

MANUALE DI CONSERVAZIONE DI SOGEI S.P.A.

EMISSIONE DEL DOCUMENTO.

Azione	Nominativo	Funzione	Data
<i>Redazione:</i>	F. Quai	SOT.ADE	12/09/2017
<i>Verifica:</i>	S.A. Ocone	SOT.ADE Responsabile	18/09/2017
<i>Approvazione:</i>	M. Magnarelli	SOT Responsabile	18/09/2017

REGISTRO DELLE VERSIONI.

Versione	Data approvazione	Descrizione
1.0	04 febbraio 2014	Manuale della conservazione sostitutiva Avvio del servizio di conservazione delle fatture Sogei del ciclo attivo
1.1	10 luglio 2014	Adeguamento ai sensi del decreto: <i>MINISTERO DELL'ECONOMIA E DELLE FINANZE</i> <i>DECRETO 17 giugno 2014</i> <i>Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005. (14A04778) (GU n.146 del 26-6-2014).</i>

Versione	Data approvazione	Descrizione
		Nomina nuovo responsabile della conservazione (<i>Comunicazione Organizzativa 8 luglio 2014</i>). Modifica frequenza assemblaggio pacchetti di archiviazione. Inserimento annotazioni. Storico responsabili della conservazione.
1.2	17 ottobre 2014	Revisione architetture del sistema di conservazione
1.3	23 marzo 2015	Estensione del servizio di conservazione Fatture Sogei alle fatture del ciclo passivo
1.4	11 maggio 2015	Estensione del servizio di conservazione ai documenti prodotti dal Sistema di Posta Elettronica Certificata
1.5	9 novembre 2015	Modifiche formali per la pubblicazione sulla Intranet aziendale
1.6	16 novembre 2015	Estensione del servizio di conservazione ai Registri giornalieri di protocollo
1.7	28 dicembre 2015	Estensione del servizio di conservazione ai Documenti contabili – Libro giornale
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.

INDICE

1. SCOPO E AMBITO DEL DOCUMENTO	6
2. TERMINOLOGIA (GLOSSARIO E ACRONIMI)	7
3. NORMATIVA E STANDARD DI RIFERIMENTO	11
3.1 NORMATIVA DI RIFERIMENTO	11
3.2 STANDARD DI RIFERIMENTO	12
4. RUOLI E RESPONSABILITÀ	13
4.1 RUOLI E RESPONSABILITÀ DEL CLIENTE	13
4.2 RUOLI E RESPONSABILITÀ DI SOGEI S.P.A.	15
5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE	21
5.1 ORGANIGRAMMA	21
5.2 STRUTTURE ORGANIZZATIVE	22
5.3 OSSERVATORIO DEI FORMATI	22
6. OGGETTI SOTTOPOSTI A CONSERVAZIONE	24
6.1 OGGETTI CONSERVATI	24
6.2 PACCHETTO DI VERSAMENTO	25
6.3 PACCHETTO DI ARCHIVIAZIONE	27
6.4 PACCHETTO DI DISTRIBUZIONE	29
6.5 DELEGA ALLA FIRMA DEI PDA	31
7. IL PROCESSO DI CONSERVAZIONE	32

7.1	MODALITÀ DI ACQUISIZIONE DEI PACCHETTI DI VERSAMENTO PER LA LORO PRESA IN CARICO	33
7.2	VERIFICHE EFFETTUATE SUI PACCHETTI DI VERSAMENTO E SUGLI OGGETTI IN ESSI CONTENUTI	34
7.3	ACCETTAZIONE DEI PACCHETTI DI VERSAMENTO E GENERAZIONE DEL RAPPORTO DI VERSAMENTO DI PRESA IN CARICO	36
7.4	RIFIUTO DEI PACCHETTI DI VERSAMENTO E MODALITÀ DI COMUNICAZIONE DELLE ANOMALIE	37
7.5	PREPARAZIONE E GESTIONE DEL PACCHETTO DI ARCHIVIAZIONE	38
7.6	PREPARAZIONE E GESTIONE DEL PACCHETTO DI DISTRIBUZIONE AI FINI DELL'ESIBIZIONE	39
7.7	PRODUZIONE DI DUPLICATI E COPIE INFORMATICHE E DESCRIZIONE DELL'EVENTUALE INTERVENTO DEL PUBBLICO UFFICIALE NEI CASI PREVISTI	40
7.8	SCARTO DEI PACCHETTI DI ARCHIVIAZIONE	41
7.9	PREDISPOSIZIONE DI MISURE A GARANZIA DELL'INTEROPERABILITÀ E TRASFERIBILITÀ AD ALTRI CONSERVATORI	42
7.10	CONFIGURAZIONE DEI SERVIZI DI CONSERVAZIONE	42
7.11	LE RICEVUTE DEL SISTEMA DI CONSERVAZIONE	43
7.11.1	Ricevuta di presa in carico	43
7.11.2	Ricevuta di errore nella presa in carico	44
7.11.3	Rapporto di versamento	45
7.11.4	Rapporto di conservazione	46
7.12	IL SISTEMA DELLE DELEGHE	47
8.	IL SISTEMA DI CONSERVAZIONE	48
8.1	COMPONENTI LOGICHE	48
8.2	COMPONENTI TECNOLOGICHE	50
8.3	COMPONENTI FISICHE	53
8.4	PROCEDURE DI GESTIONE E DI EVOLUZIONE	56

8.5	RIVERSAMENTO DIGITALE	57
8.6	POLITICA PER L'INSERIMENTO DELL'UTENZA E PER IL CONTROLLO DEGLI ACCESSI LOGICI	58
9.	MONITORAGGIO E CONTROLLI	59
9.1	PROCEDURE DI MONITORAGGIO	60
9.1.1	Monitoraggio funzionale	60
9.1.2	Monitoraggio operativo	60
9.1.3	Monitoraggio dello stato delle componenti infrastrutturali	62
9.2	VERIFICA DELL'INTEGRITÀ DEGLI ARCHIVI	63
9.2.1	Ambito del processo di verifica	63
9.2.2	Fasi del processo di verifica	65
9.3	SOLUZIONI ADOTTATE IN CASO DI ANOMALIE	66

1. 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 mira a garantire le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità dei documenti informatici, definiti come "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti" (CAD art.44).

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 dei documenti informatici 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](#)

2. TERMINOLOGIA (GLOSSARIO E ACRONIMI)

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
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 e descritto nel manuale di conservazione
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	rappresentazione informatica o in formato analogico di atti, fatti e dati intelligibili direttamente o attraverso un processo di elaborazione elettronica
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), 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 ed 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

Termine	Definizione
	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 e di ottenerne copia
Evidenza informatica	una sequenza di simboli binari (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 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	una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
Impronta	la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash
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

Termine	Definizione
	tempo nel sistema di conservazione
Pacchetto di archiviazione	pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del regole tecniche in materia e secondo le modalità riportate nel manuale di conservazione.
Pacchetto di distribuzione	pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta
Pacchetto di versamento	pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato 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
Produttore	persona fisica o giuridica, 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 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	I registri dei pacchetti di versamento sono strutture documentali in cui sono memorizzati gli estremi dei pacchetti di versamento ed il loro stato durante tutto il processo di conservazione
Riferimento temporale	informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento
Riversamento diretto	processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro, non alterando la loro rappresentazione informatica. Per tale processo non sono previste particolari modalità
W.O.R.M. (write once)	l'acronimo indica la caratteristica di alcuni tipi di supporti (ottici o magnetici) che

Termine	Definizione
<i>read many)</i>	rende i dati registrati su di essi non-modificabili e non- cancellabili, ma solo accessibili in lettura ed in copia

[Torna al sommario](#)

3. NORMATIVA E STANDARD DI RIFERIMENTO

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

3.1 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;
- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis ,41,47,57-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;

- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.

[Torna al sommario](#)

3.2 STANDARD DI RIFERIMENTO

Si riportano di seguito gli standard di riferimento elencati nell'allegato 3 delle Regole Tecniche in materia di Sistema di conservazione con indicazione delle versioni aggiornate al 10 ottobre 2014.

- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- ETSI TR 101 533-2 V1.3.1 (2012-04) Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

[Torna al sommario](#)

4. RUOLI E RESPONSABILITÀ

L'ente o il soggetto diretto interessato è il titolare dei documenti informatici posti in 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 riguardo i Modelli organizzativi della conservazione - art. 5 nella figura del Responsabile del servizio di conservazione.

[Torna al sommario](#)

4.1 RUOLI E RESPONSABILITÀ DEL CLIENTE

Nel caso di Sogei S.p.A. si intende per cliente Sogei stessa, per gli ambiti di applicazione ad essa pertinenti, salvaguardando il modello organizzativo generale della conservazione.

Il Responsabile della Conservazione effettua le seguenti attività:

- definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente;
- gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
- genera il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
- genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
- effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
- assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
- 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;

- provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
- adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12;
- 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;
- assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
- provvede, per gli organi giudiziari e amministrativi dello Stato, al versamento dei documenti conservati all'archivio centrale dello Stato e agli archivi di Stato secondo quanto previsto dalle norme vigenti;
- predispone il manuale di conservazione di cui all'art. 8 e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Il Produttore è la persona fisica o giuridica, responsabile della produzione del pacchetto di versamento e del suo trasferimento al sistema di conservazione. Ove previsto il responsabile della gestione documentale o il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, assicura la trasmissione del contenuto del pacchetto di versamento al sistema di conservazione secondo le modalità operative definite nel manuale di conservazione

Gli Utenti - delegati del Responsabile della conservazione - sono figure che possono effettuare l'esibizione dei documenti nello specifico ambito di delega.

Il Pubblico ufficiale è colui che su richiesta del Responsabile della conservazione espleta le proprie attività, in particolare nella fase di esibizione dei documenti conservati.

[Torna al sommario](#)

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

Responsabile del Servizio di Conservazione

E' 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.

E' il riferimento aziendale per la definizione degli aspetti contrattuali, dei costi del servizio e della qualità del processo di conservazione e risulta, nel contempo, 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) 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 dell'infrastruttura;
- 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 documenti 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 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;
- 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:

- garantisce il rispetto delle vigenti disposizioni in materia di trattamento dei dati personali;
- garantisce che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.

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

- Un Delegato Privacy, con responsabilità di indirizzo e vigilanza
- Responsabili del trattamento identificati nei responsabili di Direzione (responsabili o preposti privacy), con il supporto delle rispettive strutture (coordinatori privacy), con specifico riferimento ai trattamenti di competenza.

Si precisa che per il Modello Organizzativo Sogei relativo alla Privacy si rinvia al documento aziendale noto come "IS-91-PR-04 - Politiche e istruzioni relative all'organizzazione ed alla gestione dei trattamenti di dati personali e degli adempimenti previsti dalla normativa sulla Privacy, D.Lgs. n. 196/2003 – Codice in materia di protezione dei dati personali".

Responsabile della sicurezza dei sistemi per la conservazione

È responsabile della definizione delle politiche di sicurezza che devono essere implementate dalle strutture di competenza per la corretta conservazione, coerentemente con i requisiti stabiliti. Inoltre:

- 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 si avvale, tramite delega, del Responsabile dell'infrastruttura per l'individuazione e la pianificazione delle necessarie azioni correttive.

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, del Responsabile dell'infrastruttura per la pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione e per la progettazione e l'implementazione dell'architettura del Servizio di Conservazione e delle eventuali evoluzioni. Ha infine il compito di:

- archiviare e rendere disponibili, con l'impiego di procedure elaborative, relativamente i pacchetti di archiviazione, le informazioni previste dall'allegato 4 "Standard e specifiche tecniche del pacchetto di archiviazione" della normativa in materia;
- adottare le misure necessarie per la sicurezza fisica e logica del sistema preposto al Servizio di Conservazione e delle copie di sicurezza effettuate;
- verificare periodicamente, con cadenza non superiore a cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti;
- assicurare l'apposizione della firma digitale e del riferimento temporale alla fine di ciascun processo di conservazione;
- assicurare l'organizzazione del contenuto 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

E' la persona che in base alla catena delle deleghe effettua la firma dei pacchetti di archiviazione (PdA).

Responsabile dell'Infrastruttura

Ha il compito di:

- garantire la completa funzionalità dell'architettura anche sotto il profilo della sicurezza adottando quanto definito dal Responsabile della sicurezza dei sistemi per la conservazione
- presidiare l'evoluzione tecnologica e normativa del servizio con particolare riferimento ai formati documentali trattati, all'utilizzo della marca temporale e all'utilizzo della firma digitale, al fine di individuare tempestivamente necessità di adeguamenti alle normative ed alle soluzioni per il processo di riversamento.
- 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, conforme ai requisiti in materia;
- amministratore della piattaforma, che implementa e rende disponibili i servizi "documentali".

Ruolo	Nominativo	Periodo nel ruolo	Eventuali deleghe
<i>Responsabile del servizio di conservazione</i>	M. Magnarelli - Responsabile della struttura SOT - Soluzioni Trasversali	Dal 25/02/2015	Nessuna.
<i>Responsabile della funzione archivistica di conservazione</i>	E. Lisi	Dal 01/09/2017	Nessuna.
<i>Responsabile della sicurezza dei sistemi per la conservazione</i>	F. Lazzini - Responsabile della struttura "Security Governance e Privacy"	Dal 01/06/2011	Responsabile dell'infrastruttura
<i>Responsabile del trattamento dati personali</i>	F. Lazzini - Responsabile della struttura "Sicurezza Informatica e Privacy"	Dal 01/06/2011	Nessuna.
<i>Responsabile dei sistemi informativi per la conservazione</i>	M. Burchietti - Responsabile della struttura "Esercizio e Gestione"	Dal 01/06/2011	- Responsabile dell'infrastruttura - I tecnici di conservazione
<i>Responsabile sviluppo e manutenzione del sistema di conservazione</i>	S. Ocone - Responsabile della struttura "Soluzioni audit, documentale e e-learning"	Dal 08/06/2012	Nessuna.

Ruolo	Nominativo	Periodo nel ruolo	Eventuali deleghe
<i>Responsabile dell'infrastruttura</i>	L. Bargellini - Responsabile della struttura "Infrastrutture Tecnologiche e Innovazione"	Dal 01/06/2011	

[Torna al sommario](#)

5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 ORGANIGRAMMA

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

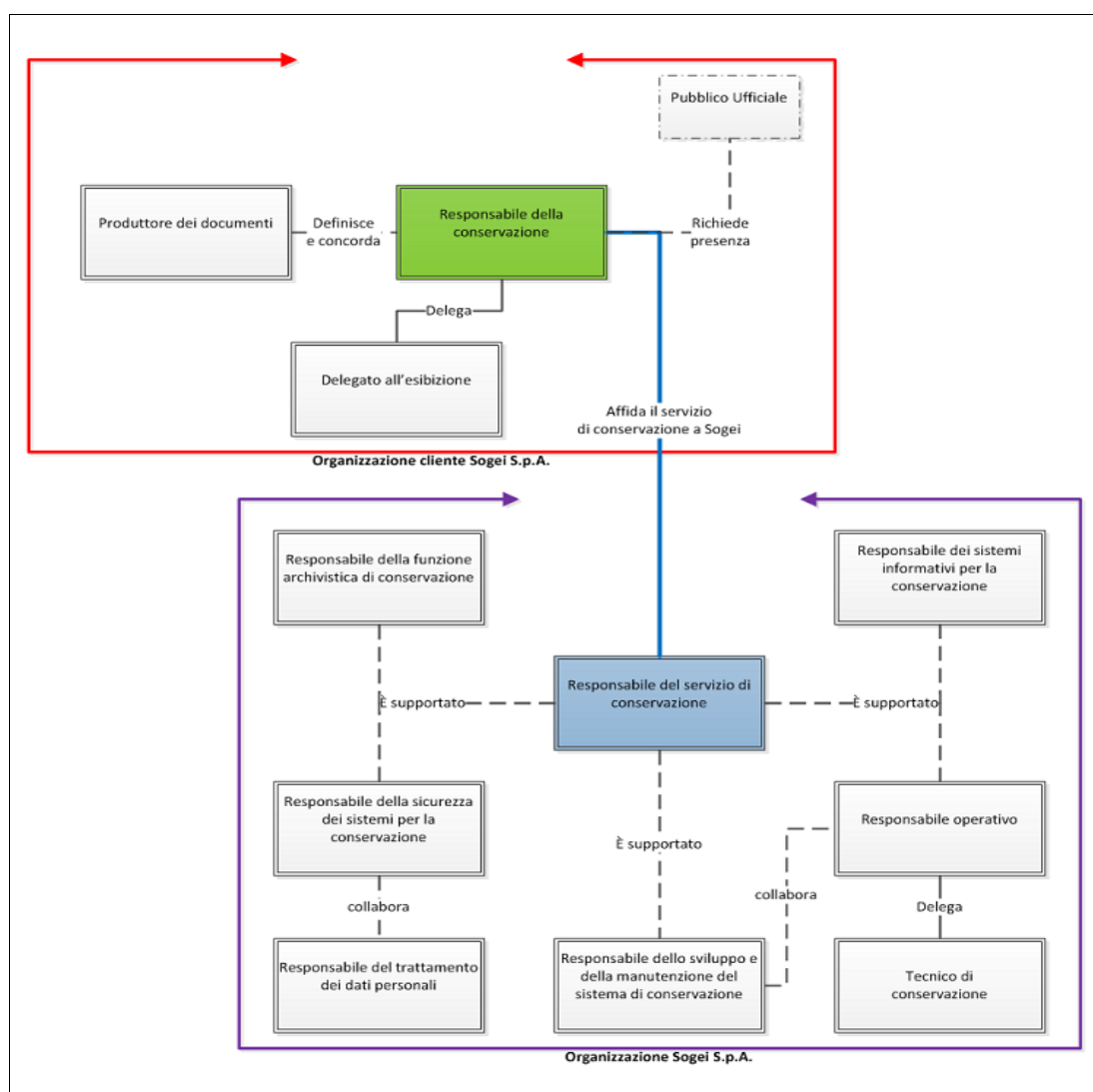


Figura 1 – Organigramma e relazioni tra i responsabili

[Torna al sommario](#)

5.2 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”, 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](#)

5.3 OSSERVATORIO DEI FORMATI

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 di competenza del team di “Change Management” che è una struttura organizzativa virtuale multidisciplinare in materia di formati e tecnologie.

Il team di “Change Management” effettua un monitoraggio periodico sui risultati relativi alla leggibilità dei documenti 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 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](#)

6. OGGETTI SOTTOPOSTI A CONSERVAZIONE

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

6.1 OGGETTI CONSERVATI

Di seguito l'elenco delle tipologie di documenti cui viene applicato il procedimento di conservazione dei documenti:

- Documenti informatici / amministrativi informatici generati all'esterno del Sistema Informativo della Fiscalità e ricevuti tramite i servizi telematici dedicati ai clienti.
- Documenti informatici / amministrativi informatici generati dalle applicazioni del Sistema Informativo della Fiscalità secondo quanto previsto dai flussi dei processi e/o procedimenti automatizzati.

Di tali documenti 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.

Nella tabella seguente sono indicati i formati gestiti dal sistema di conservazione.

CODICE FORMATO	PROGRAMMA	VERSIONE PROGRAMMA	PRODUTTORE	ESTENSIONE	XSD
PDFA-1a e PDFA-1b	ACROBAT READER	6.0	ADOBE	PDF	non previsto
TIF43	IrfanView	4.30	Irfan Skiljan	TIF	non previsto
TIFF43	IrfanView	4.30	Irfan Skiljan	TIFF	non previsto
UTF8	Notepad	qualsiasi	Microsoft	TXT	non previsto
XMLFE10	un EDITOR	DI TESTO	qualsiasi produttore	XML	FatturaP A 1.0
XMLFE11	un EDITOR	DI TESTO	qualsiasi produttore	XML	FatturaP A 1.1

Figura 2 - Elenco dei formati gestiti

[Torna al sommario](#)

6.2 PACCHETTO DI VERSAMENTO

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

Responsabile del contenuto del PDV è il produttore del documento, che deve formarlo, sottoscriverlo con firma digitale (ove previsto) e trasmetterlo al sistema di conservazione secondo le modalità operative definite nel presente Manuale.

Ogni PDV può contenere esclusivamente documenti della stessa tipologia, ovvero della stessa Classe Documentale. In questo senso l'elenco dei metadati dei singoli documenti è 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.

La struttura dell'indice del pacchetto di versamento è di seguito definita.

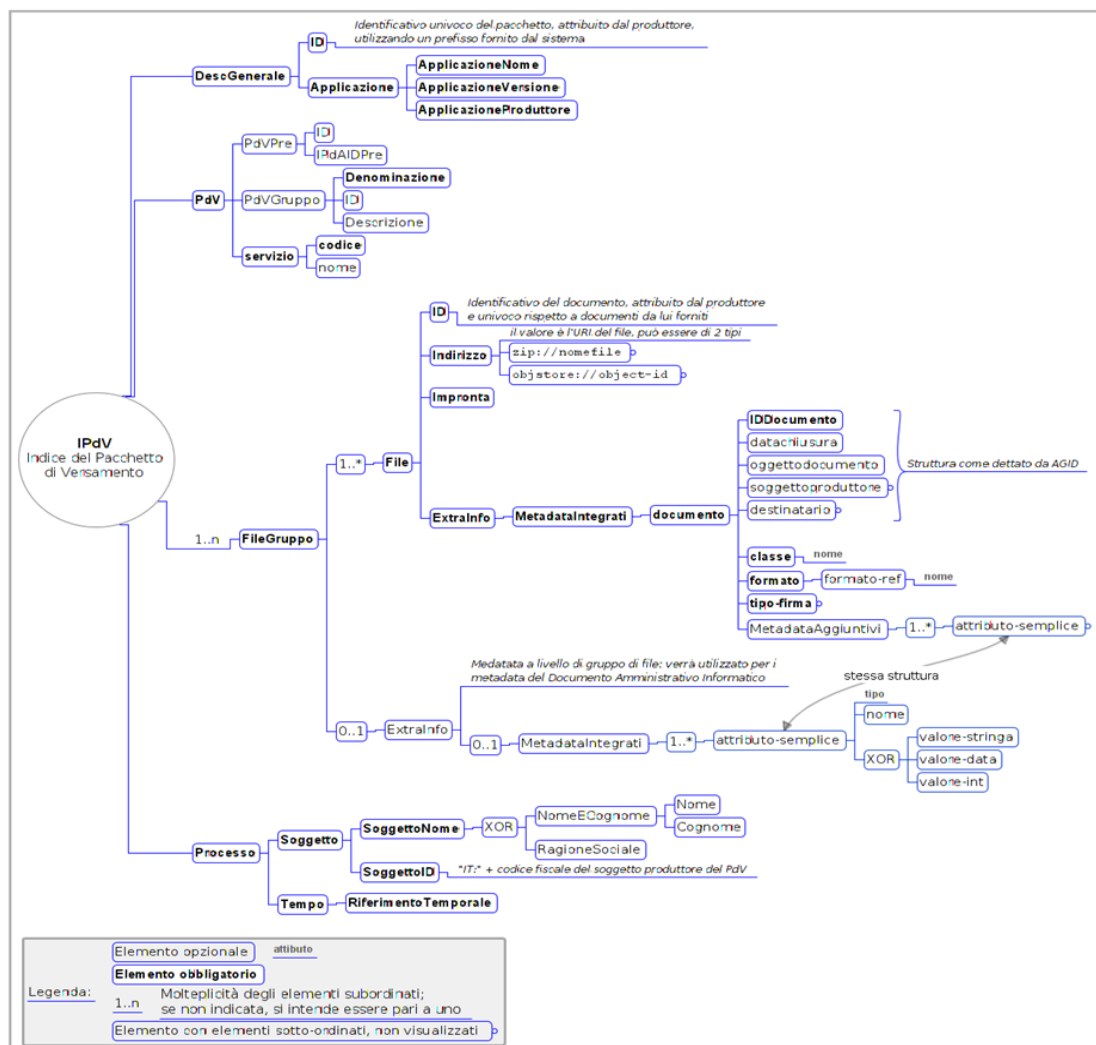


Figura 3 - Struttura IPdV

[Torna al sommario](#)

6.3 PACCHETTO DI ARCHIVIAZIONE

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

La struttura del PDA è costruita sulla base delle specifiche contenute nell'allegato 4 delle regole tecniche in materia e secondo le modalità riportate nel presente documento.

Responsabile del contenuto del PDA è il sistema di conservazione.

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.

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 quella prevista dallo standard SInCRO (UNI 11386) di seguito rappresentato.

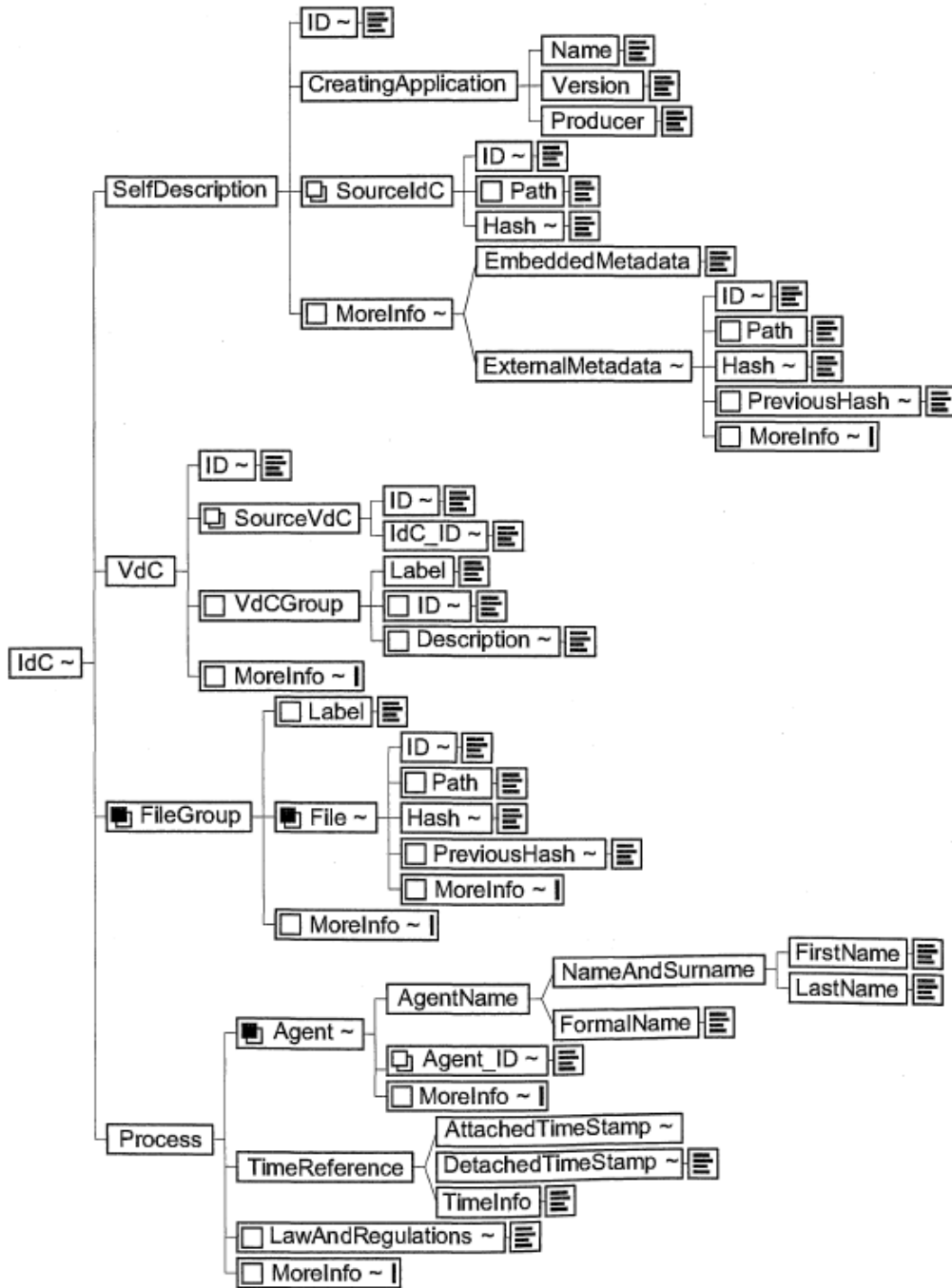


Figura 4 - Struttura IPdA

[Torna al sommario](#)

6.4 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.

Responsabile del contenuto del PDD è il sistema di conservazione a seguito di una richiesta da parte di un 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 elettronica 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.

La struttura dell'indice del pacchetto di distribuzione è di seguito definita.

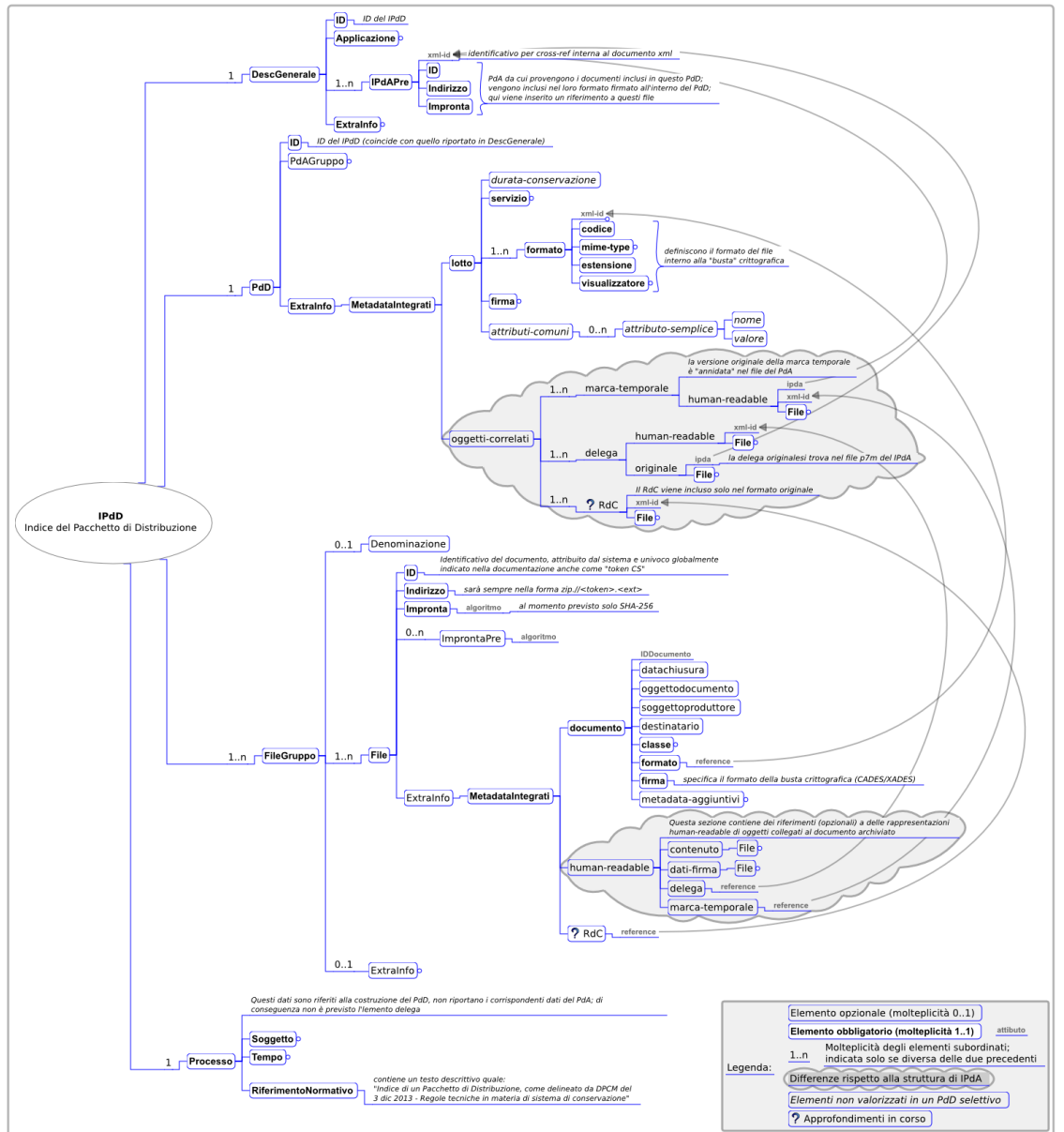


Figura 5 - Struttura IPdD

[Torna al sommario](#)

6.5 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

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:

- 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 la delega univocamente
- versione della delega, corrisponde alla versione della delega in relazione al delegato; la versione varia ogni volta che interviene un aggiornamento nella gerarchia delle deleghe oppure ogni volta che è modificato l'ambito di azione (servizio e/o attributi su cui si è autorizzati a firmare);
- data Versione della delega, corrisponde alla data di creazione della delega ovvero la data di generazione della versione contenuta nel tag Versione 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;
- dati del responsabile dei sistemi informativi per la conservazione, ruolo, denominazione;
- dati del delegante, ruolo nome cognome codice fiscale;
- data di autorizzazione alla firma del delegato, data di generazione della delega;
- 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](#)

7. IL PROCESSO DI CONSERVAZIONE

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



Figura 6 - Il processo di conservazione

- Ingestion dei documenti: rappresenta la fase invio del pacchetto di versamento da parte del produttore e 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. 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 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 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. È l'unica fase manuale del processo di conservazione in cui i Tecnici della conservazione apportano la firma digitale sui pacchetti di archiviazione per attestare il corretto svolgimento del processo di 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, 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 sono svolte le attività del processo di conservazione.

[Torna al sommario](#)

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

L'operazione di versamento consiste nella trasmissione da parte del produttore dei documenti 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 web di ingestione 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:

- IPdV¹, 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](#)

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

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

- Verifica abilitazione del produttore per l'invio del PDV tramite confronto tra l'utenza chiamante e l'utenza definita nel sistema di controllo accessi (par. 8.6) (identificazione certa del produttore).

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

- Confronto tra l'impronta (hash del PDV) dichiarata e quella calcolata dal sistema di conservazione in fase di ingestione.
- 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 in una apposita classe documentale (registro del pacchetto di versamento).

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

- Genera la ricevuta di presa in carico.
- Firma elettronicamente la 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.

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.

- 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 alla data di firma 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](#)

7.3 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 sono 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 sono 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 elettronicamente 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](#)

7.4 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.

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 web di ingestion.

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](#)

7.5 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 saranno generati ogni X giorni e conterranno un numero massimo N di documenti.

I PDA sono numerati progressivamente nel sistema di conservazione.

I PDA sono sottoposti alla firma digitale da parte dei tecnici della conservazione.

Il Responsabile dei Sistemi Informativi per la conservazione ha delegato 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.

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.

Nei casi previsti contestualmente alla firma digitale del PDA è apposta 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.
- Verifica dei dati di firma presenti nella specifica sezione con le deleghe attive al momento della firma.

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.

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](#)

7.6 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 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 devono 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 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.
- Firma elettronicamente il PDD.
- Rende disponibile il PDD nella destinazione nota e condivisa per il recupero da parte del produttore.
- Memorizza il PDD nei propri archivi per un periodo di tempo prestabilito per eventuali riscontri e poi lo rimuove.

[Torna al sommario](#)

7.7 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 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 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 sono disciplinate interamente dalla normativa in materia con riferimento all'articolo 6 del DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 13 novembre 2014. Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23 -bis , 23 -ter , 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

Il sistema documentale in uso presso il Sistema Informativo della Fiscalità implementa una serie di funzionalità per supportare l'utente nella gestione di tale processo.

Nei casi è prevista, il responsabile della conservazione assicura la presenza di un pubblico ufficiale secondo l'Art. 7 delle regole tecniche in materia di conservazione al fine di dichiarare la conformità della copia all'originale conservato.

[Torna al sommario](#)

7.8 SCARTO DEI PACCHETTI DI ARCHIVIAZIONE

Il sistema di conservazione prevede specifiche funzionalità per effettuare lo scarto dei pacchetti di archiviazione in ordine al massimario di scarto.

Le attività di scarto dei documenti dal sistema di conservazione avvengono secondo le norme in materia ed in particolare, nel caso di archivi pubblici o privati di particolare interesse culturale, le procedure di scarto avvengono previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo.

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 produttore dei documenti;
- Effettuazione dello scarto.

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](#)

7.9 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 produttore sono tutti presenti nell'allegato "Formati" delle regole tecniche a garanzia dei principi dell'interoperabilità tra i sistemi di conservazione

I pacchetti di archiviazione sono realizzati secondo i requisiti previsti nell'allegato "Specifiche tecniche del pacchetto di archiviazione", tali specifiche fanno riferimento allo standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010), che è lo standard nazionale 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.

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](#)

7.10 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 dei servizi di conservazione descritte nel documento "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 secondo particolari 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, ed 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](#)

7.11 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 documenti.

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

[Torna al sommario](#)

7.11.1 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.

Responsabile del contenuto della RPC è il sistema di conservazione, che deve formarla, sottoscriverla con firma elettronica.

Ogni RPC si riferisce ad un pacchetto di versamento.

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

La struttura della ricevuta di presa in carico è di seguito definita.

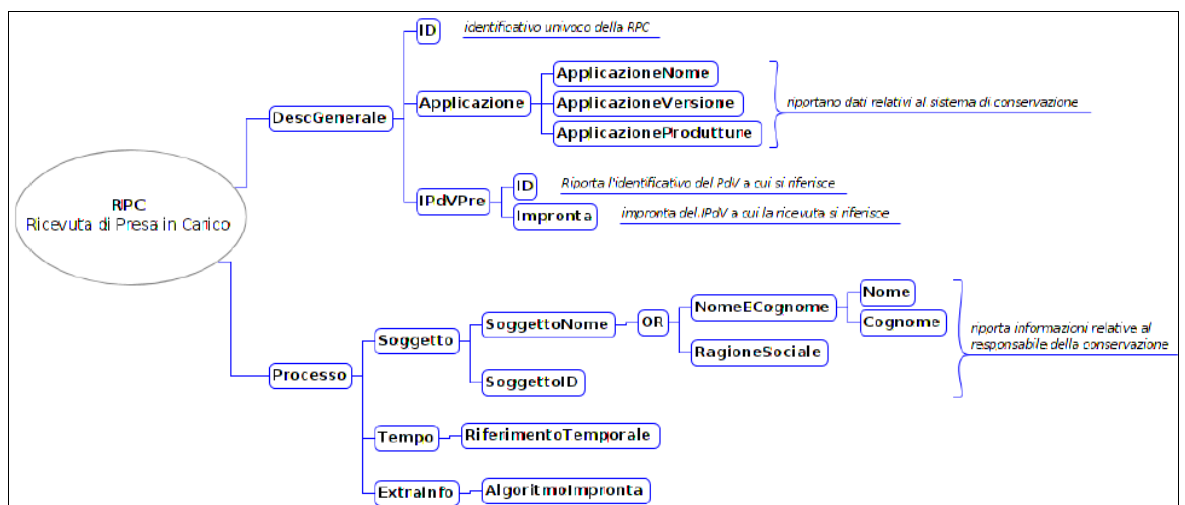


Figura 7 - Ricevuta di presa in carico

7.11.2 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.

Responsabile del contenuto della RPC_E è il sistema di conservazione, che deve formarla, sottoscriverla con firma elettronica.

Ogni RPC_E si riferisce ad un pacchetto di versamento.

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

La struttura della ricevuta di errore nella presa in carico è di seguito definita.

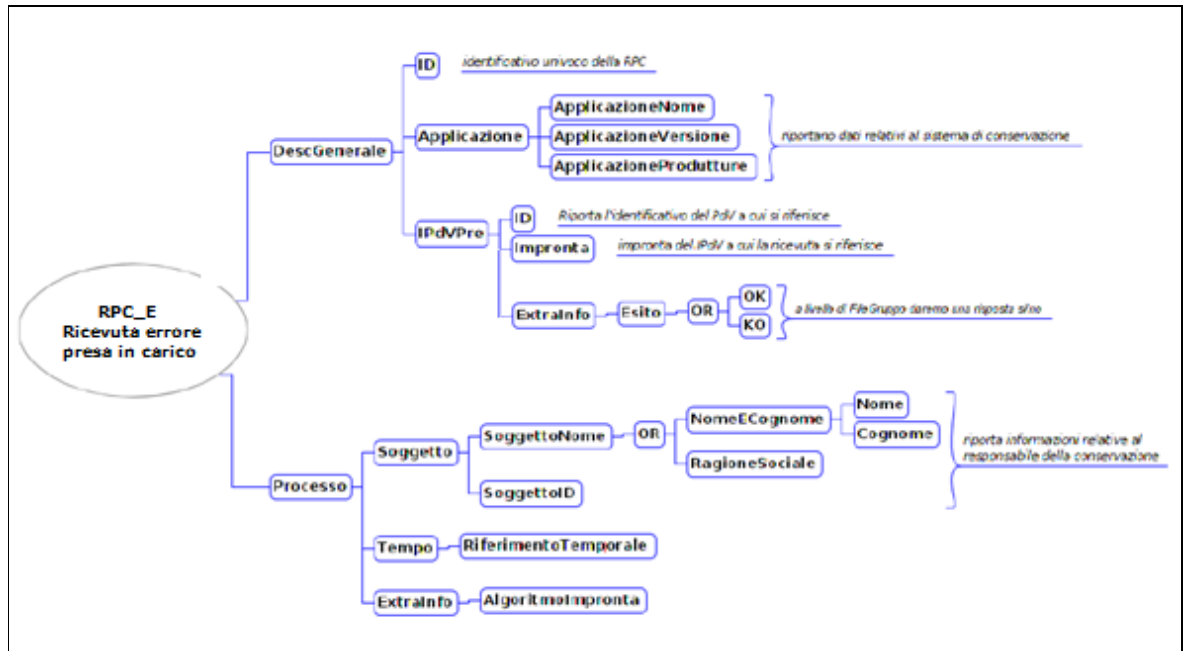


Figura 8 - Ricevuta di errore presa in carico

[Torna al sommario](#)

7.11.3 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 effettuato dal sistema di conservazione sui singoli documenti contenuti in un pacchetto di versamento.

Responsabile del contenuto del RDV è il sistema di conservazione, che deve formarlo, sottoscriverlo con firma elettronica e renderlo disponibile al produttore 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.

La struttura rapporto di versamento è di seguito definita.

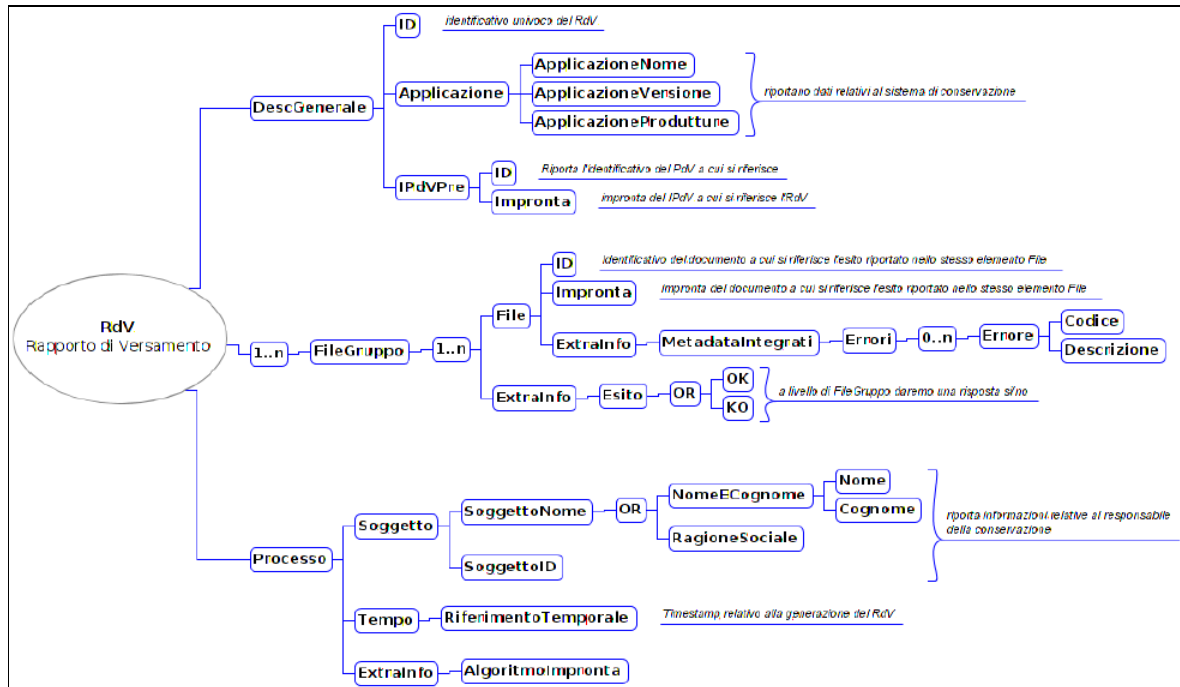


Figura 9 - Rapporto di versamento

[Torna al sommario](#)

7.11.4 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.

Responsabile del contenuto del RDC è il sistema di conservazione, che deve formarlo, sottoscriverlo con firma elettronica e renderlo disponibile al produttore in una destinazione nota e condivisa con il sistema di conservazione.

Ogni 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.

La struttura rapporto di conservazione è di seguito definita.

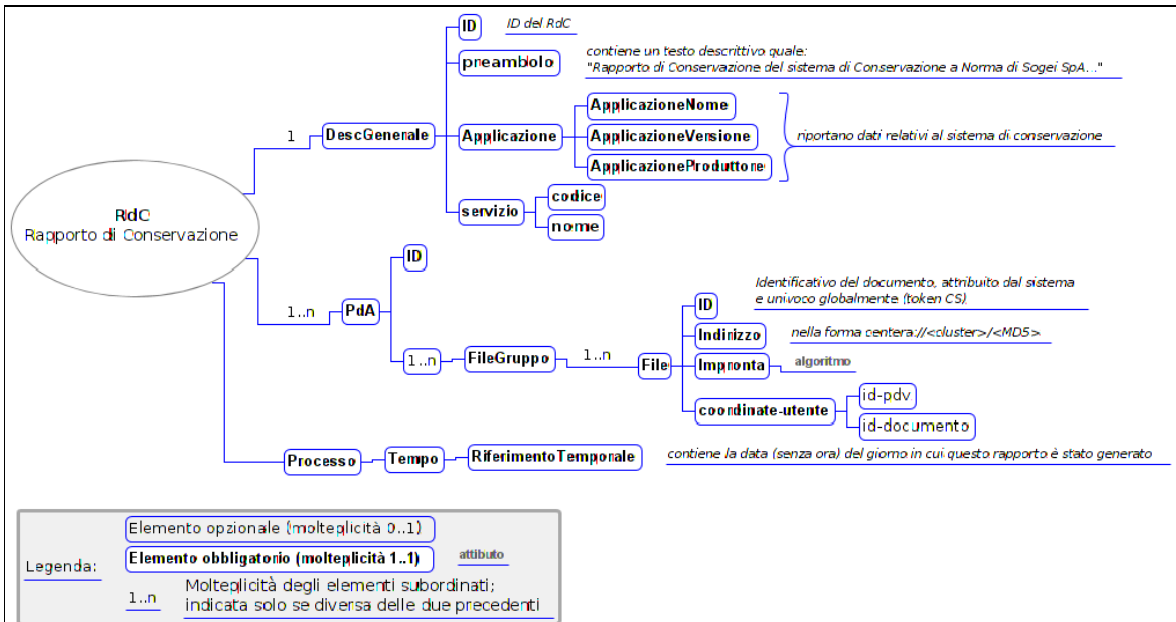


Figura 10 - Reporto di conservazione

[Torna al sommario](#)

7.12 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 con firma elettronica tramite un certificato di servizio emesso dalla CA Sogei.

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](#)

8. IL SISTEMA DI CONSERVAZIONE

Di seguito sono descritte le componenti del sistema di conservazione.

8.1 COMPONENTI LOGICHE

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

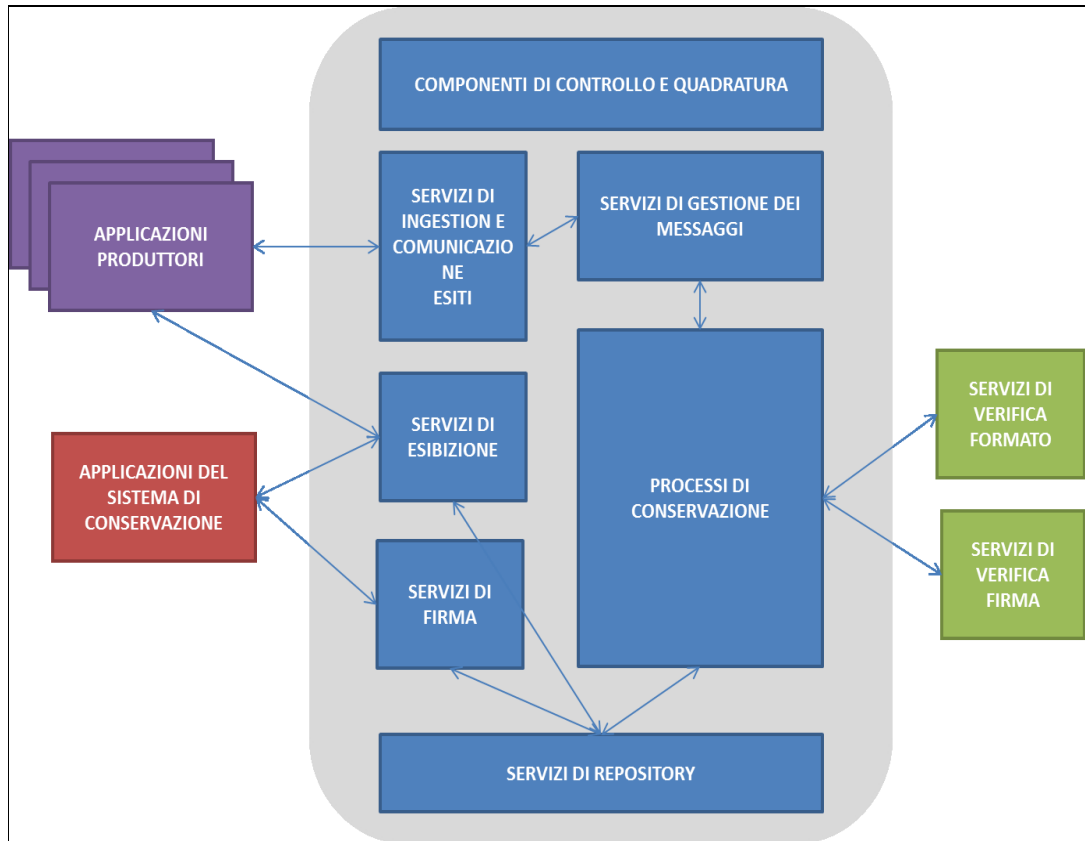


Figura 11 - Componenti logiche

- Applicazioni produttori: sono le applicazioni del sistema informativo che producono e inviano in conservazione i documenti.
- Applicazioni del sistema di conservazione: sono le applicazioni rese disponibili dal sistema di conservazione che forniscono le funzionalità di ricerca ed esibizione dei documenti conservati rivolte al responsabile della conservazione e relativi delegati.
- Componenti di controllo e quadratura: sono i componenti di monitoraggio operativo del sistema, sia automatici sia fruibili dagli utenti che fanno parte dell'infrastruttura organizzativa del responsabile del servizio di conservazione.
- Servizi di ingestione e comunicazione esiti: sono i servizi esposti dal sistema di conservazione per la ricezione dei documenti da conservare e la comunicazione degli esiti da parte dei produttori.
- Servizi di esibizione: sono i servizi esposti dal sistema di conservazione per ottenere l'esibizione dei documenti conservati; tali servizi possono essere richiamati da applicazione del sistema informativo se previsto nel manuale di conservazione.

- Servizi di firma: sono i servizi esposti dal sistema di conservazione per la firma dei pacchetti di archiviazione dei documenti; tali servizi prevedono l'utilizzo della smartcard per l'apposizione della firma digitale da parte degli utenti autorizzati.
- Servizi di gestione dei messaggi: sono i servizi che gestiscono le code di lavoro della fase di ingestione dei documenti.
- 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.
- Servizi di repository: sono i servizi che realizzano le funzionalità di tipo dati per gli archivi operazionali, temporanei, documentali e W.O.R.M. utilizzati dal sistema di conservazione.
- Servizi di verifica formato: sono servizi esterni al sistema di conservazione disponibili nell'ambito del sistema informativo della fiscalità che permettono la verifica del formato dei documenti da conservare per garantire la coerenza con i formati previsti dalla normativa.
- Servizi di verifica firma: sono servizi esterni al sistema di conservazione disponibili nell'ambito del sistema informativo della fiscalità che permettono la verifica della firma e del certificato di firma dei documenti da conservare per garantire le caratteristiche di integrità ed autenticità.

[Torna al sommario](#)

8.2 COMPONENTI TECNOLOGICHE

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

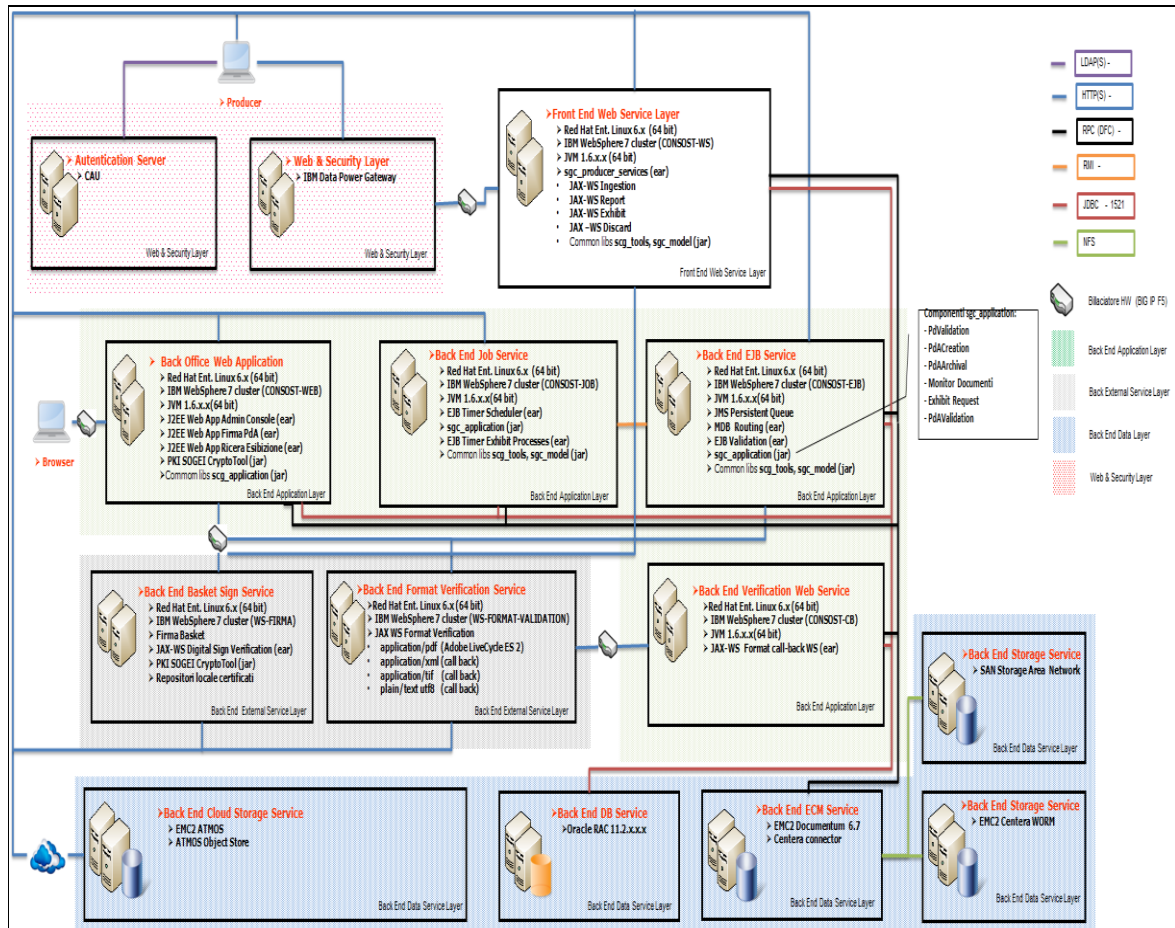


Figura 12 - Componenti tecnologiche

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

- **Web & Security Layer:** fornisce il gateway (IBM DataPower) che espone gli end-point per i chiamanti esterni e che proteggono le risorse interne al sistema. L'accesso da internet avviene richiamando una risorsa protetta dal gateway il quale, prima di inviare la chiamata all'Application Server (WAS), recupera le credenziali e verifica l'autorizzazione in Single Sign-On (SSO) secondo quanto previsto dall'architettura di sicurezza.
- **Front End Web Service Layer:** fornisce le risorse J2EE che espongono i Web Service per la ricezione dei PDV in fase di ingestione dei documenti. Tutte le risorse protette dal Web & Security Layer risiedono nello stesso livello. Le altre interfacce Web Service esposte sono i Web Service per l'esibizione, i Web Service per report e i Web Service per lo scarto.
- **Back End Application Layer:** fornisce le risorse J2EE per i seguenti servizi:

- Back End Job Service: fornisce le risorse J2EE che realizzano i job asincroni del flusso di conservazione a partire dall'ingestion dei PdV. L'esecuzione dei job avviene ad opera dell'EJB Timer Scheduler che utilizza librerie java per comunicare con gli altri layer coinvolti nel processo.
- Back End EJB Service: fornisce le risorse J2EE che realizzano i controlli asincroni, disaccoppiati mediante tecnologia Java Message Service (JMS) nelle varie fasi del flusso.
- Back End Verification Web Service: fornisce le risorse J2EE di tipo Web Service call back per le operazioni di verifica del formato dei file e della firma digitale.
- Back Office Web Application: fornisce le risorse J2EE Web Application utilizzate dagli utenti di back-office per la verifica dei PdV che non hanno superato il workflow di validazione e per effettuare la firma digitale per la chiusura dei PdA. In tale livello si trova l'applicazione web per la ricerca e l'esibizione a norma dei documenti, attraverso la generazione e il retrieve di uno o più pacchetti di distribuzione. Non espone risorse protette dal gateway pertanto si può accedere a questo layer solo dalla intranet del cliente.
- Back End External Service Layer: fornisce le risorse J2EE per i seguenti servizi:
 - Back End Format Verification Service: fornisce le risorse per la verifica dei formati. I formati accettati sono PDF/A 1-b, XML, TIFF, TXT UTF-8. Per la verifica del PDF/A1b utilizza un servizio di Adobe LiveCycle ES2.
 - Back End Basket Digital Sign Service: fornisce le risorse per la verifica della firma digitale PKCS#7 p7m, XADES.
- Back End Data Service Layer: fornisce i servizi dati RDMS. Storage e Storage WORM:
 - Back End Cloud Storage Service: fornisce le risorse di storage nel Cloud accessibili mediante protocollo http sia dai livelli di Back End che dal chiamante esterno (Producer).
 - Back End DataBase Service: fornisce la risorsa Relational DataBase Management System (RDBMS) Oracle Real Application Cluster (RAC).
 - Back End ECM Service: fornisce le componenti standard ECM di EMC2 Documentum.
 - Back End Storage Layer: fornisce i servizi di storage NFS (Network FileSystem) SAN (Storage Area Network) per le librerie di Documentum e lo storage EMC2 Centera WORM (Write Once, Read Many) utilizzato per il salvataggio finale dei PdA.

[Torna al sommario](#)

8.3 COMPONENTI FISICHE

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

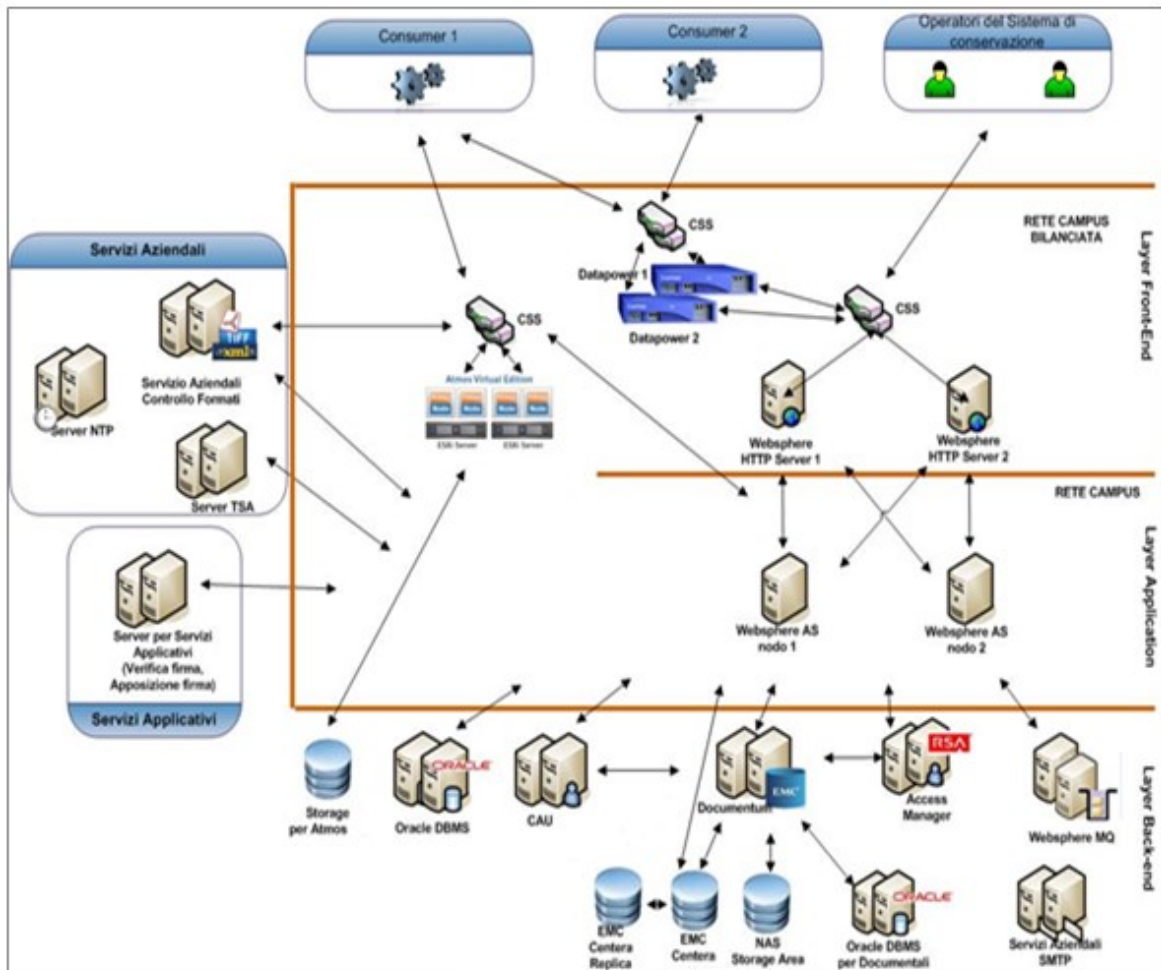


Figura 13 - Componenti fisiche

Sul layer di Front-end sono disposti i componenti infrastrutturali in rete bilanciata per bilanciare il carico e soddisfare i requisiti alta affidabilità, in particolare:

- Piattaforma Atmos in versione hardware. Tale componente è acceduto dalle applicazioni attraverso la libreria aziendale che ne astrae l'utilizzo, ha lo scopo di facilitare lo scambio di documenti tra applicazioni e servizi. Esso mantiene i documenti per il tempo necessario al completamento del processo di conservazione, secondo politiche definite in base ai requisiti applicativi;

- componenti di sicurezza IBM Datapower, per implementare la sicurezza dei servizi di acquisizione;
- componenti IBM Websphere http server a servizio del sistema di conservazione per disaccoppiare il componente web server, dal componente application server.

Sul layer application, in rete non bilanciata, sono disposti i server per ospitare il componente IBM Websphere Application Server, su cui sono installati i componenti applicativi del sistema di conservazione, rappresentati da:

- i servizi web per l'acquisizione dei documenti; tali servizi prevedono, per lo scambio dei documenti, sia l'utilizzo di ATMOS che il caricamento diretto tramite upload del documento;
- le applicazioni web previste per il sistema di conservazione (esibizione, firma dei pacchetti di archiviazione, configurazione, gestione);
- moduli applicativi EJB, per gestire tutte le attività di tipo schedulato previste dal sistema di conservazione.

Per quanto riguarda il dimensionamento dell'ambiente sono utilizzati sistemi in ambito virtuale con 2 nodi in ambiente Linux con almeno 4 core e 16 gb di ram. L'utilizzo degli ambienti virtuali potrà consentire una più facile scalabilità degli ambienti.

Sul layer di back-end sono disposti i seguenti componenti infrastrutturali:

- il sistema di controllo accessi LDAP-CAU, per la gestione degli utenti del sistema di conservazione;
- il sistema RSA Access Manager, utilizzato per l'implementazione della propagazione dell'identità dall'applicazione al sistema documentale e per la profilazione degli utenti applicativi;
- la piattaforma documentale EMC Documentum. La piattaforma, per indirizzare i requisiti applicativi, necessita delle seguenti componenti;
- DBMS oracle per la gestione del repository documentale;
- area di storage di tipo nas per la memorizzazione di documenti nella fase di verifica e per l'esibizione dei documenti;
- area di storage di tipo CENTERA (per la memorizzazione dei documenti e dei pacchetti di archiviazione per la conservazione a norma);
- lo storage EMC CENTERA, già utilizzato dal precedente sistema di conservazione, è presente nell'infrastruttura in replica locale (backup) e remota (Disaster Recovery). Lo storage è acceduto direttamente dalla piattaforma documentale sia in fase di scrittura sia in fase di lettura.

- Il DBMS Oracle assicura la persistenza di dati applicativi a supporto del sistema di conservazione.
- Il sistema di gestione delle code IBM WEBSPPHERE MQ consente la gestione dei documenti sottoposti alle varie fasi di trattamento eseguendo con modalità asincrona i vari processi del sistema di conservazione.
- Il sistema di posta elettronica aziendale acceduto tramite protocollo smtp, per la gestione degli allarmi o eventi generati dai vari componenti del sistema di conservazione.
- Il servizio Time Stamping Authority aziendale per garantire l'apposizione di una marca temporale all'atto della conservazione per la categoria di documenti che ne hanno l'esplicito obbligo di legge.
- Il servizio NTP aziendale utilizzato per la sincronizzazione della data di sistema. Il sistema di conservazione sincronizza il proprio orario contattando una volta al giorno il "nist telephone time-of-day service" per l'apposizione del riferimento temporale.
- 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. I servizi fanno uso del pattern "claim-check" basato su EMC Atmos.

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.

I metadati del Sistema di Conservazione dei documenti sono memorizzati in un database definito su una istanza Oracle di Consolidamento.

I dischi su cui risiede il database sono oggetto di replica automatica presso il sito secondario deputato alle funzionalità di Disaster Recovery.

Per il salvataggio diretto dei documenti e dei dati rilevanti è utilizzato il dispositivo storage EMC2 Centera configurato in modalità WORM (Write Once Read Many): il dato, cioè, viene archiviato in modo non modificabile e permanente nel rispetto delle normative in materia di conservazione.

Lo storage è attestato su LAN. Il colloquio con il dispositivo avviene esclusivamente tramite API native del dispositivo stesso: si tratta, infatti, di un sottosistema dischi non fruibile attraverso la tipica modalità di file system.

L'oggetto da memorizzare viene considerato una sequenza distinta di bit, indipendentemente dal suo nome e dalla locazione fisica che occuperà; al

momento dell'archiviazione sul dispositivo, viene generata una stringa di controllo di 128 bit, la stessa da utilizzare per reperire l'oggetto. Questo identificatore di controllo è in realtà una impronta che assicura l'autenticità dell'oggetto archiviato, per cui se un oggetto è recuperato e alterato anche solo per un bit, la successiva archiviazione su storage determina il ricalcolo dell'identificatore di controllo, mentre l'oggetto originario sarà ancora accessibile mediante il vecchio identificatore.

Il dispositivo di memorizzazione è in configurazione RAID-1, dunque c'è ridondanza del dato sulla stessa apparecchiatura.

L'intero sottosistema storage, a sua volta, è automaticamente replicato su una seconda apparecchiatura gemella presente in SOGEI e su una terza apparecchiatura, installata in un sito secondario a supporto della soluzione di DR.

Date le peculiarità del dispositivo di memorizzazione adottato, si evidenzia la predisposizione di flussi applicativi, integrati nel Sistema di Conservazione dei documenti, in grado di ripristinare i dati dell'intero Sistema partendo dalle informazioni presenti sul dispositivo WORM.

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](#)

8.4 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 dell'Infrastruttura, 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](#)

8.5 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 o di suoi delegati.

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.

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](#)

8.6 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 applicazione 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 sul 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 dall'applicazione di firma 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 della 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 sul 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 della 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](#)

9. 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 nello stato;
- specificazione di un indirizzo di posta elettronica presso il quale inviare le segnalazioni sull'esito dell'avvenuta esecuzione del processo.

[Torna al sommario](#)

9.1 PROCEDURE DI MONITORAGGIO

9.1.1 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;

con 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 dopo l'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 del Responsabile del servizio di conservazione.

[Torna al sommario](#)

9.1.2 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 acquisizione, assemblaggio nei pacchetti di archiviazione, apposizione della firma digitale e conservazione dei documenti.

In particolare i controlli effettuati si dividono in:

- Monitoring, effettua i controlli rispetto alla permanenza negli stati di lavorazione e relativamente ai documenti che si trovano nello stato acquisito, da firmare e firmato;
- Quadratura, sulla base di un intervallo temporale, calcola il totale dei documenti per i quali è stato richiesto il processo di conservazione,

evidenziando il numero di documenti acquisiti, assemblati, firmati, conservati e cancellati;

- integrità referenziale, esegue i controlli di bilanciamento dei pacchetti di archiviazione, dei documenti e dei relativi metadati presenti nelle basi dati memorizzate.

Le statistiche e l'esito dei controlli sono messi a disposizione del Responsabile del servizio di conservazione, del Responsabile dei sistemi informativi per la conservazione e del Responsabile della Sicurezza dei sistemi per la conservazione.

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 il processo che governa i documenti per i quali è stata richiesta la conservazione digitale dalla fase di acquisizione fino alla fase di conservazione dei pacchetti di archiviazione:

- segnalando tramite colorazioni diverse lo stato dei documenti e 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:

- Grafico a livello mensile del numero dei documenti firmati nel corso degli ultimi 3 anni.
- Classificazione in quattro 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
 - pacchetti di archiviazione da conservare
 - pacchetti di archiviazione firmati e conservati

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

- Classificazione in due item documenti prima di essere assemblati in pacchetti di archiviazione
 - Documenti non acquisiti
 - Documenti non assemblati in pacchetti di archiviazione.

Entrambi gli item possono essere ulteriormente esplosi 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.

Effettuando l'analisi delle informazioni dei report è possibile per l'addetto e per gli utenti interni interessati, verificare l'andamento dell'intero processo della conservazione digitale.

Parallelamente è previsto nel corso della giornata lavorativa e precisamente ogni ora, 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](#)

9.1.3 MONITORAGGIO DELLO STATO DELLE COMPONENTI INFRASTRUTTURALI

L'infrastruttura del sistema di conservazione è sottoposta ad un sistema di monitoraggio dedicata alle strutture organizzative del Responsabile della conservazione e del Responsabile dell'infrastruttura con i seguenti obiettivi:

- controllo delle componenti di base come riempimento file system, carico elaborativo, guasti device 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 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 dell'infrastruttura.

[Torna al sommario](#)

9.2 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](#)

9.2.1 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.

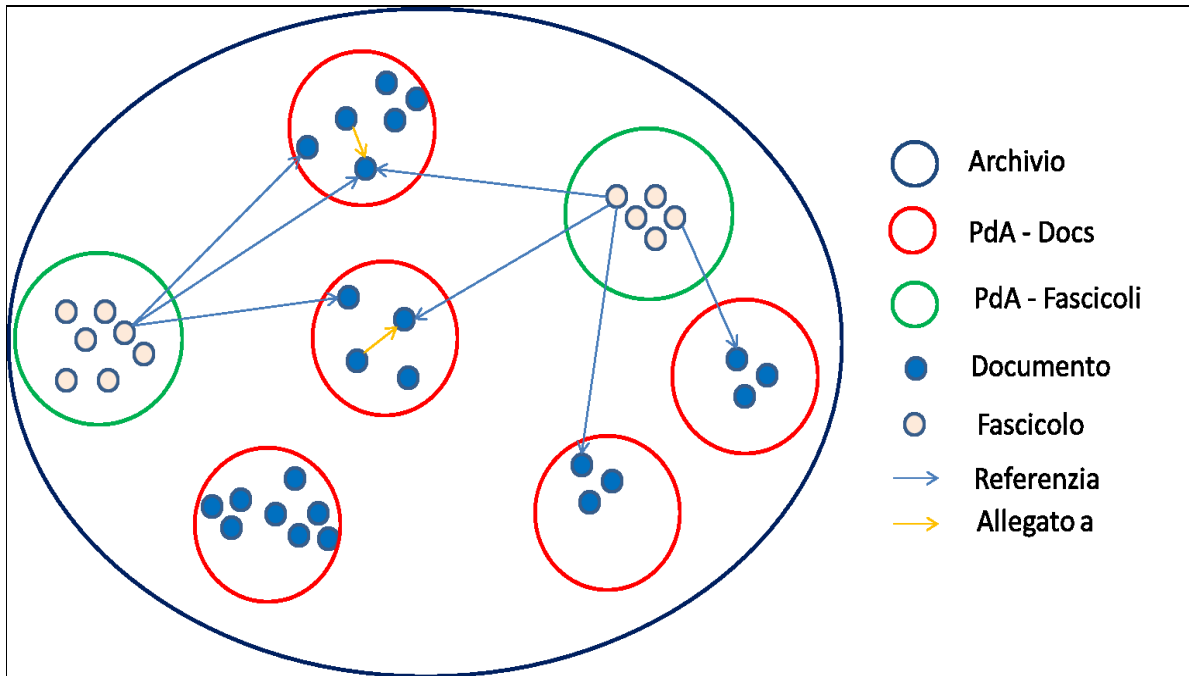


Figura 14 - I componenti dell'archivio

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 dopo cinque anni di permanenza dei documenti nel sistema di conservazione è avviata la verifica dell'archivio procedendo su un campione di documenti 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.

Il campione è ripetuto per ciascun servizio di conservazione.

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

[Torna al sommario](#)

9.2.2 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](#)

9.3 SOLUZIONI ADOTTATE IN CASO DI ANOMALIE

Le anomalie che possono manifestarsi nel corso dell'esecuzione del processo di conservazione sono classificabili in macrotipologie, per le 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
Sistemi / infrastruttura	Indisponibilità / malfunzionamenti di sistema	Verifica interna	Responsabile dell'infrastruttura
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](#)