Manuale della Conservazione a Norma

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	Novembre 2018	Ufficio Cybersecurity Architecture and Standard	Cybersecurity and Business Continuity Management – Area di Governo Chief IT, Digital and Innovation Officer
Approvazione	Novembre 2018	Giorgio Cusmà Lorenzo	Responsabile Cybersecurity, Business Continuity Strategy and Group Governance Responsabile Servizio Conservazione a Norma

REGISTRO DELLE VERSIONI

N° Ver/Rev/Bozza	Data emissione	Modifiche apportate
1.0	Novembre 2016	Adeguamento normativo
1.1	Settembre 2017	Aggiornamento Nomine Responsabili
1.2	Novembre 2017	Aggiornamento documento a seguito di indicazioni Agid
1.3	Marzo 2018	Aggiornamento documento a seguito di nuove nomine Responsabile funzione archivistica, Responsabile Trattamento dati personali
1.4	Ottobre 2018	Aggiornamento documento a seguito della cessione di Infogroup e riorganizzazione aziendale
1.5	Novembre 2018	Modifiche per cambio societario: recepita l'incorporazione di Intesa Sanpaolo Group Services in Intesa Sanpaolo; modificata organizzazione ed altri dettagli legati alla denominazione Aziendale

INDICE

1 Scopo e ambito del documento

Il presente manuale descrive il Servizio di Conservazione a Norma erogato da Intesa Sanpaolo S.p.a. (di seguito ISP). In particolare il documento ha i seguenti obiettivi:

- descrivere il modello organizzativo adottato da ISP per l'erogazione del Servizio verso i propri Clienti, in cui sono evidenziati i ruoli e le responsabilità attribuite ad attori interni o delegate a soggetti esterni;
- fornire una descrizione dei processi di erogazione del Servizio, facendo riferimento anche a documentazione operativa esterna per la descrizione di attività di dettaglio;
- le attività di controllo sul processo e sugli archivi in modo da verificare la corretta gestione dei processi di erogazione del servizio;
- l'infrastruttura tecnologica a supporto del servizio;
- le misure di sicurezza logiche e fisiche.

Il Servizio di Conservazione a Norma erogato da ISP permette di conservare i documenti in maniera tale che risultino disponibili nel tempo nella loro integrità e autenticità e che ne venga mantenuta la validità legale e fiscale.

La Conservazione a Norma di documenti informatici, avviene attraverso la memorizzazione in supporti e si conclude con l'apposizione della firma digitale e del riferimento temporale (marca temporale nel caso di documenti con valenza tributaria) da parte del Responsabile del Servizio di Conservazione che attesta il corretto svolgimento del processo.

Il documento conservato è reso leggibile, in qualunque momento, presso il sistema di Conservazione ed esibito per via telematica.

Inoltre, le normative sopra riportate, sono applicate nel rispetto della disciplina rilevante in materia di tutela dei dati personali e, in particolare, del Codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196.

Il Servizio di Conservazione è erogato nei confronti:

- dei Clienti, verso i quali il presente Manuale è parte integrante del contratto di servizio, come espressamente richiamato nel contratto stesso come previsto dall'art. 5 del DPCM.
- di Società del Gruppo, compresa Intesa Sanpaolo, che richiedono la Conservazione a Norma dei documenti prodotti verso la Clientela (es. contabili di sportello) o nell'ambito dei processi aziendali (es. Libro Inventari; documenti commerciali del ciclo passivo).

Il Servizio è offerto avvalendosi del supporto della società Engineering Ingegneria Informatica S.p.A. (di seguito Engineering in qualità di outsourcer) relativamente alle attività che riguardano le infrastrutture per la memorizzazione, trasmissione ed elaborazione dei dati.

Il presente documento rappresenta il riferimento principale relativo a qualsiasi aspetto che regola il corretto funzionamento del Servizio.

In particolare, esso, rappresenta la linea guida per la gestione della comunicazione tra ISP e il Cliente ed è approvato dal Responsabile del Servizio di Conservazione.
Eventuali modifiche e aggiornamenti al presente Manuale della conservazione possono essere effettuate dal Responsabile del Servizio di Conservazione previa condivisione con le altre figure responsabili della struttura organizzativa del Servizio.

➔ Torna al Sommario

2 Definizioni

In questo paragrafo sono riportate in ordine alfabetico le principali definizioni, termini, e concetti direttamente riferiti o collegati al processo di Conservazione a Norma.

Accesso	Operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici
Accreditamento	Riconoscimento, da parte dell'Agenzia per l'Italia digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione
Affidabilità	Caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico
Aggregazione documentale informatica	Aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente
Archiviazione elettronica o digitale	Processo di memorizzazione, su un qualsiasi idoneo supporto, di documenti informatici, univocamente identificati mediante un codice di riferimento, con modalità che possono non soddisfare i requisiti definiti dalle regole tecniche definite in normativa
Archivio	Complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività
Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico
Autenticità	Caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico
Base di dati	Collezione di dati registrati e correlati tra loro

Certificatore accreditato	Soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, dall' Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
Ciclo di gestione	Arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo
Classificazione	Attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati
Codice	Codice dell'Amministrazione digitale (CAD) - Decreto Legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni
Codice eseguibile	Insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici
Conservatore accreditato	Soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, dall'Agenzia per l'Italia Digitale
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
Destinatario	Identifica il soggetto/sistema al quale il documento informatico è indirizzato
Documento analogico	Documento formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta, le immagini su film, le magnetizzazioni su nastro. Si distingue in originale e copia
Documento informatico	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Duplicazione dei documenti informatici	Produzione di duplicati informatici
Esibizione	Operazione che consente di visualizzare un documento conservato e di ottenerne copia
Evidenza informatica	Sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica

Fascicolo informatico	Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del Codice.
Firma digitale	Particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare l'autenticità e l'integrità di un documento informatico o di un insieme di documenti informatici
Firma elettronica qualificata	Firma elettronica avanzata che sia basata su un certificato qualificato e creata mediante un dispositivo sicuro per la creazione della firma
Formato	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
Funzione di *hash*	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
Identificativo univoco	Sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione
Impronta	Sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione di una opportuna funzione di *hash* ad una evidenza informatica
Insieme minimo di metadati del documento informatico	Complesso dei metadati, la cui struttura è descritta nell'allegato 5 del DPCM [8], da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta
Integrità	Insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato
Interoperabilità	Capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi
Leggibilità	Insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti

Log di sistema	Registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati
Manuale di conservazione	Strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 8 del DPCM [8]
Marca temporale	Evidenza informatica che consente di rendere opponibile a terzi un riferimento temporale. La marca temporale può essere rilasciata solamente da un certificatore
Memorizzazione	Processo di trasposizione in formato digitale su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o digitali, anche informatici
Metadati	Insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 del DPCM [8]
Pacchetto di archiviazione	Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del DPCM [8] 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
Pacchetto informativo	Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare
Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza
Presa in carico	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione
Processo di conservazione	Insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 9 DPCM [8]

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	Oltre al notaio, anche i cancellieri, i segretari comunali, o altri funzionari incaricati dal sindaco (delibera CNIPA articolo 1, comma 1, lettera q e Testo Unico articolo 18, comma 2)
Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore
Registro di protocollo	Registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti
Responsabile del trattamento dei dati	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali
Riferimento temporale	Informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici; l'operazione di associazione deve rispettare le procedure di sicurezza definite e documentate, a seconda della tipologia dei documenti da conservare, dal soggetto pubblico o privato che intende o è tenuto ad effettuare la Conservazione digitale ovvero dal responsabile della Conservazione nominato dal soggetto stesso
Duplicato	Processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro, non alterando la loro rappresentazione digitale.
Copia informatica	Processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro, modificando la loro rappresentazione digitale.
Scarto	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale
Sistema di conservazione	Sistema di conservazione dei documenti informatici di cui all'articolo 44 del CAD [6]
Sottoscrizione elettronica o digitale	Apposizione della firma elettronica qualificata

Supporto ottico	Mezzo fisico che consente la memorizzazione di documenti digitali mediante l'impiego della tecnologia laser (quali, ad esempio, dischi ottici, magneto-ottici, DVD)
Utente	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse

➔ Torna al Sommario

3 Acronimi

AgID	Agenzia per l'Italia Digitale
CAD	Codice Amministrazione Digitale
DPCM	Decreto Presidente del Consiglio dei Ministri
DPR	Decreto Presidente della Repubblica
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
HTTPS	Secure Hyper Text Transmission Protocol. Protocollo sviluppato allo scopo di cifrare e decifrare le pagine Web che vengono inviate dal server ai client.
IPdA	Indice del Pacchetto di Archiviazione
PdA	Pacchetto di Archiviazione
PdD	Pacchetto di Distribuzione
PDF	Portable Document Format
PdV	Pacchetto di Versamento
PEC	Posta Elettronica Certificata
PKI	Public Key Infrastructure (infrastruttura necessaria per creare, gestire, conservare e revocare i certificati delle firme elettroniche basati su crittografia a chiave pubblica)
RDC	Responsabile della Conservazione
RdV	Rapporto di Versamento
SLA	Service Level Agreement
SSL	Secure Socket Layer. Protocollo che consente, grazie a tecniche di crittografia, il trasferimento di dati tramite la rete Internet in modo sicuro
URL	Uniform Resource Locator (indica la modalità per individuare univocamente un sito Internet)
URN	Unified Resource Name
UTC	Universal Time Coordinated (Misura del tempo così come stabilito dall'International Radio Consultative Committee – CCIR)
WS	Web Services

➔ Torna al Sommario

4 Normativa e standard di riferimento

4.1 Riferimenti normativi

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

[1] 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;

[2] 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;

[3] 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;

[4] Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;

[5] Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;

[6] Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);

[7] Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;

[8] 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;

[9] 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.

[10] DPCM 13 novembre 2014 (G.U. 12 gennaio 2015) - 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.

➔ Torna al Sommario

4.2 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 1° ottobre 2014.

a) ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;

b) ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);

c) 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;

d) 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;

e) UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;

f) ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core;

g) ISO 15489:2016 Information and documentation - Records Management - Parte 1: Concepts and principles, capitoli 5 e 7.

➔ Torna al Sommario

5 Modello organizzativo

5.1 Ruoli e responsabilità

Il Servizio di Conservazione a Norma, che ISP eroga ai propri clienti, prevede la seguente struttura Organizzativa:

- Produttore
- Utente
- Responsabile del Servizio di Conservazione
- Responsabile della funzione archivistica di conservazione
- Responsabile sviluppo e manutenzione del sistema di conservazione
- Responsabile dei Sistemi Informativi per la conservazione
- Responsabile della Sicurezza dei sistemi per la conservazione
- Responsabile Trattamento dei Dati Personali

5.1.1 Produttore

Persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, è il responsabile della creazione del pacchetto di versamento e del suo invio verso il sistema di Conservazione. Verifica l'esito della conservazione tramite il controllo del Rapporto di Versamento.

5.1.2 Utente

Persona, ente o sistema in grado di richiedere al Sistema di Conservazione a Norma l'esibizione del pacchetto di distribuzione ovvero fruire delle informazioni di interesse.

5.1.3 Responsabile del Servizio di Conservazione

Definisce le caratteristiche e i requisiti del sistema di conservazione affinché venga garantita la leggibilità e l'integrità dei documenti conservati nel lungo periodo in conformità alla normativa vigente. Verifica la corretta applicazione delle definizioni da lui stesso impartite per il sistema di conservazione. Si preoccupa di adeguare le proprie disposizioni ai cambiamenti normativi e tecnologici che dovessero arrivare. In particolare svolge le seguenti attività:

- definizione delle caratteristiche e dei requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare e delle evoluzioni della normativa di riferimento;
- presidio della definizione delle procedure di sicurezza e tracciabilità per l'erogazione del servizio in linea con la normativa di riferimento;
- gestione del manuale della conservazione che descrive l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, il processo, le architetture, infrastrutture e le misure di sicurezza;

- collaborazione, in caso di esternalizzazione, con la Direzione Legale e Contenzioso, con la Direzione Sistemi Informativi e con il Servizio Acquisti per la definizione delle caratteristiche servizio, degli aspetti contrattuali verso l'outsourcer e per il controllo del rispetto dei requisiti di sicurezza e di servizio;
- definizione, congiuntamente alla Direzione Sistemi Informativi, dei livelli di servizio richiesti quali requisito iniziale del servizio (tale requisito avrà infatti impatti sulla stima dei costi progettuali/gestione);
- presidio nel tempo della normativa in ambito garantendo il necessario aggiornamento di tutti gli attori coinvolti in merito a possibili variazioni, assicurando gli adeguamenti obbligatori del servizio dove richiesti dagli sviluppi delle normative nel tempo;
- garanzia del buon funzionamento della Conservazione, mediante la definizione di specifici obiettivi di controllo e l'analisi di report appositamente predisposti;
- governo delle escalation sulle problematiche di servizio, in particolar modo legate all'esibizione a norma dei documenti;
- gestione delle relazioni con gli organismi esterni assicurando il supporto l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e dio vigilanza;
- supporto all'Audit nella definizione e nell'esecuzione delle verifiche ispettive nella documentazione degli esiti e nella gestione delle necessarie azioni correttive / preventive.

5.1.4 Responsabile della funzione archivistica di conservazione

Definisce in accordo con l'ente produttore le modalità di trasferimento dei documenti informatici verso il sistema di conservazione. In particolare svolge le seguenti attività:

- definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferite, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato;
- definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici;
- monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione;
- collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.

5.1.5 Responsabile trattamento dei dati personali

È la figura che garantisce il rispetto della normativa vigente in materia del trattamento dei dati personali e del rispetto delle istruzioni impartite dal Titolare del trattamento con garanzia di sicurezza e riservatezza.

5.1.6 Responsabile Sicurezza dei sistemi per la conservazione

È la figura che stabilisce e manutiene le policy di sicurezza relative al sistema di conservazione, le condivide con il Responsabile del Servizio di Conservazione e ne verifica l'applicazione nel tempo. Individua eventuali difformità, le comunica al Responsabile del Servizio di Conservazione e pianifica le azioni correttive individuate.

5.1.7 Responsabile sistemi informativi per la conservazione

È la persona che gestisce l'esercizio delle componenti hardware e software del sistema di conservazione, garantendone l'adeguatezza nel tempo. Si occupa del monitoraggio dei livelli di servizio dell'infrastruttura e segnala eventuali difformità degli SLA al Responsabile del Servizio di Conservazione, pianificando eventuali azioni correttive. Pianifica lo sviluppo delle infrastrutture tecnologiche del sistema di conservazione e controlla e verifica i livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.

5.1.8 Responsabile sviluppo e manutenzione del sistema di conservazione

È la persona di riferimento per il coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione. Pianifica e monitora i progetti di sviluppo del sistema di conservazione oltre agli SLA relativi alla manutenzione del sistema di conservazione; si 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. Ha in carico la manutenzione dell'applicazione a supporto del Servizio di Conservazione a Norma interfacciando l'outsourcer.

➔ Torna al Sommario

5.2 Attribuzione dei ruoli interni ad Intesa Sanpaolo

I ruoli **interni all'organizzazione per l'erogazione del servizio** sono stati così assegnati:

Ruoli	***Nominativo***	***Contratto***	***Eventuali deleghe***
Responsabile del servizio di conservazione / Responsabile della Conservazione	Giorgio Cusmà Lorenzo	Tempo Indeterminato	
Responsabile funzione archivistica di conservazione	Massimo Poli	Tempo Indeterminato	
Responsabile trattamento dati personali	Enrico Bagnasco	Tempo Indeterminato	
Responsabile Sicurezza dei sistemi per la conservazione	Giorgio Cusmà Lorenzo	Tempo Indeterminato	Domenico De Angelis
Responsabile sistemi informativi per la conservazione	Ezio Barbero	Tempo Indeterminato	Riccardo D'Agostini
Responsabile sviluppo e manutenzione del sistema di conservazione	Ezio Barbero	Tempo Indeterminato	Riccardo D'Agostini

➔ Torna al Sommario

5.3 Attività esternalizzate

ISP affida al seguente outsourcer le attività operative di Conservazione:

Engineering Ingegneria Informatica S.p.A.

Via San Martino della Battaglia, 56

00185 Rome

P. IVA N° 05724831002

All'outsourcer del Servizio di Conservazione (o Gestore della Conservazione) è assegnata la responsabilità di gestione operativa della Conservazione.

Vengono messe a disposizione le infrastrutture per la memorizzazione, trasmissione ed elaborazione dei dati atte a garantire integrità, autenticità, riservatezza e disponibilità nel tempo dei documenti conservati.

In particolare, al Gestore della Conservazione sono affidate le seguenti attività:

- redigere il Manuale della Conservazione sulla base delle indicazioni fornite dal Responsabile del Servizio di Conservazione e strutturarsi secondo ruoli e responsabilità coerenti con quanto definito;
- eseguire le necessarie verifiche di congruenza in fase di acquisizione documenti e in fase di predisposizione dei pacchetti informativi;
- archiviare e rendere disponibili tramite la predisposizione degli opportuni pacchetti informativi i documenti ricevuti dal Sistema di Conservazione, in conformità a quanto previsto dalla normativa vigente e a quanto concordato all'interno del contratto di servizio;
- verificare periodicamente, con cadenza non superiore a quanto previsto dai termini contrattuali, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, alla copia o duplicazione degli stessi;
- produrre la reportistica periodica di Servizio concordata in sede contrattuale;
- adottare le misure necessarie per la sicurezza fisica e logica del sistema definite dal Responsabile della Conservazione;
- supportare il Responsabile del Servizio di Conservazione nell'espletamento degli adempimenti obbligatori previsti dalla legge applicabile;
- fornire supporto operativo relativamente a tutte le segnalazioni provenienti dagli utenti e dalle strutture interne di Intesa Sanpaolo che possono accedere o interfacciarsi con il servizio di conservazione;
- assicurare il corretto funzionamento dell'applicativo di Conservazione a Norma, gestendo le eventuali segnalazioni di malfunzionamento e implementando gli opportuni aggiornamenti secondo le esigenze dei clienti e le evoluzioni della normativa vigente;
- assicurare il corretto funzionamento dell'infrastruttura tecnologica dei servizi di Conservazione a Norma, in particolare adottando misure per il rilevamento dell'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e gestendo possibili segnalazioni di malfunzionamento ripristinando la corretta funzionalità dei servizi stessi, avvisando prontamente il Responsabile del Servizio di Conservazione di ISP.

Le attività operative a carico dell'outsourcer sono descritte nel rispettivo "Manuale della Conservazione".

Il modello attuato al fine di garantire il controllo dell'esternalizzazione dei servizi di archiviazione digitale tramite Conservazione a Norma si articola sui seguenti livelli:

- 1° livello, svolto da **Cybersecurity Projects Delivery** di **Intesa Sanpaolo S.p.a.** in qualità di responsabile della gestione operativa del contratto relativo ai servizi informatici erogati dall'outsourcer. In particolare, le attività di controllo relative al Servizio di Conservazione a Norma prevedono:
  - monitoraggio continuo (su base quotidiana) degli aspetti operativi e di funzionamento del servizio per il tramite dell'outsourcer;

- partecipazione a SAL (Stato di avanzamento lavori) guidati dall'outsourcer, volti a verificare con cadenza mensile i livelli di servizio della fornitura e a gestire le attività progettuali in essere relativamente al Servizio di Conservazione a Norma;
- verifica formale, con cadenza mensile, del raggiungimento degli SLA definiti con il fornitore;
- verifica del rispetto degli obiettivi di controllo tramite l'analisi dei report prodotti dal fornitore dei servizi di Conservazione;
- partecipazione almeno annuale al Comitato per il Controllo sulla Gestione per la verifica o la modifica dell'efficacia e dell'efficienza dei servizi prestati e se necessario saranno proposte eventuali modifiche contrattuali

Si segnala che oltre a quanto già regolamentato dai contratti standard di fornitura servizi, sono stati definiti specifici KPI (Key Performance Indicator) e relativi SLA (Service Level Agreement) per il Servizio di Conservazione a Norma. Sono inoltre state previste specifiche penali da applicare in caso di disservizi e/o qualità del servizio al di sotto degli SLA definiti.

- 2° livello, svolto da **Cybersecurity, Business Continuity Strategy and Group Governance** di **Intesa Sanpaolo S.p.a**. Tale livello prevede il presidio dei controlli propri del sistema di conservazione (previsti dalla normativa di riferimento) e il monitoraggio dei livelli di sicurezza del fornitore. In particolare:
  - monitoraggio della normativa in ambito (analisi nuove normative, valutazioni impatti sui servizi di conservazione erogati dal fornitore, indirizzamento e presidio degli interventi di adeguamento);
  - realizzazione di analisi del rischio periodiche sulle infrastrutture IT del fornitore preposte all'erogazione dei servizi di Conservazione a Norma;
  - verifica periodica del livello di conformità del sistema di gestione della sicurezza informatica del fornitore rispetto agli standard del Gruppo Intesa Sanpaolo.
- 3° livello, svolto dalla struttura di **Internal Audit** di **Intesa Sanpaolo** (unità organizzativa indipendente che risponde direttamente al Consigliere Delegato della Società) al fine di monitorare l'adeguatezza complessiva del Sistema di Conservazione, valutando l'efficacia ed efficienza dei processi operativi, il rispetto della normativa interna ed esterna, l'affidabilità della struttura operativa e dei meccanismi di delega. In particolare tale struttura effettua audit periodici che interessano tutte le unità organizzative interne ed esterne coinvolte nell'erogazione dei servizi di Conservazione a Norma, con l'obiettivo di segnalare eventuali anomalie, definire e assegnare alle funzioni responsabili gli opportuni interventi di risoluzione e verificare il corretto completamento degli stessi.

L'outsourcer, accreditato presso l'Agenzia per l'Italia Digitale, in aggiunta ai livelli di controllo sopra descritti, dovrà inoltre produrre la seguente documentazione periodica, di cui dovrà fornire evidenza su richiesta (ad esclusione di eventuali informazioni riservate) al Responsabile del Servizio di Conservazione:

- certificato ISO/IEC 27001 e successivi rinnovi, oltre che le risultanze delle verifiche annuali di mantenimento;
- certificato di conformità del Sistema di Conservazione ai requisiti tecnici organizzativi stabiliti dall'Agenzia, rilasciato da un ente di certificazione accreditato da ACCREDIA,

o da altro Ente di Accreditamento firmatario degli accordi di mutuo riconoscimento nello schema specifico (da rinnovarsi almeno ogni 24 mesi);

- rapporto quadrimestrale contenente i dati di riepilogo delle attività svolte.

Tutti i controlli svolti sulle attività esternalizzate verranno adeguatamente documentati e le carenze riscontrate saranno segnalate alle funzioni aziendali di controllo unitamente alle azioni correttive identificate. Periodicamente verranno inoltre forniti aggiornamenti sullo stato di tali azioni.

Il Responsabile del Servizio di Conservazione è inoltre responsabile di valutare i casi di particolare rilevanza e fornirne tempestiva informazione agli organi aziendali al fine di garantire la piena conoscenza e governabilità dei fattori di rischio dei servizi esternalizzati.

➔ Torna al Sommario

5.4 Responsabilità del Cliente o utente interno

Nel seguito una breve descrizione delle responsabilità a cui il Cliente (interno o esterno) si deve attenere, da utilizzare come linea guida in fase di predisposizione del contratto o degli allegati tecnici e operativi o degli accordi con le Società del Gruppo:

- rispettare le classi documentali da conservare, i formati dei documenti consentiti e le) nell'allegato tecnico al contratto o in apposito accordo con le Società del Gruppo;
- concordare con il Responsabile del Servizio di Conservazione le modalità necessarie alla configurazione del sistema e alla produzione dei pacchetti informativi;
- rispettare tempi, dimensioni e volumi definiti nel contratto per l'invio in Conservazione dei documenti o in apposito accordo con le Società del Gruppo;
- richiedere la presenza di un pubblico ufficiale nei casi in cui sia previsto il suo intervento, assicurando allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite.

➔ Torna al Sommario

5.5 Struttura Organizzativa

A supporto del processo di Conservazione sono state definite specifiche figure interne all'organizzazione dell'Azienda in grado di garantire la corretta erogazione del servizio e adeguati supporti nei confronti del Produttore e dell'Utente.

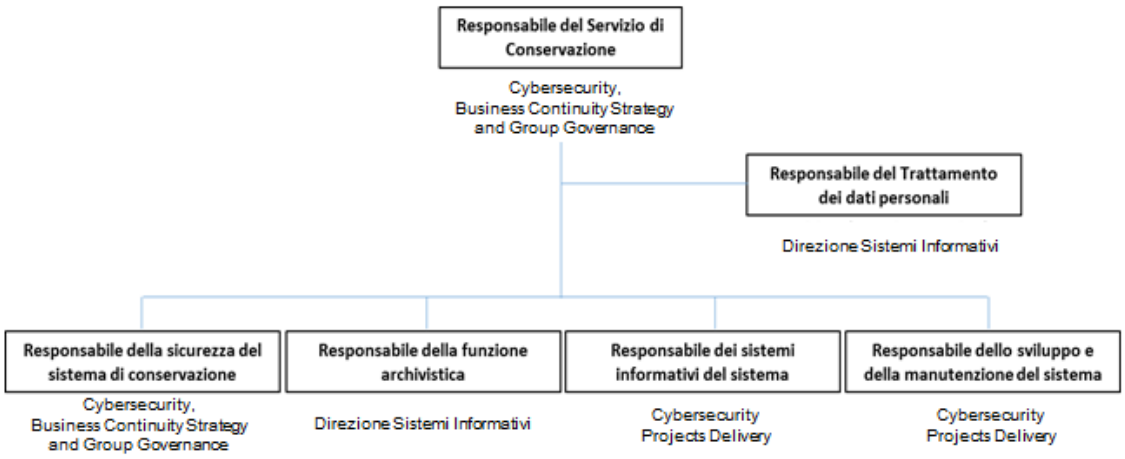

Figura 1 - Organizzazione

Rispetto al modello organizzativo di riferimento per il servizio e alle strutture coinvolte, nella seguente matrice RACI sono rappresentate le responsabilità per ciascun ruolo attribuito agli attori coinvolti nel processo di Conservazione a Norma.

➔ Torna al Sommario

Matrice RACI	Responsabile del servizio di conservazione	Responsabile della funzione archivistica di conservazione	Responsabile del trattamento dei dati personali	Responsabile della sicurezza dei sistemi per la conservazione	Responsabile dei sistemi informativi per la conservazione	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Outsourcer del sistema di conservazione
Attivazione del Servizio di Conservazione (a seguito della sottoscrizione di un contratto)	**A**	**C**	**I**	**C**		**R**	**I**
Acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento	**A**	**R**			**C**		**R**
Preparazione e gestione del pacchetto di archiviazione	**A**	**C**				**R**	**R**
Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta	**A**	**C**	**I**		**C**	**R**	**R**
Scarto dei pacchetti di archiviazione		**A**	**I**		**C**	**R**	**R**
Chiusura del Servizio di Conservazione (al termine di un contratto)	**A**	**I**	**I**		**C**	**C**	**I**
Conduzione e manutenzione del sistema di conservazione			**C**		**C**	**A**	**A**
Monitoraggio del sistema di conservazione	**I**	**I**			**A**	**R**	**R**
Change management			**C**		**C**	**A**	**R**
Verifica periodica di conformità a normativa e standard di riferimento	**A**	**C**		**C**			**R**

R = Responsible (la persona che è incaricata di svolgere operativamente l'attività)
A = Accountable (la persona con poteri decisionali ed è owner dell'attività)
C = Consulted (la persona che deve essere consultata nell'ambito dello svolgimento dell'attività)
I = Informed (la persona che deve essere informata circa lo svolgimento dell'attività)

➔ Torna al Sommario

6 Oggetti sottoposti a conservazione

Nel presente capitolo e nei successivi vengono descritte le componenti del sistema di conservazione in coerenza con le specifiche fornite dall'outsourcer del servizio (Gestore del Servizio di Conservazione a Norma).

6.1 Oggetti conservati

Le tipologie documentali che rientrano nel perimetro del servizio attive sul sistema di conservazione sono descritte nei relativi documenti di "Specificità di contratto".

Per quanto riguarda l'archiviazione dei dati, il sistema di conservazione garantisce, per ogni tipologia documentale il salvataggio dei dati, almeno per il tempo minimo previsto dalla normativa di riferimento.

Nella seguente tabella è rappresentato un esempio dei formati gestiti.

visualizzatore	Produttore	Formato del file	versione del formato	sistema operativo
Acrobat	ISP – sportello	Pdf, p7m	1.4 (Acrobat 5)	WinXP/7/8
Acrobat	ISP – Contratti	Pdf, p7m	Vari formati	WinXP/7/8
Acrobat	ISP – Easy Fattura	Xml, Pdf, p7m, tsd	Vari formati	WinXP/7/8
Acrobat	ISP – Terzo valore	Pdf, p7m	Vari formati	WinXP/7/8
Acrobat	ISP – Applicazione Data certa	Pdf, tsr	Vari formati	WinXP/7/8
Immagini	ISP – Applicazione Data certa	Tiff, tsr	Vari formati	WinXP/7/8

Nei documenti di "Specificità di contratto" condivisi tra le parti sono presenti eventuali integrazioni alla presente tabella o altri dettagli relativi alle modalità adottate per garantire la leggibilità dei formati gestiti.

Gli oggetti della conservazione sono trattati dal sistema di conservazione in pacchetti informativi come descritto nel presente documento e conformemente all'art. 4 del DPCM [8] e ai capitoli 5 e 7 dello standard ISO 15489:2017 (Rif. g)):

- Pacchetti di Versamento (PdV)

- Pacchetti di Archiviazione (PdA)
- Pacchetti di Distribuzione (PdD)

➔ Torna al Sommario

6.2 Formati e metadati

Le tipologie documentali relative agli oggetti documentali sopra descritti sono individuate dal Responsabile del Servizio di Conservazione d'intesa con la funzione archivistica ed applicativa, in fase di attivazione del servizio e conformemente a quanto stipulato in sede contrattuale, tenendo conto delle:

- peculiarità delle classi documentali;
- dei formati dei file accettabili in conservazione.

Ai sensi della normativa vigente sono conservati solo i formati di file idonei ad essere correttamente conservati, individuati dall'allegato 2 alle Regole Tecniche (DPCM [8]), a cui integralmente si rinvia, rispettando i requisiti ivi previsti di "standard aperti", per garantire in futuro la possibilità tecnica di accedere ai dati conservati, corredati da una struttura di dati per la memorizzazione nel sistema di conservazione in grado di assicurare l'interoperabilità tra sistemi.

Tutti i documenti versati nel sistema di conservazione sono contraddistinti da un set di metadati obbligatori per il sistema, che li identificano univocamente, e che sono descritti nel capitolo relativo al Pacchetto di versamento (Rif. 6.3).

➔ Torna al Sommario

6.3 Pacchetto di Versamento

Il Servizio di Conservazione riceve i documenti inviati dal Produttore attraverso canali di comunicazione sicuri concordati col Cliente in sede di attivazione del servizio.

I documenti da sottoporre a conservazione devono essere predisposti secondo quanto previsto contrattualmente per quanto attiene la presenza della firma digitale, dei metadati e la correttezza del formato.

I documenti contenuti nel Pacchetto di Versamento (PdV) confluiscono, nelle modalità di seguito descritte, in uno o più PdA.

Il servizio offre una completa personalizzazione riguardo alla configurazione dei metadati ed alla loro obbligatorietà, consentendo totale piena libertà rispetto alla scelta di quali includere, e di conseguenza la piena adesione allo standard Dublin Core Metadata ISO 15836:2009 (Rif. f)).

A livello di documento è possibile definire un set di metadati minimi che il documento deve possedere per poter essere versato nel sistema di conservazione (il set di metadati minimi è condiviso con il Cliente/produttore e viene dettagliato nel documento Specificità di Contratto).

Di default il set di metadati minimo è il seguente:

- identificativo del documento;

- data di chiusura;
- oggetto (descrizione del contenuto del documento);
- soggetto produttore (nome, cognome, codice fiscale);
- soggetto destinatario (nome, cognome, codice fiscale).

Sono definite inoltre le specifiche del pacchetto di versamento e del relativo indice in corrispondenza di ogni tipologia documentale. Ogni pacchetto di versamento deve prevedere un indice, in formato XML, che include almeno i seguenti contenuti minimi validi per tutte le tipologie documentali:

- nome file del pacchetto;
- impronta (hash) di ogni file contenuto nel pacchetto;
- metadati dei file del pacchetto.

A livello di PDV si sono definiti i seguenti metadati:

Nome metadato	**Produttore**
CHIAVE/NUMERO	Obbligatorio. Questo dato deve essere sempre presente all'interno
ANNO	Concorre a formare l'univocità della chiave
REGISTRO	Concorre a formare l'univocità della chiave

Non tutti i seguenti sono obbligatori:

Nome metadato	**Produttore**
COD_SOC	Obbligatorio. È un valore che consente di "sezionare" i dati conservati. Tipicamente la family coincide con il servizio (es. Contabili)
COD_UO	Obbligatorio. Questo dato deve essere sempre presente all'interno
COD_SPORTELLO	Concorre a formare l'univocità della chiave
WORKSTATION	Concorre a formare l'univocità della chiave
OPERATORE	Matricola dell'operatore (del produttore)
COD_RAPPORTO	Rapporto del Cliente (per documento Clientela)
NDG	NDG del Cliente
NOME	Nome del Cliente
COGNOME	Cognome del Cliente

Nome metadato	Produttore
IMPORTO	Importo dell'operazione
COD_ADESIONE	Specifico per Fascicolo
FG_ANNULLO	flag
EMAIL_CLIENTE	e-mail del Cliente
TRANSAZIONE	Tipo di transazione (es. BONIF)
DATA_CONTABILE	Se operazioni contabile
DATA_CREAZIONE	Obbligatoria
DATA_FIRMA	Se documento firmato
VERSIONE	Dettaglio del viewer/applicativo generatore

Le strutture dati di colloquio tra Cliente e Conservatore sono dettagliate nell'allegato Specificità del Contratto e concordate con il cliente.

➔ Torna al Sommario

6.4 Pacchetto di Archiviazione

Il Pacchetto di Archiviazione (PdA) contiene un numero variabile di documenti ed un indice. La modalità di conservazione mediante indice permette di **verificare l'integrità** di ogni singolo file, indipendentemente da tutti gli altri file conservati nello stesso blocco.

L'indice del PdA è un file in formato XML che riporta, per ognuno dei file inclusi nel blocco, alcune informazioni tra cui un URN (unified resource name) e un "hash".

L'urn è una stringa univoca che identifica l'oggetto digitale, mentre l'hash è un'impronta del documento, ovvero una sequenza di bit che può essere ricavata dal file in modo ripetibile e standardizzato e che garantisce una corrispondenza esatta col contenuto originale.

Infatti sarà sufficiente essere in possesso di un file "candidato" e conoscere il suo URN identificativo per poter eseguire la funzione di hash e confrontare l'impronta ricalcolata con la stringa riportata nell'indice.

➔ Torna al Sommario

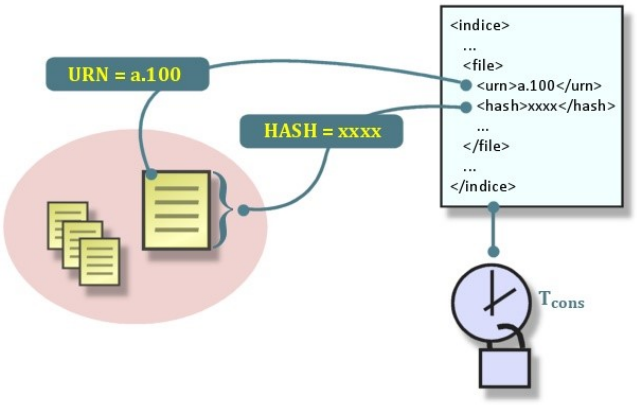

Figura 2 - Struttura dell'indice del PdA

Il Pacchetto di Archiviazione viene composto a partire da uno o più PdV ed è un'entità logica nella quale sono contenuti uno o più documenti, in base a criteri definiti con il Produttore.

➔ Torna al Sommario

6.4.1 Contenuti dell'indice del PdA (SinCRO)

La soluzione adottata è compliant con lo standard UNI 11386 [UNI 11386:2010 - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (SinCRO)].

All'interno della sottocommissione DIAM/SC11 (Gestione dei documenti archivistici) dell'Ente nazionale italiano di unificazione (UNI), un apposito gruppo di lavoro denominato SInCRO, ha definito la struttura dell'insieme dei dati a supporto del processo di conservazione individuando gli elementi informativi necessari alla creazione di un Indice di Conservazione ("indice del pacchetto di archiviazione ").

L'implementazione di tale indice, del quale SinCRO ha descritto sia la semantica sia l'articolazione, permette di utilizzare una struttura-dati condivisa e raggiungere un soddisfacente grado d'interoperabilità nei processi di migrazione, mediante l'adozione di uno Schema XML appositamente elaborato.

In aggiunta a quanto previsto dalla normativa, il software prevede alcuni metadati aggiuntivi sfruttando il tag MoreInfo.

A livello generale:

- CRL al momento dell'avvenuto versamento
- CRL al momento della chiusura del RdV relativo al documento specifico (come specificato al par. "Costruzione e conservazione del Pacchetto di Archiviazione")
- Certificati-Trusted. Vengono inseriti i nomi dei certificati Trusted relativi alle firme presenti nei documenti contenuti nel PdA.

A livello di singolo file:

- Informazioni sulle verifiche di firma effettuate (Forza Accettazione / Forza Conservazione).
- Nome e cognome del firmatario (se le verifiche sono attivate e la firma è presente).
- Esiti di verifica firma. Informazioni sulla validità della firma, verifica crittografica, controllo certificato stato della revoca, con riferimento alle CRL reperite nella sezione “Generale”, sopra menzionata.

Esempio di marca Sincro prodotta dall’applicativo

```
<?xml version="1.0"?>
<sincro:IdC xmlns:eng="ns://eng-sincro/" xmlns:sincro="http://www.uni.com/U3011/sincro/">
 <sincro:SelfDescription>
  <sincro:ID sincro:scheme="local">Marca-blocco_1108994_2472_ITOD24721510906201131_CONSERVAZIONE</sincro:ID>
  <sincro:CreatingApplication>
   <sincro:Name>Canopi</sincro:Name>
   <sincro:Version>1.2.2-snapshot-02</sincro:Version>
   <sincro:Producer>Engineering Ingegneria Informatica S.p.A</sincro:Producer>
  </sincro:CreatingApplication>
 </sincro:SelfDescription>
 <sincro:VdC>
  <sincro:ID sincro:scheme="local">1108994</sincro:ID>
  <sincro:VdCGroup>
   <sincro:Label>00438000481</sincro:Label>
   <sincro:ID sincro:scheme="local">2472</sincro:ID>
   <sincro:Description sincro:language="it">Struttura Centro Leasing Spa</sincro:Description>
  </sincro:VdCGroup>
  <sincro:MoreInfo sincro:XMLScheme="ns://eng-sincro/TagEng.xsd">
   <sincro:EmbeddedMetadata>
    <sincro:EngInfo>
     <eng:VdCInfo>
      <eng:RapportiDiVersamento>
       <eng:RapportoDiVersamento>
        <eng:ID>1083</eng:ID>
        <eng:Urn>EFAT:XXXXXXXXXXXSpa:00438000481:30102017:1</eng:Urn>
        <eng:Hash eng:algoritmo="SHA-256" eng:codifica="B64">hsnjuRp9eKZC7zJZUM3AAKWPtA3mlB+UxkxZpjt2glU=</eng:Hash>
       </eng:RapportoDiVersamento>
      </eng:RapportiDiVersamento>
      <eng:ElencoCRL>
       <eng:CRL>
        <eng:file id="432994" crl-number="67750" this-update="2017-08-03T15:30:04+02:00" next-update="2017-08-04T15:30:00+02:00" download-
date="2017-08-03T16:00:09+02:00">201708031530_IntesaSanpaoloS.p.A.IdenTrustCertificationAuthority_CRL01.crl</eng:file>
        <eng:hash eng:algoritmo="SHA1" eng:codifica="B64">YdQaQP8w79c4pQ8MB9+z6PV3BRU=</eng:hash>
       </eng:CRL>
       <eng:CRL>
```

<eng:file id="433502" crl-number="70629" this-update="2017-11-16T16:30:07+01:00" next-update="2017-11-17T16:30:00+01:00" download-date="2017-11-16T17:04:07+01:00">201711161630_IntesaSanpaoloS.p.A.IdenTrustCertificationAuthority_CRL01.crl</eng:file>

<eng:hash eng:algoritmo="SHA1" eng:codifica="B64">0F57JqpoHRb7y0wcDMsEkXHrhHk=</eng:hash>

</eng:CRL>

<eng:CRL>

<eng:file id="432963" crl-number="616" this-update="2017-08-01T22:49:38+02:00" next-update="2017-08-06T22:49:38+02:00" download-date="2017-08-02T15:00:06+02:00">201708012249_ActalisTimeStampingCAG1.crl</eng:file>

<eng:hash eng:algoritmo="SHA1" eng:codifica="B64">24ooXwezTKxBf/5hwhClwslSVbc=</eng:hash>

</eng:CRL>

</eng:ElencoCRL>

</eng:VdCInfo>

</sincro:EngInfo>

</sincro:EmbeddedMetadata>

</sincro:MoreInfo>

</sincro:VdC>

<sincro:FileGroup>

<sincro:Label>11-2016-IVARGE_2016_666_4385-IVARGE</sincro:Label>

<sincro:File sincro:encoding="base64" sincro:extension="PDF.P7M.TSD" sincro:format="PDF_PKCS7_TSD">

<sincro:ID sincro:scheme="locale">2692818</sincro:ID>

<sincro:Path>MF_BOLDEBIT_2016_05.PDF.p7m.tsd.PDF_PKCS7_TSD</sincro:Path>

<sincro:Hash sincro:function="SHA-256">miNY2Hes83EavUE5w9jxBGxYOA5FJff9MDL1Kd1k/KA=</sincro:Hash>

<sincro:MoreInfo sincro:XMLScheme="ns://eng-sincro/TagEng.xsd">

<sincro:EmbeddedMetadata>

<sincro:EngInfo>

<eng:FileInfo>

<eng:Urn>urn:EFAT:XXXXXXXXXXXX:00438000481:IVARGE_2016_666_4385:2016:11:REGISTRI:0:0:MF_BOLDEBIT_2016_05.PDF.p7m.tsd</eng:Urn>

<eng:RdV>1083</eng:RdV>

<eng:Forza-Accettazione>si</eng:Forza-Accettazione>

<eng:Forza-Conservazione>si</eng:Forza-Conservazione>

<eng:Firmato>si</eng:Firmato>

<eng:Firma-Info>

<eng:Valore>TUTTE_LE_FIRME_SONO_VERIFICATE</eng:Valore>

<eng:Codice>0000</eng:Codice>

</eng:Firma-Info>

<eng:Firme>

<eng:Firma>

<eng:Tipo>S</eng:Tipo>

<eng:Codice-Fiscale>MZZRRT40S03F205F</eng:Codice-Fiscale>

<eng:Nome>NOME</eng:Nome>

<eng:Cognome>COGNOME</eng:Cognome>

<eng:Verifiche>

<eng:Esito-Verifica eng:tipo-verifica="VERSAMENTO" eng:id="2144572">

<eng:Codice>1111100</eng:Codice>

```
      <eng:Controllo-Crittografico>POSITIVO</eng:Controllo-Crittografico>
      <eng:Controllo-Certificato-Valido>POSITIVO</eng:Controllo-Certificato-Valido>
      <eng:Controllo-Certificato-Qualificato>POSITIVO</eng:Controllo-Certificato-Qualificato>
      <eng:Controllo-Catena-Trusted>POSITIVO</eng:Controllo-Catena-Trusted>
      <eng:Controllo-Certificate-Revocation-List>POSITIVO</eng:Controllo-Certificate-Revocation-List>
      <eng:Controllo-Timestamp>NON_APPLICABILE</eng:Controllo-Timestamp>
      <eng:crlFile>432994</eng:crlFile>
    </eng:Esito-Verifica>
  </eng:Verifiche>
</eng:Firma>
<eng:Firma>
  <eng:Tipo>T</eng:Tipo>
  <eng:Verifiche>
    <eng:Esito-Verifica eng:tipo-verifica="VERSAMENTO" eng:id="2144573">
      <eng:Codice>1141110</eng:Codice>
      <eng:Controllo-Crittografico>POSITIVO</eng:Controllo-Crittografico>
      <eng:Controllo-Certificato-Valido>POSITIVO</eng:Controllo-Certificato-Valido>
      <eng:Controllo-Certificato-Qualificato>NEGATIVO</eng:Controllo-Certificato-Qualificato>
      <eng:Controllo-Catena-Trusted>POSITIVO</eng:Controllo-Catena-Trusted>
      <eng:Controllo-Certificate-Revocation-List>POSITIVO</eng:Controllo-Certificate-Revocation-List>
      <eng:Controllo-Timestamp>POSITIVO</eng:Controllo-Timestamp>
      <eng:crlFile>432963</eng:crlFile>
    </eng:Esito-Verifica>
  </eng:Verifiche>
</eng:Firma>
<eng:Firma>
  <eng:Tipo>S</eng:Tipo>
  <eng:Codice-Fiscale>MZZRRT40S03F205F</eng:Codice-Fiscale>
  <eng:Nome>NOME</eng:Nome>
  <eng:Cognome>COGNOME</eng:Cognome>
  <eng:Verifiche>
    <eng:Esito-Verifica eng:tipo-verifica="CONSERVAZIONE" eng:id="2150853">
      <eng:Codice>11111011</eng:Codice>
      <eng:Controllo-Crittografico>POSITIVO</eng:Controllo-Crittografico>
      <eng:Controllo-Certificato-Valido>POSITIVO</eng:Controllo-Certificato-Valido>
      <eng:Controllo-Certificato-Qualificato>POSITIVO</eng:Controllo-Certificato-Qualificato>
      <eng:Controllo-Catena-Trusted>POSITIVO</eng:Controllo-Catena-Trusted>
      <eng:Controllo-Certificate-Revocation-List>POSITIVO</eng:Controllo-Certificate-Revocation-List>
      <eng:Controllo-Timestamp>NON_APPLICABILE</eng:Controllo-Timestamp>
      <eng:crlFile>433502</eng:crlFile>
    </eng:Esito-Verifica>
  </eng:Verifiche>
</eng:Firma>
```

```
          </eng:Firme>
         </eng:FileInfo>
        </sincro:EngInfo>
       </sincro:EmbeddedMetadata>
     </sincro:MoreInfo>
   </sincro:File>
 </sincro:FileGroup>
 <sincro:Process>
   <sincro:Agent sincro:type="organization" sincro:role="PreservationManager">
     <sincro:AgentName>
       <sincro:FormalName>Engineering Ingegneria Informatica S.p.A.</sincro:FormalName>
     </sincro:AgentName>
     <sincro:Agent_ID sincro:scheme="TaxCode">IT:05724831002</sincro:Agent_ID>
   </sincro:Agent>
   <sincro:TimeReference>
     <sincro:AttachedTimeStamp sincro:normal="2018-05-16T13:42:11.222+02:00"></sincro:AttachedTimeStamp>
   </sincro:TimeReference>
   <sincro:MoreInfo sincro:XMLScheme="ns://eng-sincro/TagEng.xsd">
     <sincro:EmbeddedMetadata>
       <sincro:EngInfo>
         <eng:ProcessInfo>
           <eng:Blocca-Crl-Scadute eng:time="0">si</eng:Blocca-Crl-Scadute>
           <eng:Catena-Trust>si</eng:Catena-Trust>
           <eng:Certificato-Valido>si</eng:Certificato-Valido>
           <eng:Controllo-Crl>si</eng:Controllo-Crl>
           <eng:Verifica-Crittografica>si</eng:Verifica-Crittografica>
           <eng:Verifica-Timestamp>si</eng:Verifica-Timestamp>
         </eng:ProcessInfo>
       </sincro:EngInfo>
     </sincro:EmbeddedMetadata>
   </sincro:MoreInfo>
 </sincro:Process>
</sincro:IdC>
```

➔ Torna al Sommario

6.5 Pacchetto di Distribuzione

Il sistema permette all'utente la ricerca e la visualizzazione degli oggetti conservati.

La visualizzazione avviene tramite un sistema di autenticazione e autorizzazione anche da remoto. L'oggetto che il sistema genera per la consultazione è il Pacchetto di Distribuzione (PdD) che viene confezionato dal Servizio di Conservazione secondo quanto previsto dalla normativa vigente.

L'accesso ai documenti avviene tramite una serie di servizi web service (WS) esposti dall'applicazione (in modalità sicura) che restituiscono:

- il documento conservato all'interno dell'archivio a norma;
- le prove di conservazione (idPdA).

Se il Cliente lo richiede può essere effettuata una ricerca massiva con produzione di specifico PdD veicolato al cliente o sotto forma di supporto o tramite canali precedentemente definiti dal Responsabile del Servizio di Conservazione.

Il Pacchetto di distribuzione relativo ad un PdA è composto da:

- idPdA.xml.p7m (firmato dal RdC);
- idPdA.xml.tsr (marca temporale);
- RdV del (o dei) PdV relativi ai documenti presenti nel PdD;
- dati e metadati (collocati su file XML);
- documento o documenti di cui l'indice idPdA (in sequenza).

➔ Torna al Sommario

7 Processo di conservazione

7.1 Descrizione del servizio

Nel seguito una breve descrizione delle caratteristiche principali del Servizio di Conservazione a Norma erogato dall'outsourcer:

- **Conservazione a Norma dei documenti**: memorizzazione dei documenti informatici inviati dal Cliente su un supporto di cui sia garantita l'integrità e la leggibilità nel tempo secondo le prescrizioni stabilite dalla normativa vigente in materia, con le modalità, nei tempi e limiti definiti contrattualmente. Il servizio comprende la verifica periodica dell'integrità dei documenti, l'eventuale riversamento diretto e le attività necessarie per le ottemperanze fiscali, ove richiesto.
- **Consultazione dei documenti conservati a Norma**: ricerca e visualizzazione dei documenti inviati in conservazione. Tale servizio ed il relativo software di visualizzazione è garantito per il tempo definito contrattualmente per la Conservazione a Norma dei documenti.
- **Produzione di supporti dei documenti conservati a Norma**: il servizio consiste nella generazione e invio di supporti fisici a Norma contenenti i Pacchetti di Distribuzione, a seguito di una specifica richiesta del Cliente.
- **Riversamento dei documenti**, su richiesta esplicita del Cliente, secondo quanto stabilito contrattualmente e definito successivamente.

Il processo di conservazione è erogato utilizzando le infrastrutture tecnologiche dell'outsourcer Engineering Ingegneria Informatica S.p.A. che soddisfano i requisiti di alta affidabilità richiesti dalla normativa.

Il servizio è erogato su due siti per garantirne la continuità:

- **Primario**: Settimo Torinese (TO) presso il Data Center di Intesa Sanpaolo

  Viale della Costituzione, 3 – 10036 Settimo Torinese (TO)
- **Secondario**: Firenze presso il Data Center di Intesa Sanpaolo

  Via della Toscana, 31 – 50127 Firenze (FI)

Si descrive di seguito il processo di Conservazione.

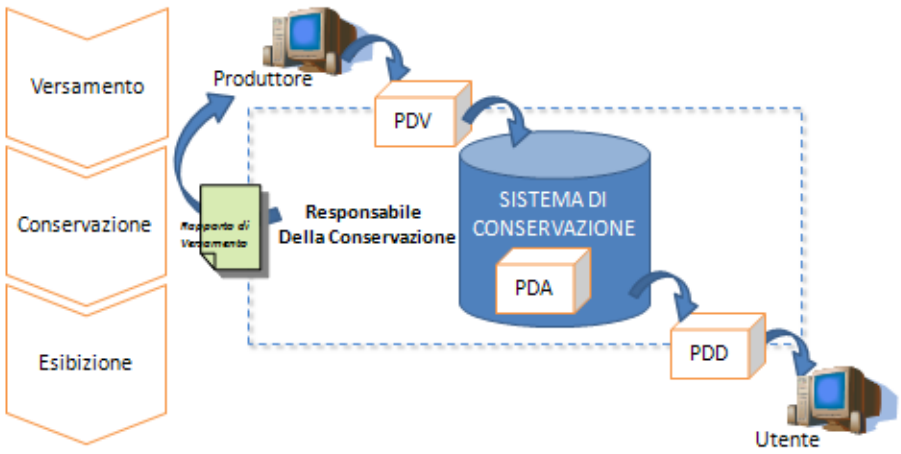

Figura 3 - Schema del processo di conservazione

➔ Torna al Sommario

7.2 Attivazione e chiusura del Servizio

Il Servizio di Conservazione a Norma per ogni Cliente/Famiglia Documentale viene attivato al termine di un processo di configurazione che segue queste fasi fondamentali:

a) reperimento dal produttore (Cliente o utente interno) delle informazioni tecniche propedeutiche all'attivazione del servizio:
   - tipologia di famiglie di documenti da conservare (fatture attive, fatture passive, libri fiscali, etc.);
   - informazioni anagrafiche dell'azienda (Ragione Sociale e Partiva IVA);
   - indicazione della chiave univoca e della logica di numerazione utilizzata per effettuare il controllo di consecutività della numerazione dei documenti (laddove richiesto);
   - dati del produttore;
   - tempi di conservazione;
   - specifica dei metadati da associare ai documenti;

b) definizione e configurazione dei PdV;

c) validazione delle configurazioni da parte del Responsabile del Servizio di Conservazione;

d) configurazione ambiente di test;

e) ricezione ed elaborazione Pacchetti di Versamento da conservare in ambiente di Test;

f) configurazione ambiente di produzione e start-up del servizio;

g) attivazione canali di comunicazione per la ricezione dei Pacchetti di Versamento e produzione del Rapporto di Versamento.

Ognuna delle fasi sopra indicate viene eseguita per ogni tipologia di configurazione e tipologia documentale richiesta.

Nella fase di attivazione del servizio vengono definiti canali utilizzati per lo scambio informativo tra Produttore e Conservatore. Tali canali avranno caratteristiche di sicurezza ed identificazione del mittente:

- SFTP
- https
- Certificato lato Client
- Ecc.

Il canale utilizzato e relativi livelli di servizio sono definiti nell'allegato Specificità del Contratto.

Il processo di **cessazione** del Servizio di Conservazione per ogni Cliente/Famiglia Documentale segue queste fasi principali:

a) condivisione informazioni tecniche di richiesta cessazione;

b) consolidamento delle informazioni tecniche propedeutiche alla cessazione del servizio, definizione della data formale di cessazione;

c) notifica della chiusura e delle sue modalità al Responsabile del Servizio di Conservazione;

d) cessazione tecnica;

e) attivazione di un piano di riversamento su richiesta del cliente.

Le modalità di riversamento previste, sono riportate più avanti nel presente capitolo.

➔ Torna al Sommario

7.3 Controlli sulla ricezione dei PdV

La corretta ricezione dei PdV, proveniente dal Produttore/Cliente, è monitorata dal Servizio Sistemistico dell'outsourcer tramite presidio del canale di comunicazione concordato.

In caso di anomalie il Supporto Operativo prende in carico la segnalazione proveniente dal Servizio Sistemistico dell'outsourcer, contattando i riferimenti tecnici del cliente.

➔ Torna al Sommario

7.4 Verifiche del pacchetto di versamento

Il processo di conservazione dei documenti prevede il mantenimento nel tempo di un insieme di evidenze informatiche (documenti e metadati) contenute nel pacchetto di versamento.

Queste evidenze comprovano l'integrità dei dati e l'autenticità dei documenti firmati digitalmente dal Produttore.

All'atto della ricezione dei documenti contenuti all'interno del PdV, il sistema esegue le seguenti operazioni:

- Controlli pregiudiziali (propedeutici alla conservazione):
  - Verifica della presenza dei metadati minimi e di quelli concordati;
  - Verifica della correttezza dell'impronta hash del documento ricevuto;
  - Verifica del formato del documento con quanto concordato col Produttore;
  - Verifica della firma digitale su ogni documento. Il sistema non solo verifica le firme presenti su tutti i documenti inviati ed acquisisce le informazioni sulla validità e scadenza dei certificati, ma permette di eseguire specifiche azioni a fronte di questi controlli. Ad esempio è possibile dare precedenza all'invio in conservazione a quei documenti il cui certificato di firma è prossimo alla scadenza.
- Altri controlli attivabili:
  - specifici relativi alla tipologia di documento da inviare in conservazione;
  - possibilità di definire ulteriori controlli che sono concordati con il Cliente in sede contrattuale e definiti nella fase di attivazione del servizio.

Nel caso in cui uno di questi controlli abbia un esito negativo si genera un'eccezione che può essere gestita come:

- **warning**: si segnala che c'è una difformità rispetto a quanto atteso, ma il processo prosegue nella conservazione;
- **error**: l'esito ha generato un blocco del processo per lo specifico pacchetto/documento e necessita di un intervento da parte del Supporto Operativo (p.e. il controllo dell'hash è bloccante).

Un controllo pregiudiziale genera sempre un errore bloccante.

Le operazioni di versamento, come tutte le operazioni di rilievo normativo, vengono tracciate in specifici log applicativi, su tabelle del database ovvero su file system, a seconda della tipologia delle informazioni ivi contenute.

I log memorizzati su database vengono mantenuti online per tutta la durata del periodo di conservazione, mentre quelli su file system vengono opportunamente suddivisi per mese / anno per una maggior facilità di consultazione.

Esempio di log delle operazioni riguardanti le interazioni con l'esterno (con documenti esito negativo per doppia chiave primaria):

ID	Data	Operazione	User	Ruolo	ID oggetto	Cliente	Chiave logica	Esito
713308	13/07/2017 22:16	CENSIMENTO	usr_vers	Versatore	450451	Cliente 1	CONS201707120151000	OK
768392	13/07/2017 23:11	VERSAMENTO	usr_vers	Versatore	238737049	Cliente 2	3960620170712CAMVA111145330	OK
1107672	30/06/2017 17:18	RECUPERO	usr_recupero	Versatore				KO
1107660	30/06/2017 11:46	RECUPERO	usr_recupero	Recuperatore	231196691	Cliente 3	15_2016_File79	OK

➔ Torna al Sommario

7.5 Accettazione o Rifiuto del PdV

Qualora i controlli precedentemente descritti sui documenti ricevuti abbiano dato **esito positivo**, il sistema:

- memorizza i documenti nella propria base dati di lavoro e sono disponibili per essere inseriti in un PdA;
- procede alla costruzione del PdA conformemente alle regole specifiche per la tipologia di documento;
- predispone i dati per la restituzione al sistema mittente degli esiti di avvenuta presa in carico del documento (Rapporto di Versamento).

Nel caso in cui venga rilevato un **esito negativo** di uno dei controlli sui documenti ricevuti, il sistema può procedere un tre differenti modalità:

1. Accettazione parziale del PdV: se “esito negativo” ha gravita “ERRORE” si rifiuta il documento e si segnala nel RdV l’impossibilità di conservare il documento e se ne tiene traccia nel RdV.
2. Accettazione dell’intero PdV: se “esito negativo” ha gavita “WARNING” si accetta l’intero contenuto del PdV e si tiene traccia del warning nei log Applicativi.
3. Rifiuto del PdV: se tutti i records contenuti nel PdV generano errore, oppure il PdV non risulta elaborabile (p.e. problemi di integrità) si rifiuta l’intero PdV e si genera un esito di ricezione con stato KO.

Nel terzo caso il mittente/cliente concorda con il Responsabile del Servizio di Conservazione una modalità per sanare l’errore. Le verifiche e controlli eseguiti vengono tracciati nel log applicativi che per loro natura conservano un riferimento temporale.

➔ Torna al Sommario

7.6 Rapporto di Versamento (RdV)

E’ un file XML generato in modo automatico alla chiusura della fase di controllo ed è relativo ad uno o più pacchetti di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo universale coordinato (UTC) e l’impronta relativa al PdV (o ai PdV) oltre alle chiavi univoche dei documenti eventualmente rifiutati.

Su tale XML si appone firma e marca temporale che avviene contestualmente alla sua creazione ed attesta il contenuto del PdV e l'istante in cui vengono terminate le attività di verifica.

Esempio di rapporto di versamento

```
<RDV id="351">
 <DataGenerazione>06072017</DataGenerazione>
 <PacchettiDiVersamento>
  <PDV>
   <NomePacchetto>CONS201706222xxxx.zip</NomePacchetto>
   <DataVersamento>06072017</DataVersamento>
   <Canale>FLUSSO</Canale>
   <DocumentiVersati>887</DocumentiVersati>
   <ElementiPDV>
    <ElementoPDV id="8276158" tipo="IDX_STD">
     <URN>IntesaSanPaolo:Paperless:2500:448530:INDICE.xml</URN>
     <Hash algoritmo="SHA-256" codifica="B64">kS09eBJW5HMuYzqJCLQbVO/v5PMBfUW/yYcVA2s61dI=</Hash>
     <Path>
      S3://000001/2500/001/PDV/CONS201706222500000-INDICE.xml
     </Path>
    </ElementoPDV>
    <ElementoPDV id="8276160" tipo="IDX_CLI">
     <URN>
      IntesaSanPaolo:Paperless:2500:448530:INDICE-CLIENTE.xml
     </URN>
     <Hash algoritmo="SHA-256" codifica="B64">RwgkIZ3FltYAyhxyCQBiAwji0nEnlBfa2oykX29Pbkg=</Hash>
     <Path>
      S3://000001/2500/001/PDV/CONS201706222500000-INDICE-CLIENTE.xml
     </Path>
    </ElementoPDV>
   </ElementiPDV>
   <Motivazione/>
  </PDV>
 </PacchettiDiVersamento>
</RDV>
```

Il Rapporto di Versamento viene conservato, memorizzato su DB e legato ai documenti che sono oggetto dei PDV a cui si riferisce. Sarà possibile risalire al RdV dal singolo documento ricercato.

Il sistema provvede ad un primo reperimento delle CRL di tutti i certificati TRUSTED corrispondenti ai certificati di firma al momento dei controlli che vengono eseguiti sul pacchetto di versamento. Avremo quindi tante CRL quante sono le autorità di certificazione riconducibili alle firme presenti sui documenti.

Le seconde CRL vengono invece reperite per consolidare la fase di costruzione del Rapporto di Versamento con l'assoluta certezza della validità dei certificati delle firme dei documenti ricevuti.

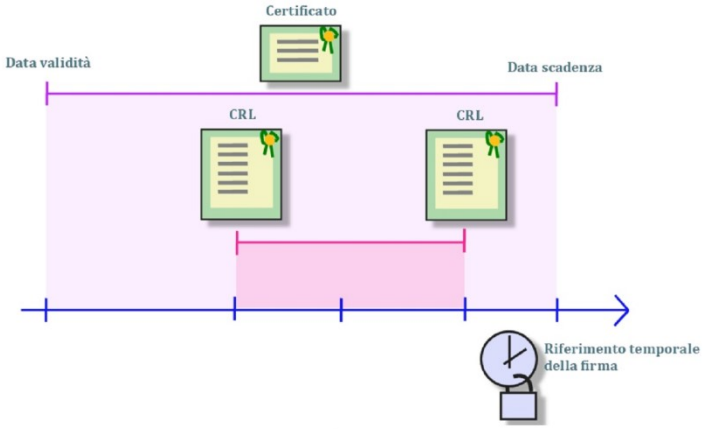

Figura 4 - Controllo CRL

➔ Torna al Sommario

7.7 Preparazione e gestione del Pacchetto di Archiviazione

Superate le fasi di controllo sui PdV e generazione del RdV, il sistema abilita l'esecuzione di una serie di regole completamente configurabili che permette la formazione del Pacchetto di Archiviazione (PdA), e riguarda in particolare:

- Dimensione del semilavorato (che formerà il pacchetto);
- Anzianità del documento (dal tempo di ingresso nel sistema);
- Firmato o non firmato (o certificato di firma in scadenza);
- Regole basate su specifici metadati (codice fiscale, mittente, …altro).
- PdA coincidenti con un PdV ricevuto

Opportuni allarmi segnalano la presenza di documenti che sono in attesa di conservazione e non vengono inclusi in nessuna regola di costruzione PdA.

Può essere anche attivato un processo di costruzione manuale del PdA, per eventuali documenti che non sono stati inclusi in nessun insieme di regole. Tale processo è tracciato a livello di inserimento singolo documento nel PdA nei file di log del sistema.

I documenti così lavorati e che hanno superato le fasi precedenti, concorrono a formare il PdA, che è assemblato dal sistema nei tempi e con i criteri di raggruppamento scelti e concordati in fase di attivazione del servizio di conservazione.

Il PdA si forma contestualmente alla creazione del suo indice; il processo è descritto nei punti seguenti:

a) Creazione dell'indice xml (in formato Sincro) relativo al blocco di documenti da inviare in conservazione.

b) Reperimento delle prove di conservazione (certificati trusted delle firme dei documenti, CRL dei certificati) per la totalità dei documenti firmati presenti nel Pacchetto, che verranno inserite nel "more info" dell'indice.

c) Sottoscrizione dell'indice xml (in formato Sincro) con firma digitale del Responsabile della Conservazione e successiva apposizione di una marca temporale per fornire data certa al Pacchetto di Archiviazione.

Al termine di queste fasi è formato il PdA che è costituito da un insieme di file comprovanti la autenticità dei documenti in conservazione.

L'indice del PdA è strutturato secondo lo standard e contiene:

- Informazioni varie previste dallo standard Sincro

- Per ogni documento:

  - Hash
  - Urn
  - Nel campo "more info": le CRL relative al documento e l'esito dei controlli effettuati.
  - Riferimento al RdV

La conservazione dei documenti digitali vera e propria ha inizio con la formazione del PdA e la costruzione dell'indice.

Una volta terminata la raccolta delle prove, queste vengono associate ai documenti conservati. A questo punto il sistema provvede a creare l'indice Sincro, sottoscriverlo ed apporre il timestamp definitivo di conservazione.

Parte integrante di questo processo è la sottoscrizione digitale dell'Indice (Sincro) da parte del Responsabile della Conservazione. In questa fase è inclusa anche l'apposizione di un "time-stamp", ovvero un riferimento temporale certificato che costituisce evidenza dell'esistenza e dell'esatta composizione del file collegato all'istante indicato.

Apponendo un timestamp all'indice lo si "sigilla" e contemporaneamente si fissa il riferimento temporale.

Con questo procedimento, dunque, si viene a costituire un riferimento temporale certificato per ognuno dei file inclusi nel PdA.

In conclusione di tale processo abbiamo il PdA così costituito:

- idPdA.xml.p7m (firmato dal RdC);

- idPdA.xml.tsr (marca temporale);

- dati e metadati;

- documento o documenti di cui l'indice idPdA (collocati su DB o filesystem).

➔ Torna al Sommario

7.8 Processo di esibizione tramite Pacchetto di Distribuzione

L'esibizione dei documenti avviene tramite autenticazione. Il sistema può rendere disponibili dei WS verso applicazioni chiamanti (di canale) che si occupano di gestire l'autenticazione e autorizzazione dell'utente richiedente.

L'utente può richiedere al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge. Tali informazioni vengono fornite ai soggetti autorizzati tramite l'accesso diretto, anche da remoto, al documento informatico conservato, attraverso la produzione di un pacchetto di distribuzione (PdD) selettivo tramite specifica ricerca nel sistema di Conservazione a Norma.

Per quanto riguarda l'attività di ricerca e l'esibizione a norma dei documenti conservati (anche a fronte di una verifica ispettiva da parte delle Autorità competenti) lo strumento di accesso all'archivio documentale a norma del Cliente è consentito dal WS esposto dall'applicazione. Il Cliente, tramite l'interfaccia messa a disposizione, può pertanto richiedere la visualizzazione di tutti i documenti conservati al fine di:

- Visionare e scaricare il documento conservato all'interno dell'archivio a norma;
- Verificare ed eventualmente scaricare le prove di conservazione (idPdA).

Il sistema di Conservazione a Norma può essere anche integrato con il sistema Documentale o altra applicazione del cliente per facilitare la fruizione del servizio di consultazione.

Se il Cliente lo richiede può essere effettuata una ricerca massiva con produzione di specifico PdD veicolato al cliente o sotto forma di supporto o tramite canali precedentemente definiti.

Il Pacchetto di distribuzione relativo ad un PdA risulta quindi composto da:

- idPdA.xml.p7m (firmato dal RdC)
- idPdA.xml.tsr (marcato temporalmente)
- dati e metadati (collocati su file di testo)
- documento o documenti di cui l'indice idPdA (in sequenza)
- RdV (relativo ai documenti contenuti nel PdA)

Il sistema di conservazione documentale è soggetto a meccanismi di protezione dei dati che transitano in rete, in modo da impedire accessi fraudolenti o non autorizzati. Tale protezione è realizzata mediante apparati di sicurezza che analizzano il traffico e su base di specifiche regole di abilitazione viene consentito il flusso di dati strettamente necessario al funzionamento dell'applicazione.

➔ Torna al Sommario

7.9 Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del Pubblico Ufficiale nei casi previsti

7.9.1 Produzione di duplicati

Per produzione di duplicati si intende l'effettuazione di una copia dei documenti conservati da un supporto ad un altro senza che ciò comporti una alterazione del contenuto digitale dei medesimi.

La duplicazione può essere realizzata liberamente dall'outsourcer, in quanto la normativa non prevede, al riguardo, specifiche prescrizioni formali. È una attività, ammessa dalla normativa di riferimento e consta, ad esempio, della generazione di copie di sicurezza.

Con la duplicazione viene effettuata quella che in termini tecnici viene definita clonazione del supporto, ossia, viene generato un supporto identico sia nel contenuto che nella rappresentazione dei file.

Ai fini dell'interoperabilità sarà possibile generare Pacchetti di Distribuzione coincidenti con i pacchetti di archiviazione. Questa modalità potrà essere utilizzata dal cliente per effettuare una duplicazione dei Pacchetti di Archiviazione.

L'operazione viene eseguita su richiesta del Cliente e si effettua creando un flusso per ogni Pacchetto di Archiviazione, contenente

- tutti i documenti presenti nel PdA
- la marca sincro del PdA
- le prove di conservazione del PdA

Nel caso in cui le verifiche periodiche evidenzino anomalie di leggibilità di documenti conservati, viene eseguita copia dei documenti utilizzando i dati presenti nell'archivio digitale o secondario o di Back Up.

7.9.2 Produzione di copie informatiche

Per produzione di copie informatiche si intende l'effettuazione di una copia dei documenti conservati da un supporto ad un altro con una alterazione del contenuto digitale dei medesimi. Questa è una attività ammessa dalla normativa, nel caso in cui si voglia ad esempio aggiornare tecnologicamente l'archivio sostitutivo per garantire la possibilità di esibizione della documentazione a fronte di innovazioni tecnologiche (es: obsolescenza dei formati). In questo caso occorre l'attestazione, con l'apposizione della propria firma digitale, di conformità all'archivio esistente da parte di Pubblico Ufficiale che viene coinvolto dal Responsabile della Conservazione, che ha in carico il processo di riversamento.

A differenza della duplicazione, la copia informatica è espressamente disciplinata dalla normativa di riferimento e prevede 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 della Conservazione.

Le attività operative previste per un processo di produzione di copie informatiche sono:

1. preparazione di un Piano in cui sono accuratamente descritte le motivazioni che hanno richiesto la copiatura, tutte le attività che saranno svolte durante la

copiatura, il formato di origine e quello di destinazione dei documenti, le applicazioni informatiche utilizzate e gli accorgimenti di sicurezza adottati per garantire l'affidabilità e la sicurezza della copiatura. Il Piano deve essere condiviso e approvato dal Responsabile della Conservazione e dal Cliente;
2. estrazione dall'archivio di conservazione in essere di tutti i documenti oggetto di copiatura (in linea di principio, una copia informatica viene effettuata sull'intero archivio di conservazione) e di tutti gli indici di ricerca associati a ciascun documento;
3. creazione di un report di controllo con l'elenco dettagliato di tutti i documenti che saranno copiati, e validazione dell'elenco con il Cliente;
4. implementazione della procedura di conversione che eseguirà la trasformazione del formato dei documenti e/o degli indici (in linea di principio, si presuppone la realizzazione di procedure totalmente batch e automatizzate, che durante l'esecuzione non richiedano l'intervento manuale di utenti o operatori);
5. esecuzione della procedura di conversione (questa attività può ovviamente richiedere tempi variabili in funzione della quantità di documenti da sottoporre a copiatura);
6. reimportazione dei documenti riversati nel sistema di conservazione di origine, oppure all'interno di un nuovo sistema.

7.9.3 Intervento del Pubblico Ufficiale

Il coinvolgimento di un Pubblico Ufficiale esperto in processi di conservazione può essere richiesto al fine di:

a) validare il piano di acquisizione o cessione

b) verificare che il processo di trasformazione del formato dei documenti non alteri il contenuto e la forma dei documenti stessi;

c) validare il processo di apposizione delle firme digitali sui documenti acquisiti in conformità con le normative vigenti.

➔ Torna al Sommario

7.10 Scarto dei pacchetti di archiviazione

Alla scadenza dei termini di conservazione relativi alla specifica tipologia documentale e comunque definiti in sede contrattuale con il Cliente, avviene lo scarto del Pacchetto di Archiviazione dal sistema di Conservazione a Norma.

Per dare la possibilità di poter prolungare i termini di conservazione prima dello scarto, verrà data informativa al produttore con congruo anticipo (almeno 6 mesi) al fine di confermare la cancellazione ovvero mantenere in conservazione i PdA per un ulteriore anno.

Il Responsabile delle Conservazione del produttore ha la possibilità di richiedere lo scarto di tutti o alcuni i PdA segnalati dal sistema, tramite approvazione con propria firma digitale

La cancellazione avverrà soltanto dopo che sono state eseguite le fasi di approvazione esplicita da parte del Responsabile della Conservazione del Cliente.

➔ Torna al Sommario

7.11 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori

Per interoperabilità si intende la capacità di cedere o acquisire copie o duplicati dei documenti conservati, da un supporto ad un altro senza che ciò comporti una alterazione del contenuto digitale dei medesimi e del valore degli stessi.

Tale procedimento, in carico del Responsabile del Servizio verrà concordato con il Responsabile della Conservazione (del Cliente) dei documenti oggetto di "travaso". Viene eseguito normalmente su richiesta del Cliente e si effettua mediante generazione dell'ISO oppure altro metodo da definire con il Cliente (ed eventualmente con l'altro Conservatore).

Se nel processo di acquisizione risultasse necessario una "trasformazione" dei documenti o dei PdA forniti, sarà necessario effettuare una copia dei documenti conservati da un supporto ad un altro con una alterazione del contenuto digitale dei medesimi. Questa è una attività ammessa dalla normativa, nel caso in cui si voglia ad esempio aggiornare tecnologicamente l'archivio sostitutivo per garantire la possibilità di esibizione della documentazione a fronte di innovazioni tecnologiche. In questo caso potrebbe essere necessaria l'apposizione di una ulteriore firma digitale, o l'attestazione di conformità all'archivio esistente da parte di Pubblico Ufficiale che viene coinvolto dal Responsabile della Conservazione (del Cliente) o del Servizio di Conservazione.

Per procedere all'acquisizione di documenti che risiedono presso altro conservatore, tramite un "travaso massivo" sia di copie che di duplicati informatici sarà necessario definire una mappatura dei dati o metadati forniti dal conservatore cedente ed acquisiti dal nuovo conservatore.

La procedura di import prevede:

- la costruzione di nuovi PdA a partire dai PdD forniti dal cedente che dovranno risultare coincidenti con i PdA (conservati dal conservatore cedente);
- il popolamento della base dati dei metadati a partire dal db export dati del cedente.

La procedura prevede una fase di quadratura pre e post migrazione, sotto la supervisione del Responsabile del Servizio di Conservazione.

➔ Torna al Sommario

8 Il Sistema di Conservazione

8.1 Applicativo di Conservazione

Il sistema software utilizzato per la gestione del processo di conservazione legale dei documenti digitali è costituito da un prodotto SW di Engineering, interamente (ed internamente) realizzato e manutenuto.

E' un sistema integrato e completo per la conservazione a norma dei documenti informatici ed è realizzato per "lavorare" su un sistema di storage ad oggetti, una tecnologia appositamente introdotta per questa tipologia di servizio.

Il pacchetto software esegue la conservazione nel tempo dei documenti informatici e presenta le seguenti caratteristiche generali:

- Completezza - presenza di qualsiasi documento emesso
- Robustezza - garanzia di consistenza dei dati inseriti
- Sicurezza - protezione dalla manipolazione non autorizzata dei dati
- Affidabilità - indipendenza dai guasti dell'hardware
- Chiarezza - facilità di consultazione secondo diversi criteri di ricerca

garantendo:

- la completezza e l'inalterabilità dei documenti inviati in conservazione
- la possibilità di verifica dell'integrità dei documenti conservati
- i riferimenti temporali certi.

Inoltre è in grado di gestire diverse tipologie di documenti, relativi a diversi ambiti applicativi, e diversi formati, per esempio:

- Documenti di sportello bancario
- Contratti ed allegati
- Fatture attive e Fatture passive
- Libri e registri sociali
- Libri e registri contabili
- Libri e registri assicurativi
- Assegni
- Mandati di pagamento e Reversali d'incasso
- Ricevute e quietanze di pagamento
- Delibere, determine, atti e provvedimenti
- Altro…

Ognuna di queste tipologie è caratterizzata da specifici metadati e apposite regole, definibili in modo parametrico, che consentono di gestire insiemi di documenti omogenei.

Il sistema è progettato per partizionare in maniera opportuna i dati gestiti al fine di garantire la separazione per contesto organizzativo o utente.

Il partizionamento opera tra i dati di Aziende diverse o di diversi dipartimenti o uffici afferenti ad una stessa Azienda I fascicoli e documenti, provenienti anche da flussi diversi di conservazione, identificati univocamente tramite una chiave primaria, fin dal loro ingresso in conservazione.

Il sistema di partizionamento è direttamente collegato al sistema di controllo degli accessi e tracciatura, viene quindi garantita la riservatezza dei dati presenti in archivio.

Tutti i documenti sono disponibili on-line, congiuntamente alle rispettive prove di conservazione, per le funzioni di ricerca ed esibizione, così come previsto dalla normativa vigente. La struttura architetturale del prodotto consente di definire diversi livelli operativi e garantisce che ciascuna Azienda/Ente, Area Organizzativa, Agenzia, Ufficio, Dipartimento, ecc. possa accedere solo ed esclusivamente ai suoi documenti, in base alle credenziali e alle politiche di accesso attivate.

Il pacchetto software prevede la conservazione singola e/o cumulativa, dei documenti elettronici firmati ed implementa un formato di composizione delle marche tale da permettere l'esibizione probatoria di un singolo documento.

Ogni singolo file può essere esibito insieme ai suoi metadati, registrati nel data base, e alle sue prove di conservazione in maniera assolutamente INDIPENDENTE dagli altri documenti. Infatti, nei file contenenti le prove di conservazione, associati ad ogni pacchetto di archiviazione, l'unico riferimento ai file originali è l'hash del documento stesso, che non ha quindi nessun vincolo di riservatezza.

➔ Torna al Sommario

8.2 Componenti logiche

L'applicazione è logicamente divisibile in 5 principali gruppi:

- Versamento
- Conservazione
- Verifiche e allarmi
- Esibizione
- Console di Gestione

8.2.1 Versamento

La parte di versamento è in grado di ricevere i documenti tramite 2 principali modalità :

Versamento massivo tramite flussi di documenti

Versamento singolo, tramite WebService

Si occupa di effettuare le verifiche iniziali e la creazione del RdV (verifica del formato, firma etc) e di recupero da internet delle CRL.

8.2.2 Conservazione

E' la parte che si occupa di tutti i processi di conservazione, in particolare

- Verifica del documenti ai fini della conservazione: ricalcolo e confronto hash, verifiche di firma, etc.
- Reperimento e verifica delle prove di conservazione: controllo catena trusted, CRL, etc.
- Creazione PdA
- Firma del RdC
- Apposizione marche temporali

8.2.3 Verifiche e allarmi

Tramite questa componente si rende possibile l'assoluta coerenza del sistema e di tutti i suoi processi. Un sistema di allarmi provvede infatti ad informare tempestivamente il personale addetto al presidio dell'eventuale presenza di un problema, o più semplicemente di un ritardo nelle fasi elaborative. Gli allarmi sono configurabili in base a diversi parametri e per ciascuna fase elaborativa. Gli allarmi arrivano per e-mail e contengono:

- Nel Subject: una breve descrizione del problema e della sua gravità
- Nel body: possono contenere il dettaglio del problema rilevato

Alcuni esempi di allarmi

- Presenza di documenti non conservati ad una certa ora. Questo allarme scatta nel caso in cui, ad una certa ora, almeno un documento non abbia raggiunto lo stato di "conservato". Nel subject della mail è presente una sintesi del problema (ad esempio: presenza di 2 documenti non conservati). Nel body della mail troviamo l'elenco di tutti i documenti, per un veloce riscontro
- Documenti di un determinato Cliente non pervenuti. Ad esempio, nel caso in cui un Cliente spedisca i suoi documenti sempre ad una determinata ora oppure entro un cut-off, questo allarme è utile ad individuare un eventuale problema nella spedizione dei documenti e induce il personale di presidio a verificare eventuali problemi di connettività o di file transfer

8.2.4 Esibizione

La parte di esibizione di occupa di garantire il reperimento dei documenti conservati e delle prove della loro conservazione nel tempo. L'esibizione può essere richiesta in 3 diverse modalità:

- WebService; tipicamente tramite un applicativo, che fa richiesta del documento e/o delle sue prove di conservazione
- Interfaccia WEB. L'utente può direttamente ricercare e scaricare file e prove di conservazione

- Supporti. Su richiesta del Cliente, è possibile la creazione di supporti digitali contenenti una selezione di documenti con le relative prove di conservazione

8.2.5 Console di Gestione

La console di gestione è l'applicativo web che consente di supervisionare tutte le funzionalità dell'applicazione ed è suddivisa in due grandi filoni

- Gestione applicativo
- Interrogazione contenuti

8.2.6 Gestione applicativo

La gestione dell'applicativo consente la configurazione e la gestione dei task, ovvero:

- Censimento e manutenzione delle tipologie documentali, metadati etc.
- Configurazione utenti, Clienti e loro abilitazioni e personalizzazioni
- Configurazione parametri generali dell'applicazione
- Gestione dei task, monitoraggio del sistema, stop / start dei servizi e dei singoli task

8.2.7 Interrogazione contenuti

La parte di interrogazione contenuti consente una piena navigabilità, con parametri di ricerca predefiniti e rende possibile la ricerca di documenti e files conservati, l'interrogazione ed il download dei documenti e delle loro prove di conservazione.

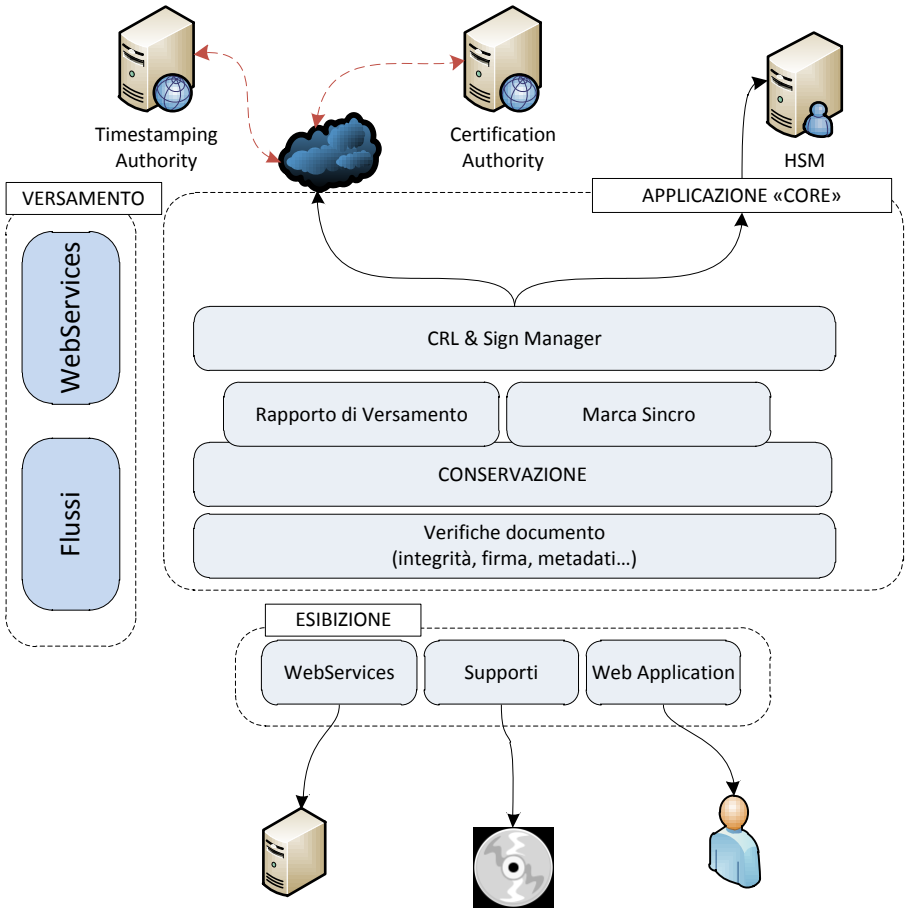

Figura 5 - Schema logico applicazione

➔ Torna al Sommario

8.3 Componenti tecnologiche

L'applicazione di conservazione è una applicazione Web a tre livelli (desktop, application e database) e utilizzabile da posti di lavoro dotati di sistema operativo Windows (XP, Vista o 7) o Linux, per mezzo di browser standard quali ad esempio Internet Explorer vers. 7 o superiore, Mozilla Firefox 3.6 o superiore, Google Chrome 11.0.696.7 o superiore, Apple Safari 5.0.5 o superiore. Per le postazioni che dovranno operare sulle funzionalità di firma è necessario che localmente siano attivi i driver del dispositivo di firma (lettore, smart card o token USB di firma, tablet per la firma grafometrica, ecc.), oppure che sia utilizzato un dispositivo HSM (Hardware Security Module) raggiungibile via rete.

Tutte le componenti applicative del sistema poggiano su una piattaforma architetturale uniforme:

- Java J2EE
- Framework ORM Hibernate
- Architettura SOA
- RDBMS

- Application server Wildfly 10+
- HCP (Hitachi Content Platform)

La base dati utilizzato è un data base relazionale interfacciato attraverso Hibernate e supporta Oracle RAC 11g Enterprise Edition.

Il bilanciamento applicativo è effettuato tramite Message Queue JMS (Active MQ).

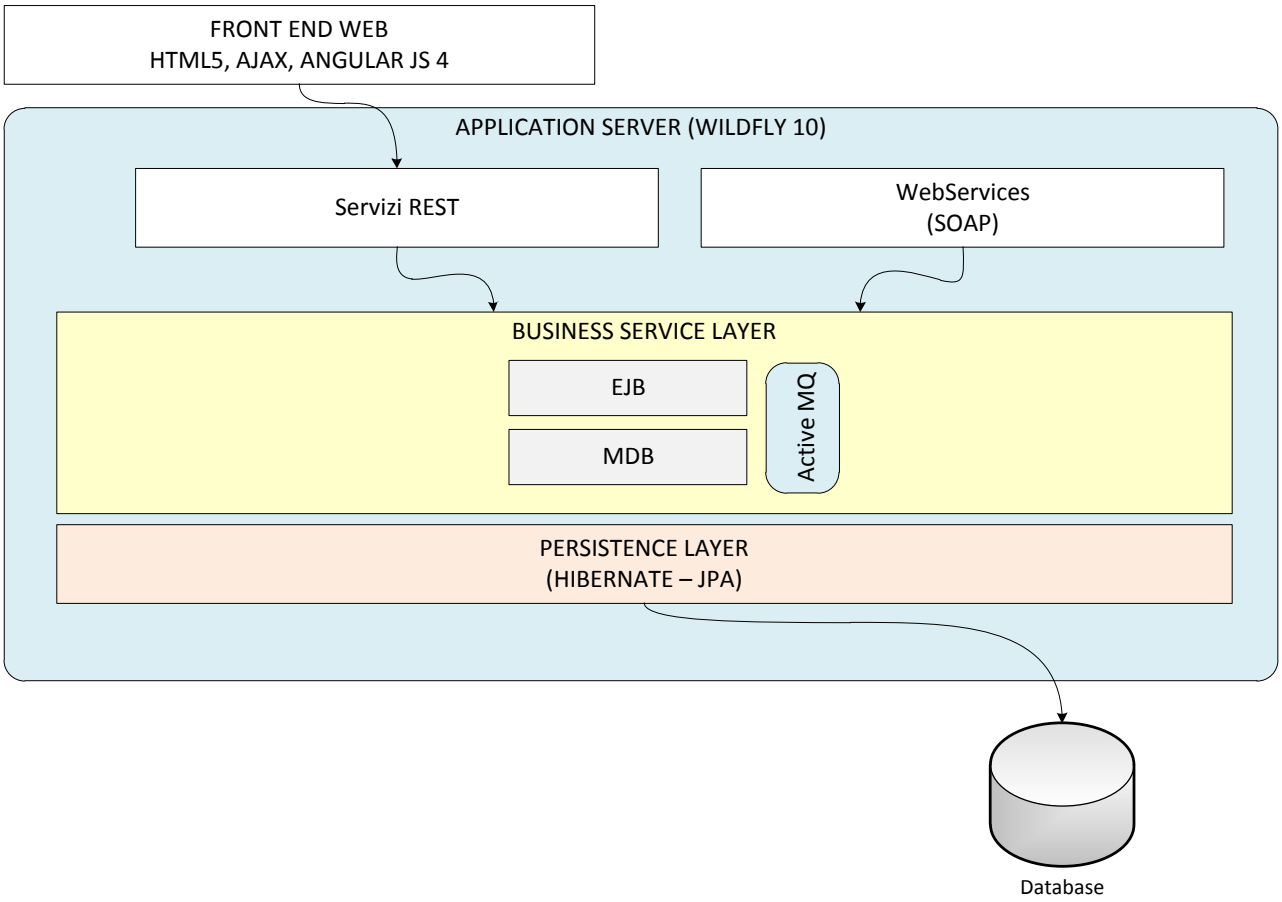

Figura 6 - Framework applicativo

➔ Torna al Sommario

8.4 Componenti fisiche

I Servizi di Conservazione sono erogati dall'outsourcer all'interno dei propri Data Center primario e secondario, attraverso i quali è in grado di offrire un servizio di alta qualità in termini di continuità ed affidabilità. Tale qualità è ottenuta grazie alle caratteristiche progettuali che hanno contraddistinto la realizzazione dei Data Center, con criteri focalizzati sempre sull'obiettivo di fornire ad ogni livello le massime garanzie di sicurezza e continuità, sia per quanto riguarda l'erogazione di energia elettrica, sia attraverso un opportuno condizionamento climatico, sia attraverso un adeguato meccanismo di

sicurezza fisica/ambientale (impianto antincendio e sorveglianza con allarmi 24x7), sia attraverso la ridondanza architetturale dei sistemi, delle infrastrutture di rete e delle connessioni verso l'esterno.

I criteri progettuali e realizzativi dei Data Center rispondono ai requisiti imposti ai datacenter di livello T4, livello massimo previsto dallo standard Uptime Institute Tier Standard.

Di seguito si riportano le principali caratteristiche dei Data Center:

- Ambiente protetto con accesso garantito solo al personale autorizzato.
- Linee elettriche doppie provenienti da rami diversi (doppia cabina elettrica, doppio G.E., doppi UPS).
- Sistema di raffreddamento ridondato.
- UPS ridondati e monitorati.
- Sistema per la rilevazione fumi e lo spegnimento incendi automatico.
- Pavimento flottante e canalizzazioni separate per l'impianto elettrico e cablaggio dati.

Le principali caratteristiche delle architetture deputate alla erogazione dei servizi sono riportate, invece, qui sotto:

- Architettura di switching layer 3 completamente ridondata con connessioni a 1Gbit/s o superiori.
- Sistemi Firewall ridondati, in diverse tecnologie.
- Storage Area Network centralizzata e ridondata con doppio fabric.
- Storage di classe Enterprise.
- Sistemi di RDBMS ridondati (principali fornitori di mercato).
- Backup Centralizzato attraverso LAN dedicata ad 1Gbit/s e via SAN.
- Sistema di Monitoring dello stato della rete, dei sistemi e dei servizi.
- Connessioni ad Internet tramite linee di differenti Carrier.
- Completa remotizzazione dei sistemi di amministrazione.

Di seguito riportiamo lo schema dell'architettura del Servizio di Conservazione a Norma.

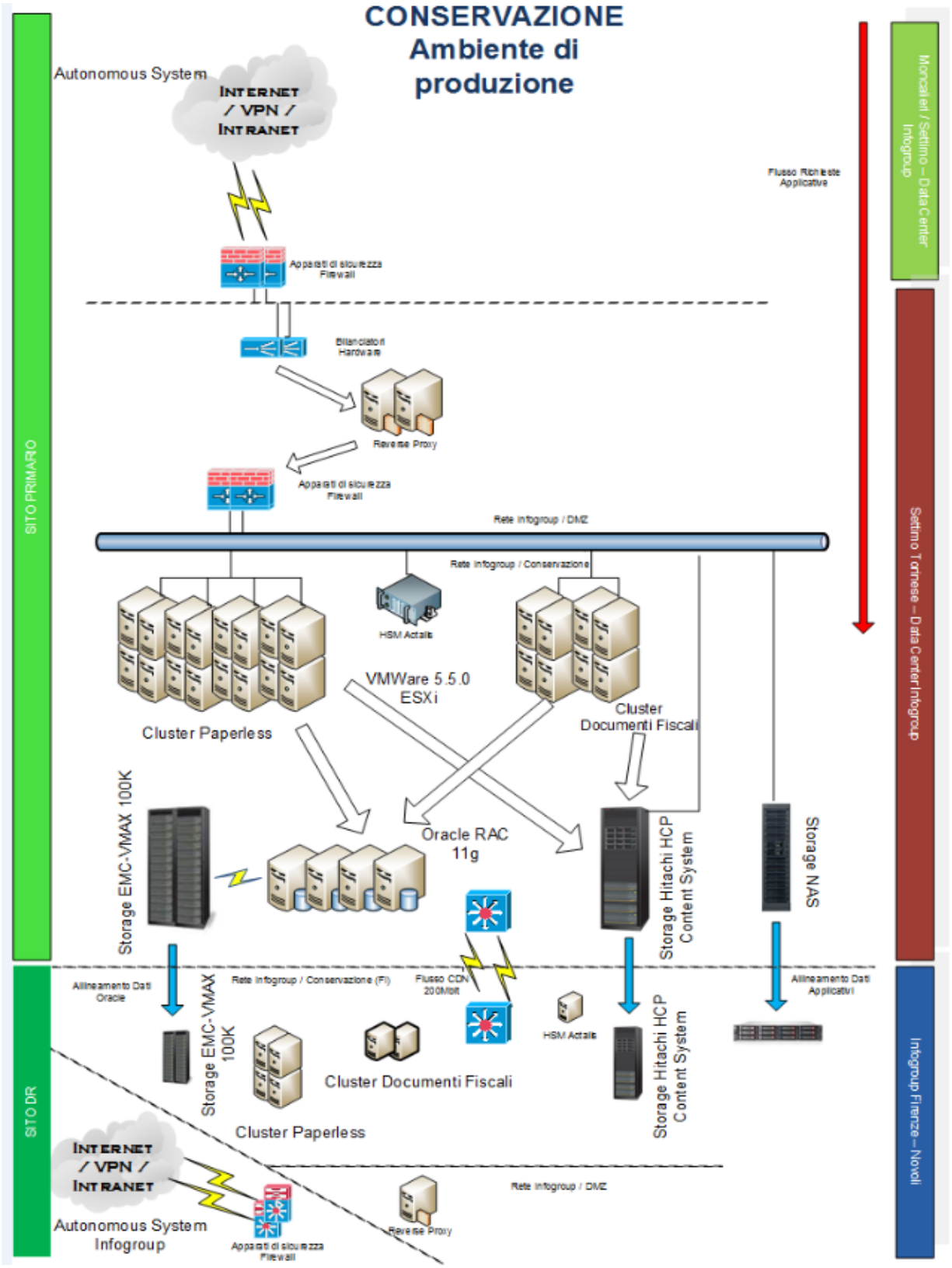

Figura 7 - Schema infrastruttura

➔ Torna al Sommario

8.5 Procedure di gestione e di evoluzione

L'erogazione del servizio è regolata dalle procedure di "ciclo di vita di una infrastruttura" e "ciclo di vita del SW".

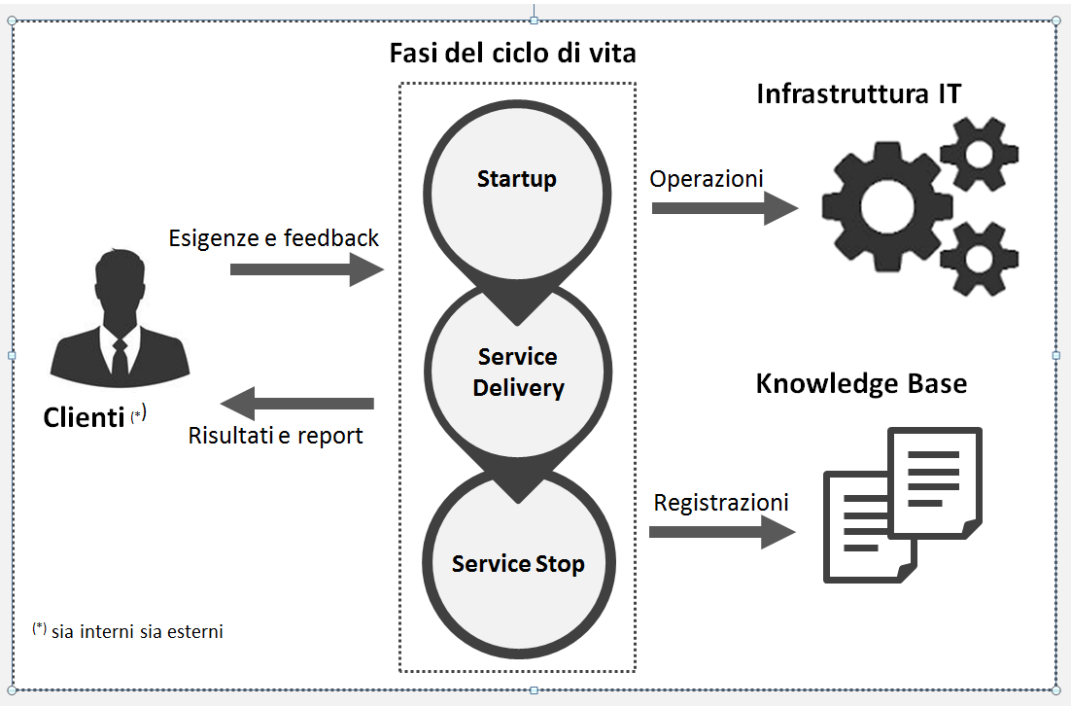

Figura 8 - Ciclo di vita del Servizio

Le procedure che regolano la gestione e l'evoluzione sono legate alla fase di Service delivery.

Nella fase Service Delivery:

- è assicurato il funzionamento del software, seguendo quanto dettato nei processi Incident Management, Change Management e Request Management,
- il software è allineato alle variazioni delle esigenze dei Clienti, seguendo quanto dettato nei processi Customer Relation Management e Change Management,
- sono individuate e messe in atto le azioni preventive e migliorative pertinenti il software, seguendo quanto dettato dai processi Review Management e Change Management.

La procedura centrale del processo di gestione è quella di Change management; queste richieste di change possono scaturire:

- da nuove esigenze dei Clienti,
- da una azione, migliorativa o preventiva, decisa in sede di review del software,
- per un workaround o per eliminarne le cause di un difetto del software.

Le richieste di change possono essere attivate dal Service Manager

Maggiori dettagli si trovano nelle procedure aziendali (iso9001)

8.5.1 Servizio di Supporto Operativo

Il Supporto operativo svolto dall'outsoucer rappresenta il Single Point of Contact relativo a tutte le segnalazioni provenienti dai clienti (Produttore e Utente) e strutture interne che possono accedere al servizio di Supporto operativo attraverso i canali concordati.

Il Supporto operativo dell'outsourcer, prende in carico la segnalazione tracciando opportunamente la richiesta nel Sistema di Trouble Ticketing (HDA), catalogando la segnalazione per tipologia e livello di gravità.

Sotto vengono riportate le tipologie selezionabili e i livelli di gravità gestiti:

Tipologie di Segnalazione:

- Incident;
- Change Request;
- Service Request.

Per la tipologia Incident vengono riportati sotto i livelli di Gravità, in ordine decrescente:

- Livello 4;
- Livello 3;
- Livello 2;
- Livello 1.

I Livelli di Gravità sono definiti in base all'impatto dell'incidente:

Descrizione	**Criticità**	**Caratteristiche per la classificazione**
Incidente	4	Evento che provoca (o può provocare) una interruzione di attività, un guasto, una perdita o una riduzione del servizio. L'evento è gestito
Malfunzionamento	3	Evento che compromette l'asset, ma in modo discontinuo
Incidente non bloccante	2	Evento dannoso che non ha impatti significativi rispetto al sistema di produzione, che continua, quindi a funzionare correttamente e completamente
Anomalia	1	Evento sporadico che non compromette gli asset e l'operatività dei processi

Sulla base dei contenuti della segnalazione, il Supporto operativo prende in carico la richiesta ed esegue quanto necessario per chiuderla autonomamente oppure la indirizza verso il livello specialistico competente per la sua risoluzione:

- Supporto Applicativo;
- Supporto Sistemistico.

In ogni caso è il Supporto operativo che comunica all'entità interessata la chiusura del ticket.

Le tipologie di **Change Request** scalabili al Supporto operativo sono:

- richiesta configurazione nuovi Clienti;
- richiesta configurazione nuove famiglie documentali;
- richiesta creazione nuovi report di servizio;
- modifica configurazione Clienti/famiglie documentali esistenti;
- modifica alla reportistica già esistente.

Le tipologie di **Service Request** scalabili al Supporto operativo sono:

- chiarimenti funzionali relativi all'utilizzo dell'interfaccia Web del sistema di conservazione;
- verifiche relative alla configurazione del servizio;
- richiesta produzione supporti.

Inoltre, nel caso in cui il sistema di Conservazione a Norma rilevi situazioni anomale dovute alla presenza di dati errati forniti dal Produttore (metadati non coerenti, problemi sui flussi, sequenze di numerazione non rispettate, ecc.), il Supporto operativo prende in carico l'anomalia, e può contattare il Produttore tramite i canali e le modalità concordate per la notifica e per eventuali azioni da intraprendere per la chiusura del ticket.

Il servizio di Supporto Operativo è attivo dal lunedì al venerdì dalle ore 08:30 alle ore 18:30.

8.5.2 Servizio di Supporto Applicativo

Il servizio di Supporto Applicativo dell'outsourcer ha lo scopo di assicurare il corretto funzionamento dell'applicativo di Conservazione a Norma ed opera di concerto con il Supporto Operativo (Back Office) per la gestione delle eventuali segnalazioni di malfunzionamento.

Il servizio, dietro indicazione del Responsabile del Servizio di Conservazione, mantiene aggiornata l'applicazione secondo le esigenze dei Clienti e secondo le evoluzioni della normativa vigente che regola la Conservazione a Norma.

Il Supporto Applicativo ha i seguenti compiti:

- monitoraggio applicativo;
- supporto specialistico di Assistenza Applicativa;
- produzione della reportistica di competenza;
- presa in carico delle Change Request provenienti dal Supporto Operativo;
- gestione delle Service Request provenienti dal Supporto Operativo.

Le principali tipologie di segnalazione gestite dal Supporto Applicativo sono:

- segnalazioni di malfunzionamenti generati dalla piattaforma di Conservazione;
- segnalazioni di malfunzionamenti dovuti ad un'errata formattazione dei pacchetti/documenti ricevuti del Produttore;
- problematiche relative ad aspetti funzionali sul processo che alimenta la piattaforma di Conservazione a Norma.

Il servizio di Supporto Applicativo è attivo in modalità 24x7.

8.5.3 Servizio Sistemistico

Il servizio ha lo scopo di assicurare il corretto funzionamento dell'infrastruttura tecnologica del Servizio di Conservazione a Norma e opera di concerto con il Supporto Operativo (Back Office) e il Supporto Applicativo per la gestione delle eventuali segnalazioni di malfunzionamento.

Di seguito sono elencate in sintesi le principali attività svolte dal Servizio Sistemistico:

- presidia e gestisce l'infrastruttura tecnologica del sistema di Conservazione a Norma (sito primario e secondario);
- configura, manutiene e monitora le trasmissioni dei dati da e verso il sistema di Conservazione a Norma;
- installa, configura e gestisce i sistemi operativi, software di base e tools propri dell'infrastruttura del sistema di Conservazione a Norma;
- risolve le anomalie sistemistiche in collaborazione con il Supporto Applicativo;
- monitora l'utilizzo delle risorse, rileva ed interpreta i "trend" relativi all'utilizzo delle risorse, definisce e realizza un piano di adeguamento delle risorse a fronte dei consumi;
- produce la reportistica di competenza;
- monitora e gestisce gli allarmi tecnologici relativi allo stato dei sistemi provenienti dagli strumenti di controllo e automazione;
- esegue e manutiene le procedure di backup standard dei dati.

8.5.4 Tracciabilità delle operazioni

Un apposito servizio centralizza i file di log di tutte le componenti HW e applicative. La sincronizzazione di tutti i sistemi sul tempo campione proveniente dalla fonte esterna prevista dalla legge consente la ricostruzione della corretta sequenzialità di accadimento delle operazioni registrate nei file di log.

Per lo scopo è stato realizzato un SIEM (Security Information and Event Management) basato su tecnologia McAfee per la gestione dei log provenienti da sistemi, apparati di rete e Firewall. Il sistema si compone di tre elementi: Event Receiver Collector, LogManager, Enterprise Security Manager.

I tre moduli svolgono compiti distinti, in particolare:

- Event Receiver Collector (ERC): McAfee Event Receiver raccoglie eventi e log in modo affidabile utilizzando un sistema integrato di raccolta dei flussi di rete.
- LogManager (ELM): McAfee Enterprise Log Manager consente la gestione automatizzata e l'analisi di log di tutti i tipi, come i log degli eventi di Windows, dei database, delle applicazioni e di sistema. I log sono firmati e convalidati per garantire autenticità e integrità (requisito per la conformità alla normativa e di valore legale).

- Enterprise Security Manager (ESM): McAfee Enterprise Security Manager fornisce i contesti in modo veloce e approfondito per identificare le minacce critiche, agire rapidamente e rispondere in modo semplice ai requisiti di conformità.

L'azione sinergica delle tre componenti permette di procedere alla raccolta dei log, alla loro correlazione e analisi nonché alla storicizzazione e retention nel rispetto delle normative attuali.

Questo servizio permette anche l'identificazione di condizioni di allarme in corrispondenza delle quali si attivano specifiche azioni fra cui anche l'apertura di trouble ticket gestiti dalla piattaforma o tramite mail verso le strutture di competenza. Contestualmente vengono segnalate le situazioni di allarme anche al Responsabile del Servizio di Conservazione di Intesa Sanpaolo.

➔ Torna al Sommario

9 Monitoraggio e controlli

9.1 Procedure di monitoraggio

Il sistema di conservazione è sottoposto a monitoraggio per garantirne l'integrità, la disponibilità ed i livelli di servizio contrattualizzati.

La struttura di monitoraggio ha due tipologie di controlli:

- Sistemistici (utilizzo risorse, controllo accessi, ……)
- Applicativi (sonde su servizi dummy, quadrature, monitoraggio picchi elaborativi)

I livelli di servizio sono regolati da SLA definiti con il Cliente i cui KPI sono monitorati e verificati periodicamente.

➔ Torna al Sommario

9.2 Verifiche dell'integrità degli archivi

I controlli periodici di integrità dei documenti conservati sono pianificati dal Responsabile della Conservazione, tenendo conto dello stato e dell'importanza dei processi e delle aree oggetto di verifica, nonché dei risultati delle precedenti verifiche. La frequenza con la quale vengono disposti i controlli di integrità è almeno annuale. Al termine delle verifiche viene predisposto il relativo verbale di verifica.

La scelta del personale verificatore viene fatta in modo da garantire obiettività ed imparzialità nel processo di verifica.

Di seguito le tipologie di verifiche attuate nel processo di controllo di integrità:

- verifiche periodiche sullo stato di conservazione dei supporti di memorizzazione, volte a verificare con l'ausilio di software appropriati, lo stato di conservazione dei supporti di memorizzazione e a ricercare eventuali anomalie, provvedendo, se necessario, alla copia o duplicazione del contenuto dei supporti;
- verifiche periodiche sui documenti conservati, volti a verificare periodicamente, con cadenza non superiore a due anni, l'effettiva integrità dei documenti stessi, provvedendo, se necessario, al loro riversamento. La procedura che gestisce il processo di conservazione presenta delle funzionalità di controllo massivo dei dati conservati: questi controlli consistono nell'impostare a livello informatico la relativa periodicità; attualmente, il sistema è configurato per verificare giornalmente un milione di documenti, eseguendo ogni giorno i controlli a rotazione su documenti diversi. L'applicazione che gestisce il processo di conservazione, effettua un check automatico registrando per ogni PdA/documento conservato, la data e ora in cui è stata eseguita l'ultima verifica di integrità. Nel caso siano verificate delle anomalie viene aperto un incident al fine di recuperare il dato dalle copie di sicurezza;
- verifiche di leggibilità dei documenti in conservazione da parte di operatori (human readability) possono essere eseguite su specifica richiesta del Committente, tramite apertura di un campione pseudocasuale statistico dei documenti. I dati rilevati, relativamente al numero di documenti verificati ed agli eventuali risultati negativi, saranno inseriti in apposito report inviato al committente.

➔ Torna al Sommario

9.3 Soluzioni adottate in caso di anomalie

Ogni evento anomalo viene gestito con la creazione di un ticket verso la struttura preposta a manutenere il servizio. E' prevista, in caso di anomalia l'apertura di un incident.

Si distinguono due tipi di incident del software: l'incident normale e l'incident grave. Gli incident gravi sono gli incident che causano un consistente danno ai Clienti.

In generale l'incident viene sempre generato se l'anomalia causa un non rispetto delle SLA contrattualizzate con un qualsiasi Cliente.

Una volta che l'anomalia viene rilevata, sono previste le seguenti azioni:

- determinazione della problematica e relativa descrizione;
- determinazione delle azioni correttive;
- attuazione delle azioni di ripristino del servizio.

Al fine di ripristinare, tempestivamente, il corretto funzionamento devono essere individuate ed eseguite, anche con la collaborazione degli utenti e dei Clienti, le operazioni necessarie alla risoluzione della problematica producendo la relativa documentazione.

Qualora questo tentativo di risoluzione non andasse a buon fine, è necessario agire tramite richiesta di change di emergenza onde ripristinare tempestivamente il corretto funzionamento del servizio.

➔ Torna al Sommario

9.4 Verifica periodica di conformità a normativa e standard di riferimento

Come descritto nel paragrafo "5.3 Attività esternalizzate", la struttura di Internal Audit di Intesa Sanpaolo ha il compito di monitorare l'adeguatezza complessiva del Sistema di Conservazione, valutando l'efficacia ed efficienza dei processi operativi, il rispetto della normativa interna ed esterna, l'affidabilità della struttura operativa e dei meccanismi di delega. In particolare tale struttura effettua audit periodici che interessano tutte le unità organizzative interne ed esterne coinvolte nell'erogazione dei servizi di Conservazione a Norma, con l'obiettivo di segnalare eventuali anomalie, definire e assegnare alle funzioni responsabili gli opportuni interventi di risoluzione e verificare il corretto completamento degli stessi.

➔ Torna al Sommario