

Manuale della Conservazione

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Usò pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 1 / 101
-----------------	--------------------	-------------------------------------	---	----------------

Copia Archiviata Elettronicamente	File: Manuale Conservazione_PI_v1.2
-----------------------------------	--

Copia cartacea Controllata in distribuzione ad enti esterni	N°: 0
Rilasciata a:	
Copia cartacea non Controllata in distribuzione ad enti esterni	N°: 0

Versione n.	Pagina n.	Motivo della revisione	Data
1.0	Tutte	Emissione	01/04/2017
1.1	Tutte	Variazione Organigramma e Responsabilità	05/04/2018
1.2	Tutte	Osservatorio dei formati documentali Variazione Organigramma e Responsabilità	06/06/2019

Versione n.	Redazione	Verifica	Approvazione	Data
1.2	Sistemi Informativi	Risorse Umane e Organizzazione; Corporate Affairs; Sistemi Informativi	Sistemi Informativi	06/06/2019

SOMMARIO

- 1 SCOPO E AMBITO DEL DOCUMENTO 5
- 2 TERMINOLOGIA (GLOSSARIO E ACRONIMI) 7
 - 2.1 DEFINIZIONI NORMATIVE 7
 - 2.2 ACRONIMI 10
 - 2.3 DEFINIZIONI PER IL FLUSSO DOCUMENTALE 12
- 3 NORMATIVA E STANDARD DI RIFERIMENTO 13
 - 3.1 NORMATIVA DI RIFERIMENTO 13
 - 3.2 STANDARD DI RIFERIMENTO 14
 - 3.3 DOCUMENTI DI RIFERIMENTO 15
 - 3.4 CERTIFICAZIONI ACQUISITE 15
- 4 RUOLI E RESPONSABILITA' 17
 - 4.1 LE RESPONSABILITÀ NEL PROCESSO DI CONSERVAZIONE 22
 - 4.2 DATI IDENTIFICATIVI DEL RESPONSABILE DEL SERVIZIO DI CONSERVAZIONE 27
 - 4.3 COMPITI E DOVERI DEL RESPONSABILE DEL SERVIZIO DI CONSERVAZIONE 27
 - 4.4 DATI IDENTIFICATIVI DELLA CERTIFICATION AUTHORITY (C.A.) 31
 - 4.5 DATI IDENTIFICATIVI DEI DOCUMENTI DA TRATTARE 31
 - 4.6 LUOGO DI CONSERVAZIONE DEI DOCUMENTI 31
- 5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE 32
 - 5.1 ORGANIGRAMMA 32
 - Strutture organizzative (Art 8 comma 2 lettera b del DPCM 3/12/2013) 32
- 6 OGGETTI SOTTOPOSTI A CONSERVAZIONE 36
 - 6.1 OGGETTI CONSERVATI 36
 - 6.2 OSSERVATORIO DEI FORMATI DOCUMENTALI 36
 - 6.3 PACCHETTO DI VERSAMENTO 37
 - 6.4 PACCHETTO DI ARCHIVIAZIONE 40
 - 6.5 PACCHETTO DI DISTRIBUZIONE 43
- 7 IL PROCESSO DI CONSERVAZIONE 44
 - 7.1 MODALITÀ DI ACQUISIZIONE DEI PACCHETTI DI VERSAMENTO PER LA LORO PRESA IN CARICO 44
 - 7.2 VERIFICHE EFFETTUATE SUI PACCHETTI DI VERSAMENTO E SUGLI OGGETTI IN ESSO CONTENUTI 45
 - 7.3 ACCETTAZIONE DEI PACCHETTI DI VERSAMENTO E GENERAZIONE DEL RAPPORTO DI VERSAMENTO DI PRESA IN CARICO 47

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 3 / 101
-----------------	--------------------	-------------------------------------	---	----------------

7.4 RIFIUTO DEI PACCHETTI DI VERSAMENTO E MODALITÀ DI COMUNICAZIONE DELLE ANOMALIE 48

7.5 PREPARAZIONE E GESTIONE DEL PACCHETTO DI ARCHIVIAZIONE 52

7.6 PREPARAZIONE E GESTIONE DEL PACCHETTO DI DISTRIBUZIONE AI FINI DELL'ESIBIZIONE 52

7.7 PRODUZIONE DI DUPLICATI E COPIE INFORMATICHE E DESCRIZIONE DELL'EVENTUALE INTERVENTO DEL PUBBLICO UFFICIALE NEI CASI PREVISTI 54

7.8 SCARTO DEL PACCHETTO DI ARCHIVIAZIONE 56

7.9 PREDISPOSIZIONE DI MISURE E GARANZIA DELL'INTEROPERABILITÀ E TRASFERIBILITÀ AD ALTRI CONSERVATORI 56

8 IL SISTEMA DI CONSERVAZIONE 57

8.1 COMPONENTI LOGICHE 57

8.2 COMPONENTI TECNOLOGICHE 60

8.3 COMPONENTI FISICHE 61

8.4 PROCEDURE DI GESTIONE E DI EVOLUZIONE 62

9 MONITORAGGIO E CONTROLLI 78

9.1 PROCEDURE DI MONITORAGGIO 78

9.2 VERIFICA DELL'INTEGRITÀ DEGLI ARCHIVI 81

9.3 SOLUZIONI ADOTTATE IN CASO DI ANOMALIE - INCIDENT MANAGEMENT 82

10 PROCEDURE DI GESTIONE DELLA PRIVACY 84

11 ALLEGATO A - SPECIFICHE PER LA DEFINIZIONE DELLE CLASSI DOCUMENTALI 85

11.1 CLASSE DOCUMENTALE 85

11.2 ESEMPIO DI XML 88

11.3 CLASSE DOCUMENTALE CONDIVISA 89

11.4 ESEMPIO DI CLASSE CONDIVISA 90

11.5 ESEMPIO DI XML PER CLASSE COINDIVISA 91

12 ALLEGATO B - SPECIFICHE PER L'INVIO DEI FLUSSI DOCUMENTALI 92

12.1 PDV - PACCHETTO DI VERSAMENTO 92

12.2 CARATTERISTICHE DEL FLUSSO DOCUMENTALE 92

12.3 PDA - PACCHETTO DI ARCHIVIAZIONE 97

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 4 / 101
-----------------	--------------------	-------------------------------------	---	----------------

1 SCOPO E AMBITO DEL DOCUMENTO

La Conservazione è una procedura informatica, regolamentata dalla legge italiana secondo le norme contenute nel DPCM 3/12/2013, che garantisce nel tempo la validità legale di un documento informatico. La normativa in materia di conservazione equipara, sotto certe condizioni i documenti cartacei a quelli elettronici da essi derivati.

La conservazione di materiale digitale nativo o cartaceo a seguito della sua trasformazione in documenti equivalenti in formato elettronico, è resa valida ai fini legali e sicura attraverso l'utilizzo della "Firma Digitale" e del sistema di "Marcatura Temporale", che garantisce la non alterabilità del documento, la sua effettiva paternità e la sua esatta datazione.

Il presente manuale descrive il Sistema di Conservazione offerto dal servizio "Postedoc", erogato da Poste Italiane S.p.A, per il Cliente che intende sottoporre i propri documenti al processo di Conservazione, secondo quanto prescritto dalla vigente normativa.

Il manuale, in generale, ha lo scopo di:

- Descrivere le competenze, i ruoli e le responsabilità degli attori coinvolti nel processo;
- Descrivere come è stato implementato il processo di conservazione e gli aspetti operativi per arrivare alla produzione del dispositivo contenente la documentazione digitale;
- Descrivere il processo di apposizione della Firma Digitale, della Marca Temporale e tutti gli aspetti procedurali inerenti la Conservazione dei documenti nel Sistema di Conservazione;
- Descrivere le procedure di verifica dei documenti e di gestione delle copie di sicurezza.

Il documento recepisce le indicazioni fornite dall'AgID in conformità a quanto espresso dalle nuove **Regole Tecniche derivanti dal DPCM del 3/12/2013** che introduce nuovi criteri inerenti il trattamento dei documenti, apportando modifiche e superando quanto espresso dalla deliberazione CNIPA n. 11/2004; è stato inoltre introdotto il concetto di "**Sistema di Conservazione**", che assicura la conservazione a norma dei

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 5 / 101
-----------------	--------------------	-------------------------------------	---	----------------

documenti elettronici e la disponibilità dei fascicoli informatici, stabilendo le regole, le procedure, le tecnologie e i modelli organizzativi da adottare per la gestione di tali processi.

In riferimento al DPCM del 3/12/2013 si veda in particolare l'Art 8 (Manuale della Conservazione) e l'Art 9 (Processo di Conservazione).

Il manuale consente una puntuale attività di controllo nei casi in cui l'AgID attraverso l'autorità di vigilanza predisponga visite o ispezioni ai fini della verifica di congruenza di quanto dichiarato.

[Torna al sommario](#)

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 6 / 101
-----------------	--------------------	-------------------------------------	---	----------------

2 TERMINOLOGIA (GLOSSARIO E ACRONIMI)

2.1 DEFINIZIONI NORMATIVE

Termine/Acronimo	Definizione
Accreditamento	Processo attraverso il quale l'AgID riconosce ad un soggetto pubblico o privato operante nel settore della conservazione documentale o nella certificazione del processo stesso il possesso di requisiti di un livello più elevato in termini di qualità e sicurezza.
Archivio	Insieme organico di documenti e di loro aggregazioni generato da un Produttore durante le attività previste dal processo di cui è attore o proprietario.
Copia	Processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro, non alterando la loro rappresentazione informatica. Per tale processo non sono previste particolari modalità.
Distribuzione	Processo di estrazione dei documenti conservati ai fini della consultazione o del loro trasferimento ad altro conservatore.
Documento	Per documento s'intende la rappresentazione informatica o in formato analogico di atti, fatti e dati intelligibili direttamente o attraverso un processo di elaborazione elettronica.
Documento informatico	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
Esibizione	Operazione che consente di visualizzare un documento conservato e di ottenerne copia.
Firma digitale	Il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.
Funzione di hash	Una funzione matematica che genera, a partire da una generica sequenza di simboli binari (bit), un'impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari (bit) che la generi, ed altresì risulti di fatto impossibile determinare una coppia di

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 7 / 101
-----------------	--------------------	-------------------------------------	---	----------------

Termine/Acronimo	Definizione
	sequenze di simboli binari per le quali la funzione generi impronte uguali.
Impronta	La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash.
Integrità	Condizione di un documento informatico che non ha subito alterazioni nel contenuto o troncamenti rispetto allo stato originale.
Interoperabilità	Capacità di un Sistema di Conservazione di interagire con sistemi che rispettino almeno le modalità base di indicizzazione e strutturazione del Pacchetto di Archiviazione PdA previste dalla normativa UNI SInCRO 11386:2010.
Leggibilità	Condizione di un documento informatico che ne consentono la fruibilità durante il ciclo di vita e nel successivo periodo di conservazione.
Marca temporale	Una marca temporale (definita all'art. 1 comma 1 lettera "i" del DPCM 30/03/2009) è un'evidenza informatica risultato di una processo informatico, con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi.
Metadati	Insieme dei dati associati ad un documento informatico o a una aggregazione di essi, generati secondo le specifiche previste nell'allegato 5 del DPCM del 3/12/2013, per descriverne nel dettaglio le caratteristiche di struttura, contesto e contenuto ai fini della loro gestione nel tempo durante il processo di conservazione.
Pacchetto Informativo	Contenitore atto a racchiudere un oggetto/i da conservare, documenti informatici e i relativi metadati o i soli metadati di riferimento.
Rapporto di Versamento	Documento informatico contenente le informazioni sulla avvenuta presa in carico da parte del Sistema di Conservazione dei Pacchetti di Versamento (PdV) inviati dal Produttore.
Responsabile della Conservazione	Soggetto che nell'ambito del processo di conservazione ha responsabilità, lato Produttore, nella creazione dei PdV e del loro contenuto e può affidare ad un soggetto esterno il processo di conservazione secondo quanto espresso dal comma 7 e 8 dell'art. 7 del DPCM del 3/12/2013.

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 8 / 101
-----------------	--------------------	-------------------------------------	---	----------------

Termine/Acronimo	Definizione
Responsabile del Servizio di Conservazione	Soggetto che nell'ambito del processo di conservazione ha responsabilità e agisce funzionalmente in conformità a quanto previsto all'art 7 del DPCM del 3/12/2013.
Riferimento temporale	Informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici da una procedura informatica.
Scarto	Processo di eliminazione dei documenti alla fine del loro periodo di conservazione in riferimento al previsto "retention time" per la specifica tipologia di documento.
Sistema di Conservazione	Sistema che assicura: la presa in carico dal Produttore di cui all'art 6 del DPCM 3/12/2013 fino all'eventuale scarto, la conservazione tramite l'adozione di regole, procedure, tecnologie degli oggetti in esso conservati garantendone le caratteristiche di autenticità, integrità, leggibilità, reperibilità.
Supporto ottico di memorizzazione	Mezzo fisico che consente la memorizzazione di documenti informatici mediante l'impiego della tecnologia laser (quali, ad esempio, dischi ottici, DVD, Blu Ray).
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.
Versamento	Processo con cui il Produttore invia al Sistema di Conservazione il Pacchetto di Versamento (PdV) contenente i metadati e i documenti da sottoporre al processo di conservazione.

2.2 ACRONIMI

AgID	Agenzia per l'Italia Digitale (EX DigitPA).
CA	Certification Authority.
CAD	Codice dell'Amministrazione Digitale.
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione (già AIPA).
DigitPA	Agenzia per la PA Digitale (subentrata al CNIPA).
DPCM	Decreto del Presidente del Consiglio dei Ministri.
DPR	Decreto del Presidente della Repubblica.
GU	Gazzetta Ufficiale.
HSM	Hardware Security Model (sistema hardware di firma automatica dei documenti, nel Sistema di Conservazione contiene i dati di firma del Responsabile del Servizio di Conservazione).
IdC	Indice di Conservazione del pacchetto.
PA	Pubblica Amministrazione.
PdA	Pacchetto di Archiviazione.
PdV	Pacchetto di Versamento.
PdD	Pacchetto di Distribuzione.
PEC	Posta Elettronica Certificata.
PU	Pubblico Ufficiale.
RdV	Rapporto di versamento.

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 10 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

TSA	Ente che emette i certificati di marcatura temporale.
TSS	Servizio di marcatura temporale che emette marche temporali utilizzando il certificato emesso da una TSA.
UTC	(Universal Coordinated Time) – Tempo Universale Coordinato – fuso orario di riferimento da cui sono calcolati tutti gli altri fusi orari del mondo.
PDF/PDFA	(Portable Document Format) - Formato per la creazione di documenti complessi indipendenti dalle caratteristiche dell'ambiente di sviluppo del documento stesso.
TIFF	(Tagged Image File Format) - Formato immagine raster – per file di alta qualità. Il formato TIFF è un formato grafico, che permette di memorizzare delle immagini bitmap (raster) di dimensioni notevoli (più di 4Gb compresse), senza perdere qualità e indipendentemente dalla piattaforma o periferiche usate.
JPG	Formato per conservare immagini, compresso con perdita di qualità.
XML	XML (sigla di eXtensible Markup Language) è un metalinguaggio per la definizione di linguaggi di markup ovvero un linguaggio basato su un meccanismo sintattico che consente di definire e controllare il significato degli elementi contenuti in un documento o in un testo.
ODF	(Open Document Format) – Standard documentale basato su XML.

[Torna al sommario](#)

2.3 DEFINIZIONI PER IL FLUSSO DOCUMENTALE

Nome	Descrizione
CLASSE DOCUMENTALE	Insieme di informazioni registrate sul Sistema di Conservazione che identificano il tipo di documento.
NICK AZIENDA	Nome identificativo dell'azienda sul Sistema di Conservazione.
NOME TIPOLOGIA	Nome della Classe Documentale.
DATA CREAZIONE PdV	Data creazione contenuta nel nome stesso del PdV.
ID PdV AZIENDA	Identificativo del PdV assegnato dall'azienda che lo invia.
NOME AZIENDA	Nome descrittivo dell'azienda.
SEQUENZIALE DOCUMENTO	Numero sequenziale assegnato dal Sistema di Conservazione, univoco all'interno di una Classe Documentale che identifica il documento.
SEQUENZIALE FILE	Numero sequenziale assegnato dal Sistema di Conservazione utilizzato per distinguere i diversi file che possono essere presenti all'interno di un singolo documento.

[Torna al sommario](#)

3 NORMATIVA E STANDARD DI RIFERIMENTO

3.1 NORMATIVA DI RIFERIMENTO

- 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;
- [1] D.Lgs.196/2003 e s.m.i. - Codice in materia di protezione dei dati personali recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE»;
- Decreto Legislativo n. 101 del 10 Agosto 2018 - Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati”.
- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. - Codice dei Beni Culturali e del Paesaggio;

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 13 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

- Decreto Legislativo n.52 del 20 Febbraio 2004 - Attuazione della direttiva 2001/115/CE che semplifica ed armonizza le modalità di fatturazione in materia di IVA;
- Decreto Legislativo 13 dicembre 2017 e successive modificazioni – Codice dell'Amministrazione Digitale (CAD);
- Decreto del Presidente del Consiglio dei Ministri 30 Marzo 2009 (GU n. 129 del 6 Giugno 2009) - Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici;
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 (GU n. 59 del 12 Marzo 2014) - 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.

[Torna al sommario](#)

3.2 STANDARD DI RIFERIMENTO

- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ISO/IEC 27001:2017 Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015);
- ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security;

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 14 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

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](#)

3.3 DOCUMENTI DI RIFERIMENTO

Codice Documento	Descrizione
PS_POSTEDOC_PI_2017	Piano della Sicurezza Servizio Conservazione di Postedoc vers. 1.0

3.4 CERTIFICAZIONI ACQUISITE

Certificazione UNI EN ISO 9001:2015

Certificazione ISO/IEC 27001:2013

Certificazione ISO/IEC 20000-1:2011

“Servizio di Conservatore di documenti informatici ai sensi dell’art. 29, comma 1, del D.lgs. 7 marzo 2005, n. 82 in conformità ai requisiti individuati all’Art. 24 del Regolamento (UE) 910/2014 eIDAS come definito nella Circolare di Accreditamento di ACCREDIA e Valutati sulla base della Lista di Riscontro di AgID” [certificato AGID 693172].

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 15 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

“Conformità ai requisiti previsti dal Regolamento (UE) 901/2014 eIDAS per i Prestatori di Servizi Fiduciari Qualificati – Emissione di certificati Qualificati EU, Emissione di validazioni temporali elettroniche qualificate” [validità 21/02/2019 - 23/02/2021].

[Torna al sommario](#)

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Usò pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 16 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

4 RUOLI E RESPONSABILITA'

L'Organizzazione Poste Italiane è basata su processi e ruoli che ne garantiscono il corretto ed efficace funzionamento, in coerenza con il **Sistema Gestione Qualità e Sicurezza aziendale**. La presente sezione illustra i ruoli e le responsabilità degli attori coinvolti nelle principali fasi del processo di Conservazione dei documenti secondo la norma vigente. Poste Italiane copre il ruolo di Responsabile del Servizio di Conservazione assolvendo tutti gli obblighi e le responsabilità in coerenza con la normativa AgID.

È compito del Cliente indicare il proprio Responsabile della Conservazione e uno o più referenti con cui Poste Italiane possa dialogare per il corretto svolgimento di particolari attività che richiedono la presenza attiva del Cliente. (Ad es: verifica del sistema, accesso ai documenti, verifica dello stato e monitoraggio delle prestazioni, autorizzazione alla firma dei documenti nei casi previsti).

Si riporta di seguito lo schema base della matrice di responsabilità che Poste Italiane utilizza per l'erogazione del Servizio di Conservazione, nella tabella sono indicati nelle colonne i ruoli, i referenti, le attività associate, la tipologia contrattuale:

Ruolo	Nominativo	Attività	Tipologia di Rapporto Contrattuale
Responsabile del Servizio di Conservazione	Marco Bongiovanni	Definizione e attuazione delle politiche complessive del Sistema di Conservazione, nonché del governo della gestione del Sistema di Conservazione. Definizione delle caratteristiche e dei requisiti del Sistema di Conservazione in conformità alla normativa vigente. Corretta erogazione del Servizio di Conservazione all'ente Produttore Gestione delle convenzioni, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.	Assunzione a tempo indeterminato

Ruolo	Nominativo	Attività	Tipologia di Rapporto Contrattuale
Responsabile della Sicurezza dei Sistemi per la Conservazione	Rocco Mammoliti	Rispetto e monitoraggio dei requisiti di sicurezza del Sistema di Conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza. Segnalazione delle eventuali difformità al Responsabile del Servizio di Conservazione e individuazione e pianificazione delle necessarie azioni correttive.	Assunzione a tempo indeterminato
Responsabile della Funzione Archivistica di Conservazione	Renzo Mammetti	Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente Produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato. Definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici. Monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del Sistema di Conservazione. Collaborazione 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.	Assunzione a tempo indeterminato

Ruolo	Nominativo	Attività	Tipologia di Rapporto Contrattuale
Responsabile del Trattamento dei Dati Personali	Fabio Sensidoni	Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali. Garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.	Assunzione a tempo indeterminato
Responsabile dei Sistemi Informativi per la Conservazione	Sandra Stefani	Gestione dell'esercizio delle componenti hardware e software di base del Sistema di Conservazione. Monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente Produttore in collaborazione con il Responsabile della manutenzione del Sistema di Conservazione; segnalazione delle eventuali difformità degli SLA al Responsabile del Servizio di Conservazione e individuazione e pianificazione delle necessarie azioni correttive. Pianificazione dello sviluppo delle infrastrutture tecnologiche del Sistema di Conservazione. Controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del Servizio di Conservazione.	Assunzione a tempo indeterminato

Ruolo	Nominativo	Attività	Tipologia di Rapporto Contrattuale
Responsabile dello Sviluppo e della Manutenzione del Sistema di Conservazione	Alessandro Roma	<p>Coordinamento dello sviluppo e manutenzione delle componenti software del Sistema di Conservazione.</p> <p>Pianificazione e monitoraggio dei progetti di sviluppo del Sistema di Conservazione.</p> <p>Monitoraggio degli SLA relativi alla manutenzione del Sistema di Conservazione.</p> <p>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 in collaborazione con il Responsabile funzione archivistica di conservazione.</p> <p>Gestione dello sviluppo di siti web e portali connessi al Servizio di Conservazione.</p>	Assunzione a tempo indeterminato
Referente per la protezione dei dati personali	Francesco Tavone	<p>Collabora con i Responsabili della Sicurezza per la gestione degli adempimenti del "Codice in materia di protezione dei dati personali" definito con Decreto Legislativo 30 giugno 2003, n° 196 e del "Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati".</p> <p>Il Referente: verifica il rispetto della normativa in materia di privacy e supporta l'esercizio dei controlli da parte del Garante;</p>	Assunzione a tempo indeterminato

Ruolo	Nominativo	Attività	Tipologia di Rapporto Contrattuale
		interloquisce con l'AgID ed il Garante per la protezione dei dati personali, anche in relazione ai casi di eventuali violazioni dei dati personali (art. 11, comma 1, lett. o), DPCM); garantisce la corretta gestione dei casi di violazione riguardanti il trattamento dei dati personali dei clienti fino alla loro chiusura.	
Responsabile della gestione degli incidenti di sicurezza per la Conservazione	Nicola Sotira	Assicura le attività di Cyber Threat Intelligence, Early Warning, Brand Protection e Monitoraggio al fine di acquisire conoscenza sulle potenziali minacce, metodi di attacco e vulnerabilità di cyber security e di correlare tali informazioni con i dati interni di sistema, forniti dalle funzioni preposte per prevenire e contrastare potenziali attacchi Coordina il Processo di Gestione Eventi e Incidenti di sicurezza informatica di Gruppo, attraverso la raccolta delle informazioni, la classificazione degli incidenti e la gestione della fase di escalation con l'eventuale notifica ad AgID informando, come descritto nella procedura per la gestione degli incidenti. Gestisce i rapporti di collaborazione e di information sharing interni ed esterni all'organizzazione, assicurando, inoltre, l'interfaccia verso le forze di Polizia e le Istituzioni pubbliche preposte alla sicurezza delle informazioni, ivi incluse le reti CERT nazionali e internazionali Definisce il processo di incident management per la conservazione e lo gestisce in raccordo con le strutture aziendali preposte e con AgID.	Assunzione a tempo indeterminato

Ruolo	Nominativo	Attività	Tipologia di Rapporto Contrattuale
Responsabile delle verifiche e delle ispezioni	Alessandra Toma	Predisposizione ed attuazione dei programmi delle verifiche ed ispezioni periodiche interne, volte ad accertare che i processi siano conformi a quanto richiesto dalla normativa in materia e dalle procedure aziendali di riferimento. Redazione dei rapporti di verifica con i relativi esiti. Monitoraggio dei piani di rientro emessi a seguito delle predette verifiche ed ispezioni. Interfaccia, unitamente al Responsabile del Servizio, dell'organismo di valutazione accreditato per le attività di audit nell'ambito della sorveglianza annuale e del riesame completo della qualifica di prestatore di servizio fiduciario qualificato.	Assunzione a tempo indeterminato

4.1 LE RESPONSABILITÀ NEL PROCESSO DI CONSERVAZIONE

Nel processo di conservazione digitale intervengono numerosi soggetti, a differenti livelli e con diverse responsabilità, sintetizzate nella tabella seguente e dettagliate per singola attività.

Responsabilità Attività	Produttore	Responsabile del Servizio di Conservazione	Responsabile della Funzione Archivistica di Conservazione	Responsabile del trattamento dei Dati Personali	Responsabile della Sicurezza dei Sistemi per la Conservazione	Responsabile dei Sistemi Informativi per la Conservazione	Responsabile dello Sviluppo e della Manutenzione del Sistema di Conservazione	Referente per la Protezione dei Dati Personali	Responsabile della gestione degli incidenti di sicurezza per la Conservazione	Responsabile delle verifiche e delle ispezioni
1 Condizioni Generali di Contratto		R-A								
2 Richiesta di Attivazione		R-A	V	V	V	V	V-E			
3 Specifiche		V			A	A	R-E			

Responsabilità Attività	Produttore	Responsabile del Servizio di Conservazione	Responsabile della Funzione Archivistica di Conservazione	Responsabile del trattamento dei Dati Personali	Responsabile della Sicurezza dei Sistemi per la Conservazione	Responsabile dei Sistemi Informativi per la Conservazione	Responsabile dello Sviluppo e della Manutenzione del Sistema di Conservazione	Referente per la Protezione dei Dati Personali	Responsabile della gestione degli incidenti di sicurezza per la Conservazione	Responsabile delle verifiche e delle ispezioni
Tecniche di Integrazione										
4 Impegno alla Riservatezza		V		R	A			V		
5 Acquisizione del Documento da Conservare		R-A				E	V			
6 Metadati ed Archiviazione		A	R			E	V			
7 Eventuale attestazione e della conformità di quanto memorizzato nel documento d'origine da parte di un Pubblico Ufficiale		R								
8 Creazione del Pacchetto di Versamento (*)	R									
9 Invio al Sistema di Conservazione del Pacchetto	R									

Responsabilità Attività	Produttore	Responsabile del Servizio di Conservazione	Responsabile della Funzione Archivistica di Conservazione	Responsabile del trattamento dei Dati Personali	Responsabile della Sicurezza dei Sistemi per la Conservazione	Responsabile dei Sistemi Informativi per la Conservazione	Responsabile dello Sviluppo e della Manutenzione del Sistema di Conservazione	Referente per la Protezione dei Dati Personali	Responsabile della gestione degli incidenti di sicurezza per la Conservazione	Responsabile delle verifiche e delle ispezioni
di Versamento (*)										
10 Validazione del Pacchetto di Versamento		R				E	V			
11 Generazione e del Pacchetto di Archiviazione		R				E	V			
12 Generazione e del Pacchetto di Distribuzione	R	V				E				
13 Memorizzazione e Creazione delle Copie di Sicurezza		R			V	E	V			
14 Verifica del rispetto della normativa in materia di privacy e supporto all'esercizio dei controlli da								R		

Responsabilità Attività	Produttore	Responsabile del Servizio di Conservazione	Responsabile della Funzione Archivistica di Conservazione	Responsabile del trattamento dei Dati Personali	Responsabile della Sicurezza dei Sistemi per la Conservazione	Responsabile dei Sistemi Informativi per la Conservazione	Responsabile dello Sviluppo e della Manutenzione del Sistema di Conservazione	Referente per la Protezione dei Dati Personali	Responsabile della gestione degli incidenti di sicurezza per la Conservazione	Responsabile delle verifiche e delle ispezioni
parte del Garante.										
15 Interloquisce con l'AgID ed il Garante per la protezione dei dati personali, anche in relazione ai casi di eventuali violazioni dei dati personali.		V						R		
16 Garantisce la corretta gestione dei casi di violazione riguardanti il trattamento dei dati personali dei clienti fino alla loro chiusura.								R		
17 Definisce il processo di incident management per la Conservazione e lo gestisce in raccordo con le strutture		V							R	

Responsabilità Attività	Produttore	Responsabile del Servizio di Conservazione	Responsabile della Funzione Archivistica di Conservazione	Responsabile del trattamento dei Dati Personali	Responsabile della Sicurezza dei Sistemi per la Conservazione	Responsabile dei Sistemi Informativi per la Conservazione	Responsabile dello Sviluppo e della Manutenzione del Sistema di Conservazione	Referente per la Protezione dei Dati Personali	Responsabile della gestione degli incidenti di sicurezza per la Conservazione	Responsabile delle verifiche e delle ispezioni
aziendali preposte e con AgID										
18 Predisposizione ed attuazione dei programmi delle verifiche ed ispezioni periodiche interne, volte ad accertare che i processi siano conformi a quanto richiesto dalla normativa in materia e dalle procedure aziendali di riferimento. Redazione dei rapporti di verifica con i relativi esiti. Monitoraggio dei piani di rientro emessi a seguito delle predette verifiche ed ispezioni.										E-R

[A-Approva, E-Esegue-R-Responsabile-V-Verifica]

(*) Le Responsabilità proprie del Produttore sono definite nelle specifiche contrattuali.

Le attività di audit interno sono garantite dai processi aziendali vigenti in Poste Italiane e documentati nel Manuale del Sistema di Gestione Integrato Servizi ICT e Sicurezza Informatica di Poste Italiane Spa e procedure correlate che prevedono almeno un audit interno annuale sul servizio di Conservazione a norma.

[Torna al sommario](#)

4.2 DATI IDENTIFICATIVI DEL RESPONSABILE DEL SERVIZIO DI CONSERVAZIONE

Ai fini dell'esecuzione del Servizio, Poste Italiane è Responsabile del Servizio di Conservazione nella persona incaricata del ruolo, che agisce ai sensi dell'art. 7 del DPCM del 3/12/2013.

Il Responsabile espletterà tutte le funzioni inerenti al processo di Conservazione ed in particolare i processi di apposizione di firme digitali e marche temporali, essendo dotato di un certificato qualificato emesso secondo la normativa vigente in tema di firma digitale. Tale certificato, installato su dispositivo HSM (Hardware Security Module), è utilizzato dal processo di certificazione dei PdA da sottoporre a Conservazione.

In base a quanto previsto all'art.6 comma 6 della del DPCM 3/12/2013 il Responsabile del Servizio di Conservazione, per la parte operativa delle attività, si avvale a sua volta di personale appartenente alla struttura di Esercizio e Supporto Servizi Digitali operante in SI di Poste Italiane.

Poste Italiane si riserva, a proprio insindacabile giudizio, di sostituire il Responsabile del Servizio di Conservazione, informandone in tal caso il Cliente e l'AgID e aggiornando il presente Manuale della Conservazione.

[Torna al sommario](#)

4.3 COMPITI E DOVERI DEL RESPONSABILE DEL SERVIZIO DI CONSERVAZIONE

Il DPCM del 3/12/2013 attribuisce al responsabile del procedimento di Conservazione (art. 7) precisi compiti e specifiche responsabilità. In conformità a quanto riportato nella norma appena citata viene effettuata una classificazione dei compiti del

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 27 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

Responsabile del Servizio di Conservazione; nella tabella seguente sono riportati da un lato i compiti e, in modo corrispondente, le modalità con cui tali compiti vengono eseguiti:

Responsabile del Servizio di Conservazione	Realizzazione del compito
<p>Compiti organizzativi: definisce i requisiti del Sistema di Conservazione, organizza il contenuto dei supporti di memorizzazione e gestisce le procedure di sicurezza e tracciabilità che garantiscono la corretta conservazione e consentono l'esibizione di ciascun documento conservato (Art 7 comma a).</p>	<p>Tali compiti sono svolti da personale di Poste Italiane appartenente alla struttura di Esercizio e Supporto Servizi Digitali operante in SI/ESSD, tramite le funzionalità rese disponibili dal software del Sistema di Conservazione. L'elenco dei nominativi è tenuto aggiornato dalla struttura Risorse Umane e Organizzazione di Poste Italiane.</p>
<p>Compiti di registrazione delle attività: archivia e rende disponibili, con l'impiego di procedure elaborative, per ogni supporto di memorizzazione le seguenti informazioni:</p> <ol style="list-style-type: none"> 1. Descrizione del contenuto dei documenti; 2. Estremi identificativi del Responsabile del Servizio di Conservazione; 3. Estremi identificativi delle persone delegate dal Responsabile del Servizio di Conservazione, con l'indicazione dei compiti assegnati; 4. Indicazione delle copie di sicurezza. 	<p>Tali compiti sono svolti da personale di Poste Italiane appartenente alla struttura di Esercizio e Supporto Servizi Digitali operante in SI/ESSD, mediante funzionalità rese disponibili dal software del Sistema di Conservazione.</p>
<p>Compiti di manutenzione e controllo del software del Sistema di Conservazione: mantiene e rende accessibile un archivio del software dei programmi utilizzati per il processo di conservazione (Art 7).</p>	<p>Tali compiti sono svolti da personale di Poste Italiane, appartenente alla struttura Digital Application Solutions, mediante l'utilizzo di un sistema di gestione del software, con il quale viene mantenuto il versioning del software realizzato.</p>
<p>Compiti di verifica del sistema: verifica la corretta funzionalità del sistema (monitoraggio) e dei programmi in gestione. (Art. 7 comma e).</p>	<p>Quest'attività è svolta da Poste Italiane. Periodicamente il personale di Poste Italiane appartenente alla struttura di Esercizio e Supporto Servizi Digitali operante in SI/ESSD, effettua le verifiche.</p>

Responsabile del Servizio di Conservazione	Realizzazione del compito
<p>Compiti inerenti alla sicurezza: adotta le misure necessarie per la sicurezza fisica e logica del Sistema di Conservazione e per la realizzazione delle copie di sicurezza dei supporti di memorizzazione. (Art. 7 comma i).</p>	<p>La sicurezza fisica e logica fa riferimento alla sicurezza dei sistemi e delle reti di Poste Italiane e nel rispetto di quanto riportato nel Piano della sicurezza di Poste Italiane. Le attività di creazione delle copie di sicurezza sono effettuate da personale di Poste Italiane, della struttura di Esercizio e Supporto Servizi Digitali.</p>
<p>Compito di richiedere la presenza del Pubblico Ufficiale quando previsto dalla normativa: richiede l'intervento del Pubblico Ufficiale nei casi previsti, assicurando allo stesso l'assistenza e le risorse necessarie all'espletamento delle attività al medesimo attribuite (Art. 7 comma j).</p>	<p>Allo stato attuale, nella fase di Conservazione, le tipologie di documenti oggetto del servizio non necessitano dell'intervento del Pubblico Ufficiale.</p>
<p>Compito inerenti l'espletamento delle attività di verifica e vigilanza: Assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e vigilanza. (Art. 7 comma k)</p>	<p>Predisporre attraverso i membri del team di gestione del Servizio di Conservazione e i loro collaboratori l'assistenza e le risorse necessarie all'attività.</p>
<p>Compito di definire e documentare le procedure di sicurezza per l'apposizione del riferimento temporale</p>	<p>Questo compito è realizzato in collaborazione con la CA di Poste Italiane che emette le marche temporali utilizzate dal Servizio di Conservazione</p>
<p>Compiti di verifica periodica di leggibilità e integrità: verifica periodicamente (tempo non superiore ai 5 anni) la validità e la coerenza dei supporti generati e garantisce l'assistenza alle persone da lui eventualmente delegate. (Art. 7 comma f)</p>	<p>Questo compito è svolto dal personale Poste Italiane, della struttura di Esercizio e Supporto Servizi.</p>
<p>Compiti di garanzia della conservazione e accesso ai documenti: adotta misure per rilevare tempestivamente l'eventuale degrado dei</p>	<p>Questo compito è svolto dal personale Poste Italiane, della struttura di Esercizio e Supporto Servizi Digitali.</p>

Responsabile del Servizio di Conservazione	Realizzazione del compito
sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati. (Art 7 comma g)	
Compiti di duplicazione o copia: Provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale della conservazione (Art 7 comma h)	Questo compito è svolto dal personale Poste Italiane, della struttura di Esercizio e Supporto Servizi Digitali.
Compiti di predisposizione e manutenzione del manuale della conservazione: Predisporre il manuale di conservazione e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti. (Art 7 comma m)	Questo compito è svolto in collaborazione con le strutture aziendali competenti nei rispettivi settori, legale, tecnico, sicurezza e qualità ai fini di una compilazione ed un aggiornamento coerente con le evoluzioni commerciali, tecniche e normative.
Generazione e produzione del pacchetto di distribuzione: Genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione. (Art 7 comma d)	Questo compito è svolto dal personale Poste Italiane, della struttura di Esercizio e Supporto Servizi Digitali.
Generazione del rapporto di versamento: Genera il rapporto di versamento, secondo le modalità previste dal manuale della conservazione (Art 7 comma c)	Questo compito svolto dal Sistema di Conservazione viene monitorato dal personale Poste Italiane, della struttura di Esercizio e Supporto Servizi Digitali.
Gestione del processo di conservazione: gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente. (Art 7 comma b)	Questo compito è svolto in collaborazione con il team di gestione del Sistema di Conservazione che opera nella struttura di Esercizio e Supporto Servizi Digitali.

Nota:

Il Responsabile del Servizio di Conservazione non è responsabile del contenuto dei singoli Documenti né degli indici e relativi attributi associati a

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Usò pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 30 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

ciascun Documento che sono a carico del Responsabile della Conservazione incaricato dal Cliente. È pertanto responsabile esclusivamente degli aspetti inerenti la gestione, la corretta indicizzazione in base agli attributi definiti dal Cliente, e la conservazione dei documenti stessi, nel pieno rispetto della normativa vigente. La conformità dei documenti trasmessi ai corrispondenti originali è assicurata dalla formale autorizzazione alla Conservazione da parte del Cliente, eseguita mediante la sottoscrizione del contratto per la fornitura del servizio. Per tali fini il Responsabile del Servizio di Conservazione opera d'intesa con il Responsabile del Trattamento dei Dati Personali, con il Responsabile della Sicurezza dei Sistemi per la Conservazione e con il Responsabile dei Sistemi Informativi per la Conservazione.

[Torna al sommario](#)

4.4 DATI IDENTIFICATIVI DELLA CERTIFICATION AUTHORITY (C.A.)

I certificati di firma digitale utilizzati dal processo di Conservazione sono rilasciati dalla Certification Authority di Poste Italiane con Dname: CN = Poste Italiane EU Qualified Certificates CA, 2.5.4.97 = VATIT-01114601006, O = Poste Italiane S.p.A., C = IT, mentre i certificati di marcatura temporali sono emessi dalla Certification Authority di Poste Italiane con Dname: CN = Poste Italiane Time Stamping Authority, 2.5.4.97 = VATIT-01114601006, O = Poste Italiane S.p.A., C = IT accreditata presso AgID secondo la normativa vigente.

[Torna al sommario](#)

4.5 DATI IDENTIFICATIVI DEI DOCUMENTI DA TRATTARE

I documenti da sottoporre a Conservazione fanno riferimento alle classi documentali definite per il Cliente, i cui attributi sono conformi allo standard di definizione previsto da Poste Italiane secondo la normativa vigente.

[Torna al sommario](#)

4.6 LUOGO DI CONSERVAZIONE DEI DOCUMENTI

I documenti sono conservati in appositi dispositivi di storage ad alta affidabilità all'interno dei Data Center di Esercizio di Poste Italiane così come esplicitato al paragrafo 8.4 del presente Manuale.

[Torna al sommario](#)

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 31 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 ORGANIGRAMMA

Strutture organizzative (Art 8 comma 2 lettera b del DPCM 3/12/2013)

Il Servizio di Conservazione vede la compartecipazione di più soggetti, ognuno dei quali ha specifiche responsabilità. A seguire è rappresentato l'organigramma aziendale in cui sono evidenziate le funzioni aziendali, che a vario titolo, sono maggiormente coinvolte nel Servizio di Conservazione.

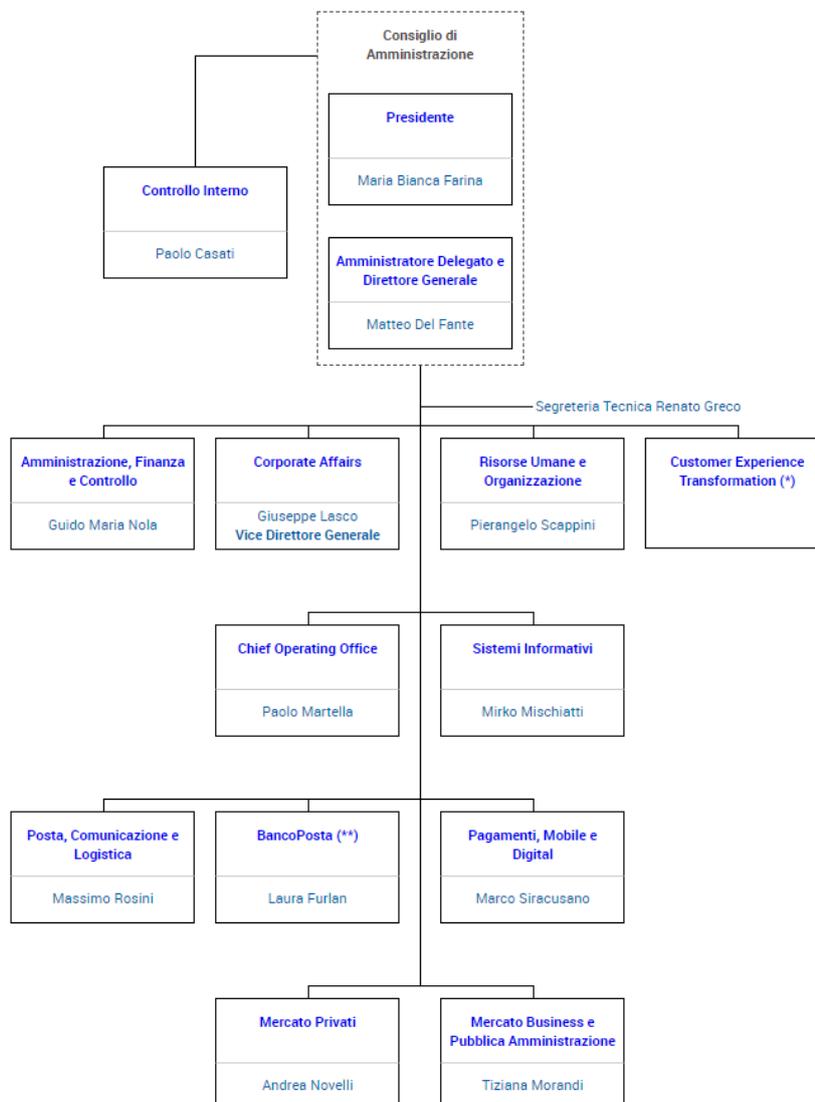


Figura 1 - Organigramma Aziendale Poste Italiane S.p.A.

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 32 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

Di seguito è riportata una breve descrizione delle suddette funzioni.

Chief Operating Office, con la responsabilità di garantire, attraverso un modello accentrato, la gestione dei servizi al cliente e di back office. All'interno operano, fra le altre, le seguenti funzioni:

- Servizi di Assistenza Clienti, con il compito di assicurare l'erogazione dei servizi di assistenza per tutta la clientela di Poste Italiane;
- Servizi di Back Office, con il compito di assicurare le lavorazioni e le attività di back office;
- Qualità e Customer Experience con la responsabilità di garantire la definizione delle metodologie per la rilevazione della customer experience e di coordinare, a livello di Gruppo e per tutti i prodotti/servizi/canali/segmenti di mercato, le attività di ascolto dei clienti attraverso la realizzazione di campagne di misurazione.

Sistemi Informativi, che presidia lo sviluppo e l'esercizio dell'ICT, rappresenta uno dei principali partner di riferimento delle funzioni di business con il compito di contribuire ad orientare l'evoluzione dell'offerta del Gruppo, favorendo l'introduzione di nuovi servizi soprattutto in chiave digitale.

Corporate Affairs, con la responsabilità di presidiare le attività di comunicazione esterna e interna, acquisti, immobiliare, relazioni istituzionali, affari legali e societari, nonché quelle relative alla tutela aziendale, al governo dei rischi di Gruppo e antiriciclaggio di Gruppo. All'interno, tra le altre funzioni, opera la funzione Tutela Aziendale che assicura le attività di:

- indirizzo e coordinamento delle tematiche di sicurezza delle informazioni;
- supporto alle altre funzioni aziendali per la corretta applicazione dei principi e delle regole di protezione dei dati personali;
- raccolta delle informazioni su tutti gli incidenti informatici di sicurezza informatica in conformità con le normative nazionali ed internazionali.

Posta, Comunicazione e Logistica, alla quale è attribuita la responsabilità di garantire la gestione e lo sviluppo dei servizi di Firma Digitale, Posta Elettronica Certificata e SPID, collaborando per il rispetto della conformità al contesto normativo di riferimento e degli adempimenti.

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 33 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

Nell'ambito delle funzioni SI e CA/TA, sono concentrate le principali responsabilità afferenti al Servizio di Conservazione.

Nella tabella seguente sono riportate le figure organizzative previste dalla normativa di riferimento e la loro collocazione nella organizzazione aziendale:

Figura Organizzativa RSO	Funzione aziendale di riferimento
Responsabile del Servizio di Conservazione	SISTEMI INFORMATIVI/ESERC E SUPP SERV DIGIT/SUP SERV DIG REG A
Resp. della Funzione Archivistica di Conservazione	SISTEMI INFORMATIVI/ESERC E SUPP SERV DIGIT/SUP SERV DIG REG A
Responsabile del Trattamento dei Dati Personali	SISTEMI INFORMATIVI/ESERC E SUPP SERV DIGIT
Responsabile della Sicurezza dei Sistemi per la Conservazione	CORPORATE AFFAIRS/TUTELA AZIENDALE/SICUREZZA INFORMATICA
Responsabile dei Sistemi Informativi per la Conservazione	SISTEMI INFORMATIVI/ESERC E SUPP SERV DIGIT/SOM WEB,CO DIG C A
Responsabile dello Sviluppo e della Manutenzione del Sistema di Conservazione	SISTEMI INFORMATIVI/DIGITAL APPL SOLUTIONS/DAS FINANZ E ASSICU
Referente per la Protezione dei Dati Personali	CORPORATE AFFAIRS/TUTELA AZIENDALE/PRIVACY
Responsabile della gestione degli incidenti di sicurezza della Conservazione	CORPORATE AFFAIRS/TUTELA AZIENDALE /CERT
Responsabile delle verifiche e delle ispezioni	CORPORATE AFFAIRS/TUTELA AZIENDALE/SICUREZZA INFORMATICA

I soggetti produttori, ai fini del trattamento dei loro documenti nel processo di conservazione a norma dei documenti offerto da Poste Italiane, affidano il Servizio di Conservazione alle sue strutture organizzative e infrastrutturali in accordo con quanto stipulato attraverso il contratto di servizio e in conformità alle clausole contenute nei moduli di **Richiesta di Attivazione** e **Condizioni Generali di Servizio**.

Di seguito la struttura organizzativa preposta alla gestione del Sistema di Conservazione:

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Usò pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 34 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

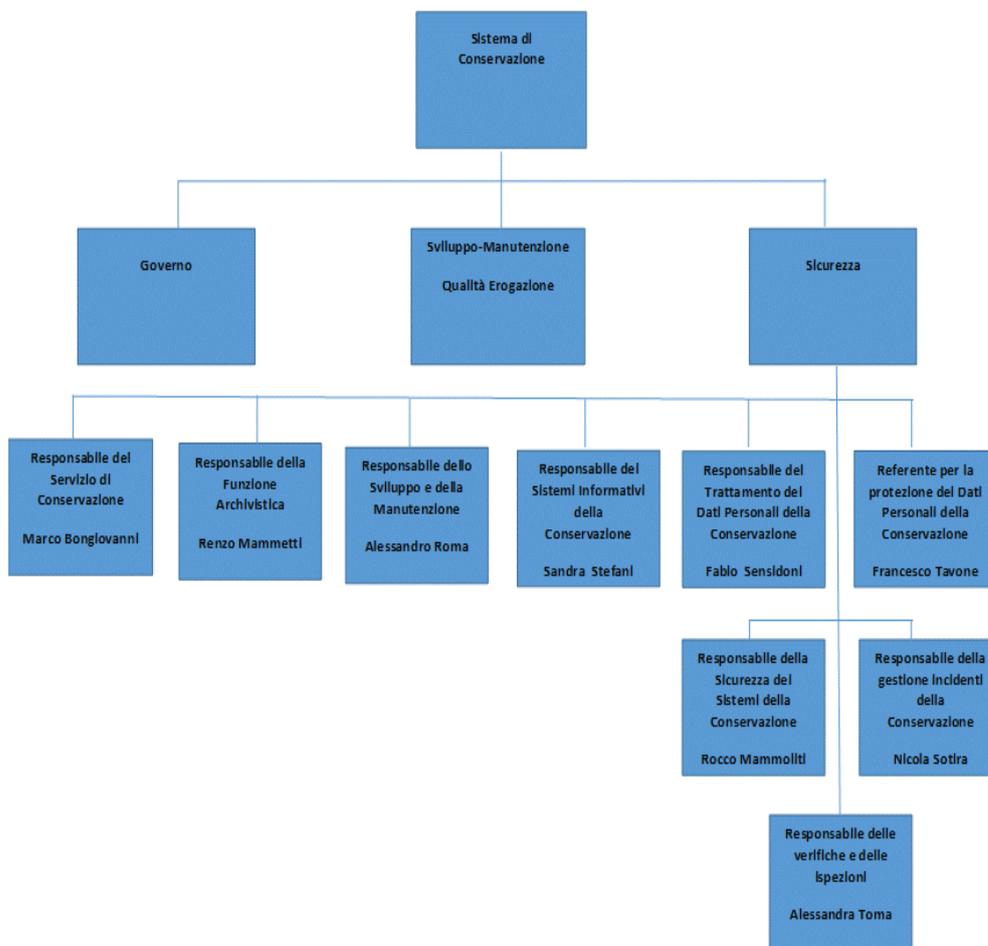


Figura 2 - Struttura Organizzativa per la Gestione del Sistema di Conservazione

[Torna al sommario](#)

6 OGGETTI SOTTOPOSTI A CONSERVAZIONE

6.1 OGGETTI CONSERVATI

I documenti trattati nel Sistema di Conservazione "POSTEDOC" sono di tipo informatico. Non sono oggetto di Conservazione i documenti analogici ed in particolare i documenti analogici unici la cui conformità al documento informatico deve essere accertata da un pubblico ufficiale.

In conformità al DPCM 31/12/2013, con riferimento all'allegato 2 del "Manuale della Conservazione" di Poste Italiane, le tipologie di documenti accettate dal processo di conservazione e i loro visualizzatori attualmente disponibili sono:

- PDF – PDF/A – Adobe Acrobat Reader DC 2018.009.20044 Italian For Windows
- TIFF – Viewer standard visualizzazione immagini su piattaforma Windows
- JPG - Viewer standard visualizzazione immagini su piattaforma Windows
- OOXML (Office Open XML) – Browser: Mozilla – Chrome - Explorer
- ODF (Open Document Format) – Browser: Mozilla – Chrome - Explorer
- XML – Browser: Mozilla – Chrome - Explorer
- TXT – Microsoft Wordpad - Notepad
- EML - RCF 2822/MIME (standard di riferimento per I messaggi di posta elettronica) – Client di Poste Elettronica – Outlook – Thunderbird
- CAdES, PAdES, XAdES

In caso di formati non previsti dalla normativa sarà compilato un allegato - **Formati fuori Standard** al documento di "**Specificità del Contratto**" nel quale saranno descritti i formati documentali di cui il cliente richiede il trattamento e le motivazioni della richiesta di trattamento in conservazione dello specifica tipologia diversa da quelle previste.

[Torna al sommario](#)

6.2 OSSERVATORIO DEI FORMATI DOCUMENTALI

Nell'ambito organizzativo dei task a supporto del servizio di conservazione è prevista l'attività periodica di un team con funzioni di osservatorio tecnologico, che effettua il

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 36 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

monitoraggio della evoluzione tecnologica dei formati in relazione al versioning dei relativi viewers.

L'analisi dell'obsolescenza dei formati svolta dall'osservatorio tecnologico è finalizzata a:

- generare la matrice di corrispondenza tra formati archiviati nel sistema di conservazione e versione corrente dei rispettivi viewers.
- pubblicare la matrice sul sito del conservatore all'url <http://postecert.poste.it/conservazione/documentazione.shtml>
- indirizzare il "Change Management" in materia di formati e tecnologie nella fase di monitoraggio periodico dei risultati relativi alla leggibilità dei documenti conservati.

Il monitoraggio periodico sui risultati relativi alla leggibilità dei documenti conservati può prevedere, se si ravvisano specifiche necessità, il riversamento digitale, come una attività subordinata alle fasi di:

- definizione dei nuovi formati e del relativo software per l'esibizione;
- individuazione/progettazione del software di controllo del nuovo formato;
- individuazione/progettazione del software di conversione dei formati;
- progettazione della elaborazione per il riversamento.

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

[Torna al sommario](#)

6.3 PACCHETTO DI VERSAMENTO

Il pacchetto di versamento (PdV) viene generato dal Produttore secondo le specifiche dettate da Poste Italiane, a seguito della definizione delle Classi Documentali da parte del Cliente. L'invio del pacchetto avviene secondo le modalità prescelte in sede di adesione al contratto, via interfaccia Web o attraverso i Web Services esposti dal Sistema di Conservazione e interfacciati dall'utente secondo le modalità indicate da Poste Italiane ovvero attraverso altri protocolli predefiniti con il cliente ma comunque sempre attraverso un canale crittografato.

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 37 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

Le modalità di creazione delle classi documentali sono descritte nell'apposito documento allegato **Specifiche per la definizione delle classi documentali - vedi Allegato A – Cap. 11**

Le modalità di preparazione del pacchetto di versamento sono descritte nell'allegato: **Specifiche per l'invio dei flussi documentali - vedi Allegato B – Cap. 12**

Eventuali personalizzazioni di tali pacchetti e protocolli di trasferimento richiesti dal cliente, sono descritte nell'allegato "**Specificità del contratto**".

Il Sistema di Conservazione Postedoc è in grado di gestire diverse tipologie di oggetti informatici.

Il Sistema di Conservazione è in grado di gestire gli oggetti informatici sottoposti a conservazione **distinti per ogni singolo Produttore.**

In tal senso consente di definire parametri personalizzati per ogni Produttore, in base a quanto contenuto negli accordi stipulati all'atto della sottoscrizione del Contratto di Servizio.

Nel Contratto di Servizio, "Specificità del Contratto" perfezionato tra Poste Italiane e il Produttore sono elencate e descritte le tipologie di documenti informatici sottoposte a conservazione e le relative politiche di conservazione.

La definizione delle politiche di conservazione da adottare in relazione ai singoli oggetti informatici che verranno trattati dal processo di Conservazione viene consolidata a valle delle attività di analisi documentale che precedono la fase di attivazione del servizio.

In particolare, le predette politiche di conservazione relative agli oggetti da conservare riguardano:

- la natura del documento;
- la classe documentale;
- la descrizione dei formati 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;
- le caratteristiche delle eventuali sottoscrizioni digitali;

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 38 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

- il periodo di conservazione per ogni tipologia di classe documentale;
- eventuali altre politiche specifiche del cliente richieste nel processo di conservazione.

La descrizione delle tipologie documentali e le politiche di conservazione sono riportate in dettaglio in una tabella allegata al documento "Specificità del contratto" e **sono caratteristiche di ciascun Produttore, dei documenti e di ogni specifica tipologia documentale di cui si richiede la conservazione.**

RdV – Rapporto di Versamento

Per ogni PdV ricevuto il Sistema di Conservazione produce il **Rapporto di Versamento** nel quale viene indicato l'esito delle verifiche e viene memorizzato su apposito database, oltre che sul file system a valle dell'apposizione di un riferimento temporale;

Il RdV è un file xml e contiene al minimo i seguenti elementi:

- Informazioni sul PdV
- Nel caso sia presente, l'identificativo sul Sistema di Conservazione dell'utente che ha caricato il PdV
- L'identificativo del PdV sul Sistema di Conservazione
- L'esito delle verifiche
- L'eventuale messaggio/codice di errore
- Il riferimento temporale della verifica
- La lista dei file contenuti nel PdV

Di seguito un esempio di Rapporto di Versamento

```
<?xml version="1.0" encoding="UTF-8"?>
<RdV>
  <file_archivio>file_archivio.zip</file_archivio>
  <file_controllo>file_controllo.zip</file_controllo>
  <hash_file_archivio alg="sha-256">hash1</hash_file_archivio>
  <hash_file_controllo alg="sha-256">hash2</hash_file_controllo>
  <utente>mario.rossi</utente>
```

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 39 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

```
<id_pdv>1234</id_pdv>
<esito>accettato</esito>
<!--           <descrizione_errore></descrizione_errore>           -->
<elenco_file>
  <file>file1.pdf</file>
<file>file2.jpg</file>
  ...
  <file>filen.doc</file>
</elenco_file>
</RdV>
```

Il RdV è reso disponibile al Produttore in vari modi:

- Tramite interfaccia web
- Tramite un apposito web-service
- Altri protocolli definiti in sede contrattuale

6.4 PACCHETTO DI ARCHIVIAZIONE

Il Sistema di Conservazione adotta le specifiche di trattamento definite dallo standard Uni SinCRO 11386:2010 per la fase di ARCHIVIAZIONE. Il livello di Implementazione è di seguito descritto.

Per l'implementazione del formato si è utilizzato come documento di specifiche tecnico-funzionali quanto definito nelle nuove regole tecniche della Conservazione emesse con il DPCM 3/12/2013.

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Usò pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 40 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

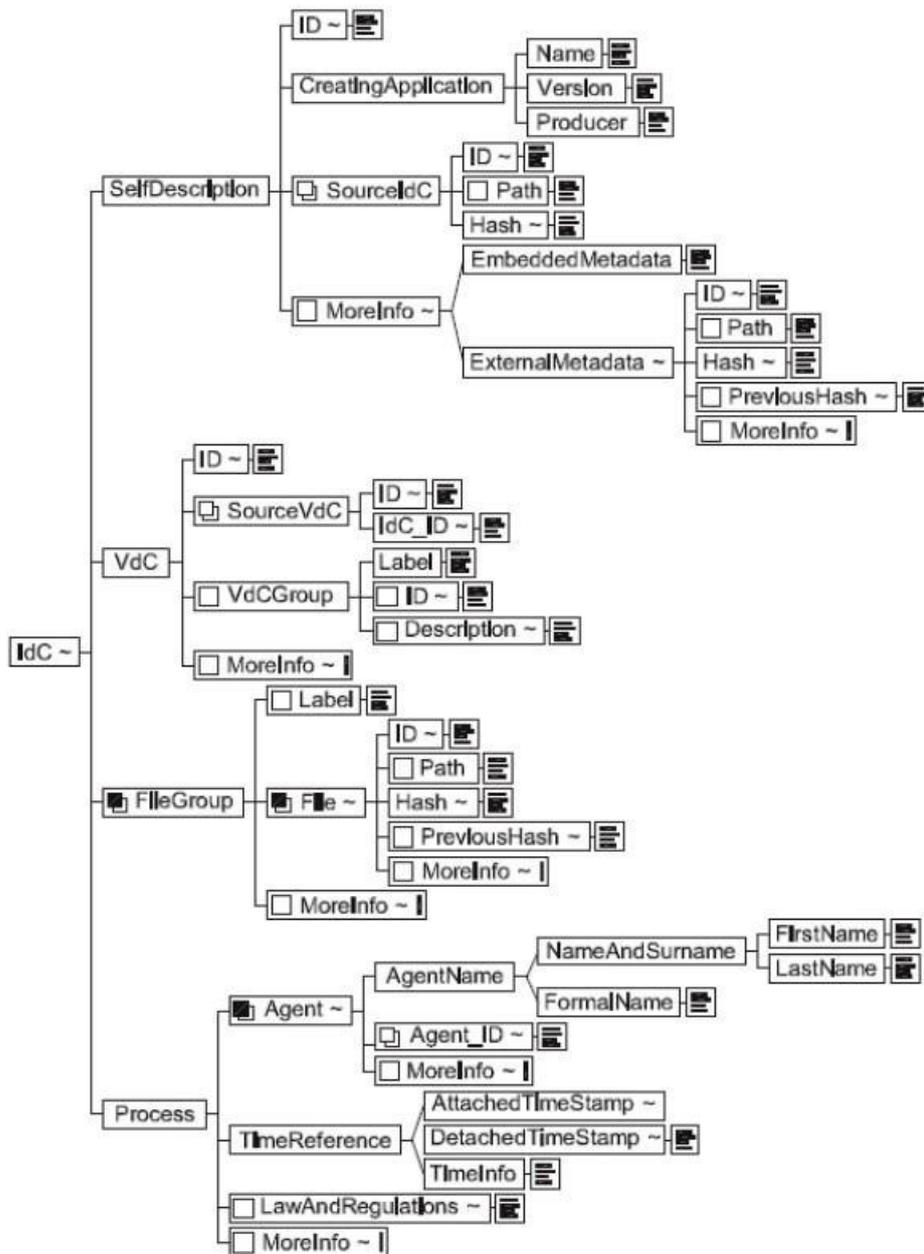


Figura 3 - Schema Logico struttura Pacchetto di Archiviazione

Significato dei Valori utilizzati

Nella tabella seguente vengono mostrati i diversi tag xml e le modalità di compilazione adottate da Poste Italiane per la valorizzazione del file richiesto da AgID per il PdA.

Nome	Tipo	Valore
------	------	--------

IdC->SelfDescripton->ID	Tag	Identificativo univoco generato dal sistema
IdC->SelfDescripton->CreatingApplication--->Name	Tag	Valorizzato con Postedoc/Jod-CS
IdC->SelfDescripton>CreatingApplication->Version	Tag	Versione del processo di conservazione
IdC->SelfDescripton>CreatingApplication->Producer	Tag	Valorizzato con Poste Italiane S.p.A
IdC-> VdC-> ID	Tag	Identificativo del Pda di conservazione
IdC-> VdC-> VdcGroup- > Label	Tag	Nome Tipologia/Aggregazione Logica
IdC-> VdC-> VdcGroup- > ID	Tag	Identificativo della Classe Documentale/Aggregazione
IdC-> VdC-> VdcGroup- > Label -> Description	Tag	Descrizione della Classe Documentale così come presente sul Sistema di Conservazione
IdC-> VdC-> MoreInfo	Tag	Provenienza PdV
IdC - > FileGroup - > Label	Tag	Etichetta assegnata dal Sistema di Conservazione
IdC - > FileGroup - > File - > ID	Tag	Identificativo univoco assegnato dal Sistema di Conservazione
IdC - > FileGroup - > File - > Hash	Tag	Checksum del file
Nome	Tipo	Valore
IdC - > FileGroup - > File - > MoreInfo	Tag	Tag valorizzato per clienti specifici

IdC - > Process -> Agent -> AgentName - > NameAndSurname - > FirstName	Tag	Nome dell'owner del certificato di firma
IdC - > Process -> Agent -> AgentName - > NameAndSurname - > LastName	Tag	Cognome dell'owner del certificato di firma
IdC - > Process -> Agent -> AgentID- > scheme	Attributo	Valorizzato con TaxCode
IdC - > Process -> Agent -> AgentID- > Numero certificato	Tag	Numero di serie del certificato di firma
IdC - > Process -> TimeReference - > Timestamp	Tag	Riferimento temporale del processo di conservazione

Il processo di conservazione termina con la creazione del l'IdC contenente l'impronta del PdV firmato e marcato temporalmente dal Responsabile del Servizio di Conservazione.

[Torna al sommario](#)

6.5 PACCHETTO DI DISTRIBUZIONE

Il Pacchetto di Distribuzione (PdD) è conforme al Pacchetto di Archiviazione. Il PdD contiene l'insieme dei documenti per i quali è stata richiesta l'esibizione, il relativo indice denominato IPdD. Le eventuali personalizzazioni di tale pacchetto, specifiche di un contratto con il Cliente, sono descritte nell'allegato "**Specificità del contratto**".

[Torna al sommario](#)

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 43 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

7 IL PROCESSO DI CONSERVAZIONE

Il Servizio di Conservazione viene erogato attraverso canali diversificati, Il Cliente può accedere alle funzionalità del servizio sia tramite apposita interfaccia Web, che tramite Web Service con la possibilità in quest'ultimo caso di integrazione diretta con i sistemi gestionali già presenti presso le proprie sedi.

Per l'erogazione del servizio Poste Italiane si avvale di una piattaforma complessa che rispetta elevati standard di sicurezza.

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

Il Cliente in fase di attivazione deve specificare in quali modalità desidera inviare i documenti da sottoporre a conservazione.

Le modalità attraverso le quali è possibile trasmettere i pacchetti di versamento sono le seguenti:

- Utilizzo di web-service;
- Trasmissione telematica tramite canale sicuro;
- Utilizzo di un interfaccia web based che permette il "caricamento" dei documenti informatici sul Sistema di Conservazione.

Tutti i canali di comunicazione instaurati con i Clienti sono cifrati per la protezione dei dati oggetto di transazione con il cliente. Verrà predisposta da Poste Italiane un'idonea infrastruttura di sicurezza per la ricezione/invio dei flussi, nel rispetto delle specifiche tecniche e di sicurezza con comunicazione protetta e firewall tramite la quale i sistemi del Cliente potranno accedere ai servizi erogati da Poste Italiane.

Tutte le fasi del processo di acquisizione dei PdV, ed in generale ogni interazione con l'utente, producono dei log di sistema necessari alla tracciatura delle attività e delle operazioni svolte sul sistema Postedoc.

L'uso della posta elettronica e della PEC non è previsto per l'invio dei pacchetti di versamento.

[Torna al sommario](#)

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 44 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

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

Per poter accedere al Sistema di Conservazione ed inviare i propri PdV, gli utenti vengono preventivamente abilitati e censiti sul sistema stesso previo il rilascio di credenziali applicative con le quali potrà inviare PdV solamente relativi alla propria utenza ed alle proprie classi documentali.

Ogni PdV è costituito da:

- ✓ Un file dati: contenente il file attributi e i documenti da conservare;
- ✓ Un file di check, chiamato anche file di controllo: contenente la dimensione in byte del file dati e la sua impronta hash.

Prima di elaborare il flusso, il sistema verificherà la coerenza tra i due file trasmessi che avranno le seguenti caratteristiche.

- ✓ **File dati, in formato archivio zip, contenente a sua volta:**
 - **Un File Attributi, in formato XML, denominato *index.xml*;**
 - **Un numero variabile di documenti.**
- ✓ **File check, in formato XML, contenente la dimensione in byte del File dati e la sua impronta hash, denominato *chk.xml*. Tale file viene utilizzato per verificare l'integrità e l'avvenuto trasferimento di ogni flusso spedito.**

Il PdV ricevuto viene quindi sottoposto ad una serie di verifiche:

- Identificazione certa del Produttore mediante credenziali e corrispondenza dei dati inviati;
- Controlli del corretto trasferimento del PdV;
- Controlli sull'integrità dei documenti contenuti nei pacchetti di versamento, attraverso il confronto delle impronte di hash;
- Controllo formale complessivo;
- Verifica dell'esistenza della classe documentale indicata da Produttore e precedentemente creata ed abilitata sul sistema;
- Verifica dei formati dei documenti contenuti nel PdV confrontandoli con quelli accettati dal sistema Postedoc;
- Verificare per ogni PdV che i file associati ai documenti siano tutti dello stesso formato (es. pdf);
- Verifica dell'esistenza dei metadati minimi obbligatori per ogni tipologia documentale definita per lo specifico cliente.

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 45 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

I controlli eseguiti dal Sistema sui PdV trasmessi il cui esito negativo risulta bloccante sono i seguenti:

- Verifica che il pacchetto di versamento contenga l'IPdV ed i files;
- Controllo validità del file IPdV con il file schema XSD;
- Controllo che il soggetto che ha formato ed è titolare dei documenti definito nell'IPdV sia presente e configurato nel Sistema di Conservazione e che per questo soggetto ci sia un soggetto Responsabile della Conservazione configurato nel sistema;
- Controllo che il numero di files presenti nel PdV corrisponda al numero di files dichiarati nell'IPdV;
- Controllo che i nomi dei files presenti nel PdV corrisponda ai files definiti nell'IPdV;
- Controllo che il MimeType dei files definito nell'IPdV sia stato specificato;
- Verifica che i formati dei files contenuti nel PdV siano nei formati previsti dall'Allegato 2 del DPCM 3 Dicembre 2013.

Di seguito si riporta un esempio di file XML per la classe documentale denominata "fattatt" contenente le fatture attive:

```
<?xml version="1.0" encoding="UTF-8" ?>
<fattatt>
<documento>
<numero_fattura>XXXXXXXXXXXXXXXXXXXX</numero_fattura>
<data_fattura>2000-01-01</data_fattura>
<codice_cliente>XXXXXXXXXXXXXXXXXXXX</codice_cliente>
<ragione_sociale>XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX</ragione_social
e>
<partita_iva>XXXXXXXXXXXXXXXXXXXX</partita_iva>
<codice_fiscale>XXXXXXXXXXXXXXXXXXXX</codice_fiscale>
<importo_euro>9999999999999999.9999</importo_euro>
<codice_protocollo>XXXXXXXXXXXXXXXXXXXX</codice_protocollo>
<numero_movimento>9999999999</numero_movimento>
<id_ged>XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX</id_ged>
<sottoclasse>XXX</sottoclasse>
<file size="123456789">d_1_f_1.txt</file>
</documento>
</fattatt>
```

Di seguito è invece riportata la struttura "tipo" di un file di controllo anch'esso in formato XML :

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 46 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

```
<?xml version="1.0" encoding="UTF-8"?>
<file_chk>
  <file_size>[size file di dati]</file_size>
  <file_hash type="MD5">[hash file di dati]</file_hash>
</file_chk>
```

Nei casi di trasmissione dei pacchetti di versamento attraverso altri protocolli sicuri sono possibili altri comportamenti regolamentati attraverso l'allegato "specificità del contratto". Ad ogni modo al ricevimento del pacchetto saranno effettuati tutti i controlli descritti concordati con il Cliente.

[Torna al sommario](#)

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

Dopo aver superato i controlli indicati nel paragrafo 7.2, il Sistema di Conservazione produce un Rapporto di Versamento (RdV) nel quale viene indicato l'esito delle verifiche.

Per ogni PdV ricevuto il Sistema di Conservazione produce quindi un RdV in formato XML il contenente i seguenti dati:

- Informazioni sul PdV;
- L'identificativo sul Sistema di Conservazione dell'utente che ha caricato il PdV;
- L'identificativo del PdV sul Sistema di Conservazione;
- L'esito delle verifiche;
- L'eventuale messaggio/codice di errore;
- Il riferimento temporale della verifica;
- La lista dei file contenuti nel PdV.

Il Sistema di Conservazione mette a disposizione del Produttore i Rapporti di versamento tramite l'utilizzo di un interfaccia web. L'interfaccia web consente quindi di monitorare lo stato di tutti i PdV inviati.

Tutte le informazioni inerenti le operazioni eseguite dagli utenti e dai processi informatici relative ai PdV vengono storicizzate su appositi log.

Il log sintetizza gli esiti del processo di verifica con le seguenti informazioni:

- Identificativo del RdV prodotto a seguito del processo di verifica;
- Identificativo del PdV associato;
- Esito del processo di controllo;

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 47 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

- Cronologia dell'evento di verifica (Data ed Ora).

[Torna al sommario](#)

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

Nei casi in cui il PdV non rispetti gli standard concordati nel contratto stipulato con il cliente o non risulti costituito da file previsti dalla normativa lo stesso viene respinto e viene generato un Rapporto di Versamento (RdV) di rifiuto contenente le motivazioni del rigetto che riceve l'apposizione di un riferimento temporale;

Sono riportate di seguito alcune possibili anomalie che determinano il rifiuto del PdV ma che non rappresentano un elenco esaustivo delle possibili cause di rifiuto:

- PdV non contiene IPdV ed i documenti;
- File IPdV non valido o mancante rispetto allo schema XSD;
- Mancata corrispondenza tra quanto configurato nel Sistema di Conservazione e quanto inviato dal Produttore;
- Numero di file presenti nel PdV non corrispondente al numero di file dichiarati nel file IPdV;
- Nomi dei file presenti nel PdV non corrispondenti ai nomi file definiti nell'IPdV;
- Estensioni dichiarate nell'IPdV non previste tra quelle ammesse dal Sistema di Conservazione;
- Presenza di file nell'IPdV con Id documento non specificato;
- Presenza di file nell'IPdV con lo stesso Id documento;
- Classe documentale configurata nel Sistema di Conservazione non corrispondente a quella definita e dichiarata nell'IPdV;
- I metadati configurati per la specifica tipologia documentale nel Sistema di Conservazione non corrispondono a quelli dichiarati nell'IPdV;
- Il nome e l'ordine dei metadati configurati per la specifica tipologia documentale nel Sistema di Conservazione non corrispondono a quelli dichiarati nell'IPdV;
- Presenza di documenti con lo stesso Id documento, all'interno del Sistema di Conservazione;
- Mancata corrispondenza degli hash (impronte) dei documenti calcolati dal conservatore con l'hash dichiarato nell'IPdV del Produttore.

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 48 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

L'RdV prodotto viene firmato digitalmente dal Responsabile del Servizio di Conservazione e viene reso disponibile al Cliente tramite un interfaccia Web per la consultazione.

Il Sistema di Conservazione registra su file di log l'operazione di rifiuto del PdV e le cause che l'hanno generato.

Il log sintetizza gli esiti del processo di verifica con le seguenti informazioni:

- Identificativo del RdV prodotto a seguito del processo di verifica;
- Identificativo del PdV associato;
- Esito del processo di controllo;
- Motivo dello scarto del Pdv;
- Cronologia dell'evento di verifica (Data ed Ora).

PdV di rettifica

I PdV di rettifica permettono di inviare versioni modificate (corrette) di documenti già conservati. Una rettifica contiene il set completo di file e attributi del documento da rettificare, e non solo i dati e/o i file da modificare, e viene sottoposta allo stesso processo di conservazione dei documenti originali; i documenti rettificati rimangono comunque a disposizione sul sistema.

Invio PdV di rettifica

Anche per questa tipologia di PdV è necessario inviare:

Un file di "dati"

Il file dei "dati" è un archivio di tipo **.zip** contenente tutti i file del PdV (uno o più file per documento) e un file `index.xml` o `index.xls` di descrizione.

Il file XML contenuto all'interno dell'archivio deve necessariamente chiamarsi "`index.xml`". Esso contiene, per ogni documento, tutti gli attributi del documento stesso, e il o i riferimenti ai file che compongono il documento.

Il file `index.xml` ha la seguente struttura:

```
<?xml version="1.0"?>
```

```
<[tipodoc]-rettifica>
```

```
<rettifica>
```

```
<documento_originale>
```

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 49 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

```

<id_documento>[id_documento_originale]</id_documento>
<id_lotto>[id_PdV_originale]</id_lotto>
<id_report>[id_report_originale]</id_report>
<versione_report>[version_report_originale]</versione_report>
</documento_originale>
<documento>
  <[attributo1]>[valore att. 1]</[attributo1]> <[attributo2]>[valore
  1 att. 2]</[attributo2]>
  ...
  <[attributo2]>[valore N att. 2]</[attributo2]>
  <[attributo3]>[valore att. 3]</[attributo3]>
  <file size= [size file 1]>[nomefile 1]</file>
  ...
  <file size= [sizefile M]>[nome file M]</file>
</documento>
</rettifica>

```

.....

.. altre rettifiche ...
 </[tipodoc]-rettifica>

La struttura del file xml dipende dalla classe documentale; il file contiene un tag principale che dipende dalla tipologia del documento (<[tipodoc]-rettifica>). All'interno del tag si trovano tanti tag <rettifica> quanti sono le rettifiche di documenti contenuti nel PdV.

Ogni tag <documento_originale> contiene quattro tag che identificano univocamente il documento originale da rettificare:

- <id_documento>: identificativo del documento originale;

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 50 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

- *<id_lotto>*: id_Pdv del documento originale;
- *<id_report>*: id_report del PdV originale;
- *<versione_report>*: versione_report del file originale.

Tali valori sono reperibili tramite il modulo web di ricerca e visualizzazione dei documenti, e all'interno del file di notifica di avvenuta conservazione.

Ogni tag *<documento>* contiene la sequenza dei tag associati agli attributi e un tag *<file>* per ciascun file che compone il documento. Inoltre, per ciascun documento, analogamente al caso dei PdV standard:

- I tag degli attributi compaiono nell'ordine definito dal parametro "indice XML" della classe documentale;
- Il tag coincide col nome dell'attributo;
- Il valore dell'attributo è specificato all'interno del tag;
- Se un attributo non obbligatorio non è valorizzato, il relativo tag non deve essere presente;
- Se un attributo è stato definito come "multiplo", il relativo tag può comparire più di una volta;
- Nel caso di classi documentali condivise, l'ultimo attributo, obbligatorio e con molteplicità 1, è sempre "codice_utente", e contiene per ciascun documento il codice univoco identificativo dell'owner del PdV di documenti (quindi deve avere lo stesso valore per tutti i documenti del PdV);
- Gli attributi di tipo DATE devono avere il formato YYYY-MM-DD;
- Gli attributi di tipo TIME devono avere il formato HH24:MM:SS;
- Il separatore per la parte decimale dei numeri è il punto;
- Il tag *<file>* ha un parametro opzionale "size" che corrisponde alla size, in byte, del file;
- Il tag *<file>* può comparire più di una volta se la classe documentale è stata creata con l'opzione "file multipli".

I file del PdV devono essere tutti dello stesso tipo (es. pdf).

[Torna al sommario](#)

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 51 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

7.5 PREPARAZIONE E GESTIONE DEL PACCHETTO DI ARCHIVIAZIONE

I PdV opportunamente verificati e validati dal Sistema di Conservazione, come descritto nei paragrafi precedenti, vengono trasformati in PdA.

Il PdA viene prodotto in conformità al formato definito nello standard SInCRO (UNI 11386:2010) come descritto al paragrafo 6.3.

Il PdA viene quindi firmato digitalmente dal Responsabile del Servizio di Conservazione e sottoposto a marcatura temporale. L'indice del PdA (IdPA o IdC) contenente i metadati e le impronte (SHA256) dei file contenuti nel PdA, insieme agli stessi file, viene archiviato/conservato all'interno del Repository Postedoc.

L'accesso al Repository Postedoc è reso disponibile ai Clienti, attraverso l'utilizzo di un portale web con credenziali private e secondo gli SLA concordati con il cliente.

Tutte le operazioni inerenti la preparazione e la gestione del PdA e dell'IdC ad esso associato vengono tracciate in appositi file di log.

Memorizzazione del PdA su storage ad alta affidabilità

I PdA vengono memorizzati su storage ad alta affidabilità. La piattaforma Poste Italiane utilizza uno storage WORM (write only read many) di tipo EMC2 Centera, che assicura le stesse caratteristiche di inalterabilità di un disco ottico ed in più offre funzionalità native di gestione del periodo di retention dei singoli file. All'atto della scrittura, per ogni PdV di documenti viene calcolata l'impronta hash utilizzando l'algoritmo standard SHA-256. Il processo di memorizzazione su storage ad alta affidabilità viene effettuato, oltre che per il PdA, anche per la Marca Temporale.

[Torna al sommario](#)

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

L'esibizione dei documenti, anche nel caso di una richiesta di verifica ispettiva da parte delle Autorità competenti, avviene da parte di personale autorizzato del Cliente dotato di specifiche credenziali mediante l'interfaccia di una applicazione web di esibizione dei documenti che il sistema rende disponibile mediante un apposito indirizzo ovvero attraverso esplicita richiesta verso il Responsabile del Servizio di Conservazione. L'interfaccia permette ad un utente abilitato di ricercare ed eventualmente visualizzare i documenti di una determinata tipologia sottoposti al processo di Conservazione presenti all'interno dell'archivio. A seguito dell'accesso a tale funzionalità è possibile

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 52 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

visualizzare la lista di tutte le classi documentali per le quali l'utente può effettuare le ricerche. Successivamente, selezionando la tipologia di interesse, viene visualizzata una form, costruita dinamicamente in base alle caratteristiche della classe documentale, per l'inserimento di tutti i parametri del documento in base ai quali effettuare la ricerca. Alla conferma dell'utente l'applicazione esegue la ricerca visualizzando la lista di documenti che rispondono ai parametri selezionati.

Per ciascun documento della lista viene mostrato:

- Un link che consente la visualizzazione di tutte le informazioni disponibili per il documento
- Un link che recupera il documento dall'archivio

Quindi in risposta ad una richiesta effettuata tramite l'interfaccia web nell'area di ricerca documenti, il Sistema di Conservazione fornisce al Cliente una lista di Pacchetti di Archiviazione, dai quali sarà possibile generare un Pacchetto di Distribuzione (PdD) secondo quanto previsto dalla norma vigente.

Il Cliente, tramite le interfacce Web, può pertanto richiedere l'esibizione di tutti i documenti conservati dal Responsabile del Servizio di Conservazione per:

- Richiedere e scaricare il PdD in formato compresso ZIP o ISO – verrà restituito al cliente attraverso un canale sicuro per il colloquio con il Servizio di Conservazione nella forma prevista dalla normativa;
- Richiedere alla struttura Esercizio e Supporto Servizi Digitali operante in SI/ESSD un supporto fisico rimovibile (DVD) contenente uno o più PdD, i supporti saranno resi anonimi rispetto alle informazioni di identificazione del Produttore e i contenuti verranno criptati con apposita chiave pubblica del Produttore.

Le attività di richiesta e della generazione di PdD vengono identificate attraverso un codice sequenziale univoco in un apposito Log e registrate nel file system dopo essere state dotate di un riferimento temporale fornito dal sistema TSA di Time Stamping di Poste Italiane.

Per garantire la qualità del PdD prima di essere emesso verrà sottoposto a test di integrità secondo le modalità già previste dal processo di conservazione.

Il riscontro da parte dell'utente di anomalie che non venissero rilevate dal sistema di controllo, o verificatesi durante il processo di trasmissione dei PdD, potranno essere

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 53 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

segnalate attraverso l'apertura automatica di un ticket alla funzione preposta di Poste Italiane attraverso l'invio di una mail all'indirizzo di posta comunicato al cliente nella documentazione allegata al contratto di servizio. L'evoluzione dello stato di risoluzione del ticket verrà comunicato al cliente attraverso i canali di comunicazione concordati e descritti nello specifico contratto stipulato con il Cliente.

[Torna al sommario](#)

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

I duplicati dei pacchetti di archiviazione possono essere richiesti come servizio opzionale, che prevede la generazione di duplicati su supporto removibile per la consegna al Produttore.

Questa operazione predispone una copia del documento nel formato richiesto apponendo le corrette indicazioni di conformità al documento in conservazione come previsto dalla normativa vigente.

Se la mole dei dati richiesti prevede l'utilizzo di un supporto fisico removibile - (DVD, HD, ecc.) contenente una o più copie informatiche di un PdA, i dati trasmessi saranno protetti con sistemi crittografici e verrà garantita la riservatezza dei dati estratti.

Per quanto riguarda l'eventuale adeguamento del formato dei file all'evoluzione tecnologica il Responsabile del Servizio di Conservazione, secondo un piano preventivo di controlli, esegue le verifiche di integrità, di leggibilità e di adeguatezza della rappresentazione informatica dei documenti all'evoluzione tecnologica, la scelta di formati consolidati, previsti dalle nuove Regole tecniche del DPCM del 3/12/2013 come il formato PDF/A o OOXML per i documenti, garantisce una corretta prevenzione e minimizzazione dei rischi legati all'obsolescenza dei formati documentali nel tempo.

L'operatore Poste Italiane, in base alla richiesta pervenuta dal cliente o dal Pubblico Ufficiale, seleziona i pacchetti di archiviazione (PdA) che devono essere duplicati, stabilisce il formato del duplicato (ISO o pacchetto zip) e il supporto finale di memorizzazione (es. CD, DVD) così come concordato preventivamente con il cliente.

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 54 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

Ogni richiesta di produzione di duplicati e copie informatiche viene tracciata con un identificativo univoco all'interno del sistema di log della Conservazione al quale viene associato un riferimento temporale rilasciato dalla TSA di Poste Italiane.

In sostanza la richiesta di esibizione di uno o più PdD, può più semplicemente essere sostituita con una richiesta di download dei duplicati dei documenti informatici conservati, questa operazione predispone una copia del documento nel formato richiesto come previsto dalla normativa vigente.

La produzione di duplicati dei pacchetti di archiviazione (PdA) è una funzione che il Cliente tramite il personale abilitato può attivare tramite interfaccia web mediante autenticazione con le proprie credenziali (username e password) e attivazione del download del PdA. Il download avverrà tramite un canale crittografato (protocollo HTTPS).

In alternativa, il Cliente (o in alternativa il Pubblico Ufficiale) può richiedere a Poste Italiane la fornitura di un - supporto fisico rimovibile - (DVD, HD, etc.) contenente una o più copie informatiche di un PdA. In questo caso i dati trasmessi saranno protetti con opportuna criptazione.

Il personale incaricato del trasporto dei supporti fisici viene scelto sulla base dei requisiti definiti dal Responsabile del Servizio di Conservazione.

Il processo di produzione di duplicati, viene realizzato mediante strumenti affidabili presenti nella struttura Esercizio e Supporto Servizi Digitali di Poste Italiane che garantiscono la corrispondenza del contenuto della copia alle informazioni del documento informatico di origine. La creazione dei duplicati si conclude con l'apposizione, sull'insieme dei documenti, del riferimento temporale e della firma digitale da parte del Responsabile del Servizio di Conservazione, e ove previsto dalla legge con la presenza di un Pubblico Ufficiale a chiusura del processo.

Anche in questo caso, ogni volta che l'utente richiede la produzione di duplicati e copie informatiche ogni azione di richiesta viene tracciata con un identificativo univoco all'interno del sistema di Log e con la registrazione di un riferimento temporale emesso dalla TSA di Poste Italiane.

Il sistema prevede un apposito processo per la generazione di copie di sicurezza nel rispetto della vigente normativa. Ciascuna copia di sicurezza può contenere uno o più PdD.

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 55 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

Conservazione delle copie di sicurezza

Le copie di sicurezza verranno generate in unica copia (su richiesta duplice copia). Una copia sarà custodita dal Responsabile della Conservazione, che provvederà a conservarla opportunamente, impegnandosi a mantenerne la riservatezza e a verificarne periodicamente la leggibilità. Opzionalmente e previo accordo tra il Cliente e Poste Italiane potrà essere generata una seconda copia di sicurezza, su supporto removibile, che verrà consegnata al Cliente.

[Torna al sommario](#)

7.8 SCARTO DEL PACCHETTO DI ARCHIVIAZIONE

Il Sistema di Conservazione di Poste Italiane è dotato di una procedura automatica di scarto che si occupa di controllare quotidianamente se esistono pacchetti di archiviazione la cui Retention Time sia scaduta e che quindi debbano essere scartati.

Qualora venga trovato un pacchetto che può essere scartato, il sistema provvederà in automatico a cancellare il pacchetto stesso dal Centera ed a rimuovere tutti i suoi riferimenti dal DB.

La procedura di scarto è irreversibile ed ogni attività eseguita viene tracciata in appositi log applicativi.

Nel caso di archivi pubblici o privati di particolare interesse culturale, le procedure di scarto avverranno previa autorizzazione del Ministero dei Beni e delle Attività Culturali e del Turismo.

[Torna al sommario](#)

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

Il sistema genera PdA conformi alla norma Uni SinCRO 11386:2010 che garantiscono la trasferibilità dei documenti attraverso la generazione dei corrispondenti PdD.

[Torna al sommario](#)

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 56 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

8 IL SISTEMA DI CONSERVAZIONE

8.1 COMPONENTI LOGICHE

I Macro Processi



Figura 4 - Schema Macro-processi Conservazione

Si riporta lo schema a blocchi con un livello macroscopico dei principali Processi del servizio offerto:

- ✓ *Produzione dei documenti da parte del Cliente*: il cliente genera all'interno della propria organizzazione i documenti da sottoporre a Conservazione;
- ✓ *Invio del flusso di dati da parte del Cliente (Versamento)*: Il cliente invia a Poste Italiane i documenti tramite Interfaccia Web o tramite accesso ai Web Services o altro protocollo. Il flusso documentale deve essere costituito nelle modalità indicate da Poste Italiane nella documentazione consegnata la cliente;
- ✓ *Processo di Archiviazione e indicizzazione*: Poste Italiane dopo aver acquisito i documenti inviati dal cliente e verificata la loro consistenza, procede all'archiviazione e indicizzazione dei documenti sulla base degli attributi definiti;
- ✓ *Processo di Conservazione*: Poste Italiane esegue sui PdV in ingresso, il processo di Conservazione che può essere brevemente sintetizzato nelle seguenti operazioni:

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 57 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

1. Generazione dell'impronta (*hash*) del PdV,
2. Memorizzazione dell'impronta del PdV nel IdC del PdA,
3. Apposizione della Firma Digitale all'IdC,
4. Richiesta di una Marca Temporale,
5. Memorizzazione del PdA, firmato digitalmente e della Marca Temporale su supporto con caratteristiche di alta affidabilità e alta permanenza del dato, per un periodo temporale definito in base alla tipologia di documento conservato in accordo con la normativa vigente.

A seguito della corretta esecuzione del processo di Conservazione il sistema genera un file di notifica di avvenuta conservazione, firmato digitalmente dal Responsabile: da quel momento i documenti possono ritenersi correttamente conservati, legalmente validi ed opponibili a Terzi con la possibilità ove previsto dalla normativa di eliminare la copia cartacea eventualmente esistente.

La figura riporta il dettaglio del processo di conservazione:

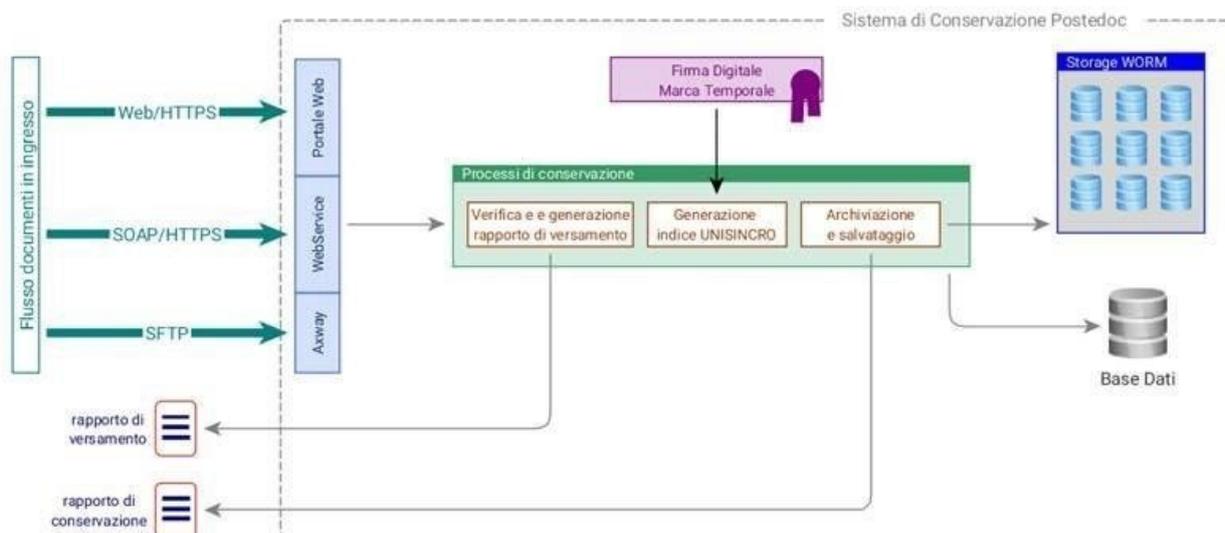


Figura 5 - Schema Processo di Conservazione

- Front End costituito dall'interfaccia web per gli utenti del sistema, che espone le funzionalità necessarie a caricare i documenti sul sistema, attivare i processi di

conservazione, eseguire ricerche nell'archivio, gestire utenti e tipologie di documenti;

- Back End che esegue i processi di conservazione, elaborando sia i dati caricati tramite interfaccia Web, sia quelli trasferiti sul sistema in modalità batch;
- Software di archiviazione;
- Modulo che esplica le seguenti funzionalità:
 - Archiviazione dei dati e delle coordinate di archivio di ciascun documento
 - Monitoraggio e storicizzazione dei processi di lavorazione
 - Sincronizzazione dei processi di lavorazione
- Sistema di storage;
- Un file system di supporto (area temporanea).

[Torna al sommario](#)

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Usò pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 59 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

8.2 COMPONENTI TECNOLOGICHE

Di seguito lo schema di massima dell'architettura del Sistema di Conservazione.

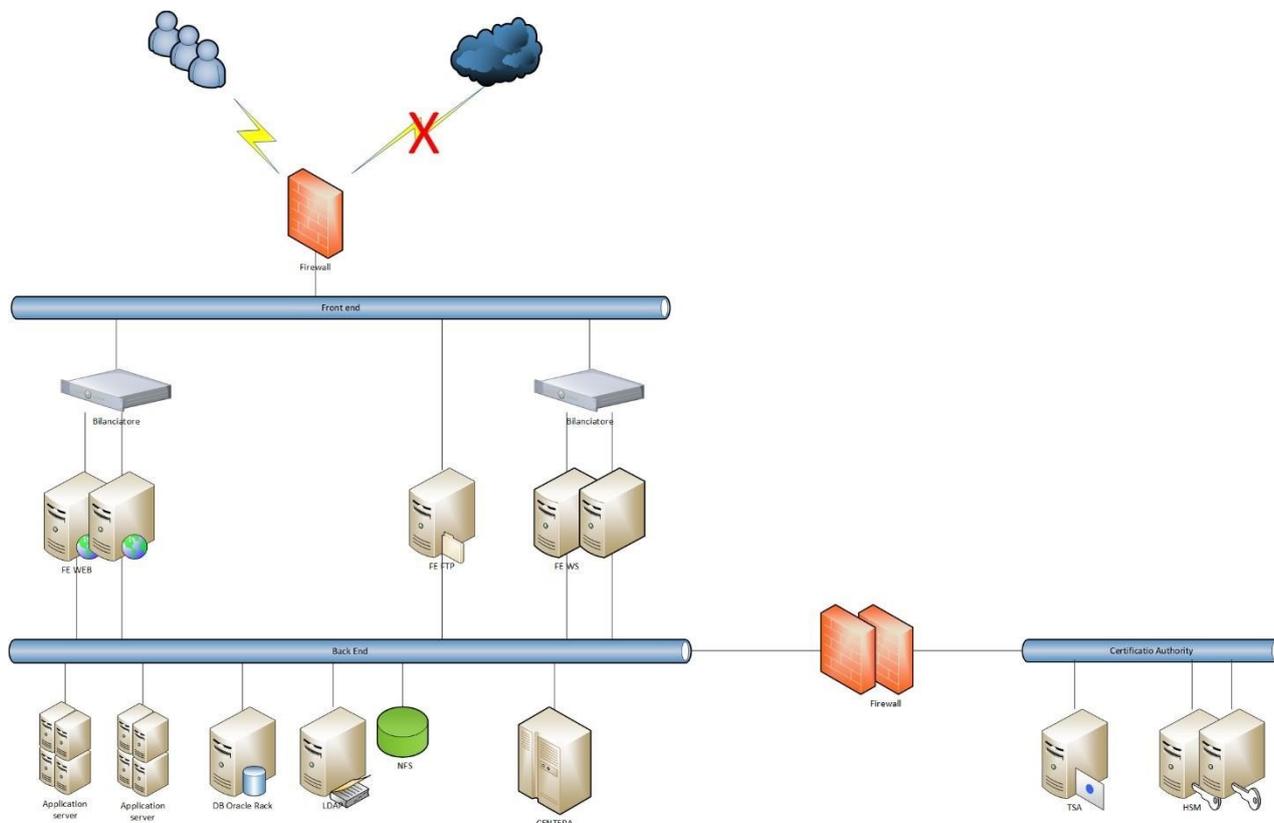


Figura 6 - Schema Logico dell'architettura del Sistema di Conservazione

Il servizio Postedoc può essere erogato sia attraverso una interfaccia web browser, sia tramite una interfaccia Web Service che consente di eseguire le seguenti operazioni:

- Monitoraggio dei PdV sottoposti a conservazione;
- Ricerca di documenti all'interno del repository documentale;
- Get di un singolo documento (a validità probatoria);
- Get di un singolo documento e dei suoi attributi in versione firmata (a validità legale);
- Upload di PdV;
- Recupero del file di notifica di avvenuta conservazione;
- Gestione Utente e permessi.

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 60 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

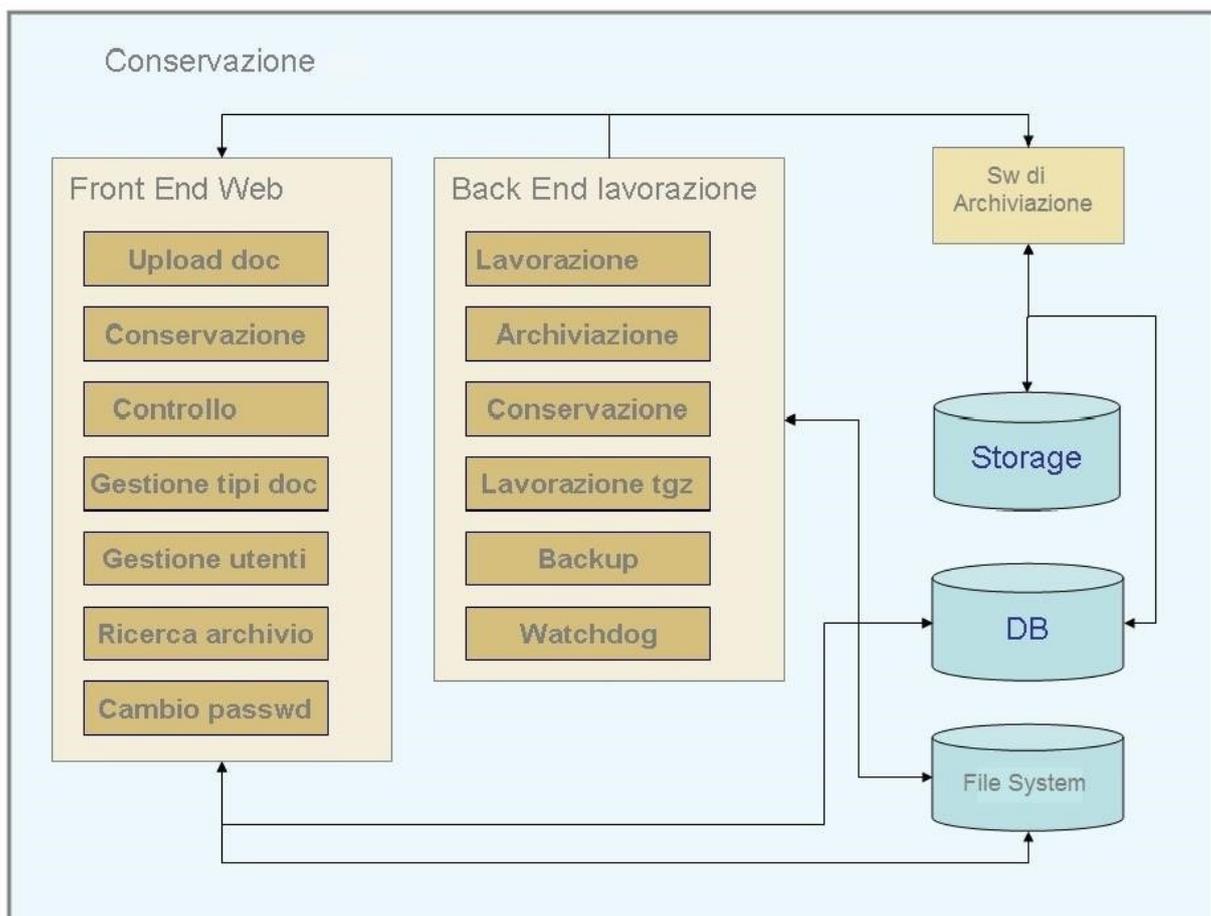


Figura 7 - Schema Logico delle Funzionalità del Servizio di Conservazione

[Torna al sommario](#)

8.3 COMPONENTI FISICHE

L'architettura della rete adottata per il Servizio di Conservazione è strutturata su più livelli al fine di realizzare ambienti di rete separati destinati ad ospitare sistemi diversi livelli di criticità:

- LAN 1 LAN Pubblica <> È la rete più esterna ed è costituita dai dispositivi di rete, quali i router, deputati a distribuire e filtrare il traffico proveniente da Internet verso un primo sistema di firewall;
- LAN 2 (DMZ) LAN Privata – Fast Ethernet, Switched <> Viene acceduta da LAN 1 tramite NAT (solo per le chiamate dirette da IP pubblici, per quelle provenienti da RP – vedi LAN 1.5 – il NAT non viene utilizzato). Vi appartengono i server resi accessibili dall'esterno; su tale rete sono presenti i sistemi che ospitano i Web Server del Portale Postedoc ed i Web Services;

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 61 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

- LAN 3 (BackEnd) LAN Privata – Fast Ethernet, Switched <> Costituisce la rete più interna, suddivisa in ulteriori diverse VLAN, su cui sono allocati gli Application Server, i Server Bach, lo Storage Temporaneo, il Cryptoserver, il DB Oracle, lo storage EMC Centera, ecc.;
- LAN 4 di CA (BackEnd Sistema rilascio delle marche temporali e Firma Digitale) LAN Privata – Fast Ethernet, Switched <> È la rete di back end su cui sono allocati i server TSS per la emissione delle Marche Temporali e l’HSM per la erogazione del servizio di firma digitale dei PdA. Si accede a questa LAN attraverso un ulteriore livello di controllo realizzato da un sistema di firewall.

Di seguito lo schema semplificato dell’architettura di produzione:

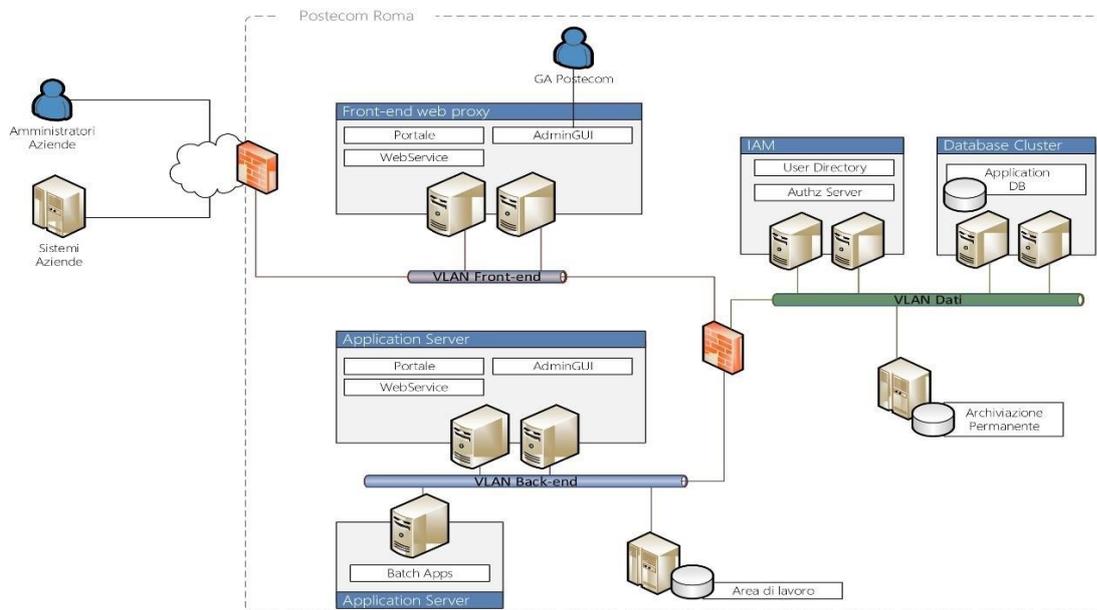


Figura 8 - Architettura di Produzione

[Torna al sommario](#)

8.4 PROCEDURE DI GESTIONE E DI EVOLUZIONE

L’attuale sistema di gestione integrato della sicurezza delle informazioni presente in azienda prevede l’individuazione di ruoli, responsabilità e procedure operative relative agli aspetti di sicurezza legati all’erogazione dei servizi aziendali, in particolare è previsto un documento di Piano della Sicurezza specifico per il servizio di conservazione, che costituisce lo strumento primario per l’identificazione, l’implementazione e lo sviluppo evolutivo delle misure di sicurezza applicate alle infrastrutture, alle piattaforme e alle applicazioni ICT.

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 62 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

Poste Italiane ha conseguito la certificazione iso 9001:2008 e ISO 27001:2017 sui processi e servizi di:

Pianificazione, progettazione e sviluppo di sistemi informativi e manutenzione dei sistemi/servizi ICT. Pianificazione, progettazione, sviluppo, realizzazione ed esercizio di sistemi/servizi di TLC per il Gruppo Poste Italiane. Distribuzione, installazione e manutenzione delle infrastrutture ICT per Poste Italiane. Erogazione dei Servizi ICT. Servizio ICT di "Firma grafometrica" nell'area della "Gestione Elettronica dei Contratti e delle Transazioni". Servizio ICT di "SPID Sistema Pubblico per la gestione dell'Identità Digitale di cittadini e imprese, secondo direttive AgID". Servizio ICT di "Posta Elettronica Certificata", secondo direttive AgID. Servizio ICT fiduciario qualificato di "Firma digitale e marca temporale", secondo direttive AgID e eIDAS. Servizio ICT di "Conservazione a norma", secondo direttive AgID.

In particolare il documento di Piano della Sicurezza è organizzato in:

- **Assessment**

- Analisi della piattaforma prendendo in considerazione tutte le componenti che rientrano nel perimetro d'analisi. L'analisi si sofferma sia sui servizi di business, sia sulla caratterizzazione di dettaglio in termini di dati trattati, flussi caratterizzanti ed utenze che accedono alla piattaforma;
- Identificazione del contesto normativo e delle politiche di sviluppo sicuro a cui è soggetta la piattaforma;
- Attività di verifica della conformità rispetto a quanto indirizzato dalla normativa cogente e dalle politiche applicabili.

- **Analisi del rischio**

- Fase di Analisi del rischio i relativi output in termini di valutazione vulnerabilità, minacce, impatti e livello di rischio potenziale ed effettivo.

Accesso ai sistemi di Erogazione del Servizio

Le operazioni di gestione e manutenzione (ordinaria e straordinaria) sarà effettuato esclusivamente da personale addetto alle attività specifiche siano esse configurazioni di Sistema Operativo o di livello Applicativo, il personale addetto riceverà nomina specifica di Amministratore di Sistema per gli ambiti del servizio specifico, inoltre i sistemi saranno configurati in modo da consentire la registrazione in apposito

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 63 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

repository centralizzato – in modo inalterabile e crittografato – tutte le principali informazioni relative agli accessi effettuati sugli stessi (ad es. utenze, data e ora, log-in, log-off, fault log-in, ecc..).

La diversificazione dei profili previsti per gli utenti garantirà, inoltre, la corretta attribuzione dei trattamenti previsti ed il tracciamento della coerenza tra il compito assegnato e il dato gestito.

Poste Italiane garantisce un elevato livello di protezione delle informazioni siano esse in transito – protezione dei canali di comunicazione con metodi crittografici - HTTPS, SSL 2 – o residenti presso le nostre infrastrutture – applicazione di metodi crittografici per la conservazione di dati quali credenziali-utente sia a livello applicativo o di Sistema Operativo.

La sicurezza dei dati raccolti è garantita dal titolare del trattamento e dal responsabile del trattamento chiamati a mettere in atto misure tecniche e organizzative idonee per garantire un livello di sicurezza adeguato al rischio.

Tali vincoli di Riservatezza, Integrità e disponibilità dell'informazione sarà garantita a tutti i dati gestiti/trattati da Poste Italiane.

Le procedure in essere in Poste Italiane prevedono il processo di Hardening e Patching dei sistemi mirato alla riduzione della superficie di attacco dei sistemi, sia in termini di servizi esposti – eliminazione dei servizi non necessari allo svolgimento delle attività previste, applicazione delle politiche password, personalizzazione credenziali, sia in termini di tempo, grazie all'applicazione delle patch di sicurezza in modo strutturato.

I sistemi che ospitano i servizi sono altresì protetti da un sistema di individuazione ed eliminazione di attacchi virali, gli engine di rilevazione si basano sia su metodologia basata su firme (con aggiornamenti frequenti) sia su metodologia di analisi del "comportamento".

Sono pianificate ed attuate sessioni periodiche di Vulnerability Assessment e di Penetration Test, intese ad individuare in tempi brevi le nuove vulnerabilità emerse e che possano impattare sulla confidenzialità, integrità e disponibilità delle risorse infrastrutturali del sistema di conservazione.

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 64 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

Backup

Le procedure presenti in azienda in tema di procedure di back-up dei dati, consentono di individuare in modo puntuale, in base alla normativa e/o alle esigenze di business la periodicità dei salvataggi.

Periodicamente è prevista un'attività di verifica della leggibilità dei supporti backup, le copie di Back-up sono conservate in aree il cui accesso fisico e logico è regolamentato e controllato e video sorvegliato in aree distinte da quelle che ospitano i dati, è prevista la cancellazione sicura dei supporti una volta destinati i supporti ad altro scopo.

Il personale addetto alle attività di backup è individuato e rientra tra il personale di con il ruolo di Amministratore di Sistema per l'ambito specifico.

Le figure con ruolo rilevante nella gestione dei sistemi, dei middleware, della applicazioni (responsabili della conservazione, amministratori di sistema, ecc.) utilizzano per accedere ai sistemi, criteri di accesso sicuri in relazione al livello richiesto.

Manutenzione

Poste Italiane prevede la redazione di un piano manutenzione programmata per l'intera infrastruttura componente la soluzione di conservazione, sia la parte applicativa si l'architettura tecnologica di supporto.

La gestione delle evoluzioni del configurazioni del strato applicativo e del sistema operativo è garantita dalle procedure di **Change Management**, che tengono in considerazione anche i riversamenti effettuati a fronte di adeguamento tecnologico.

Controllo degli accessi fisici e logici

In Poste Italiane la gestione del ciclo di vita delle identità aziendali, l'attribuzione degli accessi fisici e logici è regolata da una procedura di **Authorization Process Management**.

Tale procedura, supportata da strumenti tecnologici, garantisce la corretta gestione del ciclo di vita delle autorizzazioni agli accessi, siano essi fisici sia logici.

In particolare i Data Center di Poste Italiane prevedono un accesso mediante badge affidato in modo esclusivo al personale identificato dalla struttura aziendale preposta, in base al profilo aziendale è di conseguenza attribuito l'accesso ai sistemi aziendali di pertinenza.

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 65 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

Il sistema sarà predisposto per completare la fase di provisioning delle utenze secondo il modello previsto che prevede:

- Procedura autorizzativa interna, il Process Owner o un suo delegato inviano a Poste Italiane un elenco con i nominativi abilitati e i permessi richiesti;
- Le successive identificazione ed assegnazione delle login avvengono a cura del Process Owner o del suo delegato.

Sarà quindi garantito l'accesso al portale basato sulla profilazione indicata, le singole attività svolte durante la sessione saranno registrate in appositi audit log.

Il processo a fronte delle esigenze espresse dalla normativa prevede:

- Modalità per la registrazione e la cancellazione degli accessi degli utenti ai sistemi e servizi;
- Assegnazione delle password ed utilizzo dei privilegi;
- Processo formale di verifica semestrale della revisione dei diritto di accesso;
- Policy di qualità e sicurezza delle userid e password;
- Scadenza credenziali per non utilizzo, errori in fase di autenticazione;
- Credenziali univoche e non riutilizzabili.

L'accesso logico alle applicazioni è mediato da distinti sistemi di protezione:

- Sistema Sicurezza Perimetrale: Firewall allo scopo di limitare gli accessi alle sole risorse desiderate;
- Sistema Antiintrusione: composto da Intrusion Prevention System, in grado di intercettare attacchi ai sistemi ed interrompere le sessioni di attacco in real-time;
- Sistema di Web Application Firewall: in grado di individuare abusi e attacchi "in application";
- Sistema di Autenticazione/Controllo Accessi: Definizione delle politiche delle risorse protette in base ai profili e richiesta di autenticazione.

Creazione utenti e loro profilazione

Il Cliente, attraverso l'utente Amministratore a lui assegnato in fase di attivazione, ha il compito di definire il "profilo" di ciascun utente appartenente alla propria organizzazione:

- ✓ Utenza di Invio documenti

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 66 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

Questa tipologia di utenza ha la possibilità di caricare ed inviare in modalità manuale il PdV contenente uno o più documenti.

- ✓ Utenze di Ricerca, Visualizzazione e Esibizione dei documenti

Questa tipologia di utenza può effettuare la ricerca (sulle chiavi di ricerca definite in fase di creazione delle classi documentali) e visualizzare i documenti conservati con la possibilità di monitorare lo stato dei PdV. Oltre alla possibilità di scaricare il documento è possibile visualizzare la notifica di conservazione, il PdA firmato dal Responsabile del Servizio di Conservazione.

Tutte le tipologie di utenze hanno anche la possibilità di verificare la Firma Digitale e la Marca Temporale. Tali utenze utilizzano l'interfaccia web del servizio.

Le funzionalità che possono essere assegnate sono:

- ✓ Upload e Acquisizione dei documenti con procedura di caricamento manuale;
- ✓ Ricerca e Visualizzazione dei Documenti sottoposti a Conservazione.

Per ognuna delle suddette funzionalità l'Amministratore dovrà specificare quali classi documentali possono essere trattate dall'utente a meno che queste non siano state predefinite in fase contrattuale. Ad ogni utente è cioè possibile associare la possibilità di leggere o caricare solo un insieme specifico di classi documentali.

Le principali funzionalità a disposizione del Cliente

Il Cliente può, attraverso un'opportuna interfaccia, accedere alle numerose funzionalità del servizio. Di seguito sono sintetizzate le principali funzionalità:

- ✓ *Upload dei documenti:*

Caricamento del PdV contenente un singolo documento o più documenti da sottoporre a conservazione (il caricamento dei documenti può essere svolto sia in modalità automatica che manuale);

- ✓ *Ricerca e Visualizzazione dei documenti conservati:*

- Effettuare ricerche all'interno del repository documentale, sulla base degli indici definiti,
- Visualizzare i risultati della ricerca,
- Visualizzare il documento risultante dalla ricerca effettuata,
- Effettuare il download di uno o di tutti i documenti risultanti dalla ricerca effettuata;

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 67 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

- ✓ *Configurazione del Servizio:*
 - Creazione delle classi documentali e degli attributi necessari per definire le chiavi di ricerca dei documenti,
 - Configurazione delle utenze non amministrative che accedono al Sistema di Conservazione;
- ✓ *Monitoraggio PdV*
 - Visualizzazione dello stato di avanzamento nel trattamento dei PdV inviati in conservazione.

Configurazione del servizio

Attivazione dell'utenze per la gestione del sistema amministratore

A seguito della stipula del contratto, Poste Italiane definisce le utenze base che verranno utilizzate per gestire l'intero Sistema di Conservazione.

Le utenze di base fornite al Cliente sono:

- ✓ Utente Amministratore - E' l'utente che ha il compito di gestire l'intero sistema; al suo profilo sono associate le principali funzionalità, tra le quali:
 - Definire le tipologie di documenti da archiviare e conservare;
 - Definire altre utenze del sistema e stabilirne i privilegi;
 - Verificare lo stato dei PdV da sottoporre a conservazione; □ Effettuare la conservazione dei documenti archiviati.
- ✓ Utente Batch - E' l'utente che viene utilizzato per effettuare l'upload e l'acquisizione dei pacchetti in modalità Batch (automatica).

L'attivazione di queste utenze viene fatta una sola volta in fase di configurazione iniziale del servizio.

Definizione modalità di acquisizione dei documenti Definizione Classi documentali

Una classe documentale definisce tutte le caratteristiche di un tipo di documento da sottoporre a conservazione. A partire dalla definizione della classe documentale vengono generati i file **DTD** e **XSD** da utilizzare per la validazione del file XML che descrive i documenti contenuti nei PdV da archiviare.

Una classe documentale è definita dai seguenti parametri:

- ✓ Nome;

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 68 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

- ✓ Descrizione;
- ✓ Periodo di conservazione;
- ✓ Insieme di attributi.

Gli attributi sono i parametri che caratterizzano una Classe documentale e che possono essere successivamente oggetto di ricerca. I parametri che devono essere definiti per ogni attributo sono:

- ✓ Nome;
- ✓ Tipo Dato e Lunghezza (testo, data, numerico);
- ✓ Obbligatorietà;
- ✓ Molteplicità;
- ✓ Indice;
- ✓ Descrizione.

Gli attributi sono definiti utilizzando la notazione standard XML. Il Cliente può creare autonomamente le classi documentali direttamente da applicativo Web utilizzando l'apposita form Web e compilando opportunamente i campi indicati.

La creazione delle classi documentali è un'operazione necessaria per poter inviare in conservazione i documenti. Il Cliente, attraverso l'utenza amministratore può creare le classi documentali in qualsiasi momento purché rientri nel periodo di attivazione del servizio.

La definizione di una classe documentale genera un file XSD.

Condizione e manutenzione del Sistema di conservazione

Manutenzione del software applicativo

Il personale delegato dal Responsabile dello Sviluppo e dal Responsabile della Manutenzione del Sistema di Conservazione ha cura di mantenere le versioni aggiornate del SW per la generazione dei PdA sottoposti a Conservazione.

A tale scopo, tutto il software realizzato per il processo di Conservazione e per i processi ad esso collegati si trova all'interno di un sistema di gestione del software in grado di mantenere il versioning del codice sorgente sviluppato.

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 69 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

Registro cronologico degli eventi di gestione del Sistema di Conservazione comprensivo delle risoluzioni adottate per rimuovere le anomalie

Durante l'attività di esercizio del Sistema di Conservazione si verificano diversi eventi registrabili:

- Eventi di sistema/DB;
- Eventi applicativi relativi alle fasi del processo di conservazione;
- Eventi di accesso ed attività degli operatori;
- Eventi legati alle evoluzioni delle componenti applicative (Maven, Versioning, Configuration, Management, Change Management, etc.).

Tali eventi vengono trattati in base a processi ben definiti per tutta la Service Operation e la Service Design e Transition:

- Event management (EM);
- Incident management (IM);
- Problem management (PM);
- Request fulfillment (RF);
- Change Management (CM);
- Service Asset & Configuration Mngt (SA&CM);
- Release & Deployment Management (R&DM);
- Service Validation and Testing (SVT);
- Capacity Management (CAPM);
- Service Level Management (SLM);
- Service Catalogue Management (SCM).

Lo strumento di trouble ticketing, utilizzato in queste attività è particolarmente efficace, garantendo la correlazione tra gli eventi rilevati nell'erogazione del servizio e le attività di carattere correttivo, con particolare riferimento al processo di Problem Management.

L'elemento abilitante a tali correlazioni è la definizione dell'albero del servizio, per il quale si utilizza un modello proprietario che consente la rappresentazione dei singoli sottoprocessi di business con le singole funzionalità afferenti associate agli elementi hardware e software che concorrono alla loro erogazione, coerentemente alle nomenclature utilizzate nel CMDB e quindi nell'Inventory Hardware. L'aggiornamento

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 70 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

continuo di tale rappresentazione è assicurata dal processo di SCM. Questo livello di integrazione, all'interno di un unico strumento, consente la produzione di reportistiche ad hoc per ciascun processo piuttosto che tra processi coerenti, per esempio quante Request For Change generate a partire da un Problem su determinati sotto-processi di business che permettono di alimentare poi il Known Error Database.

Sistema di Monitoring

A supporto in particolare del processo di Event Management si utilizzano apposite suite per la rilevazione degli eventi sia sui sistemi che sulle parti applicative e di servizio.

In particolare la soluzione opera sulle seguenti modalità:

- interrogazione proattiva periodica sui sistemi mediante agent a bordo degli stessi;
- interrogazione diretta dei server predisposti dal fornitore (modalità SNMP agentless);
- invio spontaneo di informazioni relative ad eventi notevoli (trap SNMP);
- interrogazione E2E proattiva periodica sul singolo servizio, ove possibile.

Inoltre, attraverso gli agent, vengono rilevati i livelli di performance di sistema e applicativi.

il monitoraggio infrastrutturale prevede:

- monitoraggio infrastrutturale attraverso la connessione con agent installati su tutte le macchine di cui interessa raccogliere lo stato degli indicatori di sistema/applicativi.
- monitoraggio infrastrutturale in modalità "agentless" attraverso plugin/script di monitoraggio lanciati dal Manager.

Il monitoraggio delle performance di sistema prevede indicatori delle performance di sistema collezionati attraverso gli agent di performance e i valori vengono resi fruibile attraverso appositi cruscotti e grafici

Di seguito lo schema dell'architettura della piattaforma:

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 71 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

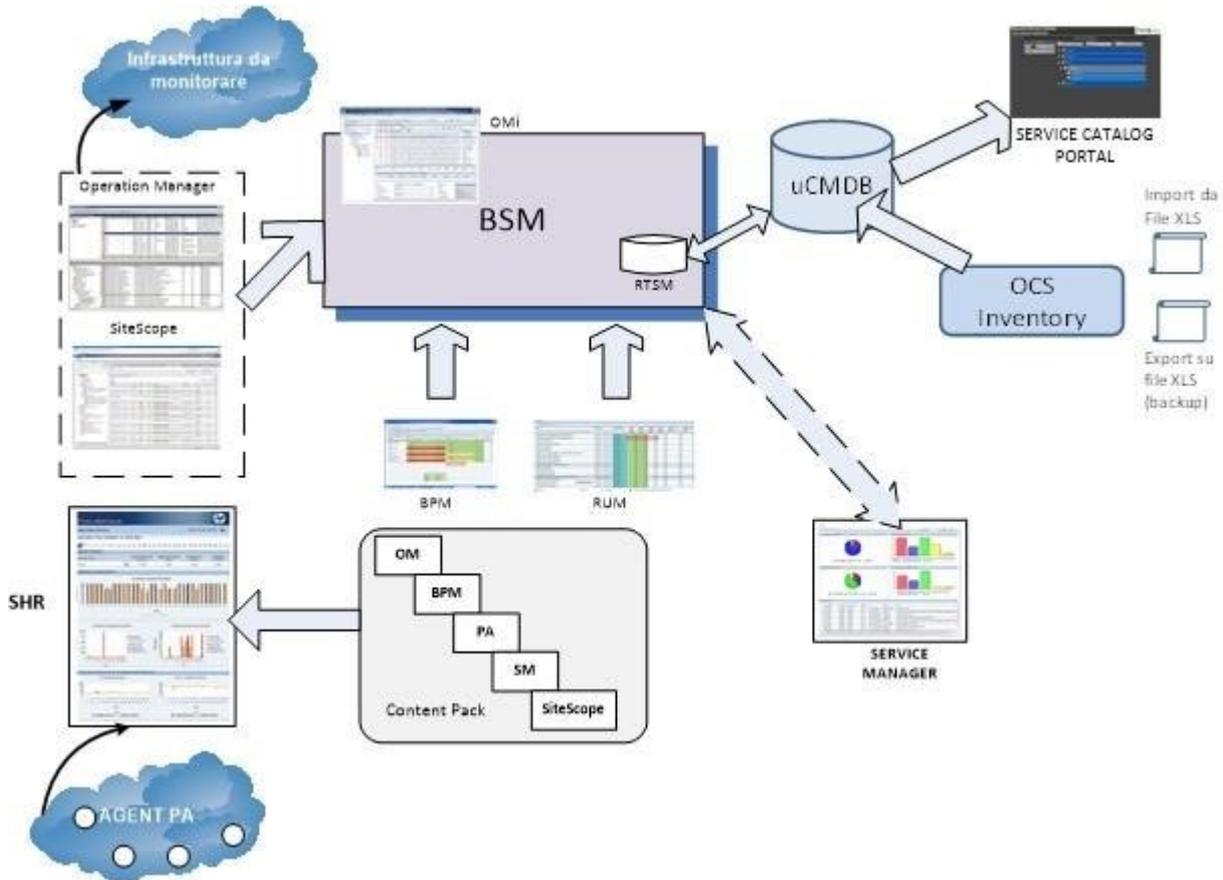


Figura 9 - Architettura Logica del Sistema di Monitoraggio

Sistema di Source Code Management

Lo strumento in uso fornisce una robusta piattaforma per il coordinamento e la gestione dell'intero processo di erogazione del software, ottimizzato per soddisfare le esigenze di scalabilità.

Le principali funzionalità sono le seguenti:

- File Versioning e tracciabilità automatica del codice sorgente, per garantire il tracciamento nel tempo delle modifiche di ogni componente software in relazione al codice sorgente originario;
- Workflow flessibile e integrato, per agevolare l'interazione congiunta delle diverse funzioni aziendali, favorendo il processo di rilascio del software in linea con gli obiettivi prefissati;
- Funzionalità grafiche per una comprensione rapida dello stato dei cambiamenti per ogni build e release software, con generazione automatizzata dei report inerenti l'operazione di rilascio.

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 72 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

Procedure di Sicurezza - Requisiti generali

La sicurezza di Poste Italiane è basata sul rispetto delle politiche aziendali di salvaguardia delle informazioni anche in coerenza con quanto previsto dalla ISO 27001. Gli aspetti di dettaglio delle procedure di Sicurezza applicate al Servizio di Conservazione sono declinate nel Piano di Sicurezza.

Si riporta di seguito un elenco, non esaustivo, dei principali requisiti e servizi ritenuti fondamentali nella attuale implementazione dei livelli di sicurezza sui sistemi informatici di Poste Italiane:

✓ *Requisiti generali:*

- Autenticazione, ovvero la sicurezza che i processi/applicazioni e gli utenti siano appropriatamente identificati prima di ottenere l'accesso alle risorse;
- Autorizzazione, ovvero la effettiva verifica dell'abilitazione all'accesso delle risorse da parte dell'utente;
- Riservatezza, ovvero la garanzia che il personale che accede le informazioni sia abilitato alla lettura delle stesse;
- Integrità, ovvero la certezza della correttezza del dato e delle applicazioni lungo il loro ciclo di vita;
- Privacy, ovvero la garanzia che le informazioni (di clienti, di impiegati e di altro genere) di cui si è in possesso sono utilizzate secondo quanto previsto dalle policy di sicurezza aziendale e che le persone sono abilitate all'uso di tali informazioni in conformità alla legislazione vigente in merito alla riservatezza;
- Non ripudio, sicurezza che il fornitore ed il ricevente di una informazione possono inequivocabilmente provare uno scambio avvenuto tra di essi;
- Disponibilità, la garanzia che l'infrastruttura IT è opportunamente dimensionata a gestire il recupero e la protezione da anomalie, da disastri naturali e/o da attacchi dolosi;
- Non interferenza, ovvero la sicurezza dei controlli dell'accesso e dell'uso delle risorse.

✓ *Gestione dei rischi con:*

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 73 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

- Le modalità di analisi dei rischi;
 - La scelta delle salvaguardie a protezione delle informazioni.
- ✓ *Continuità del servizio con:*
- La ridondanza dell'infrastruttura del sistema di conservazione;
 - La distribuzione geografica dei Data Center;
 - La pianificazione per fronteggiare eventi imprevisti e mancanze di continuità garantendo prioritariamente la disponibilità e l'accesso ai pacchetti di archiviazione;
 - La definizione di eventuali specifiche contrattuali con il cliente per requisiti aggiuntivi di continuità del servizio.
- ✓ *Risposta agli incidenti con:*
- L'organizzazione del servizio e dei presidi di emergenza;
 - I processi di incident management;
 - I processi di problem management;
 - L'analisi delle cause e le conseguenti azioni correttive.

Le procedure di Sicurezza del Riferimento Temporale

Il sistema utilizza, per soddisfare il requisito di apposizione del riferimento temporale richiesto per la procedura di conservazione le Marche Temporalì fornite dal servizio di Time Stamping di Poste Italiane. Le marche temporalì emesse sono firmate da un certificato emesso annualmente dalla TSA di Poste Italiane accreditata presso AgID.

La generazione di una Marca Temporale è ottenuta attraverso una sottoscrizione digitale apposta su una evidenza informatica e fornisce la prova dell'esistenza di tale evidenza informatica al momento di generazione della marca stessa. Apporre una marca temporale ai documenti informatici sottoscritti digitalmente permette di verificare la firma oltre il periodo di validità del certificato di sottoscrizione.

Le marche temporalì utilizzate nel processo di Conservazione sono di tipo "detached" (ovvero sono contenute in un file distinto da quello per il quale si richiede il servizio di marcatura temporale) e hanno una validità di 20 anni dall'emissione in quanto conservate dall'Ente Certificatore Poste Italiane per l'intero periodo come indicato nella normativa vigente.

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 74 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

Modalità di apposizione della firma digitale da parte del Responsabile del Servizio di Conservazione

Le chiavi crittografiche corrispondenti al certificato qualificato del Responsabile del Servizio di Conservazione per l'apposizione della firma digitale sono memorizzate in un dispositivo HSM conforme alla normativa vigente relativa ai dispositivi sicuri per la creazione della firma digitale.

La firma digitale del Responsabile del Servizio di Conservazione è apposta tramite una procedura automatica la cui attivazione è effettuata tramite l'inserimento di un pin da parte del responsabile medesimo, il quale in questo modo afferma la propria volontà nell'apposizione della firma stessa sui singoli IdC.

Procedura di Backup

Lo scopo dell'attività è quello di garantire la continuità nel caso di un guasto di sistema, rendendo sempre possibile la ricostruzione del sistema informativo a partire dal momento dell'ultimo salvataggio.

Per garantire il recupero dei dati a fronte di situazioni di emergenza, sono definite e mantenute aggiornate le regole procedurali riguardanti il salvataggio, l'archiviazione ed il ripristino dei dati stessi, differenziate per tipo ed ambiente e location geografiche.

Sistemi di Business Continuity e Disaster Recovery

L'infrastruttura adottata prevede tutti gli strumenti software necessari all'implementazione di soluzioni di Disaster Recovery (DR) e Business Continuity (BC) con garanzia di integrità, disponibilità e accesso ai pacchetti di archiviazione entro le 24h a seguito di malfunzionamento del sito primario.

I servizi accessori saranno ripristinati a seguire secondo specifici accordi contrattuali.

Le funzionalità software che permettono di effettuare la replica non richiedono modifiche del livello applicativo ed interruzione del servizio (chiusura applicazioni). Il reindirizzamento dei flussi informativi verso i sistemi del Sito Remoto (di Disaster Recovery) si avvale di meccanismi di aggiornamento dei record dei DNS con gli indirizzi dei sistemi ospitati nel Sito di Disaster Recovery. E' pertanto prevista l'integrazione con i sistemi di gestione dei Domain Names e con i sistemi di Global Services Load Balancing presenti nei Data Center.

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 75 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

Tale strategia è implementata tramite l'adozione sul territorio nazionale di architetture di sistema distribuito su più data center in particolare:

□ *Sito Primario (di Produzione)*

Postedoc, Postedoc SIN: Data Center Digital, Viale Europa, 175/190 – 00144 Roma

Postedoc Bollettino Report: Data Center RMB - Palazzo dei Congressi, viale della Pittura 20 -00144 Roma

□ *Sito Remoto (di Disaster Recovery)* a distanza geografica che garantisce la replica asincrona dati o una eventuale 'Business Continuity'

Postedoc, Postedoc SIN: Data Center Torino – DC Torino, Corso Tazzoli 235 - 10137 Torino

Postedoc Bollettino Report:

Data Center MI1 Rozzano – IDC Milano, Viale Toscana 3/5 – 20089 Rozzano (MI)

(Sito in colocation presso fornitore Telecom Italia, privo di personale Poste Italiane residente)

La seguente immagine sintetizza le caratteristiche funzionali dell'architettura di replica fin qui descritta.

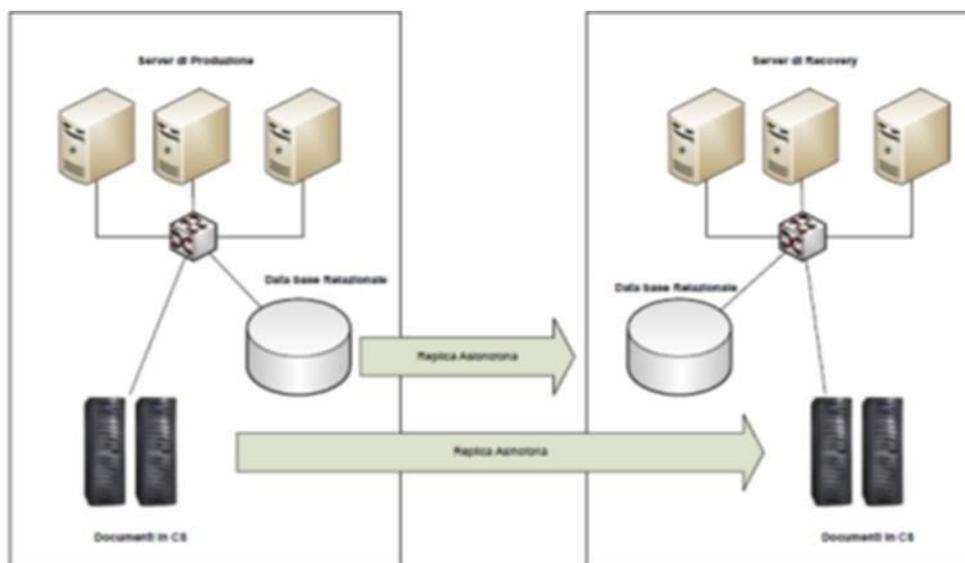


Figura 10 - Architettura Logica del sistema di Disaster Recovery

L'infrastruttura di storage EMC Centera consente l'effettuazione di repliche dei documenti in conservazione sia a livello locale, tra dischi in "mirror", sia remote tra sito primario e sito di DR. La replica dei dati applicativi tra sito primario e sito di DR è invece garantita dal software **Oracle Data Guard** che permette il ripristino dell'operatività del sistema a partire dall'ultima transazione completata. La replica delle configurazioni interne alle istanze virtuali di sistema operativo è gestita mediante funzionalità enterprise che costituiscono parte integrante della soluzione infrastrutturale di virtualizzazione impiegata nei siti primario e di DR.

[Torna al sommario](#)

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Usò pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 77 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

9 MONITORAGGIO E CONTROLLI

9.1 PROCEDURE DI MONITORAGGIO

Come già descritto Il Servizio di Conservazione può essere suddiviso nelle seguenti fasi:

- Fase 1: Invio dei Documenti da parte del Cliente, secondo formati indicati da Poste Italiane;
- Fase 2: Acquisizione dei documenti e relativi attributi attraverso un collegamento telematico;
- Fase 3: Archiviazione e indicizzazione dei documenti sulla base degli attributi definiti;
- Fase 4: Esecuzione del processo di Conservazione.

Fase 1: Invio dei Documenti da parte del Cliente, rispettando i formati indicati da Poste Italiane.

Ogni flusso inviato dal cliente è costituito da:

- Un *file dati* contenente il file attributi e i documenti da conservare;
- Un *file check*, chiamato anche file di controllo contenente la dimensione in byte del file dati e la sua *impronta hash* per la verifica dell'integrità binaria.

Il monitoraggio di questa prima fase prevede:

- Sonda che simula l'upload per verificare che non ci siano problemi di raggiungimento del servizio (via web-service, web);
- Monitoraggio sul numero upload effettuati sul DB che scatena un allarme sullo strumento di Event Management al di sotto di una certa soglia oraria;
- Controllo della dimensione dei PdV secondo quanto concordato in fase di contratto.

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 78 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

Il successivo passo prevede delle verifiche pre-elaborazione:

- *File dati*, in formato archivio zip, dovrà contenere a sua volta:
 - Un File Attributi, in formato XML, denominato index.xml;
 - Un numero variabile di documenti.
- *File check*, in formato XML e denominato chk.xml che dovrà contenere:
 - La dimensione in byte del File dati;
 - La sua impronta hash.

Il sistema Postedoc verifica la coerenza tra i due file trasmessi segnalando al cliente se tale verifica di coerenza non viene soddisfatta.

Viene inoltre monitorato che i file di dati che superano le verifiche di coerenza passino alla successiva fase di acquisizione.

Fase 2: Acquisizione dei documenti e relativi attributi attraverso un collegamento telematico

In questa fase vengono effettuati i seguenti passi:

- I PdA vengono memorizzati su storage ad alta affidabilità;
- Per ogni PdA viene calcolata l'impronta hash utilizzando l'algoritmo standard SHA-256;
- Viene creato il file IdC e associata la marca temporale ed entrambi vengono memorizzati sullo storage ad alta affidabilità.

I monitoraggi implementati sulle verifiche post-acquisizione prevedono:

- Per ogni PdV viene effettuato il confronto tra l'impronta hash contenuta nel *File Check* inviato dal cliente e quella calcolata in seguito all'acquisizione;
- Se il confronto dà un riscontro negativo il PdV viene scartato e inviata notifica al cliente con la motivazione dello scarto;
- Viene inoltre verificato se i PdV che superano i test di post-acquisizione siano effettivamente passati alla successiva fase di archiviazione.

Fase 3: Archiviazione e indicizzazione dei documenti sulla base degli attributi definiti
La fase di archiviazione è costituita dai seguenti passi:

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 79 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

- Inserimento nel Database di storage delle informazioni contenute nel file index.xml.

I monitoraggi implementati sulle verifiche pre-archiviazione:

- Verifica della congruenza tra le informazioni dei documenti del PdV e quelli dichiarati in fase di creazione della classe documentale di riferimento;
- Se il confronto dà un riscontro negativo il PdV viene scartato e inviata notifica al cliente con la motivazione dello scarto;
- Viene inoltre verificato se i PdV che superano i test di post-acquisizione siano effettivamente passati alla successiva fase di archiviazione.

Fase 4: Esecuzione del processo di Conservazione

Questa fase prevede

- La creazione di un file archivio compresso, in formato ZIP, col nome dell'identificativo univoco del PdA contenente:
 - Il flusso dati sorgente (file ".zip");
 - Il file di controllo del flusso dati (file "-chk.xml");
 - La marca temporale associata all'IdC (file ".tsr");
 - Il file di notifica di avvenuta conservazione (file "-cert.xml.p7m");
- Memorizzazione del suddetto archivio su supporto con caratteristiche di alta affidabilità e alta permanenza del dato, per un periodo temporale definito dalla classe documentale.

Le Verifiche della fase di conservazione consistono in:

- Conferma della corretta creazione del file di archivio contenente il file di notifica di conservazione;
- Conferma che i PdA superino la precedenti verifiche e vengano correttamente conservati.

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 80 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

[Torna al sommario](#)

9.2 VERIFICA DELL'INTEGRITÀ DEGLI ARCHIVI

Il sistema di memorizzazione utilizzato, grazie alle caratteristiche intrinseche dei supporti ad alta affidabilità EMC2 e alla "non modificabilità" e memorizzazione permanente dei dati, garantisce il reperimento certo nel sistema di quanto conservato, ai fini di ogni funzionalità di verifica ed esibizione a terzi come prescritto dalla norma vigente.

Il sistema mantiene traccia di tutte le operazioni effettuate sui documenti in appositi file di log; inoltre, è garantita la tracciatura di tutti i documenti richiamati dal Produttore mediante interrogazione al sistema e conseguentemente esibiti, che rappresenta una ulteriore prova di leggibilità, effettuata direttamente dal Produttore.

Inoltre, le procedure di gestione del sistema prevedono un elenco di controlli manuali effettuati direttamente dal Responsabile del servizio della conservazione o dai suoi incaricati.

Come descritto nell'art. 7 comma 1 lettera f), il Responsabile del Servizio di Conservazione, *"assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità" dei documenti conservati con procedure automatiche e manuali, al fine di prevenire il rischio che i documenti non possano essere visualizzabili, inficiando il mantenimento della loro validità legale nel tempo."*

A tale scopo, Poste Italiane prevede un elenco di controlli manuali effettuati direttamente dal Responsabile del Servizio di Conservazione o dai suoi incaricati.

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

- Con cadenza non superiore a 5 anni, l'estrazione di un campione di PdA sottoposti a conservazione;
- La verifica della firma digitale e della marca temporale apposte sul PdA;
- La verifica che l'hash ricalcolato sul PdA estratto sia identico all'hash salvato sul sistema nel momento in cui il PdV stesso è stato conservato;

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 81 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

- Sull'insieme dei PdA estratti per la verifica di integrità verrà ulteriormente creato un sottoinsieme di documenti che saranno visualizzati da un operatore delegato che verificherà se il documento è correttamente leggibile ad occhio umano.

A seguito di ogni operazione di controllo verrà prodotto un Verbale di controllo e conservato nel repository documentale aziendale.

In generale i formati accettati dal Sistema di Conservazione e di cui garantiamo la disponibilità di viewer sono quelli previsti dalla normativa vigente PDF/PDF-A/, TIFF, JPG, XML, TXT ed email (.eml).

Poste Italiane NON garantisce il processo di leggibilità per i formati fuori normativa quindi è il cliente che dovrà munirsi dei software di visualizzazione necessari per le verifiche con i quali dopo aver scaricato il/i documenti potrà provvedere alla loro visualizzazione.

L'integrità binaria viene assicurata tramite il confronto dell'HASH.

Rimane a carico del cliente la verifica dell'integrità laddove il documento contenga cifrature, compressione, java script o altre logiche applicative.

[Torna al sommario](#)

9.3 SOLUZIONI ADOTTATE IN CASO DI ANOMALIE – INCIDENT MANAGEMENT

Le procedure messe in campo in caso di anomalie sono effettuate in base a quanto previsto dalla certificazioni ottenute dal Sistema di Conservazione e dai relativi processi di escalation.

Il processo di intervento a seguito della rilevazione di un incidente viene condotto in conformità a quanto previsto dal sistema di gestione integrato (conforme alle normative ISO 9001 e ISO 27001) per la gestione delle anomalie e secondo quanto previsto nella procedura 'Gestione Eventi e Incidenti di sicurezza informatica di Gruppo'.

Il processo viene gestito dalla struttura di CORPORATE AFFAIRS/TUTELA AZIENDALE /CERT attraverso la raccolta delle informazioni, la classificazione degli incidenti e la gestione della fase di escalation con la notifica ad AgID, in collaborazione con le strutture di CORPORATE AFFAIRS/TUTELA AZIENDALE/Sicurezza Informatica e di

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 82 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

Esercizio e Supporto Servizi Digitali, preposta al mantenimento della continuità del Servizio di Conservazione.

[Torna al sommario](#)

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Usò pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 83 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

10 PROCEDURE DI GESTIONE DELLA PRIVACY

Per quanto riguarda l'accesso ai dati da parte di personale Poste Italiane si farà riferimento alle procedure di gestione della privacy presenti nella documentazione ufficiale emessa da Poste Italiane sullo specifico tema.

Per quanto riguarda l'accesso ai dati da parte di personale del Cliente, e in particolare al personale che avrà accesso all'interfaccia web di ricerca, visualizzazione e esibizione dei documenti, si farà riferimento alle procedure di gestione della privacy del Cliente.

Allo scopo e per le sole finalità legata all'esecuzione del servizio, il Cliente delega e autorizza il Responsabile del Servizio di Conservazione e il Responsabile del Trattamento dei dati di Poste Italiane, ai sensi Regolamento Europeo della Privacy n. 2016/679, GDPR, ad accedere e a visualizzare i documenti sottoposti a Conservazione ai fini e per i soli scopi di verifica della leggibilità dei documenti conservati.

[Torna al sommario](#)

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Usò pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 84 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

11 ALLEGATO A - SPECIFICHE PER LA DEFINIZIONE DELLE CLASSI DOCUMENTALI

11.1 CLASSE DOCUMENTALE

La classe documentale definisce tutte le caratteristiche di un tipo di documento da sottoporre a conservazione. A partire dalla definizione della classe documentale vengono generati i file DTD e XSD da utilizzare per la validazione del file XML che descrive i documenti dei PdV da archiviare.

Una classe documentale è definita dai seguenti parametri:

- ✓ Nome della classe documentale (massimo 10 caratteri);
- ✓ Descrizione;
- ✓ Periodo di conservazione;
- ✓ Abilitazione alla conservazione automatica dei documenti;
- ✓ Numero massimo di file per documento (se sono accettati file multipli il limite è 10 altrimenti 1);
- ✓ Abilitazione all'obbligatorietà di firma per il file di controllo;
- ✓ Abilitazione all'obbligatorietà di specifica dell'impronta hash del file di dati all'interno del file di controllo;
- ✓ Valore che indica il fatto che la tipologia sia condivisa per un insieme di attributi.

Gli attributi sono definiti da:

- ✓ Nome = nome dell'attributo;
- ✓ Descrizione = descrizione dell'attributo;
- ✓ Tipo dato = da una lista che comprende "VARCHAR, NUMBER, DATE, TIME";
- ✓ Lunghezza massima = obbligatorio per i campi VARCHAR e NUMBER (fino a 4000 per i VARCHAR, fino a 38 cifre per i NUMBER);
- ✓ Lunghezza massima della parte decimale = obbligatorio per i campi NUMBER;

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 85 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

- ✓ Molteplicità = Numero massimo di valori possibili per l'attributo per un singolo documento;
- ✓ Obbligatorio = S / N;
- ✓ Indice XML = definisce l'ordine in cui gli attributi compaiono nell'XML;
- ✓ Indice display = definisce l'ordine in cui gli attributi sono visualizzati sulle interfacce web;
- ✓ Divisore display = solo per i campi NUMBER, default 1. I valori archiviati vengono visualizzati divisi per questa quantità;
- ✓ Univoco = S/N, se S il valore dell'attributo è univoco per tutti i documenti della classe.

[Torna al sommario](#)

Esempio di classe

La definizione di una generica classe documentale "articolo" potrebbe essere la seguente:

Nome: Articolo

Descrizione: Articoli scientifici

Retention time: 10 anni

Abilitazione conservazione automatica dei documenti: S

Numero massimo di file per documento: 10

Obbligatorietà di firma per il file di controllo: N

Obbligatorietà di specifica dell'impronta: N

Tipologia condivisa: N

Attributo 1

- Nome = titolo
- Descrizione = Titolo dell'articolo
- Tipo dato = VARCHAR
- Lunghezza massima = 256
- Molteplicità = 1

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 86 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

- Obbligatorio = S
- Indice XML = 1
- Indice display = 1
- Univoco = N

Attributo 2

- Nome = autore
- Descrizione = Autore dell'articolo
- Tipo dato = VARCHAR
- Lunghezza massima 64
- Molteplicità = 5
- Obbligatorio = S
- Indice XML = 2
- Indice display = 2
- Univoco = N

Attributo 3

- Nome = data_redazione
- Descrizione = Data di redazione dell'articolo
- Tipo dato = DATE
- Molteplicità = 1
- Obbligatorio = N
- Indice XML = 3
- Indice display = 4
- Univoco = N

Attributo 4

- Nome = data_pubblicazione
- Descrizione = Data di pubblicazione dell'articolo
- Tipo dato = DATE
- Molteplicità = 1
- Obbligatorio = S
- Indice XML = 4

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 87 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

- Indice display = 3
- Univoco = N

Attributo 5

- Nome = Abstract
- Descrizione = Breve descrizione del contenuto dell'articolo
- Tipo dato = VARCHAR
- Lunghezza massima = 2000
- Molteplicità = 1
- Obbligatorio = S
- Indice XML = 5
- Indice display = 5
- Univoco = N

Nota:

- ✓ Il formato di dato per i campi di tipo DATE è obbligatoriamente il seguente: YYYY-MM-DD;
- ✓ Il formato di dato per i campi di tipo TIME è obbligatoriamente il seguente: HH24:MI:SS;
- ✓ Il carattere separatore dei decimali, per i campi di tipo NUMBER è obbligatoriamente il punto.

[Torna al sommario](#)

11.2 ESEMPIO DI XML

Di seguito un esempio di XML associato alla classe "articolo":

```
<?xml version="1.0"?>
<articolo>
  <documento>
    <titolo>Gestione Documentale for dummies</titolo>
    <autore>Nome Cognome</autore>
    <autore>Nome1 Cognome1</autore>
  </documento>
</articolo>
```

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Usò pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 88 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

```
<data_pubblicazione>2015-11-22</data_pubblicazione>
<abstract>bla bla bla</abstract>
<file size=12345>GestioneDocumentale.pdf</file>
</documento>
<documento>
  <titolo>Gestione Documentale corso avanzato</titolo>
  <autore>Nome Cognome</autore>
  <data_redazione>2006-10-10</data_redazione>
  <data_pubblicazione>2006-12-23</data_pubblicazione>
  <abstract>bla bla bla</abstract>
  <file size=1234567>GestioneDocumentaleAdvanced.pdf</file>
  <file size=123456789>GestioneDocumentaleAdv_allegati.pdf</file>
</documento>
</articolo>
```

[Torna al sommario](#)

11.3 CLASSE DOCUMENTALE CONDIVISA

Una classe documentale condivisa è un tipo particolare di classe documentale per la quale è definita una ownership dei documenti archiviati, in modo da poter configurare le regole per l'accesso ai singoli documenti.

Le classi condivise sono caratterizzate dalla presenza di un attributo obbligatorio 'codice_utente' che identifica univocamente gli owner dei PdV della classe, e conseguentemente dei relativi documenti. Il valore codice_utente, oltre che nel file index.xml per ciascun documento, è contenuto anche nel file di controllo del PdV. Gli owner sono utenti del sistema ai quali viene associato il valore del campo codice_utente relativo ai documenti sui quali avranno visibilità.

Il sistema prevede, per quanto riguarda l'accesso ai PdA/documenti delle classi condivise, la definizione di due ruoli:

- ✓ Ruolo "User": ha la visibilità dei soli PdA/documenti di sua proprietà (quelli che riportano il valore 'codice_utente' a lui associato);
- ✓ Ruolo "Supervisor": ha la visibilità su tutti i PdA/documenti della classe condivisa.

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 89 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

La definizione delle classi documentali condivise è identica a quella per le classi documentali standard. L'attributo 'codice_utente' viene inserito automaticamente, come ultimo attributo, all'atto della creazione della classe, ed è obbligatorio per tutti i documenti appartenenti alla classe documentale condivisa.

[Torna al sommario](#)

11.4 ESEMPIO DI CLASSE CONDIVISA

Ipotizziamo di voler creare la stessa classe documentale di cui al paragrafo 2.2, ma di voler suddividere gli articoli inviati per categoria, dandone l'opportuna visibilità ai soli utenti di pertinenza.

La definizione degli attributi sarà identica a quella riportata nel paragrafo 2.2, tranne per il valore di specifica della tipologia:

Nome: Articolo

Descrizione: Articoli scientifici

Retention time: 10 anni

Abilitazione conservazione automatica dei documenti: S

Numero massimo di file per documento: 10

Obbligatorietà di firma per il file di controllo: N

Obbligatorietà di specifica dell'impronta: N

Tipologia condivisa: S

Il sistema, all'atto della creazione della classe, definirà un ulteriore attributo obbligatorio, denominato 'codice_utente', che verrà valorizzato con il nome della categoria alla quale l'articolo si riferisce.

Verranno creati in seguito gli utenti, e ad ognuno verrà configurato l'accesso alla sola categoria di pertinenza.

[Torna al sommario](#)

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 90 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

11.5 ESEMPIO DI XML PER CLASSE COINDIVISA

Di seguito un esempio di XML associato alla classe "articolo", nell'ipotesi che tale classe sia stata creata come classe condivisa:

```
<?xml version="1.0"?>
<articolo>
  <documento>
    <titolo>Gestione Documentale for dummies</titolo>
    <autore> Nome Cognome </autore>
    <autore> Nome1 Cognome1 </autore>
    <data_pubblicazione>2015-11-22</data_pubblicazione>
    <abstract>bla bla bla</abstract>
    <codice_utente>principiante</codice_utente>
    <file size=12345>GestioneDocumentale.pdf</file>
  </documento>
  <documento>
    <titolo>Gestione Documentale corso avanzato</titolo>
    <autore>Nome Cognome</autore>
    <data_redazione>2015-10-10</data_redazione>
    <data_pubblicazione>2015-11-23</data_pubblicazione>
    <abstract>bla bla bla</abstract>
    <codice_utente>principiante</codice_utente>
    <file size=1234567>GestioneDocumentaleAdvanced.pdf</file>
    <file size=123456789>GestioneDocumentaleAdv_allegati.pdf</file>
  </documento>
</articolo>
```

In tal modo soltanto gli utenti che saranno associati al valore 'principiante' del campo 'codice_utente' avranno visibilità su tali documenti.

Non vi sono limitazioni al numero di possibili valori del campo 'codice_utente'.

I valori del campo 'codice_utente' vengono trattati come stringhe di lunghezza massima pari a 64 caratteri.

[Torna al sommario](#)

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 91 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

12 ALLEGATO B - SPECIFICHE PER L'INVIO DEI FLUSSI DOCUMENTALI

12.1 PdV - PACCHETTO DI VERSAMENTO

Un PdV di documenti è l'oggetto che viene inviato al sistema Postedoc per essere sottoposto al processo di archiviazione e conservazione. Il Pdv ha le seguenti caratteristiche:

- ✓ E' costituito da un insieme di documenti della stessa classe documentale e dagli attributi che descrivono ciascun documento, secondo la definizione della classe;
 - ✓ Ciascun documento può avere associato uno o più file; ✓
- Un Pdv può essere inviato al sistema Postedoc attraverso:

- Interfaccia WEB
- Interfaccia Web Service.

In casi particolari è possibile definire pacchetti di versamento personalizzabili per il cliente e descritti nell'allegato "specificità del contratto"

[Torna al sommario](#)

12.2 CARATTERISTICHE DEL FLUSSO DOCUMENTALE

Per inviare i PdV via Web è necessario possedere un'utenza che permetta l'accesso alla funzionalità Web di "upload PdV" per la relativa classe documentale.

I PdV andranno trasferiti tramite http-file-upload.

Per inviare ciascun PdV è necessario predisporre il trasferimento di una coppia di file:

- Un file di "dati"
- Un file di "controllo".

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 92 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

Per inviare PdV via Web Service è necessario possedere un'utenza che abbia i permessi di invio dei PdV per la relativa classe documentale.

I PdV andranno trasferiti tramite richiamo dell'opportuno metodo Web Service.

Per inviare ciascun PdV è necessario predisporre il trasferimento di una coppia di file:

- Un file di "dati" eventualmente inviato a blocchi
- Un file di "controllo".

[Torna al sommario](#)

12.2.1 Caratteristiche del file di "dati"

Il file dei "dati" PdV è un archivio di tipo **.zip** contenente tutti i file (uno o più file per documento) e un file XML di descrizione.

Il formato dei nomi dei file di dati è `<AZIENDA>-<TIPODOC>-YYYYMMDDXXXXXXXXX.<EXT>` dove `<AZIENDA>` è il nickname dell'utilizzatore del servizio Postedoc, `<TIPODOC>` è il nome della classe documentale, `YYYYMMDD` è la data di creazione, `XXXXXXXXX` è un identificativo univoco per quella data (gestito dall'utilizzatore del servizio), e `<EXT>` è l'estensione del tipo di archivio inviato.

Esempio:

Poste Italiane-articolo-20061122-art00001.zip

Il file XML contenuto all'interno dell'archivio deve necessariamente chiamarsi `"index.xml"`. Esso contiene, per ogni documento, tutti gli attributi del documento stesso, e i riferimenti ai file che compongono il documento.

Il file `index.xml` ha la seguente struttura:

```
<?xml version="1.0"?>
<[tipodoc]>
  <documento>
```

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 93 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

```

    <[attributo1]>[valore att. 1]</[attributo1]>
<[attributo2]>[valore 1 att. 2]</[attributo2]>
    ...
    <[attributo2]>[valore N att. 2]</[attributo2]>
<[attributo3]>[valore att. 3]</[attributo3]>
<file size=
[size file 1]>[nomefile 1]</file>
    ...
    <file size= [size file M]>[nome file M]</file>
</documento>
.....
.....
.. altri documenti ...
</[tipodoc]>

```

La struttura del file xml dipende dalla classe documentale; il file contiene un tag principale che corrisponde alla tipologia del documento (<[tipodoc]>).

All'interno del tag si trovano tanti tag <documento> quanti sono i documenti contenuti nel PdV. Ogni tag <documento> contiene la sequenza dei tag associati agli attributi e un tag <file> per ciascun file che compone il documento. Inoltre, per ciascun documento:

- I tag degli attributi compaiono nell'ordine definito dal parametro "indice XML" della classe documentale;
- Il tag coincide col nome dell'attributo;
- Il valore dell'attributo è specificato all'interno del tag;
- Se un attributo non obbligatorio non è valorizzato, il relativo tag non deve essere presente;
- Se un attributo ha molteplicità maggiore di uno il relativo tag può comparire fino a N volte, con N pari alla molteplicità;
- Gli attributi di tipo DATE devono avere il formato YYYY-MM-DD;
- Gli attributi di tipo TIME devono avere il formato HH24:MM:SS;
- Il separatore per la parte decimale dei numeri è il punto;

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 94 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

- Il tag `<file>` ha un parametro opzionale "size" che corrisponde alla size, in byte, del file;
- Il tag `<file>` può comparire fino a M volte, con M pari al parametro "molteplicità file" della classe documentale.

Segue un esempio di file XML per la classe documentale "articolo":

```
<?xml version="1.0"?>
<articolo>
  <documento>
    <titolo>Gestione Documentale for dummies</titolo>
    <autore> Nome Cognome </autore>
    <autore> Nome1 Cognome1</autore>
    <data_pubblicazione>2015-11-22</data_pubblicazione>
    <abstract>bla bla bla</abstract>
    <file size=12345>GestioneDocumentale.pdf</file>
  </documento>
  <documento>
    <titolo>Gestione Documentale corso avanzato</titolo>
    <autore>Nome Cognome</autore>
    <data_redazione>2015-10-10</data_redazione>
    <data_pubblicazione>2015-11-22</data_pubblicazione>
    <abstract>bla bla bla</abstract>
    <file size=1234567>GestioneDocumentaleAdvanced.pdf</file>
    <file size=123456789>GestioneDocumentaleAdv_allegati.pdf</file>
  </documento>
</articolo>
```

[Torna al sommario](#)

12.2.2 Caratteristiche del file di "controllo"

Il file di controllo serve a verificare l'integrità e l'avvenuto trasferimento del PdV.

E' composto da un file XML avente la seguente struttura:

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 95 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

```
<?xml version="1.0" encoding="UTF-8"?>
<file_chk>
  <file_size>[size file di dati]</file_size>
  <file_hash          type="[algoritmo          di          hashing
utilizzato]">fk56g78978jb889sd8a5904tu0</file_hash> </file_chk>
```

Il tag *file_size* contiene la size in byte del file di dati.

Il tag *file_hash* contiene l'impronta hash del file di dati, calcolata con l'algoritmo di hashing indicato nella proprietà *type*.

Nota: nel caso di classi documentali condivise, il file di controllo dovrà contenere obbligatoriamente anche il tag "codice_utente", come nell'esempio seguente:

```
<?xml version="1.0" encoding="UTF-8"?>
<file_chk>
  <file_size>[size file di dati]</file_size>
  <file_hash          type="[algoritmo          di          hashing
utilizzato]">fk56g78978jb889sd8a5904tu0</file_hash>
  <codice_utente>[valore codice utente]</codice_utente>
</file_chk>
```

Il formato dei nomi dei file di controllo è <AZIENDA>-<TIPODOC>-YYYYMMDDXXXXXXXXX-chk.xml dove <AZIENDA>-<TIPODOC>-YYYYMMDD-XXXXXXXXX coincide con il nome del relativo file di dati.

Esempio:

Poste Italiane-articolo-20061122-art00001-chk.xml

Il file di controllo può contenere altri XML-tags non obbligatori, posizionati sempre dopo il tag *file_hash* (o, nel caso di classi condivise, dopo il tag *codice_utente*

Il file di controllo può essere firmato dal Responsabile della Conservazione presso il cliente, che in tal modo certifica l'autenticità, la veridicità e l'integrità dei documenti trasmessi.

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 96 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

La firma del file di controllo produce un nuovo file, con estensione. p7m.
Quest'ultimo file deve essere trasferito insieme al file di dati.

Esempio:

Poste Italiane-articolo-20061122-art00001-chk.xml.p7m

[Torna al sommario](#)

12.3 PdA – PACCHETTO DI ARCHIVIAZIONE

A seguito del corretto invio di un flusso di documenti, composto, come sopra specificato, da un PdV e da un file di controllo, i PdV opportunamente verificati e validati dal Sistema di Conservazione, vengono trasformati in pacchetti di Archiviazione (PdA).

Il (PdA) generato nel processo di conservazione 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 quindi un contenitore informativo che contiene:

- gli oggetti informativi individuati per la conservazione (documenti, fascicoli elettronici);
- un Indice del Pacchetto di Archiviazione (IPdA) che rappresenta le Informazioni sulla Conservazione.

Il PdA viene prodotto in conformità al formato definito nello standard SInCRO (UNI 11386:2010) come descritto al paragrafo 6.3.

Il PdA viene quindi firmato digitalmente dal Responsabile del Servizio di Conservazione e sottoposto a marcatura temporale. L'indice del PdA (IdPA o IdC) contenente i metadati e le impronte (SHA256) dei file contenuti nel PdA, insieme agli stessi file, viene archiviato/conservato all'interno del Repository Postedoc.

[Torna al sommario](#)

12.3.1 PdV di rettifica

I PdV di rettifica, permettono di inviare versioni modificate (corrette) di documenti già conservati. Una rettifica contiene il set completo di file e attributi del documento da rettificare, e non solo i dati e/o i file da modificare, e viene sottoposta allo stesso

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 97 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

processo di conservazione dei documenti originali; i documenti rettificati rimangono comunque a disposizione sul sistema. È importante sottolineare che in nessun caso è possibile modificare il proprietario di un documento.

[Torna al sommario](#)

12.3.2 Invio di PdV di rettifica

Anche per questa tipologia di PdV è necessario inviare una coppia di file:

- Un file di "dati";
- Un file di "controllo".

È possibile inviare PdV di rettifica utilizzando solo il canale Web.

[Torna al sommario](#)

12.3.3 File di dati del PdV di rettifica

Il file dei "dati" è un archivio di tipo **.zip** contenente tutti i file (uno o più file per documento) e un file XML di descrizione.

Il formato dei nomi dei file di dati è R-<UNITA_1>.<...>.<UNITA_N>.<AZIENDA>-<TIPODOC>-YYYYMMDD-XXXXXXXX.<EXT> dove

- R è un carattere che lo identifica come PdV di rettifica;
- <UNITA_1> è il nickname dell'unità cui è associato il PdV;
- <AZIENDA> è il nickname dell'azienda "root" utilizzatrice del servizio Postedoc;
- <UNITA_1><...><UNITA_N><AZIENDA> è la lista di tutte le unità ordinate gerarchicamente, a partire da quella cui è associato il PdV fino alla root, separate da '.' (punto);
- <TIPODOC> è il nome della classe documentale;
- YYYYMMDD è la data di creazione;
- XXXXXXXX è un identificativo univoco per quella data (gestito dall'utilizzatore del servizio). L'univocità riguarda sia i PdV di rettifica che quelli standard;
- <EXT> è l'estensione del tipo di archivio inviato.

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 98 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

Esempio:

R-editoriali.Poste Italiane-articolo-20061122-art00001.zip

Il file XML contenuto all'interno dell'archivio deve necessariamente chiamarsi "index.xml". Esso contiene, per ogni documento, tutti gli attributi del documento stesso, e i riferimenti ai file che compongono il documento.

Il file *index.xml* ha la seguente struttura:

```
<?xml version="1.0"?>
<[tipodoc]-rettifica>
<rettifica> *
  <documento_originale>
    <id_documento>[id_documento_originale]</id_documento>
    <id_lotto>[id_PdV_originale]</id_lotto>
    <id_report>[id_report_originale]</id_report>
    <versione_report>[version_report_originale]</versione_report>
  </documento_originale>
  <documento>
    <[attributo1]>[valore att. 1]</[attributo1]>
    <[attributo2]>[valore      1          att.
2]</[attributo2]>
    ...
    <[attributo2]>[valore N att. 2]</[attributo2]>
    <[attributo3]>[valore  att. 3]</[attributo3]>
      <file size=
[size file 1]>[nomefile 1]</file>
    ...
    <file size= [sizefile M]>[nome file M]</file>
  </documento>
</rettifica>
```

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 99 / 101
-----------------	--------------------	-------------------------------------	---	-----------------

.....

.. *altre rettifiche ...*

</[tipodoc]-rettifica>

La struttura del file xml dipende dalla classe documentale; il file contiene un tag principale che dipende dalla tipologia del documento (*<[tipodoc]-rettifca>*). All'interno del tag si trovano tanti tag *<rettifica>* quanti sono le rettifiche di documenti contenuti nel PdV.

Ogni tag *<documento_originale>* contiene quattro tag che identificano univocamente il documento originale da rettificare:

- *<id_documento>*: identificativo del documento originale;
- *<id_lotto>*: identificativo del documento originale;
- *<id_report>*: id_report del PdV originale;
- *<versione_report>*: versione_report del file originale.

Tali valori sono reperibili tramite il modulo web di ricerca e visualizzazione dei documenti, e all'interno del file di notifica di avvenuta conservazione.

Ogni tag *<documento>* contiene la sequenza dei tag associati agli attributi e un tag *<file>* per ciascun file che compone il documento. Inoltre, per ciascun documento, analogamente al caso dei PdV standard:

- I tag degli attributi compaiono nell'ordine definito dal parametro "indice XML" della classe documentale il tag coincide col nome dell'attributo;
- Il valore dell'attributo è specificato all'interno del tag;
- Se un attributo non obbligatorio non è valorizzato, il relativo tag non deve essere presente;

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 100 / 101
-----------------	--------------------	-------------------------------------	---	------------------

- Se un attributo è stato definito come "multiplo", il relativo tag può comparire più di una volta;
- Nel caso di classi documentali condivise, l'ultimo attributo, obbligatorio e con molteplicità 1, è sempre "codice_utente", e contiene per ciascun documento il codice univoco identificativo dell'owner del PdV (quindi deve avere lo stesso valore per tutti i documenti del PdV);
- Gli attributi di tipo DATE devono avere il formato YYYY-MM-DD;
- Gli attributi di tipo TIME devono avere il formato HH24:MM:SS;
- Il separatore per la parte decimale dei numeri è il punto;
- Il tag <file> ha un parametro opzionale "size" che corrisponde alla size, in byte, del file;
- Il tag <file> può comparire più di una volta se la classe documentale è stata creata con l'opzione "file multipli".

[Torna al sommario](#)

12.3.4 File di controllo di un PdV di rettifica

Il file di controllo di un PdV di rettifica differisce dal file di controllo di un Pdv di documenti solo per il nome; infatti, anche per il file di controllo viene aggiunto il carattere R per identificarlo come file di controllo di un PdV di rettifica.

Il formato dei nomi dei file di controllo di PdV di rettifica sarà quindi:
R<UNITA_1>.<...>.<UNITA_N>.<AZIENDA>-<TIPODOC>-YYYYMMDD-XXXXXXXXXchk.xml dove

<UNITA_1>.<...>.<UNITA_N>.<AZIENDA>-<TIPODOC>-YYYYMMDD-XXXXXXXXX
coincide con il nome del relativo file di dati.

[Torna al sommario](#)

VERSIONE 1.2	DATA 06/06/2019	CODICE RISERVATEZZA Uso pubblico	CODIFICA Manuale Conservazione_PI_v1.2	Pagina 101 / 101
-----------------	--------------------	-------------------------------------	---	------------------