interdata
SOFTWARE & SERVICES

MANUALE DI CONSERVAZIONE
DI
INTERDATA S.R.L.

Versione 1.4

Emissione Documento

azione	data	nominativo	funzione
Redazione	24/08/2015	Italo Cimmino	Sistemi Informativi
Verifica	14/09/2015	Silvestro Ricciardi	Direzione Tecnica
Approvazione	01/10/2015	Domenico Ricciardi	Direzione Generale
Revisione	04/11/2015	Silvestro Ricciardi	Direzione Tecnica
Approvazione	10/11/2015	Domenico Ricciardi	Direzione Generale
Revisione	28/12/2015	Silvestro Ricciardi	Direzione Tecnica
Approvazione	30/12/2015	Domenico Ricciardi	Direzione Generale

Registro Versioni

versione	data	modifiche apportate	osservazioni
1.0	01/10/2015	Prima versione secondo lo schema (versione 2) del manuale AgID per l'accreditamento ai sensi dell'art. 44 bis del CAD	//
1.3	10/11/2015	Aggiornamento dei diversi paragrafi	//
1.4	30/12/2015	Revisione formati e terminologia	//

Sommario

1 SCOPO ED AMBITO DEL DOCUMENTO

Il presente "Manuale di Conservazione" è adottato secondo le disposizioni dell'art. 8 del DPCM 3 dicembre 2013.

Il documento illustra dettagliatamente l'organizzazione, i soggetti coinvolti ed i rispettivi ruoli svolti, il modello di funzionamento, le procedure adottate, la descrizione dei processi, la architetture e le infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione, utile alla gestione e alla verifica del funzionamento nel tempo, del sistema di conservazione.

Il presente documento e gli eventuali ulteriori documenti aggiuntivi rilasciati sono custoditi presso la sede del Conservatore Interdata. Il documento è identificato attraverso un livello di revisione e la data di emissione ed il Conservatore esegue periodicamente un controllo di conformità del processo di conservazione e, ove necessario, aggiorna il documento in oggetto anche in considerazione dell'evoluzione della normativa e degli standard tecnologici.

Il "Manuale di Conservazione", depositato e pubblico presso l'Agenzia per l'Italia Digitale, è un documento informatico prodotto nel formato PDF/A, su cui è apposta la firma digitale del Responsabile del Servizio di Conservazione e Rappresentante Legale ed è conservato secondo le disposizioni della normativa vigente, al fine di assicurarne l'origine, la data certa e l'integrità del contenuto dalla sua emissione e per tutto il periodo di conservazione.

Al presente "Manuale di Conservazione", sono allegati i documenti indicati nella tabella successiva che riportano in modo dettagliato i diversi aspetti del sistema e del servizio di conservazione e ne costituiscono parte integrante.

documenti collegati	
Scheda Servizio Cliente	Documento tecnico che contiene le condizioni specifiche del servizio di conservazione ed è parte integrante e sostanziale del contratto di servizio sottoscritto tra le parti e del "Manuale di Conservazione".
Specificità del Contratto	Documento redatto dal Conservatore sulla base delle informazioni condivise con il Produttore dei documenti, contenente i requisiti essenziali del Servizio, le relative specifiche tecnico-funzionali e procedurali per le varie fasi del servizio (attivazione, versamento, conservazione, distribuzione) oltre ai livelli di Servizio (SLA); tale documento è redatto in fase di analisi, prima del collaudo e della produzione del primo processo di conservazione.
Piano della Sicurezza	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici **"Coopera® *Safe*"** da possibili rischi in ambito all'organizzazione Interdata.

Torna al sommario

2 TERMINOLOGIA

2.1 Glossario

glossario dei termini	
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 dichiarazione.
Affidabilità	Caratteristica che esprime il livello di fiducia riposta nel documento.
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	Processo di trattamento e gestione dei documenti di uso corrente e/o nel medio lungo periodo che permette una loro classificazione (indicizzazione) ai fini della ricerca e consultazione.
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.
Archivio informatico	Archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico.
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.
Autenticazione del documento informatico	La validazione del documento informatico attraverso l'associazione di dati informatici relativi all'autore o alle circostanze, anche temporali, della redazione.
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 correlati e registrati tra loro.
Certificato qualificato	Il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva.
Certification authority (CA)	Il soggetto che secondo quanto disposto dall'art. 27 del CAD presta servizi di certificazione delle firme elettroniche qualificate o che fornisce altri servizi connessi con queste ultime, quali ad esempio quello delle marche temporali.
Chiave privata	L'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico.
Chiave pubblica	L'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche.
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.
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.
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.

Copia analogica del documento informatico	Documento analogico avente contenuto identico a quello del documento informatico da cui è tratto.
Copia di sicurezza	Copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell'art. 12 del DPCM 3 dicembre 2013.
Copia informatica di documento analogico	Il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto.
Copia informatica di documento informatico	Il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari.
Copia per immagine su supporto informatico di documento analogico	Il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto.
Destinatario	Identifica il soggetto / sistema al quale il documento informatico è indirizzato.
Dispositivo sicuro per la creazione della firma:	I dispositivi sicuri per la generazione della firma qualificata che devono essere dotati di certificazione di sicurezza secondo l'art. 35 del CAD.
Documento analogico	La rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.
Documento informatico	Documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario.
Esibizione	Operazione che consente di visualizzare un documento conservato e di ottenerne copia.
Evidenza informatica	Una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.
Fascicolo informatico	Aggregazione strutturata e univocamente identificata di atti, documenti o dati.
Firma elettronica	L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica.
Firma elettronica avanzata	Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.
Firma elettronica qualificata	Un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma.
Firma digitale	Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.
Formato	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
Formazione	Il processo atto ad assicurare l'autenticità dell'origine e l'integrità del contenuto dei documenti informatici, con apposizione della firma digitale su ciascun singolo documento e/o della marca temporale ai fini di associare una data certa elettronica ove richiesto.
FTP Server	Programma che permette di accettare connessioni in entrata e di comunicare in maniera sicura con un Client attraverso il protocollo FTP.
Funzioni archivistiche	Funzioni per la conservazione delle informazioni (acquisizione, archiviazione, gestione dei dati, accesso, distribuzione).
Funzione di hash	Una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
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.

Identificazione informatica	La validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso.
Immodificabilità	Caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso.
Impronta	La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione di una opportuna funzione di hash.
Indice del Pacchetto di Archiviazione	Struttura dell'insieme dei dati a supporto del processo di conservazione, riferita allo standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010)
Indice del Pacchetto di Versamento	Struttura dell'insieme dei dati a supporto del processo di versamento del pacchetto di versamento (PdV), ispirata allo standard internazionale OAIS ISO 14721:2012 e definita nello specifico dal Conservatore in accordo con il produttore dei documenti
Indice del Pacchetto di Distribuzione	Struttura dell'insieme dei dati a supporto del processo di distribuzione del pacchetto di distribuzione (PdD), ispirata allo standard internazionale OAIS ISO 14721:2012 e definita nello specifico dal Conservatore in accordo con il produttore dei documenti
Insieme minimo di metadati del documento informatico	Complesso dei metadati, la cui struttura è descritta nell'allegato 5 del DPCM 3 dicembre 2013, 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 sul 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'art. 8 del DPCM 3 dicembre 2013, regole tecniche in materia di sistema di conservazione.
Memorizzazione	Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o 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 3 dicembre 2013
Originali non unici	Documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi
Pacchetto di archiviazione	Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del DPCM 3 dicembre 2013 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 di scarto	Pacchetto contenente i documenti da scartare dal Sistema di conservazione perché hanno raggiunto il loro termine temporale 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 per la sicurezza	È il documento aziendale che analizza il contesto in cui l'azienda opera riportando i fattori interni ed esterni che lo influenzano ed evidenzia le principali criticità legate alla gestione della sicurezza delle informazioni gestite

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 delle regole tecniche sul sistema di conservazione
Produttore	Persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale
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
Responsabile della conservazione	Soggetto responsabile dell'insieme delle attività elencate nell'art. 7, c. 1, del DPCM 3 dicembre 2013 e che opera presso il Produttore
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 personal
Responsabile del servizio di conservazione	Soggetto persona fisica nominato responsabile del servizio di conservazione **"Coopera® *Safe*"** di Interdata con l'assegnazione delle attività indicate nel documento dell'Agenzia per l'Italia Digitale sui profili professionali richiamati dalla Circolare n. 65/2014 (G.U. n. 89 del 16/04/2014)
Responsabile della funzione archivistica di conservazione	Soggetto persona fisica nominato responsabile della funzione archivistica di conservazione **"Coopera® *Safe*"** di Interdata con l'assegnazione delle attività indicate nel documento dell'Agenzia per l'Italia Digitale sui profili professionali richiamati dalla Circolare n. 65/2014 (G.U. n. 89 del 16/04/2014)
Responsabile del trattamento dei dati personali	Soggetto persona fisica nominato responsabile del trattamento dei dati personali del servizio di conservazione **"Coopera® *Safe*"** di Interdata con l'assegnazione delle attività indicate nel documento dell'Agenzia per l'Italia Digitale sui profili professionali richiamati dalla Circolare n. 65/2014 (G.U. n. 89 del 16/04/2014)
Responsabile della sicurezza dei sistemi per la conservazione	Soggetto persona fisica nominato responsabile della sicurezza dei sistemi per la conservazione **"Coopera® *Safe*"** di Interdata con l'assegnazione delle attività indicate nel documento dell'Agenzia per l'Italia Digitale sui profili professionali richiamati dalla Circolare n. 65/2014 (G.U. n. 89 del 16/04/2014)
Riferimento temporale	Informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento
Scarto	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale
Service Level Agreement	È l'accordo tra produttore e responsabile del servizio di conservazione sui livelli servizio da garantire ed indica i giorni entro cui devono essere conservati i documenti nel Sistema di conservazione
Sessione di distribuzione	Sessione telematica per la consegna (distribuzione) di uno o più Pacchetti di Distribuzione dall'Ente Conservatore all'Ente Produttore, sulla base di un modello-dati per i formati ed i contenuti definito e concordato tra le parti.
Sessione di ricerca	Una sessione telematica avviata da un Utente di un sistema di conservazione, durante la quale l'Utente usa gli Strumenti di Ricerca del sistema per individuare e consultare gli oggetti digitali in esso presenti.
Sessione di versamento	Sessione telematica per la consegna (versamento) di uno o più pacchetti di Versamento dall'Ente Produttore all'Ente Conservatore, sulla base di un modello-dati per i formati ed i contenuti definito e concordato tra le parti.
Sistema di conservazione	Sistema di conservazione dei documenti informatici di cui all'art. 44 del Codice dell'Amministrazione Digitale (D.lgs. 7 marzo 2005, n. 82 e successive modifiche ed integrazioni)
Titolare	La persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica
Utente	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse
Validazione temporale	Il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi

Versamento agli archivi di stato	Operazione con cui il responsabile della conservazione di un organo giudiziario o amministrativo dello Stato effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali

Torna al sommario

2.2 Acronimi

acronimi	
AE	Agenzia delle Entrate
AgID	Agenzia per l'Italia Digitale (già DigitPA e CNIPA)
CAD	Codice dell'Amministrazione Digitale
CNIPA	Centro Nazionale per l'Informatica della Pubblica Amministrazione, ora AgID
FTP	File Transfer Protocol
SFTP	SSH File Transfer Protocol o SFTP è un protocollo di rete che prevede il trasferimento dei dati e funzionalità di manipolazione. Usato con protocollo SSH-2 per il trasferimento dei file sicuro.
IDM	Identity Management
IPA	Indice delle Pubbliche Amministrazioni
IPdA	Indice del Pacchetto di Archiviazione
IPdD	Indice del Pacchetto di Distribuzione (o Rapporto di distribuzione)
IPdV	Indice del Pacchetto di Versamento
ISO	International Organization for Standardization
OAIS	Open Archival Information System, ISO 14721:2012
PdA / AIP	Pacchetto di Archiviazione
PdD / DIP	Pacchetto di Distribuzione
PdS	Pacchetto di Scarto
PdV	Pacchetto di Versamento
RdV / SIP	Rapporto di Versamento
SdI	Sistema d'Interscambio per la fatturazione elettronica PA per lo scambio delle fatture e delle relative notifiche/ricevute ai sensi del DM 3 aprile 2013, n. 55
SGSI	Sistema di Gestione della Sicurezza delle Informazioni
SLA	Service Level Agreement
TSA	Time Stamping Authority

Torna al sommario

3 NORMATIVA E STANDARD DI RIFERIMENTO

3.1 Normativa di riferimento

Nel presente paragrafo è riportata la principale normativa di riferimento per l'attività di conservazione a livello nazionale, ordinata secondo il criterio della gerarchia delle fonti:

- **Codice Civile** [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- **Legge 7 agosto 1990, n. 241 e s.m.i.** – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- **Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i.** – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- **Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i.** – Codice in materia di protezione dei dati personali;
- **Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i.** – Codice dei Beni Culturali e del Paesaggio;
- **Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i.** – Codice dell'amministrazione digitale (CAD);
- **Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013** – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
- **Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013** - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- **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.
- **Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014** - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

La normativa specifica, relativa alle diverse tipologie di documenti, riguardanti il contratto di erogazione del servizio di conservazione è riportata nel documento "Scheda Servizio Cliente – Specificità del Contratto".

Torna al sommario

3.2 Standard di riferimento

Si riportano di seguito gli standard di riferimento a cui l'attività di conservazione del Conservatore Interdata si riferisce, elencati nell'allegato 3 delle Regole Tecniche in materia di Sistema di conservazione con indicazione delle versioni aggiornate al 1° ottobre 2014, come indicato nelle regole tecniche di cui al DPCM 3 Dicembre 2013.

- **ISO 14721:2012 OAIS** (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- **ISO/IEC 27001:2013**, Information technology - Security techniques - Information security management systems – Requirements, requisito di un ISMS (Information Security Management System);

- **ETSI TS 101 533-1 V1.3.1 (2012-04)** Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- **ETSI TR 101 533-2 V1.3.1 (2012-04)** Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- **UNI 11386:2010 Standard SInCRO** - Supporto all' Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- **ISO 15836:2009** Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

Torna al sommario

4 RUOLI E RESPONSABILITÀ

Il sistema di conservazione descritto nel presente manuale, come prescritto dall'art. 5 del DPCM 3 dicembre 2013, descrive l'adozione del modello organizzativo governato dal conservatore Interdata, che coinvolge soggetti, strutture e/o funzioni deputate al versamento, all'implementazione, all'erogazione del processo, alla gestione e al controllo del sistema di conservazione di documenti informatici.

Torna al sommario

4.1 Compiti e responsabilità della conservazione

Ragione Sociale	Interdata S.r.l.
Partita Iva	01236711212
Codice Fiscale	00331650614
Sede Legale ed Operativa	Via Gaetano Pelella 1° traversa, 1 – 80026 Casoria (NA)

Interdata utilizza personale altamente specializzato e formato sulle problematiche connesse alla conservazione ed alla archiviazione digitale.

Tutto il personale preposto è costantemente aggiornato sulle nuove normative e sugli aspetti tecnologici attraverso documentazione resa disponibile dall'azienda e la partecipazione a corsi di approfondimento, interni ed esterni.

Torna al sommario

4.2 Ruoli e responsabilità

L'art.6 comma 1 del DPCM 3 dicembre 2013 su regole tecniche in materia di sistemi di conservazione, individua all'interno della struttura organizzativa i ruoli di:

- Soggetto Produttore
- Responsabile della Conservazione
- Utente

Il ruolo di **Soggetto Produttore** e **Utente** è svolto da persona fisica o giuridica che si preoccupa della produzione dei Pacchetti di Versamento ed è responsabile del trasferimento di questi, dal proprio sistema di gestione documentale al sistema di conservazione a norma denominato **"Coopera® *Safe*"**.

Per tutta la durata del contratto il Soggetto Produttore resterà titolare degli oggetti documentali versati.

Il **Soggetto Produttore** affida le attività di gestione e la supervisione dei processi di conservazione al Responsabile del Servizio di Conservazione (RSC) della Interdata. Il **RSC** definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti informatici da conservare e definisce in accordo con il Responsabile della Conservazione (RC) del Soggetto Produttore, i metadati minimi da ricevere nel Pacchetto di Versamento ed i controlli logici da effettuare sui singoli metadati.

Torna al sommario

4.3 Funzioni e Responsabilità

Il sistema di conservazione a norma della Interdata**,** gestito dal Responsabile del Servizio di Conservazione, è basato su un modello di riferimento, definito formalmente nei ruoli e nelle responsabilità dei vari attori

coinvolti, nel processo di conservazione dei documenti informatici, come riportato nella tabella successiva in conformità ai ruoli e alle attività ad essi associati indicati nel documento “Profili Professionali” pubblicato da AgID sul proprio sito istituzionale.

ruolo	nominativo	attività di competenza	periodo	deleghe
Responsabile del servizio di conservazione - RSC -	Silvestro Ricciardi	**Definisce** ed attua le politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione; **Definisce** le caratteristiche ed i requisiti del sistema di conservazione in conformità alla normativa vigente; **Eroga** il corretto servizio di conservazione all’ente produttore; **Definisce** gli aspetti tecnico-operativi e valida i disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative dei servizi di conservazione.	01/10/2015	
Responsabile della sicurezza dei sistemi di conservazione – RSCC -	Gianfranco Rispoli	**Rispetta** e monitora i requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; **Segnala** le eventuali difformità al Responsabile del servizio di conservazione ed individua e pianifica le necessarie azioni correttive.	01/10/2015	
Responsabile della funzione archivistica di conservazione – RFA -	Silvestro Ricciardi	**Definisce** e gestisce il 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 trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; **Definisce** i set di metadati di conservazione dei documenti e dei fascicoli informatici; **Monitora** il processo di conservazione e di analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione; **Collabora** 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.	01/10/2015	
Responsabile del trattamento dei dati personali – RTD -	Eduardo Chierchia	**Garantisce** il rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; **Garantisce** che il trattamento dei dati dell’Ente avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.	01/10/2015	
Responsabile dei sistemi informativi per la conservazione – RSIC -	Gianfranco Rispoli	**Gestisce** l’esercizio delle componenti hardware e software del sistema di conservazione; **Monitora** il mantenimento dei livelli di servizio (SLA) concordati con l’ente produttore; **Segnala** le eventuali difformità degli SLA al Responsabile del servizio di conservazione e individua e pianifica le necessarie azioni correttive; **Pianifica** lo sviluppo delle infrastrutture tecnologiche del sistema di conservazione; **Controlla** e verifica i livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.	01/10/2015	
Responsabile dello sviluppo e della manutenzione del sistema di conservazione – RSM -	Maurizio Triunfo	**Coordina** lo sviluppo e la manutenzione delle componenti hardware e software del sistema di conservazione; **Pianifica** e monitora i progetti di sviluppo del sistema di conservazione; **Monitora** gli 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; **Gestisce** lo sviluppo di siti web e portali connessi al servizio di conservazione.	01/10/2015	

Torna al sommario

5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

Interdata, per il servizio di conservazione dei documenti informatici, ha certificato il proprio sistema di gestione della sicurezza delle informazioni nel dominio logico, fisico e organizzativo nel quale viene eseguito il processo di conservazione (certificazione ISO/IEC 27001:2013).

Torna al sommario

5.1 Organigramma

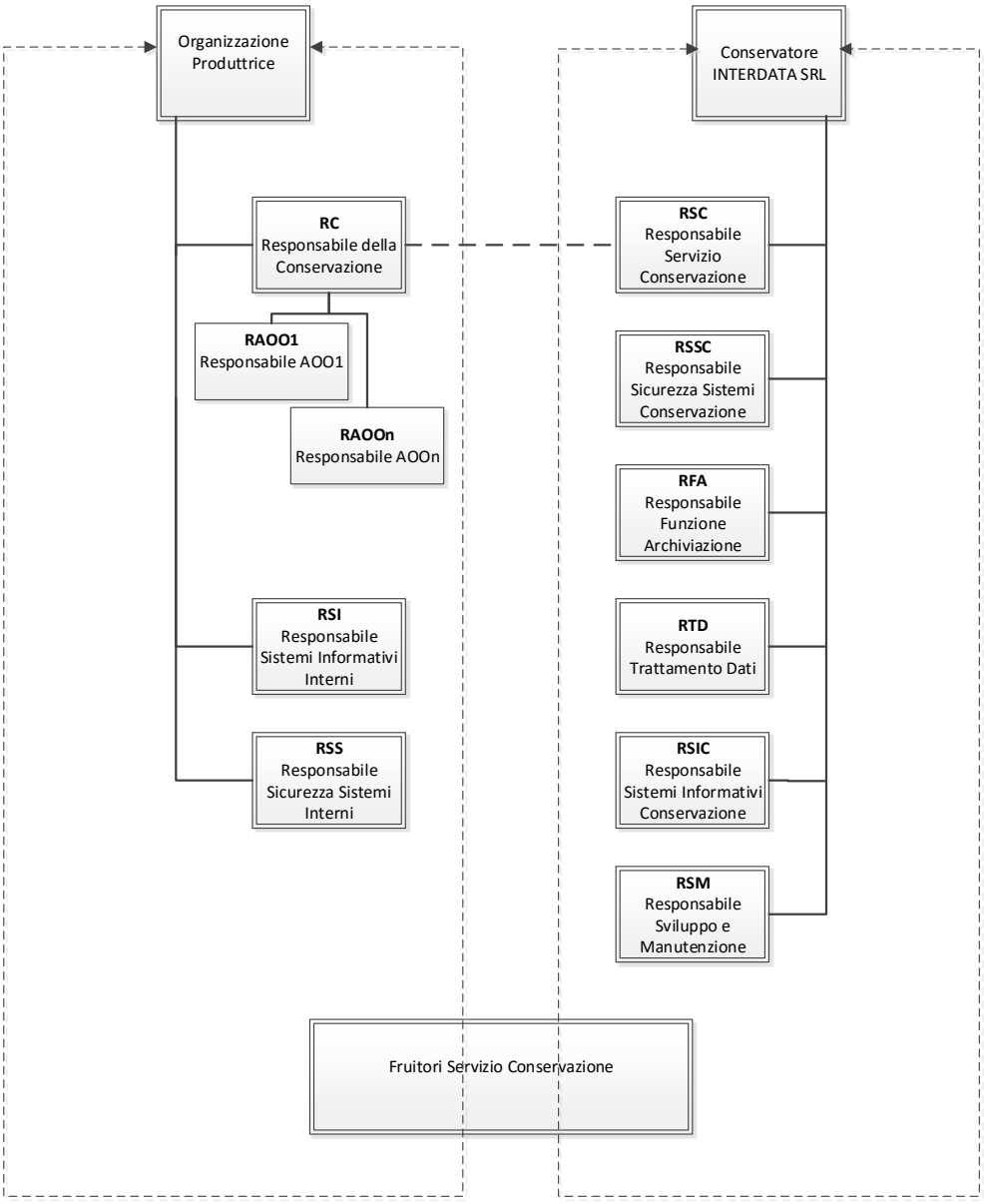


Figura 1 - organigramma

L'Organizzazione Produttrice, affida a Interdata il servizio di conservazione dei propri documenti informatici in applicazione del modello organizzativo previsto dall'art. 5 comma 2 lett. b del DCPM 3 dicembre 2013 e rappresentato dall'organigramma (VEDI: FIGURA 1 - ORGANIGRAMMA)

L'Organizzazione Produttrice mantiene la responsabilità della produzione e gestione dei propri documenti informatici e, come previsto dall'art. 5 comma 2 lett. b, affida al Responsabile del Servizio Conservazione (**RSC**) della Interdata la Conservazione dei propri documenti informatici.

Torna al sommario

5.2 Struttura Organizzativa

La Interdata è da sempre protesa al miglioramento delle performance dei propri processi e servizi con particolare riguardo al Sistema della Sicurezza delle informazioni per il quale ha conseguito la certificazione ISO/IEC 27001:2013 nel suo dominio fisico, logico ed organizzativo dove sono svolti i servizi di conservazione.

Il servizio di conservazione è descritto sinteticamente nelle fasi che lo compongono con le indicazioni delle figure che ne assumono la responsabilità.

Attivazione

- L'attivazione del servizio avviene a fronte di formale accettazione dell'offerta commerciale e di tutte le condizioni contrattuali da parte del Cliente/Produttore dei Documenti, inclusi gli atti di nomina sottoscritti tra le parti per svolgere il ruolo di Responsabile Servizio Conservazione (**RSC**) e di Responsabile Trattamento Dati (**RTD**) (VEDI: FIGURA 1 - ORGANIGRAMMA).
- Interdata, al ricevimento dell'offerta commerciale accettata provvede, tramite l'Ufficio Amministrativo, all'inserimento nei sistemi informativi dell'anagrafica del Cliente ed alla compilazione della conferma d'ordine da inviare al Cliente.
- A seguito dell'invio della conferma d'ordine al Cliente, tramite il sistema informativo interno, sono avviate tutte le attività dall'Area di Supporto che contatta il Cliente ed avvia la predispone del "Contratto", la "Scheda Servizio Cliente" e le "Specificità del Contratto". Quest'ultimo documento è fondamentale per l'erogazione del servizio e, redatto dal Conservatore sulla base delle informazioni condivise con il Produttore dei Documenti (Cliente), contiene i requisiti essenziali del servizio e ne è parte integrante del manuale di conservazione.
- Dopo la fase di avvio formale, L'Area Supporto di Interdata prende contatto con il Cliente per la definizione di eventuali attività propedeutiche alla creazione del Pacchetto di Versamento (PdV) e nel caso fornisce supporto tecnico.
- La corretta definizione iniziale dei requisiti e la conformità alla normativa vigente in materia di sistemi di conservazione, con anche l'individuazione degli adempimenti correlati, è assicurata dalla predisposizione della "Scheda Servizio Cliente" redatta con il controllo e la supervisione del Responsabile Funzione Archiviazione (**RFA**), del Responsabile Trattamento Dati (**RTD**), nel caso di documenti sensibili, e del Responsabile Servizio Conservazione (**RSC**) che provvede alla approvazione finale.
- Ad ogni variazione e/o implementazione del Servizio è necessario aggiornare la "Scheda Servizio Cliente" e nuovamente essere condivisa tra le parti con la validazione del Responsabile Servizio Conservazione (**RSC**) di Interdata e del Cliente.
- L' area di Supporto, ricevuta la nuova SSC, dà mandato all'Area di Produzione di avviare le attività di configurazione nel sistema **"Coopera® *Safe*"** di test per il collaudo interno. Al superamento del collaudo interno, viene predisposto, previa pianificazione, il collaudo con il Cliente.
- Le modalità del collaudo sono indicate nella "Scheda Servizio Cliente"; a seguito del collaudo e della sua validazione formale da parte del Cliente si procede con la messa in produzione.

Esercizio

- L'Area di Produzione si occupa di gestire le componenti hardware e software del servizio di conservazione e di presidiare, controllare e monitorare il corretto funzionamento dei sistemi per la sua erogazione tramite l'ausilio del sistema di monitoraggio *Spiceworks*, report ed altri strumenti di controllo.
- Inoltre, l'Area di Produzione presidia e gestisce le attività previste e la corretta esecuzione del processo, in particolare: la fase di presa in carico, il controllo di coerenza, la generazione del rapporto

di versamento, la preparazione e gestione dei pacchetti di archiviazione, la preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione, la produzione di duplicati e copie informatiche su richiesta dell'Utente.

- Il Responsabile Sistemi Informativi Conservazione (**RSIC**) ha la responsabilità delle attività di controllo e di monitorare il corretto svolgimento del servizio. In caso di riscontro di anomalie attiva il processo di gestione e risoluzione mediante l'apertura di un ticket automatico al fine di tracciare l'accaduto e risolvere l'anomalia. Eventuali anomalia di rilievo e difformità sono segnalate al Responsabile Servizio Conservazione (**RSC**) attraverso la procedura prevista dallo standard ISO/IEC 27001:2013.
- Ogni processo di conservazione completato con esito positivo è mantenuto nel tempo anche nella fase di post produzione per tutta la durata contrattuale, garantendo ai documenti ed ai pacchetti informativi integrità, autenticità dell'origine, leggibilità nel tempo, disponibilità, reperibilità, sicurezza e riservatezza.

Post Produzione

- Il mantenimento dei documenti e dei pacchetti generati nel processo di conservazione è garantito dalle attività dell'Area di Produzione nella figura del Responsabile Sistemi Informativi Conservazione (**RSIC**) e dall'Area di Ricerca e Sviluppo nella figura del Responsabile Sviluppo e Manutenzione (**RSM**) che garantiscono sia dal punto di vista infrastrutturale che applicativo il presidio e il controllo delle attività del servizio e quindi il corretto mantenimento dei documenti e dei pacchetti per tutto il periodo di conservazione concordato con il Produttore dei Documenti.
- Durante la fase di post-produzione la struttura organizzativa di Interdata, in particolare con le attività dell'Area di Assistenza e di Produzione, supporta gli adempimenti previsti dalla normativa (a titolo di esempio non esaustivo la dichiarazione art. 52, decimo comma, D.P.R. 633/72 riguardante gli Accessi, Ispezioni, Verifiche).
- Scaduto il periodo di conservazione, viene redatto un verbale delle attività e comunicato al Produttore dei Documenti l'avvio della chiusura del Servizio e dello scarto entro 60 gg., ciò al fine di fornire un periodo di tempo utile per richiedere un'estensione, tramite apposito contratto, del periodo di conservazione. Inoltre come da disposizioni del codice dei beni culturali (D. Lgs. 22 gennaio 2004, n. 42) nel caso di Enti Pubblici o Privati dichiarati di notevole interesse storico, per effettuare lo scarto verrà richiesta l'autorizzazione preventiva alla Soprintendenza Archivistica da parte del Produttore dei Documenti.

Torna al sommario

6 OGGETTI SOTTOPOSTI A CONSERVAZIONE

Il sistema di conservazione **"Coopera® *Safe*"** è conforme alle regole tecniche di cui al DPCM 3 dicembre 2013 e 13 novembre 2014 ed allo standard ISO 14721:2012 OAIS (Open Archival Information System), standard per la conservazione a lungo termine del digitale e individuato come modello di riferimento delle nuove regole tecniche sulla conservazione. Alla base del funzionamento vi è il concetto di informazione da conservare e quindi di pacchetto informativo contenenti documenti e dati.

Il versamento dei pacchetti informativi nel sistema **"Coopera® *Safe*"** da parte di un Ente Produttore può avvenire con una o più trasmissioni distinte (sessioni), tali pacchetti contengono due tipologie di informazioni:

- contenuto informativo
- informazioni sulla Conservazione (Preservation Description Info - PDI)

Contenuto informativo

L'insieme delle informazioni che costituisce l'obiettivo originario della conservazione è un oggetto informativo composto dai dati e dalle proprie Informazioni di rappresentazione:

- dati composto da un insieme di sequenze di bit
- informazioni di rappresentazione che devono essere mantenute nel tempo (es.: alcuni elementi della formattazione, ecc.)

Informazioni sulla Conservazione (PDI)

Si tratta delle informazioni necessarie ad un'adeguata conservazione del contenuto informativo (metadati) classificate in:

- informazioni sulla provenienza (documentano la storia del contenuto informativo: ad esempio forniscono informazioni sull'origine/sulla fonte del contenuto informativo e su chi ne ha curato la custodia sin dalla sua origine)
- informazioni sull'identificazione (identificano e se necessario descrivono uno o più meccanismi di attribuzione di identificatori al contenuto informativo)
- informazioni sull'integrità (garantiscono che il contenuto informativo non sia stato alterato senza una documentazione dell'evento)
- informazioni sul contesto (riportano le relazioni del contenuto informativo con il suo ambiente, inclusi i motivi della creazione e la modalità di relazione con altri contenuti informativi)

Torna al sommario

6.1 Oggetti conservati

Nel documento "Specificità del Contratto" sono elencate e descritte le tipologie di documenti sottoposte a conservazione e le relative politiche di conservazione che riguardano, per ciascuna tipologia:

- la natura e l'oggetto della tipologia documentale
- l'elenco e la descrizione dei formati (comprensivi della relativa versione) dei file utilizzati
- l'indicazione dei visualizzatori relativi ai formati gestiti, necessari per garantire la leggibilità nel tempo dei documenti conservati
- l'elenco e la descrizione dei metadati associati ai documenti
- il periodo di conservazione
- i livelli di servizio (SLA) concordati
- altre politiche (regole) che caratterizzano il processo di conservazione

Le tipologie di documenti che caratterizzano gli oggetti digitali da versare nel sistema di conservazione **"Coopera® *Safe*"** sono definite attraverso le attività di analisi e di classificazione documentale nella fase di attivazione del servizio.

La descrizione delle tipologie documentali (Descrizione Archivistica – DA), con l'indicazione della loro natura, dei formati, dei metadati obbligatori e dei metadati opzionali, delle regole e della durata di conservazione (piano di conservazione e successivo scarto) sono riportate nel dettaglio in una tabella per ciascuna tipologia nei documenti allegati "Scheda Servizio Cliente" e "Specificità del Contratto".

Di seguito si riporta un esempio della tabella da compilare nella "Specificità del Contratto" del Servizio **"Coopera® *Safe*".**

tipologia documentale		
1	Documento Informatico	…
1.1	Codice tipologia nel Sistema di conservazione	…
1.2	Natura di documento informatico	Amministrativo / Non Amministrativo
1.3	Presenza firma digitale su singolo documento	SI / NO
1.4	Apposizione della marca temporale	SI / NO
1.5	Metadati	In questa sezione sono inseriti tutti i metadati associati alla specifica tipologia documentale, indicandone la loro descrizione ed il loro valore (stringa, numero, data). Per ciascun metadato si dichiara se è un metadato "obbligatorio" in quanto richiesto dalla normativa vigente a seconda della natura della tipologia documentale ovvero in quanto richiesto dall'accordo tra ente produttore ed ente conservatore.
1.6	Presenza di fascicolo informatico o aggregazione documentale	SI / NO
1.7	Periodo di riferimento dei documenti	…
1.8	Durata di conservazione	… anni
1.9	Formato del file	… (Vedi elenco Allegato 2 del DPCM 3 dicembre 2013)

I formati dei file, contenuti nel Pacchetti di Versamento, devono essere conformi all'elenco dei formati previsti dall'Allegato 2 del DPCM 3 Dicembre 2013.

Il Produttore dei Documenti deve adeguarsi al seguente elenco dei formati ammessi. Il sistema di conservazione **"Coopera® *Safe*"** verifica, all'atto della presa in carico, la corrispondenza del formato e dello specifico mimetype per ogni documento presente nel Pacchetto di Versamento diversamente viene scartato.

formato	proprietario	estensione	standard	mimetype	visualizzatore	produttore visualizzatore
PDF	Adobe Systems - www.adobe.com	.pdf	ISO32000-1	application/pdf	Adobe Reader	Adobe Systems - www.adobe.com
PDF/A	Adobe Systems - www.adobe.com	.pdf	ISO 19005-1:2005 (vers. PDF 1.4) ISO 19005-2:2011 (vers. PDF 1.7)	application/pdf	Adobe Reader http://www.pdfa.org/doku.php	Adobe Systems - www.adobe.com
XML	W3C	.xml		application/xml text/xml	Mozilla Chrome Internet Explorer	Firefox Google Microsoft
TXT	Ai fini della conservazione nell'uso di tale formato, è	.txt			Mozilla Chrome Internet Explorer	Firefox Google Microsoft

	importante specificare la codifica del carattere (Character Encoding) adottato					
TIFF	Aldus Corporation in seguito acquistata da Adobe	.tif		image/tiff	Vari visualizzatori di immagini	
JPG	Joint Photographic Experts Group	.jpg, .jpeg	ISO/IEC 10918:1	image/jpeg	Vari visualizzatori di immagini	Per maggiori informazioni sul formato www.jpeg.org
EML	Vari	.eml	RFC2822		Client di posta elettronica supportano la visualizzazione di file eml	Vari
OOXML	Microsoft	.docx, .xlsx, .pptx	ISO/IEC DIS 29500:2008			Tale formato deve garantire alcune caratteristiche che lo rendono adatto alla conservazione nel lungo periodo, tra queste l'embedding dei font, la presenza di indicazioni di presentazione del documento, la possibilità di applicare al documento la firma digitale XML
ODF	Consorzio OASIS OpenOffice.org	.ods, .odp, .odg, .odb	ISO/IEC 26300:2006	application/vnd .oasis.opendocument.text		www.oasis-open.org

In tutti i casi riportati in tabella, il produttore dei documenti s'impegna a versare al sistema di conservazione **"Coopera® *Safe*"** documenti privi di codici eseguibili o macro istruzioni o privi di qualsiasi causa, anche non visibile all'utente, che ne possa alterare il contenuto.

Infine, gli oggetti da conservare sono versati al sistema di conservazione dall'Ente Produttore all'interno di Pacchetti Informativi denominati Pacchetti di Versamento e descritti nel paragrafo successivo.

Torna al sommario

6.2 Pacchetto di Versamento

Il Pacchetto di Versamento (PdV) del Sistema di conservazione **"Coopera® *Safe*"** è costituito da un contenitore (archivio) contenente:

- i documenti oggetti da conservare (Content Information), eventualmente firmati digitalmente (nello standard di firma CAdES ".p7m" ovvero nello standard PAdES ovvero XAdES) o eventualmente marcati temporalmente (nello standard di validazione temporale CAdES-T ovvero nello standard PAdES-T ovvero XAdES-T)
- un file Indice IPdV (Indice del Pacchetto di Versamento) ovvero le Preservation Description Information , finalizzato alla descrizione dell'oggetto della conservazione e che secondo lo standard ISO 14721:2012 OAIS permette di identificare il produttore, di contenere i dati descrittivi ed informativi sull'impacchettamento ed i dati descrittivi e di rappresentazione di ciascun documento contenuto nel pacchetto
- Distinta di versamento file testuale .dist (presente solo nella modalità di versamento sFTP) che ha la finalità di dichiarare la chiusura della sessione di versamento da parte dell'Ente Produttore

Il file Indice del Pacchetto di Versamento (IPdV) è un file nel formato XML, che in conformità allo standard UNI SINCRO 11386:2010 assicura:

- l'identificazione del soggetto che ha prodotto il Pacchetto di Versamento (Produttore dei Documenti)
- l'identificazione dell'applicativo che lo ha prodotto
- la definizione della tipologia documentale (a cui appartengono i documenti inclusi nel pacchetto) ed eventuali messaggi del Coordinatore Gestione Documentale (**CGD**) (VEDI: FIGURA 1 - ORGANIGRAMMA)
- la definizione dei documenti inclusi nel pacchetto, con le relative informazioni quali: nome file, hash calcolato, indici e relativi valori, messaggi del Coordinatore Gestione Documentale, ecc.

Il file Indice del Pacchetto di Versamento (IPdV) può essere eventualmente firmato digitalmente dal Produttore dei documenti.

Di seguito la struttura dati dell'Indice del Pacchetto di Versamento del sistema **"Coopera® *Safe*"**

- PackageGuid
- Producer (AZIENDA PRODUTTRICE)
    - Id
    - Name
    - VatNumber
    - FiscalCode
    - Address
    - ZipCode
    - City
    - District
    - Country
- Author (UTENTE CHE HA PRODOTTO IL PACCHETTO)
    - Id
    - Role
    - Type (person / organization)
    - NameAndSurname
        - FirstName
        - LastName
    - TaxCode
- Description
- ContentType
- Year
- SubmissionDate
- **FileGroups** (POSSONO ESSERE N)
    - Files (POSSONO ESSERE N)
        - ID
        - Path
        - Hash
        - MoreInfo
            - IdSDI
            - Posizione
            - Stato_documento
            - Data_documento
            - Numero_documento
            - Codice_Amministrazione
            - Identificativo_fiscale_fornitore
            - Denominazione_Fornitore
            - Importo_Totale
            - Data_scadenza
            - Data_ricezione
            - Cognome_destinatario
            - Nome_destinatario
            - Identificativo_fiscale_destinatario
            - Protocollo_iva
            - Data_registrazione

La struttura del Report di Versamento :

- HEADER
  - Id
  - ReportDateTime
  - UtcCreationDateTime
  - CustomerCompany
    - Id
    - Name
    - VatNumber
    - FiscalCode
    - Address
    - ZipCode
    - City
    - District
    - Country
  - PreserverCompany
    - Id
    - Name
    - VatNumber
    - FiscalCode
    - Address
    - ZipCode
    - City
    - District
    - Country

- BODY
  - Year
  - ElementType
  - ElementDescription
  - TotalElements
  - Status
  - Validation
  - Comments
  - Errors/Warnings (POSSONO ESSERE N)
    - ReferenceId
    - Description
    - Type (warning or error)

Torna al sommario

6.3 Pacchetto di Archiviazione

Il pacchetto di Archiviazione (PdA) generato nel processo di conservazione del sistema **"Coopera® *Safe*"** è una specializzazione del Pacchetto Informativo ed è composto dalla trasformazione di uno o più Pacchetti di Versamento secondo le modalità riportate nel presente manuale di conservazione.

Un Pacchetto di Archiviazione (PdA) è un contenitore informativo che contiene:

- gli oggetti informativi individuati per la conservazione (quindi i documenti, i fascicoli elettronici o le aggregazioni documentali sottoposti al processo di conservazione a lungo termine)
- un Indice del Pacchetto di Archiviazione (IPdA) che rappresenta le Informazioni sulla Conservazione

In particolare, la struttura dati dell'IPdA del sistema **"Coopera® *Safe*"** fa riferimento allo standard nazionale SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010), standard riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione.

L'IPdA è l'evidenza informatica nel formato XML associata ad ogni PdA, contenente un insieme di informazioni descritte nelle regole tecniche in materia, in cui è riportata nel dettaglio la struttura dati prevista. Su ciascun IPdA viene apposta una marca temporale e la firma digitale del Responsabile del Servizio di Conservazione.

Di seguito viene riportata la struttura dati dell'IPdA adottata, conforme allo standard SInCRO.

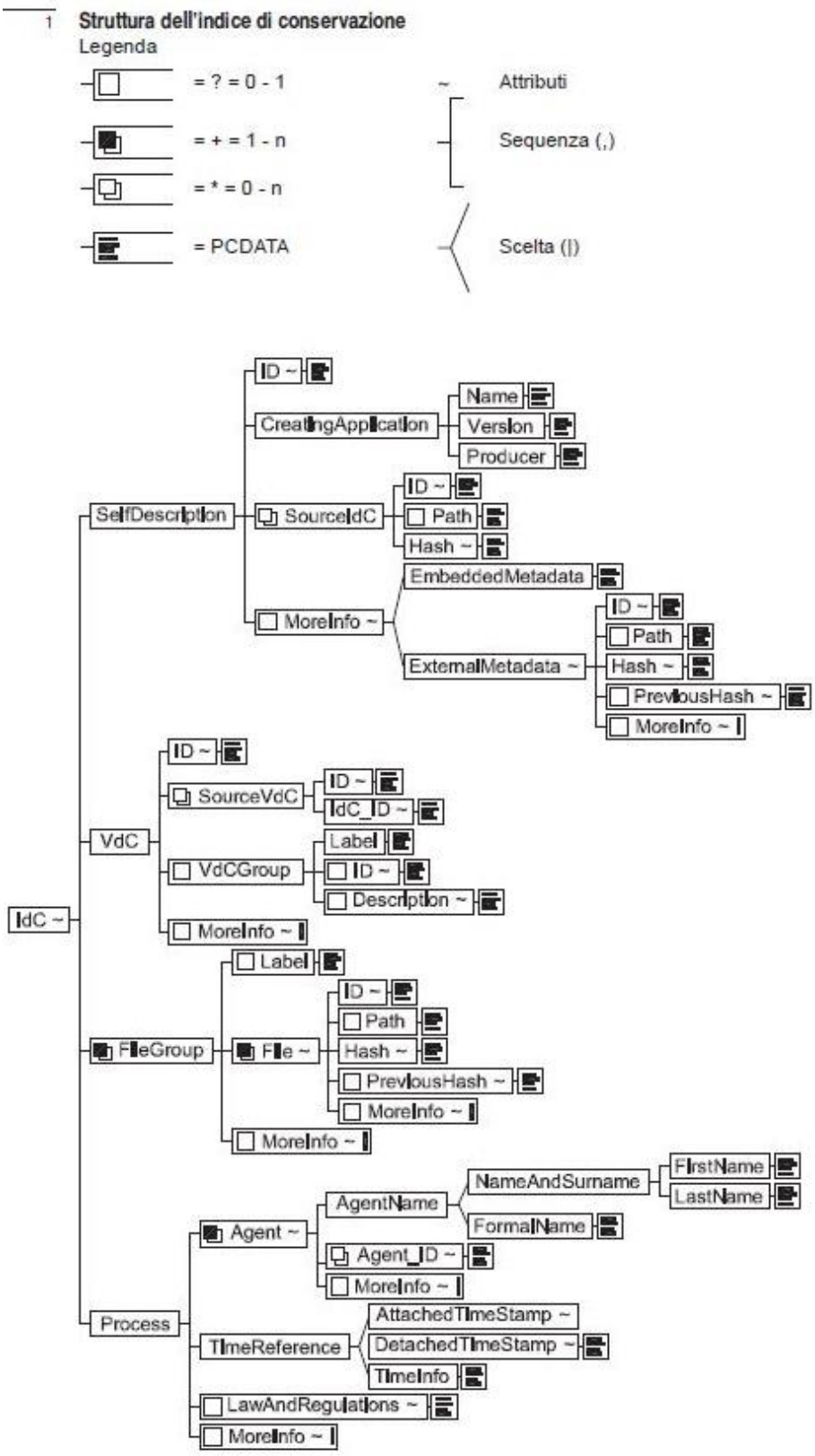


Figura 2 - Struttura dell'indice del pacchetto di archiviazione (IPdA)

La struttura dati del PdA del sistema **"Coopera® *Safe*"** completa delle ulteriori strutture collegate ai diversi elementi "MoreInfo" previsti dallo standard SInCRO.

Nelle MoreInfo del nodo SelfDescription sono presenti i campi:

- Anno (Year);
- Tipo di contenuto (ContentType);
- Descrizione del contenuto (ContentDescription);
- Descrizione generale (Description);
- Riferimento temporale (Timestamp).

Torna al sommario

6.4 Pacchetto di Distribuzione

Un Pacchetto di Distribuzione (PdD) del sistema **"Coopera® *Safe*"** può essere delle seguenti tipologie:

- PdD distribuito a seguito di ricerca di un singolo documento, in risposta alla richiesta dell'Utente;
- PdD distribuito a seguito di ricerca di più documenti, anche appartenenti a più PdA, in risposta alla richiesta dell'Utente

In entrambe le tipologie, il PdD è costituito da una cartella compressa (ad esempio zip) che contiene i seguenti elementi:

- I **documenti** (oggetti digitali conservati nel sistema) richiesti dall'Utente.
- **Uno o più files IPdA** firmati digitalmente dal Responsabile Servizio Conservazione (**RCS**) e marcati temporalmente associati ai predetti documenti richiesti dall'Utente.
- **File indice del PdD (IPdD)**: file XML ispirato allo standard UNI SINCRO 11386:2010 e firmato digitalmente dal Responsabile Servizio Conservazione (**RCS**), che contiene l'hash dell'IPdA, l'hash di ogni singolo file (documento richiesto o presente all'interno di un PdV richiesto), Super Impronta (se presente).
- La **Super Impronta** (opzionale, se presente) generata per il produttore (Azienda) a cui si riferiscono i documenti. [ad esempio presente per tutti i documenti con rilevanza tributaria oggetto di conservazione, propedeutica alla comunicazione dell'impronta dell'Archivio secondo il Provvedimento Attuativo Agenzia delle Entrate n. 2010/143663 del 25 ottobre 2010, abrogato con l'entrata in vigore del DM 17 Giugno 2014]

Per ogni PdD generato viene archiviato il file indice (IPdD) all'interno del Sistema di conservazione, per la tracciatura formale delle richieste di documenti da **"Coopera® *Safe*"**. Questo file indice contiene:

- Id del PdD, generato in seguito al salvataggio su Data Base
- Data della generazione del PdD (in formato UTC)
- Azienda a cui si riferisce il PdD (Rag. Sociale, Id setup, Id azienda, Cod. Fiscale, Partita IVA)
- L'utente che ha richiesto il PdD (Nome, Cognome, Codice Fiscale e/o Partita IVA)
- Responsabile Servizio Conservazione (**RCS**) (Nome, cognome, Cod. Fiscale e/o Partita IVA)
- L'indirizzo IP da cui è arrivata la richiesta di generazione
- PdA consegnati (Id PdA, Hash, Funzione di hash utilizzata, Url file nel Sistema di conservazione e nel PdD)
- La lista dei file richiesti (Id documento, Id tipologia, Nome tipologia, Nome file, Hash file, Funzione di hash utilizzata, Uri file nel Sistema di conservazione e nel PdD)

Le eventuali personalizzazioni di tali pacchetti, specifiche di un contratto, sono descritte nell'allegato "Specificità del contratto".

Torna al sommario

7 IL PROCESSO DI CONSERVAZIONE

Il processo di conservazione **"Coopera® *Safe*"** è governato in tutte le sue fasi dall'Amministrazione del Sistema, che interagisce con le altre entità coinvolte, con il Produttore dei Documenti, con gli Utenti e con eventuali ulteriori gruppi di utenze.

Il Responsabile Servizio Conservazione (**RSC**), in conformità a quanto previsto dall'art. 7 del DPCM 3 Dicembre 2013, gestisce i servizi e le funzioni che garantiscono l'operatività complessiva del modulo applicativo **"Coopera® *Safe*"**.

Nel seguito viene rappresentato il processo di conservazione in conformità all'art. 8 del DPCM 3 Dicembre 2013.

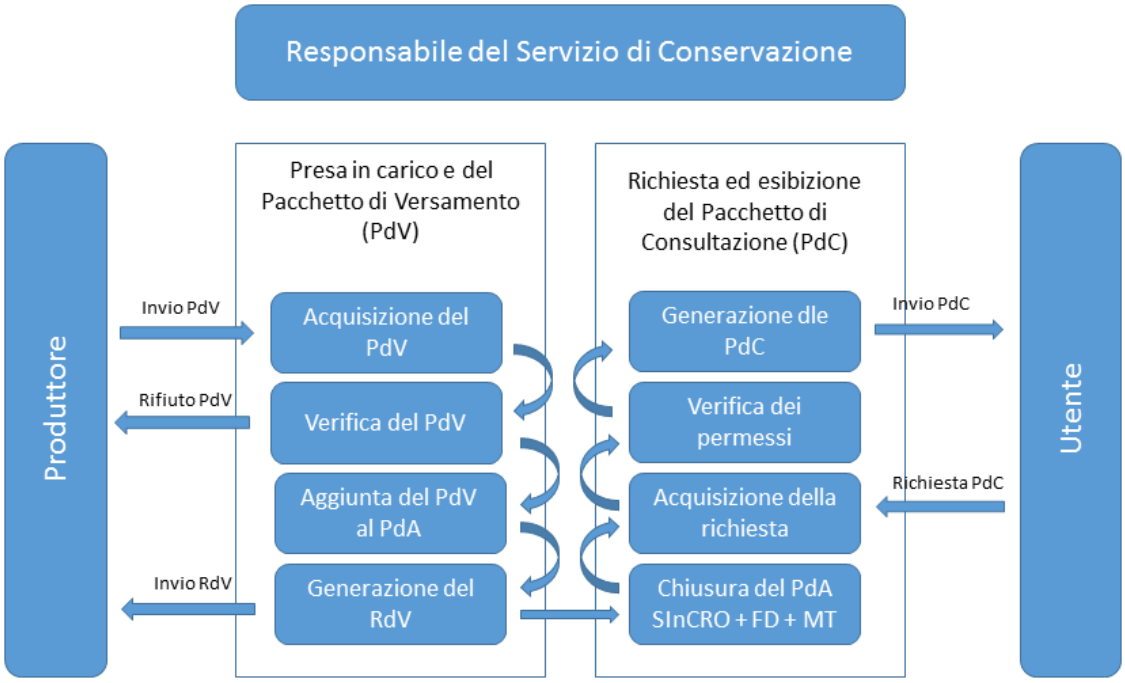


Figura 3 - Processo di versamento, conservazione e consultazione

Per ciascuna delle fasi del processo è stato dedicato un paragrafo che ne descrive i dettagli.

Torna al sommario

7.1 Modalità di acquisizione pacchetti di versamento

Il Soggetto Produttore può scegliere una modalità di utilizzo del servizio tra quelle proposte dal conservatore e riepilogate nella seguente tabella:

Modalità di Versamento	Canale	Descrizione
Integrata	Applicazione web	In questo caso la conservazione avviene in maniera manuale o pianificata direttamente dal modulo di gestione documentale "**Coopera® *Docs*"**.
Esterna	Webservice	In questo caso la conservazione avviene ad opera di un sistema terzo direttamente accedendo ai webservice esposti dal sistema di conservazione **"Coopera® *Safe*".**
Manuale	FTP	In questo caso il trasferimento degli elementi da conservare avviene, secondo specifiche concordate con il

		Cliente, depositando i file ed i relativi indici in un'area FTP appositamente predisposta.

Le funzionalità di versamento ed esibizione sono sempre disponibili anche in modalità manuale, accedendo al servizio di conservazione tramite l'applicazione web di **"Coopera® *Safe*"** con l'utenza personale dell'utente delegato dal Cliente.

Tutte le comunicazioni, inteso come il trasferimento dei dati da e per il sistema di conservazione avviene tramite canale criptato (HTTPS o sFTP), sia nel caso di utilizzo integrato del servizio, sia per tutte le integrazioni applicative previste. In ogni caso, nella definizione dei PdV, è richiesto al Produttore il rispetto dei seguenti paramentri:

- Massimo 4 GB per ogni PdV, allegati ed indici inclusi;
- Massimo 20 mila documenti per lotto (50 mila, allegati inclusi);
- Massimo 5 MB per ogni file versato.

Per quanto riguarda i dati sensibili e giudiziari, così come definito dall'art 22 del Decreto Legislativo 196/2003, essi vengono trattati con tecniche di cifratura, e sono resi illeggibili anche a chi è autorizzato ad accedervi.

Nello specifico la creazione di PdV prevede la restituzione di un identificativo Id (GUID) assegnato al pacchetto che consente di identificarlo in maniera univoca nel sistema di conservazione in tutto il suo ciclo di vita. In particolare, nella modalità sFTP l'identificativo viene restituito mediante un file testuale che viene depositato in una cartella di output definita e concordata tra Produttore e Conservatore.

Il sistema di versamento mette a disposizione del soggetto produttore una serie di funzionalità di validazione che consentono, se necessario, di correggere la composizione del pacchetto di versamento prima della sua acquisizione da parte del conservatore. Il produttore potrà correggere i metadati descrittivi e le relazioni con il contesto archivistico laddove queste non fossero state correttamente impostate in fase di prima produzione dei singoli PdV.

I sistemi di Interdata per la presa in carico dei pacchetti di versamento sono tutti in alta disponibilità e garantiscono la ridondanza dei dati.

Inoltre, nel servizio di conservazione offerto da **"Coopera® *Safe*"**, sono attive procedure per la generazione di backup dei PdV versati dal produttore. Le politiche di salvataggio e backup possono essere definite a livello di classe documentale, tale impostazione consente di specificare per quanto tempo la copia di sicurezza del PdV debba essere mantenuta nello storage dedicato.

Pertanto, in caso di necessità di un recupero dei dati dei PdV ancora non conservati, l'Ente Produttore può richiedere, attraverso un ticket all'area di assistenza tecnico-operativa di Interdata, di attivare la procedura di "restore" delle copie dei PdV mantenute nell'area di storage dedicata, al fine di ricreare il processo di acquisizione dei PdV e quindi dare il via ad un nuovo processo di presa in carico.

Le specifiche sulla sessione di versamento e presa in carico del PdV, il modello-dati del PdV sono dettagliate nella "Scheda Servizio Cliente - Specificità del Contratto."

Tutte le attività di presa in carico dei singoli PdV vengono tracciate tramite il sistema di Log Management integrato nel sistema di conservazione. I log vengono mantenuti per tutto il periodo di conservazione degli oggetti versati.

Identificazione certa del Produttore

Il soggetto Produttore dei pacchetti versati nel sistema di conservazione è soggetto ad una fase di identificazione, che, insieme all'accettazione delle clausole contrattuali, costituisce parte fondamentale della stipula del contratto di erogazione dei servizi.

In fase di identificazione, il Produttore ha l'obbligo di fornire dati anagrafici completi, inclusi i propri punti di contatto e l'indirizzo PEC del Responsabile della Conservazione individuato (e dell'eventuale facente funzione di vicario).

A valle dell'identificazione, le credenziali utente sono generate e trasmesse via PEC al Responsabile della Conservazione (ed all'eventuale vicario), che dovrà attivare il proprio account entro cinque giorni lavorativi effettuando l'accesso al sistema.

Una volta ottenute le credenziali di accesso, il Produttore potrà accedere ai servizi applicativi per i quali si sia registrato. L'identificazione dell'utente avviene mediante lo scambio di tali credenziali fra il client (interfaccia web, nel caso di accesso per versamento manuale, o applicazione terza, nel caso di versamento tramite Web Services, etc.) ed il server di autenticazione centralizzato di Coopera®, che provvede quindi alla generazione (ed assegnazione all'utente) di un token di autenticazione.

Il token viene comunicato al client, che, a sua volta, lo invia alle applicazioni accedute (ad ogni richiesta di servizio effettuata nell'ambito della sessione corrente) nell'header dei pacchetti HTTPS contenenti i dati relativi alle richieste di elaborazione.

Torna al sommario

7.2 Verifiche sui Pacchetti di Versamento e Sugli Oggetti

Il Produttore è incaricato dal Cliente di fornire al Conservatore i Pacchetti di versamento, così come indicato nelle condizioni di fornitura. Il sistema di conservazione, verificherà il rispetto degli stessi requisiti analizzando i pacchetti di versamento sottomessi e ne potrà validare o rigettare il contenuto, ad esempio se i metadati sono formalmente errati o se il file inviato non è in un formato tra quelli abilitati per la conservazione in base alla specifica Descrizione Archivistica (DA).

La verifica prevede che il dato versato sia compatibile con quanto definito per la Descrizione Archivistica (DA) a cui è stato destinato. Vengono verificati in questo passaggio i metadati, i formati, l'univocità dei dati, e quant'altro definito in fase di attivazione del servizio tra il Produttore ed il Conservatore. In caso di esito negativo si ottiene un errore di validazione e la distruzione del pacchetto per il quale si è tentato l'invio. L'evento, a prescindere dal suo esito, è tracciato nel log specifico del Soggetto Produttore che è portato in conservazione a cadenza periodica. Nello specifico gli esiti delle verifiche sono categorizzati in due tipologie: *Warning*, relativo ad errori non bloccanti ed *Error* che indica errori che determinano un rifiuto del PdV.

I controlli eseguiti dal Sistema sui PdV trasmessi sono riassunti nella tabella seguente.

Controllo	Descrizione	Severità
Numero file e documenti	Sono segnalate eventuali incongruenze tra indici e file versati	Bloccante (Error)
Identificativo degli elementi	Sono segnalati eventuali id duplicati all'interno del pacchetto o documenti che presentino Id mancanti	Bloccante (Error)
Formato file	Vengono segnalati eventuali formati non previsti dal sistema di conservazione, dalla relativa Descrizione Archivistica o dall'Allegato 2 del DPCM 3 Dicembre 2013	Bloccante (Error)
Firme elettroniche	Vengono segnalate firme digitali non valide all'atto del versamento o che presentino specifiche anomalie	Bloccante (Error)
Integrità e leggibilità dei file	Vengono segnalati file che risultano illeggibili o incompleti	Bloccante (Error)
Indici e metadati	Vengono effettuati controlli su obbligatorietà, correttezza formale e sequenzialità degli indici di archiviazione	Bloccante (Error)
Date di chiusura future	Vengono segnalati gli elementi che presentano date di chiusura future rispetto e quella definita per il PdV	Bloccante (Error)
Anno di chiusura non coerente	Vengono segnalati gli elementi il cui anno di chiusura è antecedente a quello definito per il PdV	Non bloccante (Warning)

Ulteriori personalizzazioni sui controlli eseguiti sono riportati nella “Scheda Servizio Cliente - Specificità del Contratto” dove è anche definito il livello di severità previsto.

Nella fase di verifica del PdV, i risultati dei predetti controlli vengono tutti registrati dal sistema di logging integrato con la registrazione di un riferimento temporale e delle restanti informazioni necessarie.

Se le verifiche di coerenza eseguite nella fase di presa in carico sono positive il PdV viene accettato dal Sistema di Conservazione, altrimenti l’esito di presa in carico ne evidenzia il rifiuto definitivo come descritto nei paragrafi successivi.

Torna al sommario

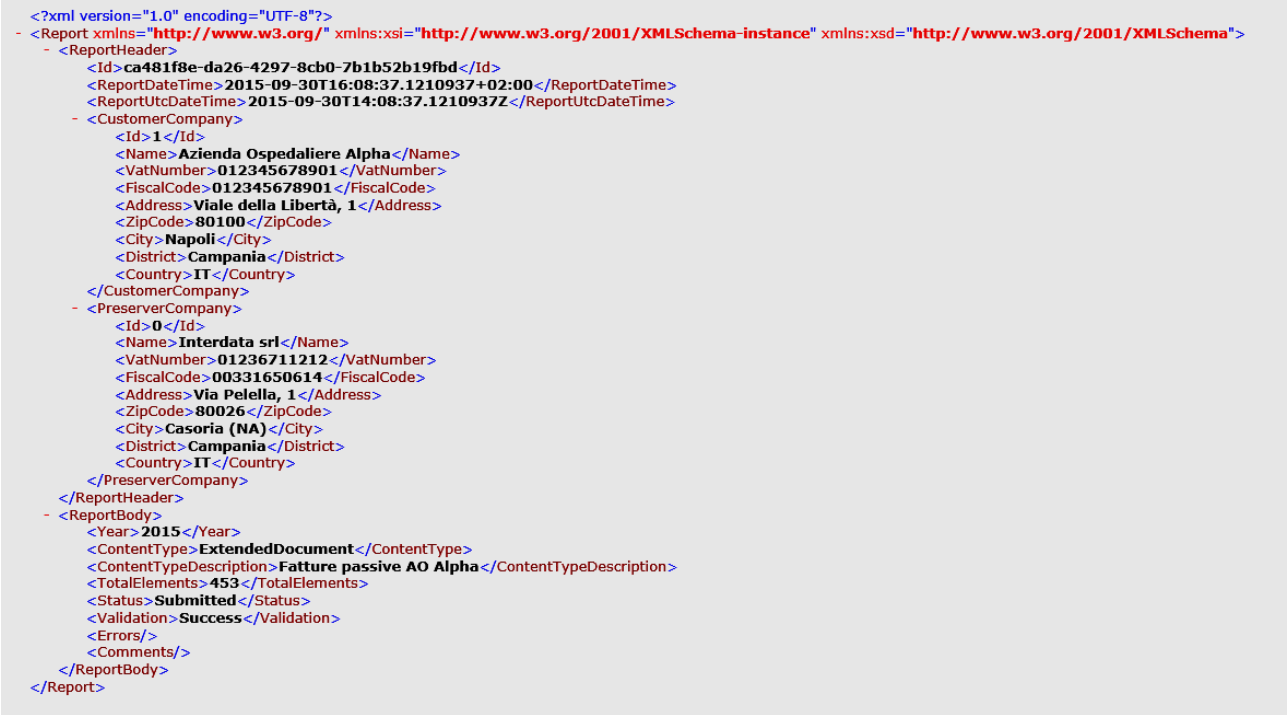
7.3 Accettazione dei Pacchetti di Versamento e generazione del Rapporto di Versamento

Nel caso in cui le verifiche abbiano avuto positivo, secondo quanto previsto dalle regole tecniche (Art. 9, comma 1, lettere d) ed e), il sistema di conservazione accetta il pacchetto e genera un rapporto di versamento, firmato dal Responsabile del Servizio di Conservazione, che attesta la presa in carico del PdV e contiene le seguenti informazioni:

- l’identificativo (UID) del PdV;
- il riferimento temporale relativo al versamento (local e UTC time);
- i dati identificativi dell’organizzazione produttrice;
- i dati identificativi del Conservatore;
- l’anno di riferimento del versamento;
- la tipologie e la descrizione degli elementi versati;
- il totale degli elementi versati;
- il risultato delle operazioni di verifica;
- lo stato di accettazione o rifiuto.

Il report di versamento è in formato xml al fine di consentirne il trattamento automatico da parte di eventuali sistemi terzi.

Di seguito un esempio di report di versamento andato a buon fine:



```
<?xml version="1.0" encoding="UTF-8"?>
- <Report xmlns="http://www.w3.org/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  - <ReportHeader>
      <Id>ca481f8e-da26-4297-8cb0-7b1b52b19fbd</Id>
      <ReportDateTime>2015-09-30T16:08:37.1210937+02:00</ReportDateTime>
      <ReportUtcDateTime>2015-09-30T14:08:37.1210937Z</ReportUtcDateTime>
    - <CustomerCompany>
        <Id>1</Id>
        <Name>Azienda Ospedaliere Alpha</Name>
        <VatNumber>012345678901</VatNumber>
        <FiscalCode>012345678901</FiscalCode>
        <Address>Viale della Libertà, 1</Address>
        <ZipCode>80100</ZipCode>
        <City>Napoli</City>
        <District>Campania</District>
        <Country>IT</Country>
      </CustomerCompany>
    - <PreserverCompany>
        <Id>0</Id>
        <Name>Interdata srl</Name>
        <VatNumber>01236711212</VatNumber>
        <FiscalCode>00331650614</FiscalCode>
        <Address>Via Pelella, 1</Address>
        <ZipCode>80026</ZipCode>
        <City>Casoria (NA)</City>
        <District>Campania</District>
        <Country>IT</Country>
      </PreserverCompany>
    </ReportHeader>
  - <ReportBody>
      <Year>2015</Year>
      <ContentType>ExtendedDocument</ContentType>
      <ContentTypeDescription>Fatture passive AO Alpha</ContentTypeDescription>
      <TotalElements>453</TotalElements>
      <Status>Submitted</Status>
      <Validation>Success</Validation>
      <Errors/>
      <Comments/>
    </ReportBody>
</Report>
```

Figura 4 - Report di versamento con esito positivo

I log delle attività e dei processi, così come tutti i rapporti di versamento, restano in disponibilità del cliente, all'interno del sistema di conservazione per tutta la durata del contratto e sono visionabili e scaricabili al pari di ogni dato conservato.

Torna al sommario

7.4 Rifiuto dei Pacchetti di Versamento e Modalità di Comunicazione delle Anomalie

L'eventuale esito negativo ottenuto a valle della validazione del PdV dovuto al nono superamento dei controlli previsti, implicano il rifiuto del pacchetto di versamento. In questo il sistema di Conservazione genera un rapporto di versamento negativo che, oltre alle informazioni descritte, contiene anche l'elenco degli elementi anomali con il dettaglio delle seguenti informazioni:

- Id di riferimento dell'elemento;
- Descrizione dell'anomalia riscontrata;
- Tipologia dell'anomalia: bloccante (Error) o meno (Warning).

Di seguito un esempio di report di versamento con esito di rifiuto:

```
<?xml version="1.0" encoding="UTF-8"?>
- <Report xmlns="http://www.w3.org/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  - <ReportHeader>
      <Id>5ea5e087-661c-4413-a735-0ea6911f267e</Id>
      <ReportDateTime>2015-09-30T15:55:30.234375+02:00</ReportDateTime>
      <ReportUtcDateTime>2015-09-30T13:55:30.234375Z</ReportUtcDateTime>
    - <CustomerCompany>
        <Id>1</Id>
        <Name>Azienda Ospedaliere Alpha</Name>
        <VatNumber>012345678901</VatNumber>
        <FiscalCode>012345678901</FiscalCode>
        <Address>Viale della Libertà, 1</Address>
        <ZipCode>80100</ZipCode>
        <City>Napoli</City>
        <District>Campania</District>
        <Country>IT</Country>
      </CustomerCompany>
    - <PreserverCompany>
        <Id>0</Id>
        <Name>Interdata srl</Name>
        <VatNumber>01236711212</VatNumber>
        <FiscalCode>00331650614</FiscalCode>
        <Address>Via Pelella, 1</Address>
        <ZipCode>80026</ZipCode>
        <City>Casoria (NA)</City>
        <District>Campania</District>
        <Country>IT</Country>
      </PreserverCompany>
    </ReportHeader>
  - <ReportBody>
      <Year>2015</Year>
      <ContentType>ExtendedDocument</ContentType>
      <ContentTypeDescription>Fatture passive AO Alpha</ContentTypeDescription>
      <TotalElements>453</TotalElements>
      <Status>Rejected</Status>
      <Validation>Error</Validation>
    - <Errors>
      - <ValidationResultItem>
          <ReferenceId>22</ReferenceId>
          <Description>Found a duplicate ID for this element.</Description>
          <Type>Error</Type>
        </ValidationResultItem>
      </Errors>
      <Comments/>
    </ReportBody>
</Report>
```


Figura 5 - Report di versamento con esito negativo

Il rapporto di versamento è quindi chiuso, mediante apposizione di marca temporale, prima della trasmissione al produttore.

Nel caso in cui il versamento sia effettuato da un sistema terzo le notifiche delle anomalie di validazione vengono inviate al sistema produttore, mentre, in caso di versamento manuale l'utente ha la possibilità di verificare il motivo del rifiuto.

Oltre a queste segnalazioni, gli operatori e gli amministratori del sistema di conservazione, ricevono specifiche notifiche sulle cause del problema riscontrato ed il dettaglio del processo in errore.

Ulteriori controlli possono essere eseguiti in merito al rispetto della continuità della numerazione o all'ordinamento cronologico, eventualmente generando ulteriori anomalie riportate nel Rapporto di Versamento, ma ciò è concordato tra produttore e Responsabile del Servizio di Conservazione nella "Scheda Servizio Cliente – Specificità del Contratto".

Il sistema di conservazione, successivamente alla sua generazione, prevede la possibilità di inoltro al produttore dei documenti del RdV tramite e-mail o messa a disposizione via sFTP o tramite chiamata web service.

Pacchetti di versamento rifiutati

Come accennato nei paragrafi precedenti (cfr. par. 7.1), tutte le attività di presa in carico dei singoli PdV vengono tracciate tramite il sistema di Log Management integrato nel sistema di conservazione ed i log sono mantenuti per tutto il periodo di conservazione degli oggetti versati.

Oltre alle informazioni normalmente memorizzate in questo tipo di log (utente che ha richiesta l'operazione, data e tipo di richiesta, esito dell'operazione), per i pacchetti di versamento vengono anche riportati:

- esito di ciascuno dei controlli effettuati sul pacchetto (descritti in dettaglio nei paragrafi precedenti);

- link (o percorso locale) alla copia di backup del pacchetto, mantenuta in un'apposita classe documentale.

Tali log potranno quindi essere utilizzati sia per le normali attività di auditing (ad es., sicurezza e corretto funzionamento degli applicativi), sia per attività di analisi statistica (ad es., analizzando la distribuzione temporale di pacchetti rifiutati per un determinato motivo, la frequenza dei "forzamenti" per determinate tipologie di warning, etc.).

Torna al sommario

7.5 Preparazione e Gestione del Pacchetto di Archiviazione

La generazione dell'IPdA avviene secondo le specifiche dell'Allegato 4 del DPCM 3 Dicembre 2013 e secondo lo standard SInCRO – Supporto all'interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010), che è lo standard nazionale riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione.

Durante il processo di creazione dell'IPdA uno o più pacchetti di versamento vengono aggiunti al pacchetto di archiviazione, tale operazione corrisponde alla chiusura definitiva del processo di conservazione a norma.

Una volta generato l'IPdA viene apposto su di esso la firma digitale del Responsabile del Servizio di Conservazione ed una marca temporale, quindi i Pacchetti di Versamento inclusi nel PdA non potranno più essere modificati. La firma digitale e la marca temporale sono emesse, in conformità alla normativa vigente, da Interdata, rispettivamente in qualità di Certification Authority (CA) e di Time Stamping Authority, in conformità alla normativa vigente.

Il sistema, anche nel caso della generazione dei PdA, registra i log per la tracciatura delle azioni effettuate sui pacchetti di archiviazione.

La procedura di ripristino in caso di corruzione o perdita dei dati dei PdA prevede la gestione dell'incident con livello di priorità massima ed il ripristino attraverso l'utilizzo del PdA copia di backup da parte del team preposto, secondo il piano operativo esposto nella documentazione sulla continuità operativa gestita per la certificazione ISO 27001:2013.

Specifici casi in cui è necessario adottare metodi di crittografia per proteggere i dati conservati nei PdA sono descritti nell'allegato "Scheda Servizio Cliente - Specificità del contratto", che rappresenta l'accordo sulle condizioni di servizio specifiche tra Ente Conservatore ed Ente Produttore.

Periodicamente vengono effettuati dei controlli sui PdA prodotti tali verifiche vengono inserite come annotazione sul sistema di conservazione, e riportati sui report che vengono mantenuti in archiviazione.

Torna al sommario

7.6 Preparazione e Gestione del Pacchetto di Distribuzione ai Fini dell'Esibizione

In risposta ad un ordinativo da parte dell'Utente tramite l'interfaccia di ricerca documenti di **"Coopera® *Safe*"**, il sistema di conservazione fornisce all'Utente richiedente tutto o parte o una raccolta di Pacchetti di Archiviazione, sotto forma di Pacchetto di Distribuzione (PdD).

L'Utente può ricercare da interfaccia web, attraverso l'inserimento di apposite chiavi di ricerca, i documenti come output della ricerca, su cui poi richiedere la distribuzione del relativo PdD attraverso un pulsante "Genera Pacchetto di Distribuzione"; in alternativa un'utenza applicativa autorizzata può richiedere un PdD tramite chiamata web service. Il PdD distribuito dal sistema **"Coopera® *Safe*"** contiene tutte le evidenze di

un singolo documento o quelle di un sottoinsieme di documenti conservati, a seconda della tipologia di PdD richiesta.

Una volta che l'utente richiede un PdD il sistema restituisce tramite canale crittografato (protocollo HTTPS) il pacchetto PdD in formato di cartella compressa .zip dove all'interno l'utente ha a disposizione tutti i file necessari. Le tipologie di Pacchetti di Distribuzione ed i modelli-dati sono descritti nel paragrafo 6.4 del presente manuale.

L'utente può richiedere la generazione di più PdD e ogni azione di richiesta e messa a disposizione del PdD viene tracciata con un identificativo univoco all'interno del sistema di logging integrato e con la registrazione di un riferimento temporale.

Lo storage che mantiene i Pacchetti di Archiviazione e dei Pacchetti di Distribuzione è costituito da 3 repliche, due sul sito primario e una sul sito DR, questa architettura garantisce l'alta affidabilità e il recupero dei dati a seguito di corruzione o perdita dei dati.

Ulteriori informazioni di dettaglio, concordate con il soggetto Produttore, sono descritte nell'allegato "Scheda Servizio Cliente - Specificità del Contratto".

Torna al sommario

7.7 Produzione di duplicati, copie informatiche, descrizione dell'eventuale intervento del Pubblico Ufficiale

L'utente autorizzato ad accedere al sistema di conservazione **"Coopera® *Safe*"** tramite le sue credenziali e può eseguire le ricerche attraverso una interfaccia web e tramite l'ausilio di una serie di chiavi di ricerca (metadati) predefinite.

Una volta ottenuto il risultato della ricerca l'utente ha la possibilità di richiedere la distribuzione di un PdD o più semplicemente può eseguire la richiesta di download dei duplicati dei documenti informatici conservati, per singolo documento o per i di documenti.

La richiesta e l'ottenimento di un duplicato di un documento informatico conservato può essere avanzata anche attraverso chiamate web service da un utente autorizzato.

Inoltre, attraverso il sistema di ticketing aziendale e secondo quanto concordato nella "Scheda Servizio Cliente - Specificità del Contratto", l'utente può inoltrare richiesta in merito alla necessità di ricevere duplicati. Il Conservatore Interdata potrà in tal caso mettere a disposizione secondo la modalità concordata (ad esempio sFTP) in un pacchetto contenitore tutti i duplicati richiesti dall'utente.

Vi sono casi in cui è necessaria la produzione di una copia informatica con attestazione di conformità da parte di un pubblico ufficiale:

- per adeguare il formato del documento all'evoluzione tecnologica attivando un processo di riversamento sostitutivo a seguito dei controlli da parte del Responsabile del Servizio di Conservazione;
- su esplicita richiesta dell'utente in quanto concordato nella Scheda Servizio Cliente – Specificità del Contratto.

In questi casi il Responsabile del Servizio di Conservazione si assicurerà della presenza di un pubblico ufficiale, ma l'attività si intende comunque a carico del soggetto produttore.

Torna al sommario

7.8 Scarto Dei Pacchetti Di Archiviazione

Superato il periodo di conservazione di pacchetti e documenti concordato tra Ente Conservatore e Sogggetto Produttore, il sistema **"Coopera® *Safe*"** deve implementare la procedura di scarto dei pacchetti di archiviazione.

Il sistema notifica (via mail/pec) al produttore con 30 gg di anticipo l'avvio della funzione di scarto per determinati PdA dandone quindi informativa secondo la normativa vigente e fornendo le informazioni necessarie al produttore per valutare l'eventuale richiesta di estensione del periodo di conservazione.

In caso di superamento della scadenza prefissata ed in assenza di richiesta di estensione, il job della procedura di scarto si attiva e produce dei Pacchetti di Scarto (PdS) in relazione ai PdA oggetto della procedura. L'operazione è tracciata nel sistema e viene prodotto un file Indice del Pacchetto di Scarto (IPdS) nel formato UNI SInCRO 11386:2010 firmato digitalmente dal Responsabile del Servizio di Conservazione che grazie al file XSLT può essere visualizzato dal Produttore dei documenti o altri soggetti interessati per la verifica della corretta procedura eseguita.

In ultimo, nel sistema **"Coopera® *Safe*"** viene registrato se la gestione della procedura di scarto è relativa ad archivi pubblici o privati che rivestono interesse storico particolarmente importante secondo (D.Lgs. 22 gennaio 2004, n.42); in questo caso si attiva un alert e la procedura di scarto del pacchetto di archiviazione avviene solo previa autorizzazione della Soprintendenza Archivistica del Ministero dei beni e delle attività culturali e del turismo rilasciata al produttore secondo quanto previsto dalla normativa vigente in materia e secondo gli accordi definiti nella "Scheda Servizio Cliente – Specificità del Contratto".

Torna al sommario

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

La principale struttura-dati a garanzia dell'interoperabilità per Interdata è il Pacchetto di Archiviazione generato secondo le regole tecniche in materia di sistema di conservazione e secondo lo standard nazionale UNI SINCRO 11386:2010.

La sua distribuzione attraverso la richiesta di uno o più Pacchetti di Distribuzione (PdD) tramite diverse funzionalità e modalità (interfaccia web, web service, sFTP, ecc.) messe a disposizione dal servizio **"Coopera® *Safe*"** garantisce la corretta trasferibilità da parte del produttore ad altro conservatore.

Nel caso di riconsegna di tutti i PdA conservati (ad esempio per la chiusura del servizio o per la cessazione anticipata del servizio secondo quanto concordato contrattualmente) il produttore dei documenti (utente) potrà richiedere la loro distribuzione al sistema **"Coopera® *Safe*"**, selezionando la richiesta tramite dei filtri da interfaccia web e l'apposita funzionalità.

Ogni PdD contiene un Indice del PdD, generato secondo lo standard UNI SInCRO 11386:2010 e firmato dal Responsabile del Servizio di Conservazione, che rappresenta un rapporto (verbale) della distribuzione eseguita. Il PdD contiene anche il file XSLT per la corretta visualizzazione dell'IPdD.

Se il Produttore dei documenti volesse richiedere una personalizzazione del servizio di distribuzione con l'esecuzione di attività aggiuntive per la migrazione o per l'interfacciamento diretto di Interdata con altri Conservatori ai fini della trasferibilità, le attività saranno eseguite da Interdata sulla base di quanto concordato nella "Scheda Servizio Cliente – Specificità del Contratto" con il produttore stesso, tali attività restano a carico del Produttore.

Il sistema **"Coopera® *Safe*"** di Interdata e in grado di acquisire pacchetti di versamento/pacchetti di archiviazione conformi con la struttura UNI SINCRO 11386:2010 nel caso di subentro su archivi gestiti da altro conservatore che abbia adottato tale standard per la generazione dell'IPdA.

Torna al sommario

8 IL SISTEMA DI CONSERVAZIONE

Il sistema di conservazione descritto in questo capitolo, **"Coopera® *Safe*"**, è componente della suite applicativa **"Coopera® *Safe*"** di Interdata ed è sviluppato sulla base delle più recenti indicazioni normative, standard e best practice internazionali (cfr. cap. 3) in materia di archiviazione e conservazione documentale sicura e a lungo termine.

Il sistema sviluppato è modulare, configurabile, scalabile verticalmente ed orizzontalmente, multi-user e multi-tenant, basato su di un'architettura orientata ai servizi e sull'impiego di standard e meccanismi di integrazione open, che lo rendono interoperabile e facilmente manutenibile.

Torna al sommario

8.1 Componenti Logiche

Le principali componenti architetturali di **"Coopera® *Safe*®"**, e la loro organizzazione logica, sono rappresentate in figura seguente.

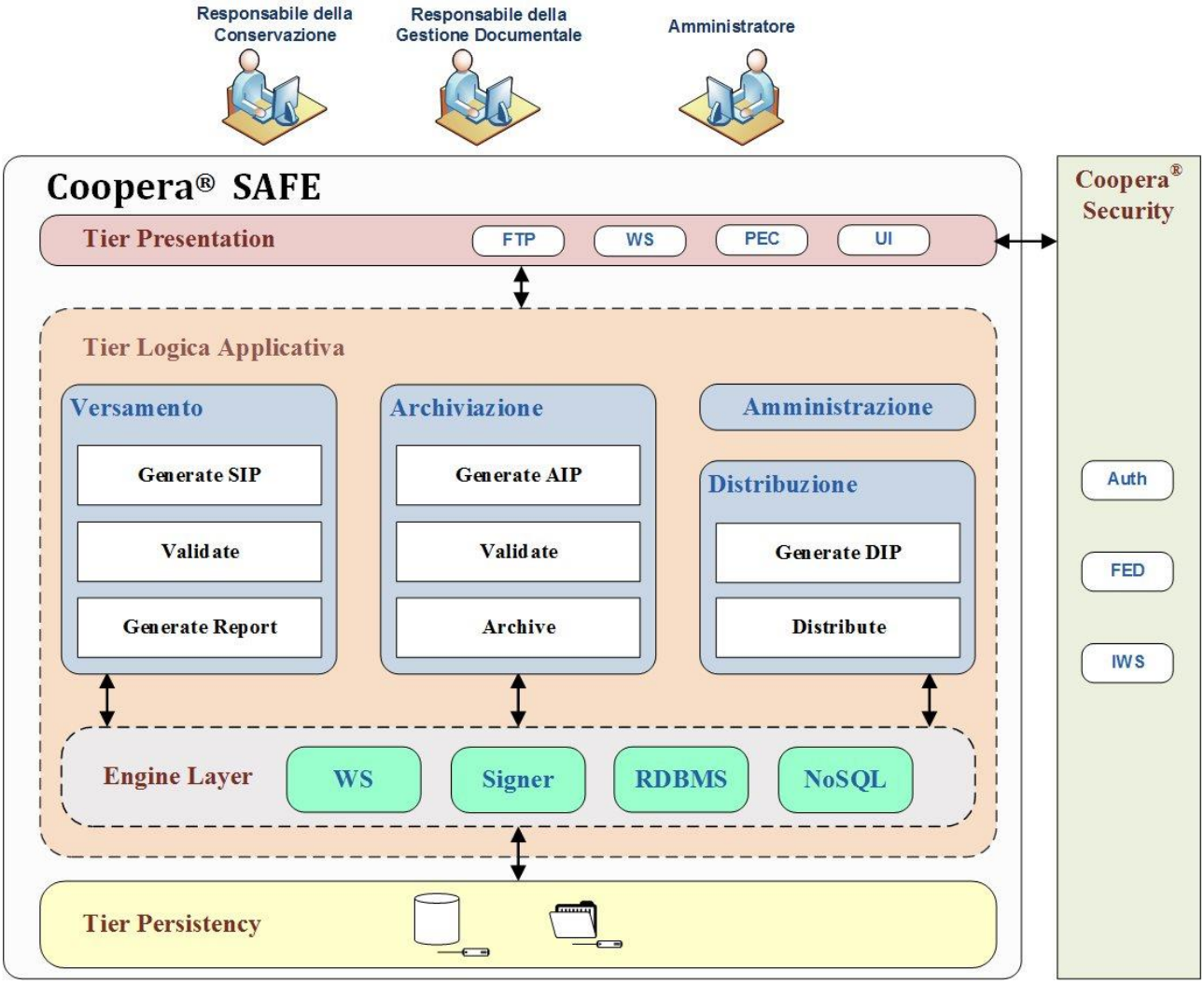


Figura 6 - schema architettura logica

L'architettura adottata da **"Coopera® *Safe*"** è multi-tier e orientata ai servizi, per favorire, attraverso il forte disaccoppiamento dei livelli di logica applicativa e persistenza dati e l'impiego dello standard Web Services,

la facile manutenibilità ed estensibilità del sistema e garantire l'interoperabilità con sistemi applicativi esterni (ad esempio, sistemi di gestione documentale, sistemi contabili e gestionali aziendali).

L'applicativo presenta quindi un livello di presentazione (verticalizzazione del sistema di "Comunicazione Unificata" orizzontale all'intera suite), che ne consente l'interazione con l'esterno e racchiude moduli di interfaccia grafica per i responsabili (ed il coordinatore) di gestione documentale, il responsabile di conservazione e l'amministratore di sistema, interfacce applicative (basate su Web Services) e strumenti di interazione asincrona, in grado di ricevere dati e documenti tramite protocollo FTP (sicuro) e PEC.

Il livello di business logic contiene i motori applicativi che realizzano i servizi di Versamento, Archiviazione e Distribuzione di pacchetti informativi, implementando funzionalità di validazione di documenti e metadati versati, generazione dei pacchetti di archiviazione, firma e marcatura temporale dei pacchetti, generazione di report e predisposizione e trasmissione dei pacchetti di distribuzione. Sono presenti inoltre funzionalità avanzate di amministrazione e configurazione del sistema (profilazione utenti, configurazione dei meccanismi di interazione, attivazione di sistemi di validazione domain-related, etc.).

Il livello di data management offre le funzionalità di gestione consistente della persistenza di dati e documenti gestiti dal sistema, e presenta due componenti fondamentali, un RDBMS (Relational DataBase Management System), per la gestione di dati e metadati strutturati, ed una banca dati document-based, basata su tecnologia NoSQL altamente efficiente e scalabile orizzontalmente, per l'archiviazione, indicizzazione e ricerca dei documenti conservati.

Il livello di security management offre funzionalità di controllo federato degli accessi ed implementa inoltre meccanismi di single sign-on per l'accesso nella medesima sessione a diversi applicativi delle suite.

Torna al sommario

8.2 Componenti Tecnologiche

L'applicativo **"Coopera® *Safe*"** è interamente sviluppato in tecnologia .Net ed è installato su macchine gestite da sistemi operativi Microsoft Server ed il sistema è realizzato per risultare indipendente dal RDBMS e dagli strumenti NoSQL utilizzati.

Lo storage dei dati è realizzato replicando gli archivi di documenti e metadati su due infrastrutture identiche localizzate presso due siti aziendali distinti, con back-up realizzati sulle singole transazioni, per minimizzare la perdita di dati in caso di guasti al sistema primario (e/o disastri presso il sito di produzione).

Sugli archivi sono inoltre applicati meccanismi di sharding e replica in grado di garantirne la consistenza (secondo un paradigma di eventual consistency) ed, al contempo, assicurare il mantenimento, con il crescere delle banche dati, dell'efficienza delle operazioni di archiviazione e ricerca.

Torna al sommario

8.3 Componenti Fisiche

L'applicativo **"Coopera® *Safe*"** è installato sulle infrastrutture CED predisposte presso i due siti aziendali di produzione e disaster recovery, speculari per caratteristiche tecnologiche e organizzate secondo una classica configurazione multi-tier, con disaccoppiamento degli ambienti Application/Data (area Servizi Interni) e Web (DMZ, cfr. figura seguente).

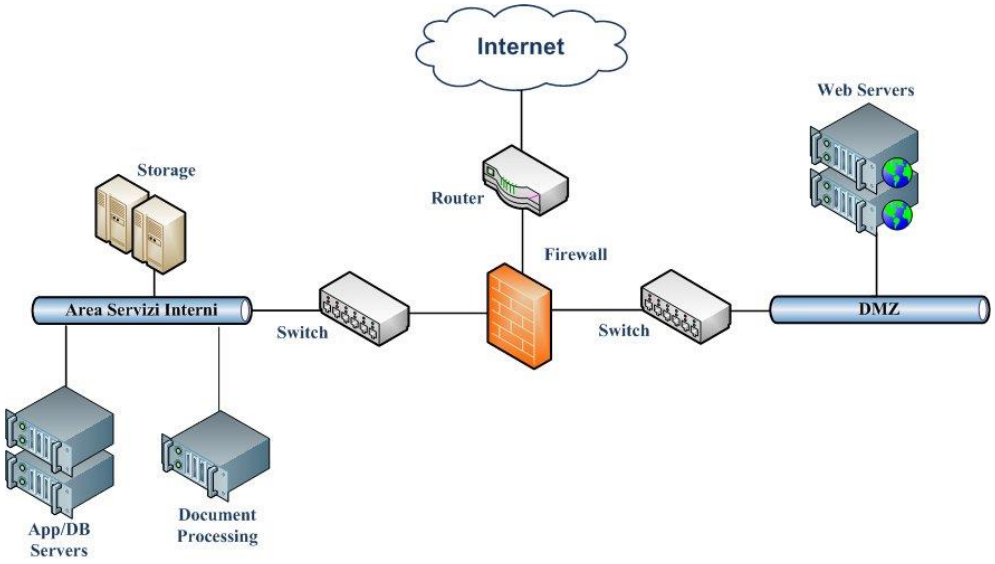


Figura 7 - schema dell'infrastruttura di supporto

Su ciascuna infrastruttura, le diverse componenti hardware sono tutte ridondate e sostituibili a caldo, sì da eliminare ogni single point of failure e ridurre i rischi di soluzione della continuità dei servizi, anche nel caso di interventi manutentivi significativi per ampiezza e durata.

Infine, è implementato un sistema di disaster recovery con backup dei dati sulla singola transazione, riducendo quindi al minimo possibile la perdita di informazioni anche nel caso di disastri o guasti critici sul sito di produzione.

Per approfondimenti ed ulteriori dettagli sulle componenti fisiche impiegate nei CED e sulle tecnologie adottate a garanzia della continuità operativa, si rimanda alla documentazione relativa al sistema Interdata di gestione della sicurezza informatica, certificato ISO/IEC 27001:2013.

Torna al sommario

8.4 Procedure di gestione e di evoluzione

In linea con le più diffuse *best practice* internazionali in materia di IT Service Management, Interdata ha istituito un servizio di conduzione in presidio del sistema **"Coopera® *Safe*"**, allo scopo di:

- garantire la riservatezza, l'integrità e la reperibilità dei documenti conservati, monitorando costantemente il sistema di sicurezza e le possibili fonti di soluzione della continuità dei servizi
- manutenere l'applicativo, in termini sia preventivi, che correttivi ed evolutivi, e garantire, in ogni momento, la conformità del sistema alle norme vigenti
- migliorare efficienza ed efficacia delle attività di incident management

Conduzione e manutenzione del sistema

I requisiti di sicurezza relativi alle attività di conduzione e manutenzione del sistema ed alla gestione dell'incident management e della continuità operativa del servizio di conservazione, così come le procedure di rilascio nel tempo di nuove versioni dei software di base e applicativi, sono specificati nella documentazione del sistema Interdata di gestione della sicurezza informatica, certificato ISO/IEC 27001:2013.

I servizi di conduzione e manutenzione implementati constano delle seguenti componenti fondamentali:

- manutenzione preventiva (conduzione), mirata ad eliminare preventivamente le possibili cause di malfunzionamento o degrado delle prestazioni e ad ottimizzare il funzionamento del sistema nel tempo. Il servizio è basato sull'esecuzione periodica delle seguenti attività
  - verifica, aggiornamento ed ottimizzazione degli ambienti di base e delle configurazioni dei server;
  - rimozione di virus, spyware, malware;
  - verifica del corretto funzionamento, delle performance e dei principali indicatori d'uso (occupazione dati, accessi, etc.) del software applicativo;
- verifica e ottimizzazione dei meccanismi di gestione della continuità operativa, in particolare del back-up dei dati e delle configurazioni sul sito secondario;
- manutenzione correttiva, volta alla rimozione di qualsiasi errore del software, causa dei malfunzionamenti delle procedure e dei programmi, e di qualsiasi difformità riscontrata tra l'effettivo funzionamento del software e quello atteso (previsto dalla documentazione tecnica);
- manutenzione adeguativa, erogata per assicurare la costante aderenza delle procedure e dei programmi all'evoluzione dell'ambiente tecnologico e delle norme e indicazioni ministeriali in materia di conservazione a norma (in un quadro di non variazione degli obiettivi primari delle applicazioni);
- manutenzione evolutiva, mirata all'aggiornamento del sistema a versioni più recenti, arricchite di nuove funzionalità, che risultino di interesse per i clienti sul mercato o consentano di migliorare le prestazioni dell'applicativo.

Di seguito viene descritto il flusso adottato nell'erogazione dei servizi di manutenzione correttiva (al di là dell'origine della richiesta, gli interventi di manutenzione adeguativa ed evolutiva seguono un flusso analogo):

- un problema viene riscontrato dagli operatori in presidio o un/più cliente/i inoltra/no richiesta di intervento correttivo;
- il personale che prende in carico la chiamata provvede a registrare la richiesta di servizio (service request - SR) su di uno strumento di trouble ticketing, impiegato allo scopo di monitorare i servizi di manutenzione (ai fini del loro miglioramento continuo) e di un più semplice tracciamento degli interventi sul sistema;
- alla ricezione della richiesta, lo specialista che l'ha presa in carico effettua una prima analisi (diagnosi) del problema, quindi eventualmente la smista ad una figura diversa (che si occuperà di richiamare l'utente per raccogliere ulteriori informazioni - call back - e dare il via ai necessari interventi);
- vengono quindi poste in essere le azioni risolutive, eventualmente coinvolgendo le ditte fornitrici dell'hardware.

Si osservi che ogni intervento è accompagnato dalla creazione e dall'aggiornamento (fino alla chiusura) di un ticket per la rendicontazione ed il monitoraggio costante dei servizi erogati, e dalla produzione, a chiusura di ciascuna attività di manutenzione e aggiornamento/configurazione, di un resoconto tecnico sugli interventi eseguiti e delle eventuali modifiche alla documentazione tecnica ed ai manuali d'uso del sistema.

Gestione e conservazione dei log

"Coopera® *Safe*" possiede nativamente la capacità di registrare su appositi log tutte le operazioni eseguite e gli eventi di sistema, tenendo traccia almeno dei seguenti dati:

- tipo e descrizione dell'operazione/evento
- nome dell'utente che ha eseguito l'operazione
- indirizzo ip di provenienza delle attività loggate
- data dell'operazione/evento

I log sono conservati per almeno dieci anni da **Interdata**, in un archivio appositamente predisposto sul sistema documentale "**Coopera® *Docs*"** della suite **"Coopera® *Safe*"**.

Monitoraggio del sistema

"Coopera® *Safe*" implementa numerosi sotto processi dediti al controllo e al monitoraggio dei processi, che segnalano eventuali errori o anomalie al personale incaricato dal Responsabile del servizio di conservazione della manutenzione del sistema.

Come indicato in precedenza, il sistema è dotato di un proprio componente di logging (cfr. par. 8.4.2), nel quale sono tracciate tutte le operazioni eseguite e quanto serva a facilitare la diagnosi di eventuali anomalie o guasti.

Inoltre, a garanzia di protezione da eventuali azioni dolose dall'esterno, Interdata ha implementato dei meccanismi automatizzati di monitoraggio (network sensing), in grado di allertare tempestivamente i tecnici in presidio nel caso di attività sospette sulle reti dell'area Servizi Interni e della DMZ, ed un sistema di videosorveglianza e controllo degli accessi alle sale CED, che impedisca ad eventuali intrusi di intervenire sulle macchine dell'infrastruttura.

Infine, sul sistema vengono periodicamente eseguite attività di audit da parte di tecnici specializzati, mirate a verificare il corretto funzionamento dell'applicativo e l'integrità di archivi e banche dati. Tutte le attività di monitoraggio e verifica sul sistema di conservazione sono riepilogate in un verbale di audit prodotto a valle della loro esecuzione.

Change management

Il processo di change management dell'applicativo è attivato dai clienti attraverso istanziazione di una specifica richiesta sulla piattaforma di ticketing adottata.

L'avvio del processo prevede l'aggiornamento e la condivisione di una nuova versione del contratto con i clienti. Tale documento recepisce le specifiche della richiesta di change e, solo se espressamente accettato e condiviso dai clienti, permette di attivare la successiva fase implementativa del change (dalla realizzazione al rilascio in produzione).

Le attività di change management dell'infrastruttura, invece, sono interamente gestite da Interdata, secondo le procedure definite nella documentazione del sistema interno di gestione della sicurezza informatica, certificato ISO/IEC 27001:2013.

Verifica della conformità a norme e standard di riferimento

Con periodicità almeno semestrale il Responsabile del servizio di conservazione (**RSC**) effettua un riesame generale dei servizi applicativi implementati da **"Coopera® *Safe*"** al fine di accertare la conformità del sistema a normative, standard, linee guida ministeriali, requisiti funzionali, etc.

Gestione della sicurezza e valutazione del rischio

Per la descrizione della gestione della sicurezza aziendale, dell'analisi dei rischi e della continuità operativa si rimanda a tutta la documentazione del sistema interno di gestione della sicurezza informatica, certificato ISO/IEC 27001:2013.

Torna al sommario

9 MONITORAGGIO E CONTROLLI

9.1 Procedure di monitoraggio

Le procedure di sicurezza implementate prevedono il monitoraggio dei log di sistema, sia per quanto riguarda i moduli applicativi che per quanto riguarda macchine server, sistemi operativi, dispositivi di rete e strumenti di controllo degli accessi. Il monitoraggio costante dei log consente, infatti, di individuare anomalie e non conformità e procedere ad una più rapida analisi e rimozione dei problemi.

Inoltre, come già accennato in precedenza e meglio dettagliato nei paragrafi seguenti, sul sistema vengono periodicamente eseguite attività di audit da parte di tecnici specializzati, mirate a verificare il corretto funzionamento dell'applicativo e l'integrità di infrastruttura, archivi e banche dati.

I risultati di tutte le verifiche eseguite sul sistema, insieme alla reportistica esaustiva delle anomalie riscontrate nel periodo di monitoraggio e dei relativi interventi risolutivi, sono oggetto di un report di audit interno e vengono inoltre mantenuti all'interno del sistema di asset management e trouble ticketing utilizzato per la gestione degli interventi manutentivi.

Monitoraggio delle funzionalità applicative

Le verifiche applicative interessano, in particolare:

- funzionalità di validazione dei pacchetti di versamento;
- funzionalità di creazione e mantenimento dei rapporti di versamento;
- funzionalità di creazione e mantenimento dei pacchetti di archiviazione;
- funzionalità di distribuzione di pacchetti informativi ai fini di esibizione e produzione di copie;
- servizi di integrazione con sistemi esterni;
- configurazione del sistema per ciascun cliente gestito (anagrafiche di responsabile della gestione documentale e responsabile della conservazione, classi documentali, metadati, profili utente e privilegi, etc.);
- strumenti per l'apposizione della firma digitale e della marca (o semplice riferimento) temporale ai documenti da archiviare o distribuire.

Tali attività sostanzialmente prevedono l'esecuzione di verifiche di conformità su ciascun modulo componente il sistema e test di integrazione mirati a verificare il corretto funzionamento di tali moduli nel realizzare l'intero flusso di archiviazione.

Alle verifiche funzionali seguono poi una serie di test mirati a verificare che il sistema, al crescere della dimensione degli archivi e del numero di utenti collegati contemporaneamente, riesca a mantenere livelli di efficienza accettabili, come definiti dai requisiti di qualità specificati per la piattaforma Coopera®.

Verifiche sull'infrastruttura

Il monitoraggio dell'infrastruttura informatica del sistema SAFE viene eseguito ricorrendo alle funzionalità di controllo offerte dal tool di asset management e trouble ticketing impiegato per le attività di manutenzione ed ai sistemi di network sensing ed access control previsti dal sistema di sicurezza Interdata certificato ISO/IEC 27001:2013.

In particolare, sono costantemente monitorati:

- raggiungibilità via Web dell'applicativo (sia da interfaccia utente che da interfacce applicative);
- funzionamento dei servizi di supporto (ad es., antivirus, servizio di firma, servizio di time stamping);
- occupazione, latenza e performance del sistema di storage;
- processi, transazioni e performance del DBMS;

- log di sistema, con dettaglio delle funzionalità e delle risorse impegnate;
- processi di backup;
- funzionamento del sistema di backup e disaster recovery;
- funzionamento e performance dei sistemi di sicurezza.

Il tool è in grado, infatti, di rilevare, grazie all'installazione di un agent sulle macchine di produzione del sistema di conservazione, i seguenti dati:

- accesso di amministratori di sistema;
- hardware e software installato sul server;
- uso di CPU e RAM, e spazio occupato sui dischi.

Mediante il tool, inoltre, è possibile generare dei report periodici, da inviare al Responsabile dei sistemi informativi e al Responsabile della sicurezza Interdata.

Il dettaglio degli indicatori da tenere sotto controllo e su cui riportare informazioni è specificato nella documentazione del sistema interno di gestione della sicurezza informatica, certificato ISO/IEC 27001:2013.

Altre verifiche

Le attività di audit interessano anche la documentazione e servizi di manutenzione (in termini di efficacia e rispetto dei livelli di servizio prestabiliti), andando a verificare:

- documentazione relativa alla conservazione, anche a fronte di variazione delle condizioni di servizio o di altri elementi di cui tenere traccia (modifiche alle normative, personale impiegato in attività previste dalla conservazione, evoluzioni tecnologiche e del software applicativo, etc.);
- reportistica sui problemi riscontrati sui software applicativi nel periodo di interesse (cadenza almeno trimestrale) e sulle modalità e tempistiche di risoluzione;
- reportistica sui problemi riscontrati su infrastruttura e software di base nel periodo di interesse (cadenza almeno semestrale) e sulle modalità e tempistiche di risoluzione.

Torna al sommario

9.2 Verifica dell'integrità degli archivi

Il processo di verifica dell'integrità dei pacchetti informativi e dei documenti nell'ambito del servizio prevede:

- la verifica automatica della coerenza del numero di documenti archiviati, effettuata confrontando il numero di documenti effettivi presenti nel sistema di conservazione e il numero di record presenti all'interno della struttura del database;
- il controllo dell'integrità delle firme e marcature temporali apposte sui documenti e sugli indici dei pacchetti di archiviazione (su una percentuale prescelta rispetto al totale presenti all'interno del sistema di conservazione).

Per quanto riguarda la verifica di leggibilità, sui documenti (o meglio, su un sottoinsieme dei documenti gestiti scelto casualmente) vengono periodicamente eseguiti i seguenti controlli:

- verifica di integrità (automatica) - attraverso il calcolo automatico dell'hash del documento e relativa comparazione con l'hash registrato in fase di creazione del PdA;
- verifica human-readable (manuale) - sull'insieme dei documenti estratti per la verifica di integrità viene nuovamente effettuata una selezione casuale (il set risultante costituisce circa l'1% del totale verificato) e i documenti visualizzati da un operatore delegato, che verifica se il documento è correttamente leggibile ad occhio umano.

L'esecuzione delle operazioni di controllo ha una cadenza almeno biennale e a valle di ciascuna di esse, viene redatto e conservato (sempre all'interno di SAFE) un verbale di controllo firmato digitalmente dal Responsabile del servizio di conservazione.

Torna al sommario

9.3 Soluzioni adottate in caso di anomalie

Nella figura seguente è schematicamente rappresentato il modello di flusso adottato da Interdata per la gestione di anomalie riscontrate durante il monitoraggio del sistema (o segnalate dagli utenti dell'applicativo).

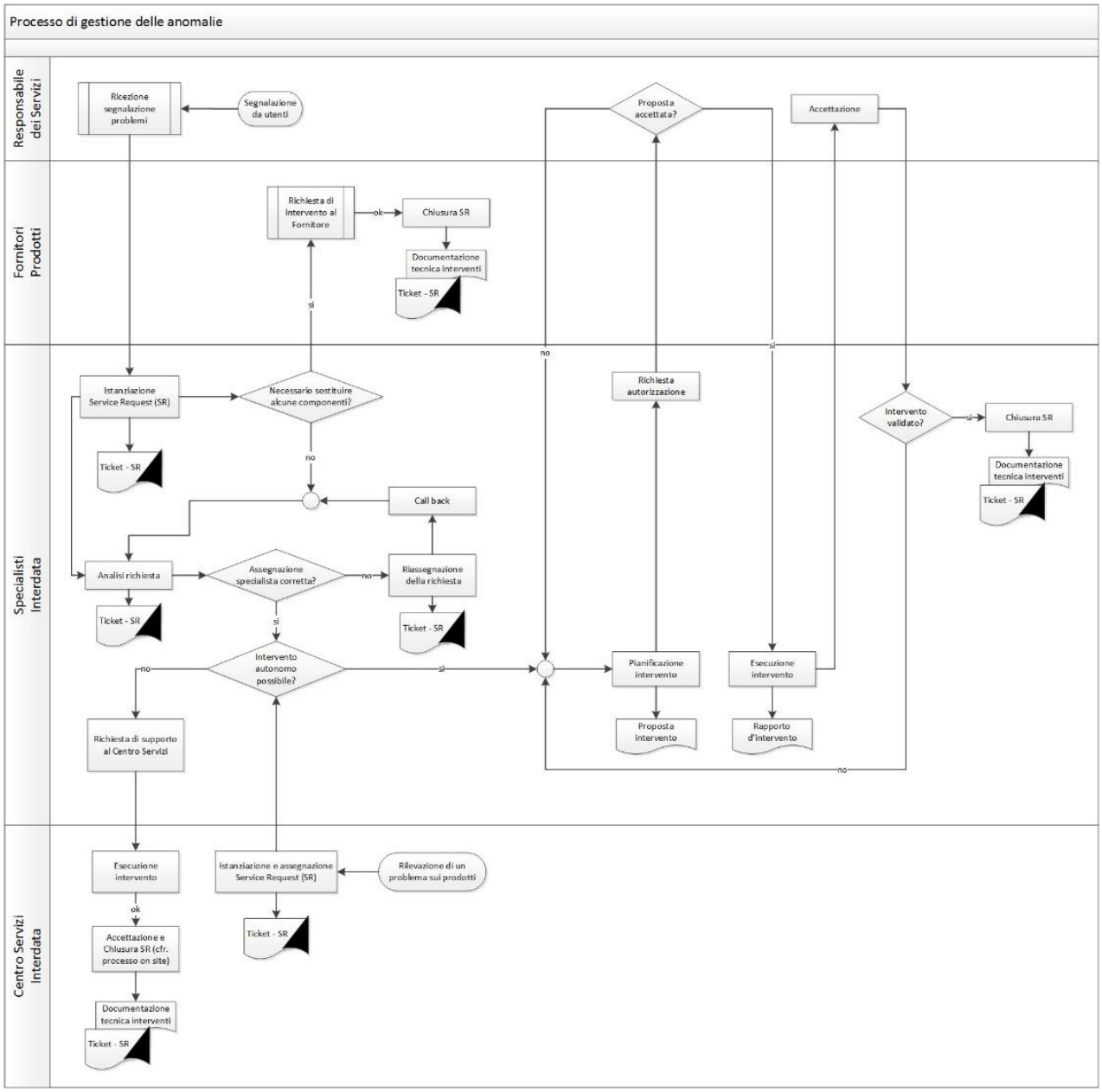


Figura 8 - Flusso di lavoro del processo di gestione delle anomalie

Come evidenziato in figura, il processo di gestione delle anomalie può essere attivato tanto dagli specialisti Interdata responsabili del monitoraggio del sistema di conservazione, quanto dagli utenti del sistema, che possono inoltrare segnalazioni di guasti e difformità o richieste di intervento attraverso diversi canali durante gli orari di erogazione dei servizi di assistenza contrattualizzati.

La richiesta viene raccolta dagli specialisti Interdata, i quali, laddove non già istanziata dall'utente (tramite richiesta online), provvedono a registrare la richiesta di servizio (service request - SR) sullo strumento di trouble ticketing adottato.

Alla ricezione della richiesta, lo specialista che ha preso inizialmente in carico la chiamata di intervento effettua una prima analisi (diagnosi) del problema, eventualmente smistando la richiesta ad una figura diversa, che si occuperà di richiamare l'utente per raccogliere ulteriori informazioni (call back) e dare il via ai necessari interventi. Vengono quindi poste in essere le azioni risolutive, eventualmente coinvolgendo le ditte fornitrici dell'hardware.

Chiaramente, nel caso in cui le richieste non siano risolvibili autonomamente dallo specialista attivato, questi potrà ricorrere alla struttura di Centro Servizi Interdata (costituita dall'insieme di tutte le figure tecniche di alto profilo dell'azienda), che fornirà supporto e supervisione fino al completamento delle attività manutentive e al ripristino del normale funzionamento del sistema.

Si osservi come ogni intervento sia accompagnato dalla creazione e dall'aggiornamento (fino alla chiusura) di un ticket per la rendicontazione ed il monitoraggio costante dei servizi erogati, e dalla produzione, in chiusura di ciascuna attività di manutenzione e aggiornamento/configurazione, di un resoconto tecnico degli interventi eseguiti, il che garantirà ai Responsabili Interdata dei servizi di manutenzione ed ai Clienti dell'azienda il costante controllo sullo stato attuale del sistema e sulla sua evoluzione nel tempo.

Torna al sommario