il sistema tramite specifiche funzionalità per il monitoraggio.
- Interfacce: sono i punti di accesso e colloquio degli utenti con il sistema e sono esposti sia come servizi web sia come applicazioni web; sono a disposizione dei consumer applicativi appositi servizi web per richiedere il versamento e gli esiti di conservazione ed appositi servizi per le richieste di esibizione, quest'ultima può essere richiesta anche tramite applicazione web, solo per utenti autorizzati. Un'ulteriore applicazione web è a disposizione degli utenti che si occupano del monitoraggio del sistema.
- Processi di conservazione: sono i processi di back-end del sistema di conservazione che realizzano tutte le funzionalità del processo di conservazione. Supportano

anche il processo di generazione delle deleghe alla firma dei pacchetti di archiviazione.

- Processi di esibizione: sono i processi di backend del sistema di conservazione che realizzano i Pacchetti di distribuzione.
- Processi di monitoraggio e verifica: sono i processi di backend del sistema di conservazione che verificano e monitorano costantemente l'esecuzione del processo di conservazione emettendo opportune segnalazioni. in caso di condizioni di allerta.
- Messaging: sono i servizi che gestiscono le code di lavoro dei processi di backend.
- DBMS e Documentale: sono i database che manutengono i dati a servizio del processo di conservazione e gli storage su cui vengono conservati i documenti e i file previsti dal processo di conservazione.
- Servizi di verifica formato: sono i servizi esterni al sistema di conservazione disponibili nell'ambito del sistema informativo che permettono la verifica del formato dei documenti da conservare per garantire la coerenza con i formati previsti dalla normativa.
- Servizi di verifica e apposizione firma: sono servizi esterni al sistema di conservazione disponibili nell'ambito del sistema informativo che permettono l'apposizione della firma digitale ove previsto e la verifica della firma e del certificato di firma dei documenti da conservare per garantire le caratteristiche di integrità ed autenticità.
- Servizi di Storage temporaneo: sono i servizi asserviti alla memorizzazione temporanea dei documenti e dei file previsti dal processo ai fini della condivisione tra le varie componenti applicative.
- Servizi di autorizzazione: sono i servizi che verificano le autorizzazioni degli utenti.

Torna al sommario

9.2 COMPONENTI TECNOLOGICHE

Di seguito è riportata la descrizione dell'architettura tecnica del sistema di conservazione rappresentata schematicamente nella figura seguente.

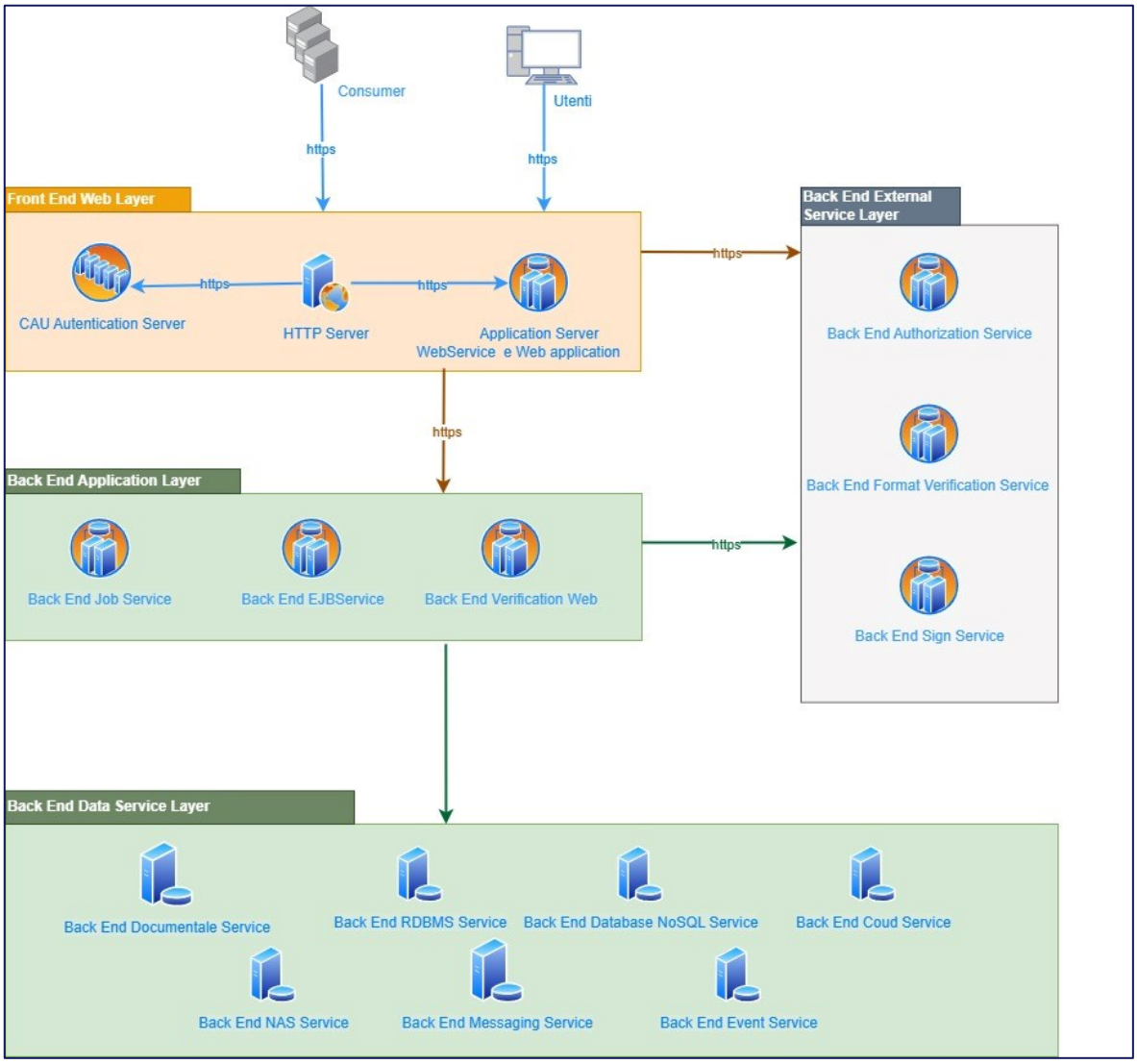

Figura 7 - Componenti tecnologiche

Di seguito sono definiti i layer architetturali che partecipano al disegno complessivo del sistema di conservazione.

- Front End Web Layer: fornisce le risorse che espongono i Web Service e le interfacce web a disposizione dei consumer e degli utenti. Tutte le risorse sono protette tramite sicurezza infrastrutturale e l'autenticazione e autorizzazione dei consumer e degli utenti è realizzata mediante il sistema di controllo accessi (CAU).
- Back End Application Layer: fornisce le risorse per i seguenti servizi:

- Back End Job Service: fornisce le risorse che realizzano i job asincroni dei processi di conservazione, di esibizione e del monitoraggio.
- Back End EJB Service: fornisce le risorse che realizzano i controlli asincroni, disaccoppiati nelle varie fasi del flusso.
- Back End Verification Web Service: fornisce le risorse di tipo Web Service call back per le operazioni di verifica del formato dei file e della firma digitale.

– Back End External Service Layer: fornisce le risorse per i seguenti servizi:
  - Back End Authorization Service: fornisce le risorse per la verifica delle autorizzazioni utenti.
  - Back End Format Verification Service: fornisce le risorse per la verifica dei formati.
  - Back End Sign Service: fornisce le risorse per la verifica della firma digitale CADES, XADES e PADES e l'apposizione di firma (ed eventuale marca temporale) in modalità HSM.

– Back End Data Service Layer: fornisce i servizi dati RDMS, Storage e Storage WORM:
  - Back End Documentale Service: fornisce la risorsa servizi documentali, storage NFS (Network FileSystem) SAN (Storage Area Network) e lo storage WORM (Write Once, Read Many).
  - Back End RDBMS Service: fornisce la risorsa Relational Database Management System (RDBMS).
  - Back End Database NoSQL Service: fornisce la risorsa Database No Sequel
  - Back End Cloud Storage Layer: fornisce la risorsa Cloud.
  - Back End NAS Service: fornisce la risorsa storage per operazioni di servizio
  - Back End Messaging Service: fornisce I servizi per la gestione dei flussi asincroni
  - Back End Event Service: fornisce I servizi per la gestione dei flussi ad eventi

Torna al sommario

9.3 COMPONENTI FISICHE

L'infrastruttura del Sistema di Conservazione dei documenti è realizzata sulla rete interna Sogei.

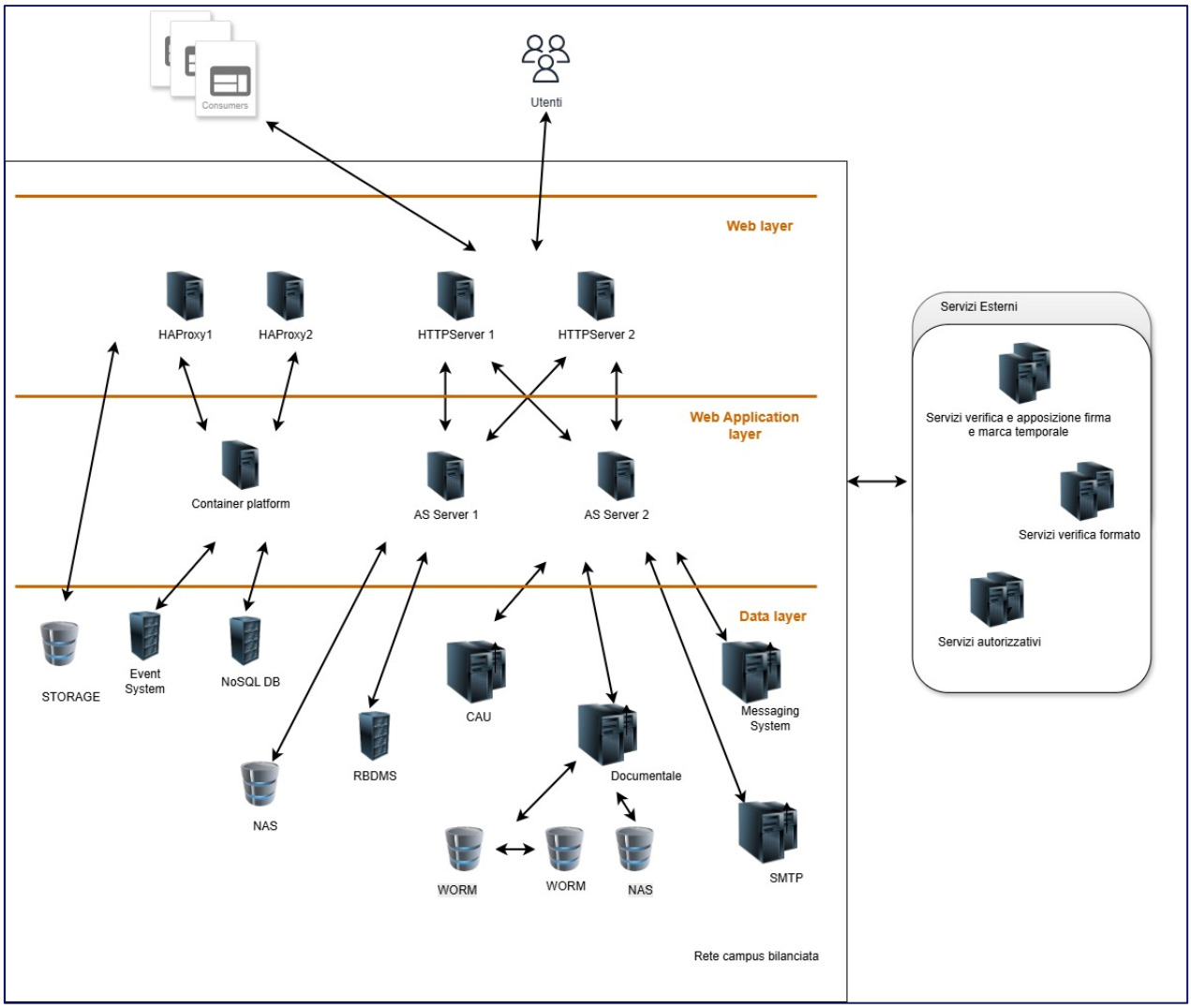

Figura 8 - Componenti fisiche

Il sistema presenta un'infrastruttura server basata su un'architettura di sistema a tre livelli

- Web layer: basato su Web Server in rete bilanciata.

- WebApplication Layer: layer di runtime che ospita le componenti applicative (i servizi web per l'acquisizione dei documenti e le applicazioni web previste per il sistema di conservazione quali esibizione, configurazione, gestione) ed i processi di backend (moduli applicativi, per gestire tutte le attività di tipo schedulato previste dal sistema di conservazione).
- Data Layer: Il sistema interagisce con i seguenti sistemi:
  - Storage: componente utilizzato come storage temporaneo per lo scambio di documenti tra applicazioni e servizi.
  - Event System: sistema di gestione degli eventi per l'esecuzione dei processi di conservazione
  - NO SQL DB: assicura la persistenza di dati applicativi a supporto del sistema di conservazione
  - NAS: storage di appoggio per le operazioni di compressione
  - RDBMS: assicura la persistenza di dati applicativi a supporto del sistema di conservazione
  - CAU: sistema di controllo accessi, per la gestione degli utenti del sistema di conservazione;
  - Documentale: piattaforma documentale che utilizza storage WORM e NAS
  - SMTP: sistema di posta elettronica aziendale acceduto tramite protocollo smtp, per la gestione degli allarmi o eventi generati dai vari componenti del sistema di conservazione.
  - Messaging system: sistema di gestione delle code che consente l'elaborazione dei documenti prevista dal processo di conservazione in modalità asincrona e parallela
- Servizi Esterni: I servizi esterni richiamati dal sistema sono i seguenti:
  - IAM – Servizi di autorizzazione per il controllo accessi degli utenti del sistema di conservazione
  - Verifica ed Apposizione Firma: servizi per la verifica della firma dei documenti e l'apposizione della firma digitale (ed eventuale marca temporale) sui pacchetti di archiviazione e distribuzione.
  - Verifica Formato: Servizi di controllo formato aziendali. I servizi sono utilizzati dal processo di acquisizione per la verifica della rispondenza del documento al formato di file dichiarato

Il Sistema di Conservazione dei documenti alimenta due tipologie di archivi:

- Il primo memorizza i metadati dei documenti, tra cui l'identificativo, fondamentale per il recupero;
- Il secondo memorizza il formato digitale dei documenti inviati in conservazione.

Entrambi i tipi di archivi sono posti in sicurezza presso il Centro di Elaborazione Dati della Sogei; i corrispondenti contenuti sono automaticamente replicati su analoghe apparecchiature installate presso il sito esterno deputato al Disaster Recovery.

Torna al sommario

9.4 PROCEDURE DI GESTIONE E DI EVOLUZIONE

Tra le attività previste per la predisposizione del servizio di conservazione vengono effettuati i controlli miranti a verificare che siano state rispettate le specifiche definite e che il sistema di conservazione sia disponibile all'uso.

La verifica viene effettuata sotto la supervisione dal Responsabile del servizio di conservazione e da tutte le componenti organizzative appartenenti alla Sogei S.p.A. in base alle competenze specifiche.

I controlli consistono nella verifica:

- del software necessario all'erogazione del servizio in un ambiente di validazione funzionalmente analogo a quello di esercizio;
- della corretta esecuzione della configurazione dei singoli sistemi, secondo quanto riportato nell'apposita documentazione aziendale;
- della corretta apposizione delle firme digitali e delle marche temporali;
- della rispondenza del sistema di conservazione ai requisiti del sistema di gestione della sicurezza delle informazioni;
- dei test di funzionamento del sistema di Disaster Recovery esteso, per il quale in particolare si controlla la copertura della funzionalità di esibizione dei documenti conservati.

Il Responsabile della Sicurezza dei sistemi per la conservazione e il Responsabile dei sistemi informativi per la conservazione vengono informati dei risultati dell'attività.

Torna al sommario

9.5 RIVERSAMENTO DIGITALE

I documenti conservati su supporti W.O.R.M. idonei a garantire la conformità agli originali vengono riprodotti mediante due tipologie di riversamento, diretto e digitale.

Il riversamento diretto consente il trasferimento di uno o più documenti conservati da un supporto di memorizzazione a un altro, senza modificare la rappresentazione informatica. Si tratta della generazione di copie di sicurezza da parte del Responsabile dei sistemi informativi per la conservazione.

Il riversamento digitale viceversa prevede il trasferimento di uno o più documenti conservati da un supporto di memorizzazione a un altro, con la modifica della rappresentazione informatica del contenuto. Si tratta, in questo caso, di un aggiornamento tecnologico dell'archivio informatico, in quanto, ad esempio, non risulta essere più conveniente mantenere nel tempo il formato di rappresentazione digitale dei documenti originariamente conservati.

In relazione alla motivazione per la quale deve essere attuato un riversamento digitale, viene definita e condivisa con il Responsabile della conservazione la strategia da applicare.

Il flusso operativo del riversamento digitale si conclude con l'apposizione, sull'insieme dei documenti o su una evidenza informatica contenente una o più impronte dei documenti, del riferimento temporale e della firma digitale da parte del Responsabile dei sistemi informativi per la conservazione o di suoi delegati.

L'adozione di formati standard, documentati e definiti per la messa in conservazione dei documenti, unitamente all'adozione di un osservatorio Tecnologico in grado di analizzare e prevenire le tendenze evolutive di formati esistenti o emergenti, rappresentano gli elementi caratterizzanti la strategia di approccio al problema del riversamento digitale.

Torna al sommario

9.6 POLITICA PER L'INSERIMENTO DELL'UTENZA E PER IL CONTROLLO DEGLI ACCESSI LOGICI

Di seguito sono descritte le misura di sicurezza logica predisposte per il controllo degli accessi alle applicazioni del sistema di conservazione.

In relazione alla funzionalità per la firma dei pacchetti di archiviazione:

- L’autenticazione è svolta dalla API di sicurezza del Sistema Informativo della Fiscalità e consiste nella verifica delle credenziali sulla directory LDAP del Controllo Accessi Unificato (CAU).
- L’identità dell’utente autenticato viene propagata a Documentum tramite un token proprietario prodotto dall’applicazione.
- L’applicazione prevede diversi profili di autorizzazione, gestiti ed assegnati agli utenti da un sistema centralizzato per la gestione dei profili di autorizzazione.
- L’autorizzazione alla firma dei pacchetti di archiviazione viene effettuata da Documentum, che utilizza l’identità dell’utente contenuta nel token proprietario ed applica le ACL attribuite ai pacchetti di archiviazione in fase di firma.
- La fase di firma digitale dei pacchetti di archiviazione è controllata dal sistema che verifica che per l’utente connesso sia presente una delega valida da parte del Responsabile dei sistemi informativi per la conservazione.
- La riservatezza è assicurata dall’uso delle funzionalità di cifratura del canale di comunicazione messe a disposizione dal protocollo TLS/SSL.
- La sessione di lavoro attivata al momento del login dell'utente è automaticamente interrotta nel caso in cui la sua inattività superi il time-out (30 minuti).

In relazione alla funzionalità di Esibizione:

- L’autenticazione è svolta dalla API di sicurezza del Sistema Informativo della Fiscalità e consiste nella verifica delle credenziali sulla directory LDAP del Controllo Accessi Unificato (CAU).
- L’identità dell’utente autenticato viene propagata a Documentum tramite un token proprietario prodotto dall’applicazione.
- L’autorizzazione all’esibizione dei documenti viene effettuata da Documentum, che utilizza l’identità dell’utente contenuta nel token proprietario ed applica le ACL attribuite al documento in fase di acquisizione.
- La riservatezza è assicurata dall’uso delle funzionalità di cifratura del canale di comunicazione messe a disposizione dal protocollo TLS/SSL.
- L’integrità e l’autenticità dei documenti esibiti sono garantite dalle procedure di estrazione dal supporto di memorizzazione, che verificano la firma digitale apposta sul pacchetto di archiviazione al momento dell’acquisizione.
- La sessione di lavoro attivata al momento del login dell'utente è automaticamente interrotta nel caso in cui la sua inattività superi il time-out (30 minuti).

In relazione alle applicazioni produttori dei documenti:

- L'autenticazione dell'applicazione produttore che richiede la conservazione dei documenti è attuata tramite certificato client e https bilanciato. L'identità specificata nel certificato è utilizzata per individuare la corrispondente applicazione produttore.
- L'autorizzazione all'uso del servizio di ingestion è effettuata applicativamente.
- La riservatezza dei documenti oggetto di acquisizione è assicurata dall'uso delle funzionalità di cifratura del canale di comunicazione messe a disposizione dal protocollo TLS/SSL.
- I documenti ricevuti sono sottoposti a controlli di formato. Inoltre, è verificata la validità della firma digitale apposta sui documenti stessi.

Torna al sommario

10. MONITORAGGIO E CONTROLLI

Di seguito sono descritte le tipologie di monitoraggio previste per il sistema di conservazione in termini qualitativi e quantitativi.

Il flusso di esecuzione di ciascun processo di monitoraggio prevede che siano svolte le seguenti attività da parte delle strutture organizzative del Responsabile del servizio di conservazione ovvero personale opportunamente autorizzato di Sogei S.p.A.:

- configurazione dei parametri di esecuzione, come ad esempio l'intervallo temporale, lo stato dei documenti in fase di elaborazione e la soglia accettabile di permanenza in ciascuno stato;
- specificazione di un indirizzo di posta elettronica presso il quale inviare le segnalazioni sull'esito dell'avvenuta esecuzione del processo.

Torna al sommario

10.1 PROCEDURE DI MONITORAGGIO

Nel capitolo sono descritti gli strumenti di monitoraggio predisposti per il controllo del servizio di conservazione.

10.1.1 MONITORAGGIO FUNZIONALE

Il monitoraggio funzionale è svolto tramite un'applicazione di data warehouse che consente il monitoraggio del processo di conservazione, in base alle fasi principali:

- Ingestion dei documenti;
- Acquisizione dei documenti nel W.O.R.M.;
- Firma dei pacchetti di archiviazione;
- Conservazione dei documenti.

Il monitoraggio funzionale ha l'obiettivo di fornire, per mezzo di statistiche predefinite, un punto di vista sulla situazione corrente (ultimo mese elaborato) e storica (tutto il periodo di tempo della gestione del processo) del fenomeno osservato.

L'applicazione di monitoraggio è accessibile a seguito dell'identificazione dell'utente e, in relazione al profilo, è possibile accedere alle diverse aree di consultazione ed alla reportistica.

Il monitoraggio è disponibile a tutti i Responsabili della conservazione e relativi delegati, al Responsabile del servizio di conservazione e alle strutture organizzative a supporto del Responsabile del servizio di conservazione.

Torna al sommario

10.1.2 MONITORAGGIO OPERATIVO

Il monitoraggio operativo è svolto dal Responsabile dei sistemi informativi per la conservazione e dai Tecnici della conservazione ed ha l'obiettivo di tenere sotto controllo le fasi di assemblaggio nei pacchetti di archiviazione, apposizione della firma digitale e conservazione dei documenti.

Il Responsabile dei sistemi informativi per la conservazione e i Tecnici della conservazione dispongono di un cruscotto riferito allo stato della conservazione che permette di monitorare la fase di archiviazione dei PDA nell'ambito del processo di Conservazione Digitale:

- segnalando tramite colorazioni diverse lo stato dei pacchetti di archiviazione;
- aggiornando le informazioni visualizzate ogni 15 minuti.

La composizione del cruscotto prevede la suddivisione in più parti sia a livello di report statistici, che delle informazioni necessarie al controllo del processo elaborativo, in particolare:

- Classificazione in due item dello stato dei pacchetti di archiviazione relativi alla data corrente, nei diversi stati di lavorazione:
  - pacchetti di archiviazione da firmare;
  - pacchetti di archiviazione firmati;

ciascun item può essere ulteriormente esploso in schermate, contenenti report di dettaglio, relative alla fase selezionata:

- ripartizione Mensile, che può essere esplosa in schermate di dettaglio con suddivisione per mese dei pacchetti di archiviazione firmati e conservati.
- OLA giornaliero e mensile per la verifica continua del livello di raggiungimento degli Operational Level Agreement che esprimono, in valore percentuale, il quantitativo di PDA firmati entro un tempo limite prestabilito rispetto al numero complessivo di PDA da firmare.

Effettuando l'analisi delle informazioni dei report è possibile per l'addetto e per gli utenti interni interessati verificare l'andamento della fase di firma digitale da parte dei tecnici di conservazione.

Parallelamente è previsto nel corso della giornata lavorativa e precisamente ogni tre ore, l'invio di un messaggio di posta elettronica ai Tecnici della conservazione, per segnalare in dettaglio i pacchetti di archiviazione da firmare.

Torna al sommario

10.1.3 MONITORAGGIO DELLO STATO DELLE COMPONENTI INFRASTRUTTURALI

L'infrastruttura del sistema di conservazione è sottoposta ad un sistema di monitoraggio dedicato alle strutture organizzative del Responsabile del servizio di conservazione e a quelle sistemistiche di riferimento con i seguenti obiettivi:

- controllo delle componenti di base come riempimento file system, carico elaborativo, guasti dispositivi HW; tali controlli vengono effettuati utilizzando gli strumenti di monitoraggio, quali Tivoli, Patrol BMC;
- controllo del database gestito attraverso procedure in uso per il monitoraggio dei data server delle applicazioni in esercizio;

- controllo dei flussi applicativi del sistema di conservazione mediante notifiche via mail integrate nei workflow applicativi;
- controllo automatico EMC2 Centera con conseguente invio di opportuni allarmi via mail.

Le attività di conduzione del sistema di Conservazione rientrano nei processi ITIL di Event ed Incident Management certificati, i sistemi sono monitorati attraverso i tool aziendali di monitoraggio base e di APM che alimentano la Service Control Room presidiata H24 365 giorni.

Le misure di sicurezza associate, a protezione di ciascuno degli ambienti ritenuti critici si istanziano nel controllo degli accessi tramite uno strumento che gestisce le utenze amministrative.

Il tracciamento di login e logout è effettuato dalla struttura organizzativa del Responsabile della sicurezza dei sistemi per la conservazione.

Torna al sommario

10.2 VERIFICA DELL'INTEGRITÀ DEGLI ARCHIVI

Il sistema di conservazione per la verifica periodica degli archivi prevede le tipologie di verifica seguenti.

- Calcolo dell'impronta e confronto con l'ultima memorizzata.
- Verifica della firma e della marca temporale.
- Verifica del formato.

Ciascuna delle tipologie di verifica è effettuata da un apposito componente di sistema che effettua la verifica secondo i seguenti criteri:

- Il periodo, dalla data alla data.
- Il servizio di conservazione.
- Il formato del documento.
- Il tipo documento / classe documentale.

L'esecuzione delle verifiche è registrata nell'archivio delle verifiche periodiche del sistema di conservazione con il relativo esito.

Torna al sommario

10.2.1 AMBITO DEL PROCESSO DI VERIFICA

Le attività di verifica di integrità e di leggibilità degli archivi vengono ricondotte alle attività di verifica di integrità e di leggibilità degli elementi componenti dello stesso.

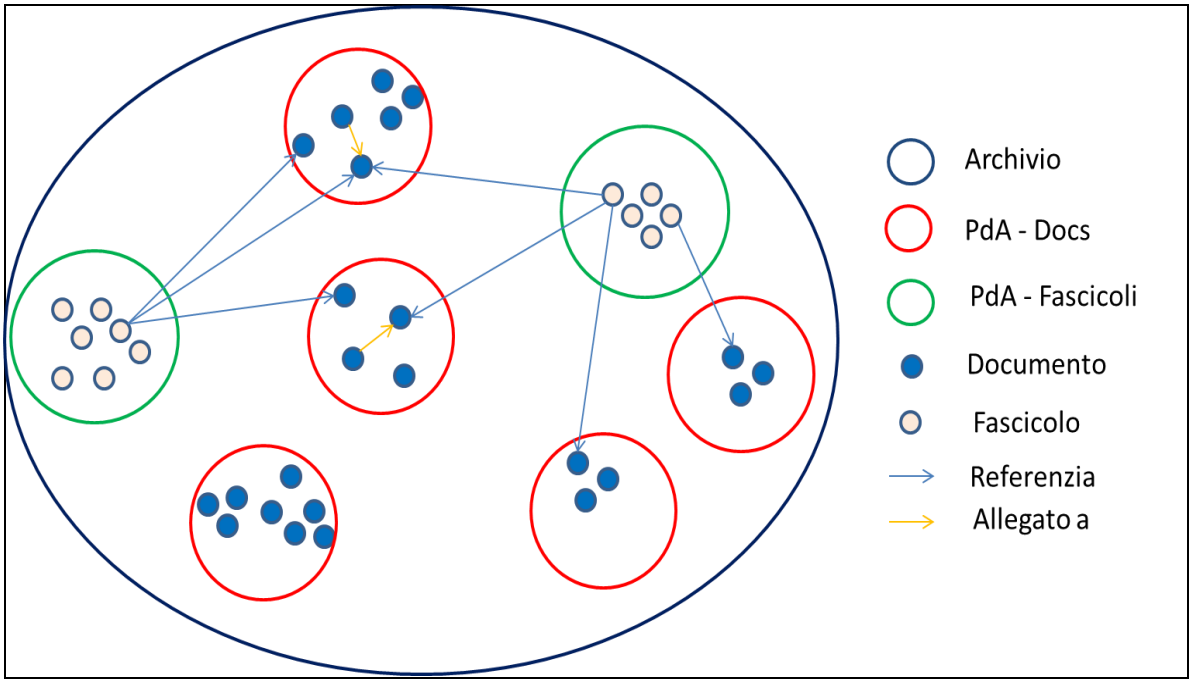

Figura 9 - I componenti dell'archivio

La verifica dell'integrità degli archivi è effettuata a partire dall'unità minima archivistica di conservazione rappresentata dal pacchetto di archiviazione.

Per ogni pacchetto di archiviazione la verifica è effettuata in modalità ricorsiva su tutti gli elementi da esso referenziati, in particolare la verifica di un documento / fascicolo contenuto in un pacchetto di archiviazione è fondata:

- sulla verifica di integrità e di leggibilità del pacchetto di archiviazione in quanto esso stesso è un elemento conservato
- dalla navigabilità delle sue associazioni con gli altri oggetti che vengono esplicitate nell'indice IPdA in cui esso è contenuto.

Il processo di verifica dell'intero archivio di conservazione è garantito dalla verifica puntuale dei singoli pacchetti di archiviazione.

Secondo la tempistica prevista ed entro cinque anni di permanenza dei documenti nel sistema di conservazione è avviata la verifica dell'archivio procedendo sull'intero archivio o su un campione di documenti, a seconda delle situazioni, composto da:

- n casi riferiti a tutte le tipologie documentali;
- n casi riferiti a tutti i formati di conservazione;
- n casi riferiti a tutte le tipologie di firma ammesse.

La verifica è ripetuta per ciascun servizio di conservazione.

Il processo di verifica dell'integrità degli archivi è monitorato e tracciato durante la sua esecuzione.

Torna al sommario

10.2.2 FASI DEL PROCESSO DI VERIFICA

Il processo di verifica dell'integrità degli archivi prevede le fasi seguenti.

- Verifica del pacchetto di archiviazione:
  - Recupero del contenuto del IPdA dal dispositivo W.O.R.M.
  - Validazione della firma digitale e della marca temporale (ove presente).
  - Verifica della presenza nel repository documentale degli oggetti che vengono esplicitati nell'indice IPdA.

Se uno dei controlli ha esito negativo per il pacchetto di archiviazione è segnalata una anomalia ed il processo di verifica si conclude.

Se non sono presenti anomalie il processo di verifica procede.

- Verifica dei contenuti del pacchetto di archiviazione, per ciascun elemento:
  - Recupero del contenuto documento.
  - Validazione della firma e del certificato rispetto alla data di firma.
  - Validazione della marca temporale (ove presente).
  - Calcolo dell'hash e confronto con il valore presente nel IPdA.
  - Verifica del percorso su W.O.R.M tramite confronto tra il valore presente nel IPdA e il percorso effettivo dell'oggetto nel dispositivo di storage.

- Verifica della presenza su W.O.R.M dei documenti dichiarati nell'indice nel IPdA come elementi di fascicolo (per i soli pacchetti di archiviazione di fascicoli).
- Verifica del formato del documento. Se uno dei controlli ha esito negativo per il documento è segnalata una anomalia ed il processo procede per il documento successivo, fino a che tutti i documenti relativi al pacchetto di archiviazione sono stati verificati.

L'esito finale della verifica è registrato nell'archivio delle verifiche periodiche per ciascun pacchetto di archiviazione e per ciascun documento.

Torna al sommario

10.3 SOLUZIONI ADOTTATE IN CASO DI ANOMALIE

Le anomalie che possono manifestarsi nel corso dell'esecuzione del processo di conservazione sono classificabili in macro-tipologie, per ciascuna delle quali sono effettuate azioni specifiche.

AMBITO	ANOMALIA	AZIONE	RESPONSABILE
Oggetti conservati	Documenti non conservabili	Verifica con il produttore ed eventuale rifiuto dal sistema di conservazione	Responsabile del servizio di conservazione
Oggetti conservati	Documenti non leggibili	Verifica con il produttore e il Responsabile della conservazione. Definizione del processo di recupero e conservazione.	Responsabile del servizio di conservazione
Sistemi / infrastruttura	Indisponibilità / malfunzionamenti di sistema	Verifica interna	Responsabile dei Sistemi Informativi
Software del sistema di conservazione	Errori del software di conservazione / esibizione	Attivazione di correttiva secondo le procedure aziendali	Responsabile del servizio di conservazione
Livelli di servizio	Mancato rispetto dei livelli di servizio definiti	In dipendenza della problematica	Responsabile del servizio di conservazione

Sicurezza logica	Incidente di sicurezza (malware, accesso ai dati non autorizzato, …)	Gestione dell'incidente, adozione di contromisure e ripristino dei sistemi	Responsabile dei Sistemi Informativi

Torna al sommario