

Manuale di conservazione

Questo manuale è stato redatto, sulla base del modello del progetto *Procedamus*, da Daniela Scialdoni e Massimiliano Forastieri

Sommario

1 Scopo e ambito del documento 3
2 Modello organizzativo della conservazione: Ruoli e Responsabilità 4
2.1 Modello organizzativo 4
2.1.1 Il modello adottato 4
2.2 Soggetto produttore 5
2.3 Organigramma 5
2.4 Struttura organizzativa 6
2.5 Utente 6
2.6 Responsabile della Conservazione 7
2.7 Organismi di tutela e di vigilanza 9
3 Organizzazione del servizio di conservazione 11
3.1 Responsabilità del Sistema di Conservazione 11
3.2 Gestione del Sistema di Conservazione 12
3.2.1 Organigramma 12
3.2.2 Struttura organizzativa 13
3.2.3 Pubblico ufficiale 13
4 Oggetti sottoposti a conservazione 13
4.1 Documenti informatici e aggregazioni documentali informatiche (fascicoli e serie) 13
4.2 Unità archivistiche e unità documentarie 16
4.3 Formati 17
4.4 Metadati 18
4.5 Pacchetto informativo 19
4.5.1 Pacchetto di versamento (PdV) 19
4.5.2 Pacchetto di archiviazione (PdA) 19
4.5.3 Pacchetto di distribuzione (PdD) 20
5 Processo di conservazione 20
5.1 Fasi del versamento e logiche di conservazione 20

5.1.1 Acquisizione dei pacchetti di versamento (PdV) 20
5.1.2 Verifiche sui pacchetti di versamento (PdV)....21
5.1.3 Rifiuto o accettazione 21
5.2 Gestione del pacchetto di archiviazione 21
5.2.1 Scarto dei pacchetti di archiviazione 21
5.3 Gestione del pacchetto di distribuzione 21
5.3.1 Modalità di esibizione 22
5.3.2 Produzione di duplicati 22
5.4 Monitoraggio e risoluzione delle anomalie....22
6 Descrizione del sistema di Conservazione 22
6.1 Componenti logiche 22
6.2 Componenti fisiche....23
6.3 Componenti tecnologiche....23
6.4 Procedure di gestione del sistema 23
6.5 Evoluzione del sistema 23
6.6 Monitoraggio e controlli....24
7 Strategie adottate a garanzia della conservazione....24
7.1 Misure a garanzia della interoperabilità....24
8 Trattamento dei dati personali....24
9 Allegati 25
9.1 Normativa di riferimento 26
9.1.1 Istruzioni, linee guida e documentazione informativa 28
9.1.2 Standard di riferimento....29
9.2 Glossario dei termini e degli acronimi 32
9.3 Elenco delle AOO e UOR 33
9.4 Elenco delle tipologie documentarie soggette a conservazione, soluzione di conservazione scelta e periodicità di invio in conservazione....34
9.5 Ruoli e Responsabilità....35
9.5.1 Figure interne (facenti capo al produttore) 35
9.5.2 Figure esterne (facenti capo al servizio di conservazione in outsourcing) 36
9.6 Manuale del Conservatore Postel....37
9.7 Manuale del Conservatore UNIMATICA....38
9.8 Manuale del Conservatore Enerj 39

1 Scopo e ambito del documento

Il manuale di conservazione (d'ora in poi manuale) dei documenti digitali, è uno strumento operativo che descrive e disciplina il modello organizzativo della conservazione adottato. Esso illustra nel dettaglio l'organizzazione del processo di conservazione, definendo i soggetti coinvolti e i ruoli svolti dagli stessi nel modello organizzativo di funzionamento dell'attività di conservazione da ASI- Agenzia Spaziale Italiana come soggetto produttore (d'ora in poi Produttore) che intende sottoporre a conservazione digitale fascicoli, serie e aggregazioni documentali, affidando il processo di conservazione a POSTEL SPA, a UNIMATICA e a ENERJ (d'ora in poi Conservatori).

La redazione del manuale di conservazione contempera l'assolvimento dell'obbligo normativo con le esigenze concrete del Produttore (cfr. l'Appendice normativa descritta nell' Allegato n. 1 [Cap.9.1]).

Il manuale costituisce una guida per gli attori coinvolti nel processo di gestione e di conservazione, per il cittadino e per le imprese. Ai primi, per porre in essere le corrette operazioni di gestione e conservazione documentale, agli ultimi due per comprendere le caratteristiche del Sistema di conservazione documentale e dei processi erogati.

Il presente manuale integra, per le parti specifiche di competenza del Produttore e per quanto riguarda i rapporti tra questi e i Conservatori, i manuali di conservazione di ciascuno, allegati al presente documento (Allegati n. 6, n. 7 e n. 8 [Cap.9.6; Cap.9.7; Cap.9.8]).

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

Per le tipologie degli oggetti sottoposti a conservazione e i rapporti con i Conservatori, il presente manuale è integrato con gli allegati ai contratti esecutivi, che definiscono le specifiche operative, le modalità di descrizione e di versamento nel Sistema di conservazione digitale dei documenti informatici e delle aggregazioni documentali informatiche oggetto di conservazione (Allegato n. 4 [Cap.9.4]).

2 Modello organizzativo della conservazione: Ruoli e Responsabilità

2.1 Modello organizzativo

Le Pubbliche Amministrazioni realizzano il processo di conservazione ai sensi all'art. 34, comma 1-bis, del CAD[1], fatte salve le competenze del Ministero per i beni e le attività culturali e del turismo ai sensi del decreto legislativo 22 gennaio 2004, n. 42.

Il processo di conservazione può essere pertanto svolto all'interno o all'esterno della struttura organizzativa dell'ente.

I requisiti del processo di conservazione, le responsabilità e i compiti del responsabile della conservazione e del responsabile del servizio di conservazione, e le loro modalità di interazione sono formalizzate nel manuale di conservazione del Titolare dell'oggetto della conservazione e nelle specifiche del contratto di servizio o dell'accordo. Tali modalità trovano riscontro anche nel manuale di conservazione del conservatore.

Al fine di garantire l'autenticità, l'integrità, l'affidabilità, la leggibilità e la reperibilità dei documenti, i fornitori di servizi di conservazione devono possedere requisiti di elevato livello in termini di qualità e sicurezza in aderenza allo standard ISO/IEC 27001 (Information security management systems - Requirements) del sistema di gestione della sicurezza delle informazioni nel dominio logico, fisico e organizzativo nel quale viene realizzato il processo di conservazione e ISO 14721 OAIS (Open Archival Information System - Sistema informativo aperto per l'archiviazione), e alle raccomandazioni ETSI TS 101 533-1 v. 1.2.1, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.

2.1.1 Il modello adottato

La scelta adottata dal Produttore è quella del modello in outsourcing per la fornitura del servizio di conservazione.

Il Produttore è il titolare delle unità documentarie informatiche poste in conservazione e, attraverso il proprio Responsabile della conservazione, definisce e attua le politiche complessive del Sistema di conservazione governandone la

[1] L'art. 34, comma 1-bis, del CAD prevede che: "Le pubbliche amministrazioni possono procedere alla conservazione dei documenti informatici:
a) all'interno della propria struttura organizzativa;
b) affidandola, in modo totale o parziale, nel rispetto della disciplina vigente, ad altri soggetti, pubblici o privati che possiedono i requisiti di qualità, di sicurezza e organizzazione individuati, nel rispetto della disciplina europea, nelle Linee guida di cui all'art 71 relative alla formazione, gestione e conservazione dei documenti informatici nonché in un regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici emanato da AgID, avuto riguardo all'esigenza di assicurare la conformità dei documenti conservati agli originali nonché la qualità e la sicurezza del sistema di conservazione".

gestione con piena responsabilità ed autonomia, in relazione al modello organizzativo adottato affida ai Conservatori la gestione del servizio di conservazione secondo quanto previsto dalla normativa in materia.

2.2 Soggetto produttore

ASI-Agenzia Spaziale Italiana è il soggetto produttore che versa le unità documentarie informatiche da conservare con gli opportuni metadati, in continuità con il processo di gestione documentale, iniziato all'interno dell'Agenzia.

I rapporti tra Produttore e Conservatore Postel, cui è stata affidata, con Determina del 6 febbraio 2018, n. 34, la gestione del servizio di conservazione, sono formalizzati e regolati per mezzo dei seguenti documenti fondamentali:

- contratto esecutivo n. 1703638121008001COE prot. ASI n. 1458 del 13 febbraio 2018;
- allegati al contratto esecutivo, incluso il Progetto dei Fabbisogni ASI del 06.12.2017

I rapporti tra Produttore e Conservatore Unimatica, sono formalizzati con Contratto n. UIS/348/2018 prot. n. 13448 del 13/12/2018 la gestione dei Servizi UNIFATTPA e UNISTORAGE

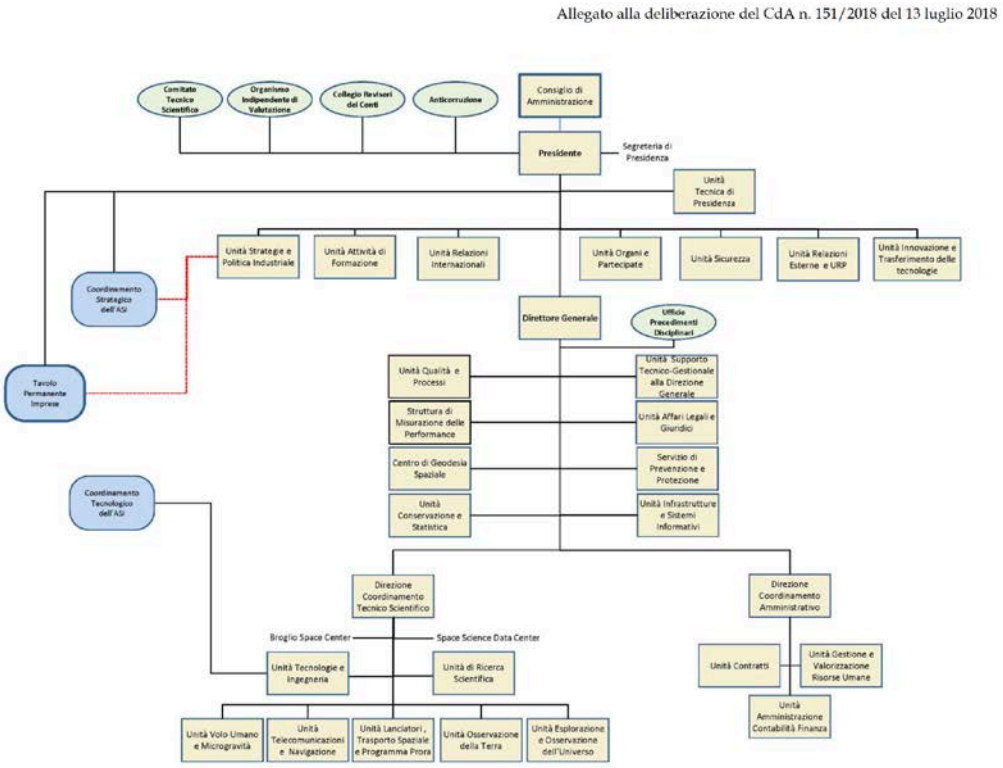
I rapporti tra Produttore e Conservatore Enerj sono formalizzati per effetto dell'affidamento alla società Dedagroup del Servizio di "*Assistenza e manutenzione sul sistema di Protocollo Informatico "Folium" e servizio di conservazione a norma del "registro giornaliero di protocollo*" per il periodo di 12 mesi dalla stipula CIG ZDC2CD71CC di cui alla Determina n. 90 del 30.04.2020. Il sistema è descritto nella nota Prot. 8697 del 09.10.2015 in cui si precisa che "L'invio del documento al sistema di conservazione a norma avviene in maniera automatica dal sistema di gestione del protocollo Folium verso il sistema di conservazione a norma distribuito da Dedagroup ed erogato dalla società Enerj".

I nominativi delle figure coinvolte e la descrizione delle principali attività svolte da coloro che hanno ruoli organizzativi all'interno del soggetto produttore sono indicati nell' Allegato n. 5 [Cap.9.5]). Con riferimento alle figure coinvolte riportate nei paragrafi precedenti e alle attività delegate a soggetti interni ed esterni all'Ente, tale tabella indica le attività delegate, i soggetti cui sono state delegate e il periodo di validità della delega.

2.3 Organigramma

L'ASI è organizzata in un'unica Area Organizzativa Omogenea (AOO), descritta nell'allegato 9.3[Cap.9.3], come previsto dalla legge 7 agosto 1990, n. 241 (artt. 4 e 6), dal DPR 28 dicembre 2000, n. 445 e dal DPCM 3 dicembre 2013, art. 3, comma 1, lett. a).

L'organigramma al momento dell'adozione del presente Manuale è il seguente:



Il versamento in conservazione dei documenti informatici gestiti nella fase corrente dalle Unità e strutture dell'ASI è effettuato unicamente dai ruoli di Responsabile della conservazione e dai Delegati del responsabile della conservazione, ove non avvenga con processi automatici.

2.4 Struttura organizzativa

Il Sistema di conservazione delle unità documentarie informatiche e delle unità archivistiche informatiche dell'ASI prevede la collaborazione tra unità organizzative e soggetti interni ed esterni cui il Produttore ha affidato il coordinamento del processo di conservazione in base agli atti di affidamento nei quali sono definite le tipologie documentali, i tempi di versamento e conservazione, i formati e i metadati descrittivi utili a garantire una corretta interazione tra Produttore e Conservatori.

2.5 Utente

L'utente abilitato è la "Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di

interesse."

L'utente abilitato può richiedere al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge e nelle modalità previste dal manuale di conservazione.

2.6 Responsabile della Conservazione

Il responsabile della conservazione opera secondo quanto previsto dall'art. 44, comma 1-quater, del CAD[2].

Nella Pubblica Amministrazione, il responsabile della conservazione:

a) è un ruolo previsto dall'organigramma del Titolare dell'oggetto di conservazione;
b) è un dirigente o un funzionario interno formalmente designato e in possesso di idonee competenze giuridiche, informatiche ed archivistiche;
c) può essere svolto dal responsabile della gestione documentale o dal coordinatore della gestione documentale, ove nominato.

Il responsabile della conservazione definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.
Il responsabile della conservazione, sotto la propria responsabilità, può delegare lo svolgimento delle proprie attività o parte di esse a uno o più soggetti, che all'interno della struttura organizzativa, abbiano specifiche competenze ed esperienze. Tale delega, riportata nel manuale di conservazione, deve individuare le specifiche funzioni e competenze delegate.
In particolare, il responsabile della conservazione:

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

[2] L'art. 44, comma 1-quater, del CAD prevede che: "Il responsabile della conservazione, che opera d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei sistemi informativi, può affidare, ai sensi dell'articolo 34, comma 1-bis, lettera b), la conservazione dei documenti informatici a altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative, e tecnologiche e di protezione dei dati personali. Il responsabile della conservazione della pubblica amministrazione, che opera d'intesa, oltre che con i responsabili di cui al comma 1-bis, anche con il responsabile della gestione documentale, effettua la conservazione dei documenti informatici secondo quanto previsto all'articolo 34, comma 1-bis".

b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
c) genera e sottoscrive il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
d) genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
f) effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;
g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;
h) provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
i) predispone le misure necessarie per la sicurezza fisica e logica del sistema di conservazione come previsto dal par. 4.11 delle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti;
j) assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
l) provvede per le amministrazioni statali centrali e periferiche a versare i documenti informatici, le aggregazioni informatiche e gli archivi informatici, nonché gli strumenti che ne garantiscono la consultazione, rispettivamente all'Archivio centrale dello Stato e agli archivi di Stato territorialmente competenti, secondo le tempistiche fissate dall'art. 41, comma 1, del Codice dei beni culturali[3];
m) predispone il manuale di conservazione di cui al par. 4.7 delle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Nel caso in cui il servizio di conservazione venga affidato ad un conservatore, le attività suddette o alcune di esse, ad esclusione della lettera m), potranno essere affidate al responsabile del servizio di conservazione, rimanendo in ogni caso inteso che la responsabilità giuridica generale sui processi di conservazione, non essendo

[3] L'art. 41, comma 1, del Codice dei beni culturali prevede che: "Gli organi giudiziari e amministrativi dello Stato versano all'archivio centrale dello Stato e agli archivi di Stato i documenti relativi agli affari esauriti da oltre trent'anni, unitamente agli strumenti che ne garantiscono la consultazione. Le liste di leva e di estrazione sono versate settant'anni dopo l'anno di nascita della classe cui si riferiscono. Gli archivi notarili versano gli atti notarili ricevuti dai notai che cessarono l'esercizio professionale anteriormente all'ultimo centennio".

delegabile, rimane in capo al responsabile della conservazione, chiamato altresì a svolgere le necessarie attività di verifica e controllo in ossequio alle norme vigenti sul servizi affidati in outsourcing dalle PA.
Si precisa che il nominativo ed i riferimenti del responsabile della conservazione devono essere indicati nelle specifiche del contratto o della convenzione di servizio con il Conservatore nel quale sono anche riportate le attività affidate al responsabile del servizio di conservazione.

In ASI, il Responsabile della conservazione è anche Responsabile della gestione documentale e in quanto tale ha il compito di:

- produrre il pacchetto di versamento secondo le regole pattuite tra Responsabile della conservazione e Conservatore;
- assicurare la trasmissione del contenuto del pacchetto di versamento nel rispetto di quanto definito nel manuale di conservazione;
- d'intesa con il Responsabile del trattamento dati personali effettuare l'analisi dei procedimenti amministrativi e una ricognizione delle tipologie documentali.

2.7 Organismi di tutela e di vigilanza

Gli archivi e i singoli documenti prodotti dagli enti di ricerca sono considerati beni culturali[4] e sottoposti, pertanto, alle disposizioni di tutela previste dal Codice dei beni culturali. Garantire la tutela di archivi e singoli documenti si concreta negli obblighi conservativi previsti nell'art. 30 del predetto Decreto Legislativo che comporta, infatti, "l'obbligo di conservare i propri archivi nella loro organicità e di ordinarli. I soggetti medesimi hanno altresì l'obbligo di inventariare i propri archivi storici"[4].

Il rispetto delle disposizioni in ordine alla corretta conservazione è in capo al Ministero dei beni e delle attività culturali e del turismo, attraverso la Direzione generale archivi e, in particolare, alla Soprintendenza archivistica e bibliografica del Lazio. Tale ente, infatti, è investito del potere di vigilanza e ispezione ai sensi degli artt. 18 e 19[5]. Per quanto riguarda il Sistema di conservazione dell'ASI, la Soprintendenza archivistica e bibliografica Lazio verifica, in particolare, che il processo di conservazione avvenga in modo conforme alla normativa e ai principi di corretta e ininterrotta custodia.

L'importanza della corretta conservazione degli archivi si evince anche dall'esplicito divieto del legislatore di smembrarli[6] (cioè distruggere l'ordine di aggregazione

[4] Codice dei beni culturali e del paesaggio, Decreto Legislativo 22 gennaio 2004, n. 42, art. 10, comma 2, lett. b).
[4] D.Lgs. 42/2004, art. 30, comma 4.
[5] D.Lgs. 42/2004, in particolare all'art. 19, comma 1: "I soprintendenti possono procedere in ogni tempo, con preavviso non inferiore a cinque giorni, fatti salvi i casi di estrema urgenza, ad ispezioni volte ad accertare l'esistenza e lo stato di conservazione o di custodia dei beni culturali".
[6] D.Lgs. 42/2004, art. 20.

dei documenti, facendo perdere all'archivio la propria organizzazione e il proprio carattere di complesso unitario) e dall'elencazione degli interventi soggetti ad autorizzazione[7] poiché potenzialmente lesivi per l'archivio e i documenti di cui è costituito.

Ai fini della conservazione digitale, è necessario soffermarsi sulla richiesta di autorizzazione che è necessario chiedere per "lo spostamento, anche temporaneo, dei beni culturali mobili" e per il "trasferimento ad altre persone giuridiche di complessi organici di documentazione di archivi pubblici"[8]. Il secondo caso, in particolare, contempla proprio il trasferimento di archivi informatici ad altri soggetti giuridici, nell'ottica della conservazione permanente sia del documento sia del contesto archivistico.

L'Ente interessato ad attivare il servizio di conservazione digitale del proprio archivio di deposito o storico [9] deve, quindi, preventivamente chiedere l'autorizzazione alla Soprintendenza archivistica competente per territorio.

In adempimento alle citate disposizioni normative, il presente manuale verrà inviato alla Soprintendenza archivistica e bibliografica del Lazio per il rilascio dell'autorizzazione all'uso.

Il legislatore ha previsto un secondo ente che, in materia di conservazione digitale, lavora a fianco delle Soprintendenza avendo però un ruolo diverso. L'Agenzia per l'Italia digitale - AgID[10], infatti, per quanto concerne i sistemi di conservazione di archivi e documenti digitali, ha il compito di gestire il processo di accreditamento dei soggetti che richiedono di essere individuati come Conservatori, ai sensi dell'art. 29 – Qualificazione e accreditamento, del Codice dell'amministrazione digitale.

L'attività di vigilanza dell'AgID riguarda, quindi, il soggetto richiedente l'accreditamento e il Sistema di conservazione nel suo complesso, inteso cioè come l'insieme di regole, di procedure e di tecnologie idonee ad assicurare la corretta conservazione dei documenti e dei fascicoli informatici e dei relativi metadati, in ogni fase della vita del documento, dalla presa in carico fino allo scarto. Il Sistema deve garantire i requisiti fondamentali del documento conservato in forma digitale come l'identificazione certa del soggetto che ha formato il documento e dell'AOO di riferimento, l'integrità del documento, la leggibilità e la reperibilità del documento e delle informazioni relative e il rispetto delle misure di sicurezza.

---

[7] D.Lgs. 42/2004, art. 21.
[8] D.Lgs. 42/2004, art. 21, comma 1, lett. e).
[9] Il trasferimento o spostamento dell'archivio corrente non richiede il rilascio dell'autorizzazione, ma è sufficiente comunicarlo alla Soprintendenza per lo svolgimento delle attività di vigilanza e ispezione, D.Lgs. 42/2004, art. 21, comma 3.
[10] http://www.agid.gov.it/ - il link aperto il 26 gennaio 2017

In materia di sistemi di conservazione e documento informatico l'AgID, inoltre, ha un ruolo di consulenza, aggiornando le specifiche tecniche in materia di sistemi di conservazione, fornendo pareri, emanando linee guida, regolamenti e standard, favorendo il coordinamento e la condivisione delle informazioni tra gli enti pubblici[11].

I Sistemi di conservazione di POSTEL, di Unimatica e di Enerj sono sottoposti alla vigilanza di AgID che prevede la materiale conservazione dei dati e delle copie di sicurezza sul territorio nazionale e l'accesso ai dati presso la sede del Produttore.
Per migliorare la qualità dell'intero processo di conservazione il Produttore e il Conservatore possono avvalersi di specifici standard di valutazione, di autovalutazione e di auditing.[12]

3 Organizzazione del servizio di conservazione

3.1 Responsabilità del Sistema di Conservazione

Il Sistema di conservazione garantisce l'autenticità, l'integrità, l'affidabilità, la leggibilità e la reperibilità degli oggetti conservati dal momento della loro presa in carico dal Produttore, fino all'eventuale scarto indipendentemente dall'evolversi del contesto tecnologico e organizzativo.

La responsabilità del Sistema di conservazione come soggetto che svolge attività di conservazione è in capo a POSTEL, a UNIMATICA e a ENERJ.

Postel S.p.A. è partecipata in via totalitaria da Poste Italiane S.p.A. Il modello di Governance adottato da Postel è quello "tradizionale" caratterizzato dalla presenza di due diversi organi, per la gestione e per il controllo della società: il Consiglio di Amministrazione ed il Collegio Sindacale. La Revisione Legale dei Conti è affidata ad una Società di Revisione. L'insieme di regole che disciplinano il funzionamento dell'Azienda è costituito dal suo Statuto, dal Modello Organizzativo 231 e dal Codice Etico. Postel S.p.A. detiene il controllo della Società Address Software Srl e la partecipazione di Consorzio Logistica e Pacchi e di Poste Tributi S.c.p.a. in liquidazione.

UNIMATICA è una S.P.A. nata nel 2000 dalla partnership tra il gruppo Logital S.p.A. e l'Università di Bologna. Nel 2009 l'azionariato di Unimatica S.p.A. si è ulteriormente esteso ed arricchito grazie all'ingresso in qualità di azionista del Gruppo Intesa Sanpaolo, che ha acquistato il 25% delle azioni della società tramite Infogroup S.p.A. L'Università di Bologna ha mantenuto la sua partecipazione, attraverso la Fondazione Alma Mater. A partire dal 2010 Unimatica ha acquisito anche la partecipazione di un nuovo socio, il Gruppo RGI, leader in Italia ed in

[11] Per una disamina esaustiva delle competenze e funzioni si vedano il Codice dell'amministrazione digitale, D.Lgs. 82/2005, e le Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici
[12] Standard ISO 16363:2012

Europa nei servizi IT per il settore Assicurativo che dal 31 luglio 2019 detiene il 71% del capitale della società.
La missione della società è lo sviluppo di applicazioni informatiche e l'erogazione dei servizi per l'amministrazione digitale, basati sulla sicurezza della firma digitale e della dematerializzazione, tramite l'archiviazione e la conservazione a norma dei documenti. Le applicazioni ed i servizi Unimatica sono tutti in tecnologia web, sicura grazie all'uso appropriato della firma digitale e delle metodologie più avanzate di autenticazione e sicurezza delle transazioni in rete.

ENERJ è una società specializzata nella consulenza e realizzazione di soluzioni e servizi nell'ambito della Gestione Elettronica Documentale, della Conservazione Sostitutiva e della Fatturazione Elettronica alla Pubblica Amministrazione.

In quanto soggetti responsabili, in coerenza con OAIS, POSTEL, UNIMATICA e ENERJ si occupano delle politiche complessive del Sistema di conservazione e ne determinano l'ambito di sviluppo e le competenze. A tal fine provvedono alla pianificazione strategica, alla ricerca dei finanziamenti, alla revisione periodica dei risultati conseguiti e ad ogni altra attività gestionale mirata a coordinare lo sviluppo del Sistema.

I dati dei soggetti che hanno assunto la responsabilità del Sistema di conservazione sono riportati nell' Allegato n. 5 [Cap.9.5]), che verrà mantenuto opportunamente aggiornato.

3.2 Gestione del Sistema di Conservazione

Si rimanda a:

- Manuale di conservazione di POSTEL, capitolo 8, Allegato n. 6 [Cap.9.6] al presente manuale.
- Manuale di conservazione di UNIMATICA, capitolo G.1, Allegato n. 7 [Cap.9.7] al presente manuale.
- Manuale di conservazione di Enerj, capitolo 8, Allegato n. 8 [Cap.9.8] al presente manuale.

3.2.1 Organigramma

Si rimanda a:

- Manuale di conservazione di POSTEL, capitolo 5.1, Allegato n. 6 [Cap.9.6] al presente manuale.
- Manuale di conservazione di UNIMATICA, capitolo E.1, Allegato n. 7 [Cap.9.7] al presente manuale.
- Manuale di conservazione di Enerj, capitolo 6.1, Allegato n. 8 [Cap.9.8] al presente manuale.

3.2.2 Struttura organizzativa

Si rimanda a:

- Manuale di conservazione di POSTEL, capitolo 5.2, Allegato n. 6 [Cap.9.6] al presente manuale.
- Manuale di conservazione di UNIMATICA, capitolo E.2, Allegato n. 7 [Cap.9.7] al presente manuale.
- Manuale di conservazione di Enerj, capitolo 6.2, Allegato n. 8 [Cap.9.8] al presente manuale.

3.2.3 Pubblico ufficiale

Nei casi previsti dalla normativa, il ruolo di pubblico ufficiale è svolto dal Responsabile della conservazione o da altri dallo stesso formalmente designati, quali Delegati del responsabile della conservazione per l'attestazione di conformità all'originale di copie di documenti informatici conservati.

Si rimanda a:

- Manuale di conservazione di POSTEL, capitolo 7.7, Allegato n. 6 [Cap.9.6] al presente manuale.
- Manuale di conservazione di UNIMATICA, capitolo G.2, Allegato n. 7 [Cap.9.7] al presente manuale.
- Manuale di conservazione di Enerj, capitolo 8.7, Allegato n. 8 [Cap.9.8] al presente manuale.

4 Oggetti sottoposti a conservazione

4.1 Documenti informatici e aggregazioni documentali informatiche (fascicoli e serie)

Nella Pubblica Amministrazione, il sistema di gestione informatica dei documenti trasferisce al sistema di conservazione, ai sensi dell'art. 44, comma 1-bis, del CAD[13],:

a) i fascicoli informatici chiusi e le serie informatiche chiuse, trasferendoli dall'archivio corrente o dall'archivio di deposito;

[13] L'art. 44, comma 1-bis, del CAD prevede che: "Il sistema di gestione dei documenti informatici delle pubbliche amministrazioni è gestito da un responsabile che opera d'intesa con il dirigente dell'ufficio di cui all'articolo 17 del presente Codice, il responsabile del trattamento dei dati personali di cui all'articolo 29 del decreto legislativo 30 giugno 2003, n. 196, ove nominato, e con il responsabile del sistema della conservazione dei documenti informatici delle pubbliche amministrazioni, nella definizione e gestione delle attività di rispettiva competenza. Almeno una volta all'anno il responsabile della gestione dei documenti informatici provvede a trasmettere al sistema di conservazione i fascicoli e le serie documentarie anche relative a procedimenti non conclusi".

b) i fascicoli informatici e le serie non ancora chiuse trasferendo i documenti in essi contenuti sulla base di specifiche esigenze dell'ente, con particolare attenzione per i rischi di obsolescenza tecnologica.

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

a) i documenti informatici e i documenti amministrativi informatici con i metadati ad essi associati;
b) le aggregazioni documentali informatiche (fascicoli e serie) con i metadati ad esse associati contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che costituiscono le aggregazioni medesime, nel rispetto di quanto indicato per le Pubbliche Amministrazioni nell'articolo 67, comma 2, del DPR 445/200014e art. 44, comma 1-bis, CAD;
c) gli archivi informatici con i metadati associati.

Il sistema di conservazione garantisce l'accesso all'oggetto conservato per il periodo previsto dal piano di conservazione del titolare dell'oggetto della conservazione e dalla normativa vigente, o per un tempo superiore eventualmente concordato tra le parti, indipendentemente dall'evoluzione del contesto tecnologico.
Il sistema di conservazione è almeno logicamente distinto dal sistema di gestione informatica dei documenti.
Gli elenchi degli standard, delle specifiche tecniche e dei formati utilizzabili quali riferimento per il sistema di conservazione sono riportati negli allegati 2 "Formati di file e riversamento" e 4 "Standard e specifiche tecniche" delle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici.

Il Codice dell'amministrazione digitale definisce all'art. 1, lettera p) cosa debba intendersi per documento informatico[15] e al successivo art. 23-ter specifica la particolare categoria di documento informatico rappresentata dal documento amministrativo informatico ribadendone la natura di informazione primaria e originale. Lo stesso art. 23-ter riassume le azioni che è possibile effettuare sul documento amministrativo informatico.

Le aggregazioni di documenti informatici o di fascicoli informatici sono l'insieme definito e qualificato di documenti riuniti per caratteristiche omogenee, in

[14] L'art. 67, comma 2, del TUDA prevede che: "Il trasferimento deve essere attuato rispettando l'organizzazione che i fascicoli e le serie avevano nell'archivio corrente".
[15] D.Lgs. 82/2005 CAD, art. 1 comma 1, lettera p): «documento informatico»: il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;". Il "documento informatico" si differenzia dal documento elettronico così come definito all'art. 3, punto 35 del Regolamento UE 23 luglio 2014 n. 910 (eIDAS), "«documento elettronico», qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva;". Ai fini del CAD, art.1, comma 1-bis "valgono le definizioni di cui all'art. 3 del Regolamento eIDAS"

relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente[16].

Il fascicolo rappresenta, quindi, la prima forma di aggregazione determinata e può essere organizzato raccogliendo documenti diversi per formato, natura, contenuto giuridico, ma prodotti nel corso di una specifica attività; oppure raccogliendo documenti della stessa tipologia o qualità o forma, raggruppati quindi in base a criteri estrinseci, e riguardanti contenuti disomogenei.

In particolare è possibile distinguere tra differenti tipologie di fascicoli: fascicolo di persona, fascicolo di progetto, fascicolo di attività, fascicolo procedimentale.
La distinzione tipologica dei fascicoli deriva dal particolare iter di produzione della documentazione per cui la catena delle azioni che pongono in essere un insieme di documenti determina anche le modalità con cui i documenti vengono organizzati e archiviati e dà luogo, nel medio e lungo periodo, al cosiddetto processo di sedimentazione.

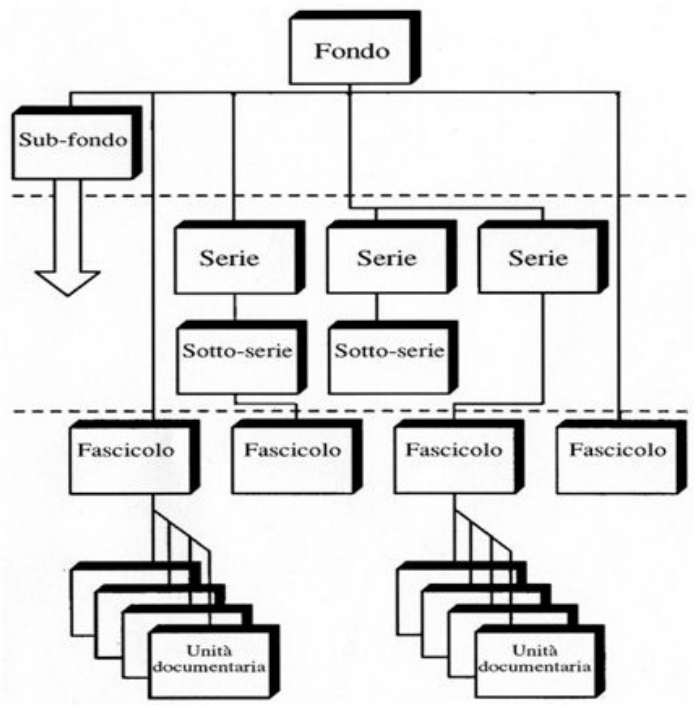
I fascicoli, così come particolari tipologie di documenti, creano ulteriori aggregazioni documentali definite serie[17]. Si tratta di articolazioni interne all'archivio createsi sulla base del processo di sedimentazione reso esplicito dall'applicazione del titolario di classificazione. Le serie sono funzionali all'individuazione di caratteristiche comuni per documenti o fascicoli, e consentono di conseguenza un'efficiente gestione dei dati oltre a rappresentare un elemento indispensabile della struttura dell'archivio. Dal punto di vista dei fascicoli, le serie si creano rispettando l'articolazione del titolario di classificazione sulla base del quale i singoli fascicoli vengono classificati e inseriti nel repertorio dei fascicoli.

La serie può corrispondere anche al raggruppamento di specifiche tipologie documentali, le quali, quindi, condividono un insieme di caratteristiche omogenee, tradotte in ambito informatico in un set di metadati.
Da un punto di vista normativo, il fascicolo informatico viene introdotto dal Codice dell'amministrazione digitale all'art. 41 in relazione al procedimento amministrativo: "La pubblica amministrazione titolare del procedimento raccoglie in un fascicolo informatico gli atti, i documenti e i dati del procedimento medesimo da chiunque formati"[18]; nel comma 2ter del predetto articolo, vengono elencate le indicazioni di cui il fascicolo deve essere provvisto per la corretta identificazione e gestione: "Il fascicolo informatico reca l'indicazione: a) dell'amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo; b) delle altre amministrazioni partecipanti; c) del Responsabile del procedimento; d)

[16] DPCM 3 dicembre 2013 Allegato 1 – Glossario
[17] ISAD(G) - Glossario: "Serie (series). Documenti ordinati secondo un sistema di archiviazione o conservati insieme perché sono il risultato di un medesimo processo di sedimentazione o archiviazione o di una medesima attività; appartengono ad una specifica tipologia; o a ragione di qualche altra relazione derivante dalle modalità della loro produzione, acquisizione o uso".
[18] D.Lgs. 82/2005 CAD, art. 41.

dell'oggetto del procedimento; e) dell'elenco dei documenti contenuti, salvo quanto disposto dal comma 2-quater. e-bis) dell'identificativo del fascicolo medesimo". Il successivo art. 44, esplicitando i Requisiti per la gestione e conservazione dei documenti informatici, dichiara che annualmente devono essere trasferiti al Sistema di conservazione "i fascicoli e le serie documentarie anche relative a procedimenti conclusi" 19. La gestione del fascicolo e delle aggregazioni documentali viene affrontata anche dalle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici al par. 3.3 Aggregazioni documentali informatiche e archivio informatico"

ISAD(G) – Schema gerarchico



L'elenco delle tipologie documentali e delle aggregazioni documentali sottoposte a conservazione e versate al Sistema di conservazione da parte dell'ASI è definito all'Allegato n. 4 [Cap.9.4]).

4.2 Unità archivistiche e unità documentarie

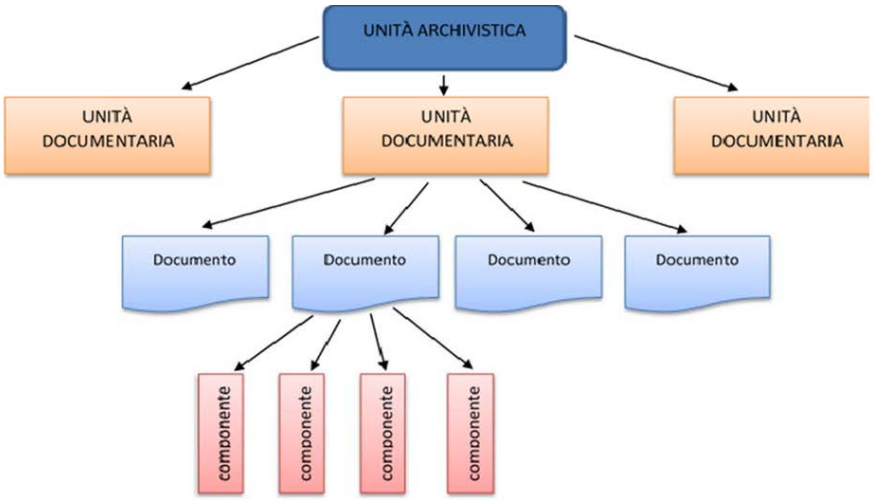
Il rapporto tra unità archivistiche e unità documentarie subisce in ambito informatico una traslazione rispetto alla tradizione archivistica e ciò è dovuto a esigenze gestionali, legate alla specificità dei supporti con cui vengono veicolate le

[19] D.Lgs. 82/2005 CAD, art. 44. A proposito è interessante osservare che il DPR 445/2000, in merito allo stato dei fascicoli versati in conservazione, afferma: "Almeno una volta ogni anno il Responsabile del servizio per la gestione dei flussi documentali e degli archivi provvede a trasferire fascicoli e serie documentarie relativi a procedimenti conclusi in un apposito archivio di deposito costituito presso ciascuna amministrazione".

unità informative in ambito informatico.

L'unità archivistica in ambito analogico è l'unità base costituita dall'insieme di documenti che condividono determinate caratteristiche identificative, risultato di un processo di produzione, che fanno dell'unità un'aggregazione qualificata e non casuale. In tal senso, l'unità archivistica è il livello di definizione e descrizione dell'aggregazione documentale oltre il quale non è possibile procedere, ossia i documenti che la costituiscono sono elementi che non possiedono un'identità propria se tolti, ad esempio, dal fascicolo, cioè se decontestualizzati.

L'unità archivistica nella maggior parte dei casi corrisponde al fascicolo, quindi un insieme di documenti, ma può corrispondere anche al singolo documento.
In ambito informatico tale rapporto, benché mantenga il rispetto dei principi archivistici, risulta più complesso, poiché l'unità documentaria diventa a sua volta un contenitore la cui natura è pre-strutturata sulla base della tipologia di informazioni che deve contenere: si articola in documenti principali, allegati, componenti. Le unità informative principali costituiscono il nucleo dell'unità documentaria e determinano la struttura e i metadati di riferimento.



L'ASI, in qualità di Produttore, determina la relazione di appartenenza tra i documenti che costituiscono l'unità documentaria e l'unità archivistica, mentre il Conservatore, in un secondo momento, si fa carico di mantenere stabili, consultabili e contestualizzate nel tempo tali informazioni, secondo i parametri definiti nel manuale di conservazione del Conservatore.

4.3 Formati

Il formato è l'insieme di informazioni che determinano la modalità con cui un oggetto digitale viene creato, memorizzato e riprodotto. Un oggetto digitale è una

sequenza di bit fissati con una certa organizzazione fisica su di una memoria. Tale contenuto digitale viene memorizzato e definito file. La possibilità di fruire e utilizzare un file è determinata dalla capacità di rappresentare la sequenza di bit per mezzo di un apposito software che riproduca, sulla base dei codici e delle regole che costituiscono il file stesso, il contenuto e la forma che gli era stata conferita dall'autore[20].
La corretta conservazione dei documenti nel tempo è determinata anche dalla scelta dei formati idonei a tale scopo, infatti, un problema di cui è necessario tener presente, è costituito dall'obsolescenza dei formati. Attualmente la soluzione più sicura è adottare, fin dal momento della formazione dei contenuti digitali, formati che abbiano le caratteristiche per fornire le maggiori garanzie in termini di conservazione a lungo termine.

4.4 Metadati

Insieme alla scelta dei formati, la definizione dei metadati è un'operazione fondamentale per l'attività conservativa delle memorie digitali a medio e lungo termine.
I metadati vengono esplicitamente citati come oggetti da sottoporre a conservazione associati ai documenti informatici, ai documenti amministrativi informatici e ai fascicoli informatici o aggregazioni documentali.

I metadati sono informazioni associate ai dati primari creati e trattati: sono a loro volta dati che descrivono, spiegano, localizzano una risorsa informativa rendendo più semplice il suo recupero, utilizzo e gestione. Ad esempio, il riferimento all'autore o alla tipologia di dato, il riferimento temporale alla creazione o registrazione del dato, la classificazione, etc.

Come si può intuire i metadati associati a una risorsa sono potenzialmente infiniti, quindi si è deciso di distinguerli in tre principali categorie[21]:

- Metadati descrittivi, descrivono una risorsa con lo scopo di scoprirla ed identificarla;

[20] In altre parole, il formato specifica la corrispondenza fra la rappresentazione binaria dell'oggetto digitale e i contenuti in esso presenti stabilendo le regole con le quali i bit che lo costituiscono devono essere interpretati; è proprio grazie ad esso che un sistema informatico è in grado di interpretare quei bit e restituire l'oggetto digitale nella stessa forma e con i contenuti che sono stati stabiliti dal suo creatore, decodificando in porzioni di testo, immagini, grafici, etc. le sequenze di bit che lo compongono. Stefano Allegrezza, Requisiti e standard dei formati elettronici per la produzione di documenti informatici, febbraio 2010.
[21] Questa distinzione funzionale è una delle tassonomie possibili e ha un carattere generale. In ambito archivistico, infatti, si preferisce distinguere tra: metadati identificativi, metadati sul contesto storico istituzionale, metadati sul contesto organizzativo, metadati sul contesto archivistico, metadati tecnologici, metadati sugli oggetti informativi digitali. Si veda: Pierluigi Feliciati, Gestione e conservazione di dati e metadati per gli archivi: quali standard ?, reperibile in Internet al 27 gennaio 2017.

- Metadati strutturali, indicano la struttura di oggetti composti, ad esempio i capitoli che assemblano le pagine;
- Metadati amministrativi, descrivono le informazioni volte a favorire la gestione del file (tipo di file, nome del produttore, riferimento temporale etc.).

Il Sistema di conservazione strutturato sul modello OAIS è predisposto per conservare queste differenti tipologie di metadati in luoghi diversi e si avvale di una caratteristica propria dei metadati per cui essi possono far parte del dato stesso o possono essere archiviati come oggetti esterni, e organizzati in gerarchie, ontologie o schemi.

Ad esempio, i dati e i metadati relativi all'oggetto informativo e alle informazioni sulla rappresentazione costituiscono un'unità denominata contenuto informativo e in tale forma viene conservata al fine di assicurare la fruibilità e la comprensibilità nel lungo periodo; i metadati descrittivi, invece, che descrivono e identificano le informazioni archiviate, vengono conservate separatamente in appositi database.

4.5 Pacchetto informativo

Gli oggetti sottoposti a conservazione, siano essi aggregazioni documentali informatiche, documenti informatici, o metadati, sono trasmessi dal Produttore, memorizzati e conservati nel Sistema e distribuiti agli Utenti sotto forma di pacchetti informativi.

Il pacchetto informativo, a seconda sia utilizzato per versare, conservare o distribuire gli oggetti sottoposti a conservazione, assume la forma, rispettivamente, di Pacchetto di versamento (PdV), Pacchetto di archiviazione (PdA) e Pacchetto di distribuzione (PdD).

4.5.1 Pacchetto di versamento (PdV)

Si rimanda a:

- Manuale di conservazione di POSTEL, capitolo 6.2 Allegato n. 6 [Cap.9.6] al presente manuale.
- Manuale di conservazione di UNIMATICA, capitolo F.3, Allegato n. 7 [Cap.9.7] al presente manuale.
- Manuale di conservazione di Enerj, capitolo 7.3, Allegato n. 8 [Cap.9.8] al presente manuale.

4.5.2 Pacchetto di archiviazione (PdA)

Si rimanda a:

- Manuale di conservazione di POSTEL, capitolo 6.2 Allegato n. 6 [Cap.9.6] al presente manuale.

- Manuale di conservazione di UNIMATICA, capitolo F.4, Allegato n. 7 [Cap.9.7] al presente manuale.
- Manuale di conservazione di Enerj, capitolo 7.4, Allegato n. 8 [Cap.9.8] al presente manuale.

4.5.3 Pacchetto di distribuzione (PdD)

Si rimanda a:

- Manuale di conservazione di POSTEL, capitolo 6.2 Allegato n. 6 [Cap.9.6] al presente manuale.
- Manuale di conservazione di UNIMATICA, capitolo F.5, Allegato n. 7 [Cap.9.7] al presente manuale.
- Manuale di conservazione di Enerj, capitolo 7.5, Allegato n. 8 [Cap.9.8] al presente manuale.

5 Processo di conservazione

5.1 Fasi del versamento e logiche di conservazione

Le procedure per l'attivazione del processo di conservazione sono dettagliate:

- nel Manuale di conservazione di POSTEL, capitolo 7 Allegato n. 6 [Cap.9.6] al presente manuale.
- Manuale di conservazione di UNIMATICA, capitolo G, Allegato n. 7 [Cap.9.7] al presente manuale.
- Manuale di conservazione di Enerj, capitolo 8, Allegato n. 8 [Cap.9.8] al presente manuale.

L'ASI chiederà il rilascio dell'autorizzazione al trasferimento in conservazione dei documenti informatici dalla Soprintendenza archivistica per il Lazio ai sensi dell'art. 21 del D.Lgs. 42/2004, Codice dei beni culturali e del paesaggio.

Il processo di conservazione si basa su di una logica di conservazione caratterizzata dal versamento da parte del Produttore degli oggetti da conservare (documenti informatici e aggregazioni documentali informatiche) secondo la tempistica definita e dettagliata nei manuali di conservazione dei Conservatori (Allegato n. 6, n. 7 e n. 8 [Cap.9.6, Cap.9.7, Cap.9.8]).

5.1.1 Acquisizione dei pacchetti di versamento (PdV)

Si rimanda a:

- Manuale di conservazione di POSTEL, capitolo 6.1 Allegato n. 6 [Cap.9.6] al presente Manuale.
- Manuale di conservazione di UNIMATICA, capitolo G, Allegato n. 7 [Cap.9.7] al presente Manuale.

- Manuale di conservazione di EnerJ, capitolo 8.1, Allegato n. 8 [Cap.9.8] al presente Manuale.

5.1.2 Verifiche sui pacchetti di versamento (PdV)

Si rimanda a:

- Manuale di conservazione di POSTEL, capitolo 6.2 Allegato n. 6 [Cap.9.6] al presente manuale.
- Manuale di conservazione di UNIMATICA, capitolo G, Allegato n. 7 [Cap.9.7] al presente manuale.
- Manuale di conservazione di Enerj, capitolo 8.2, Allegato n. 8 [Cap.9.8] al presente manuale.

5.1.3 Rifiuto o accettazione

Si rimanda a:

- Manuale di conservazione di POSTEL, capitoli 7.3 e 7.4 Allegato n. 6 [Cap.9.6] al presente atto.
- Manuale di conservazione di UNIMATICA, capitolo G, Allegato n. 7 [Cap.9.7] al presente Manuale.
- Manuale di conservazione di Enerj, capitolo 8.4, Allegato n. 8 [Cap.9.8] al presente Manuale.

5.2 Gestione del pacchetto di archiviazione

Si rimanda a:

- Manuale di conservazione di POSTEL, capitoli 7.5 e 8, Allegato n. 6 [Cap.9.6] al presente atto.
- Manuale di conservazione di UNIMATICA, capitolo G, Allegato n. 7 [Cap.9.7] al presente Manuale.
- Manuale di conservazione di Enerj, capitolo 8.5, Allegato n. 8 [Cap.9.8] al presente Manuale.

5.2.1 Scarto dei pacchetti di archiviazione

Si rimanda a:

- Manuale di conservazione di POSTEL, capitolo 7.8 Allegato n. 6 [Cap.9.6] al presente atto.
- Manuale di conservazione di UNIMATICA, capitolo G.3, Allegato n. 7 [Cap.9.7] al presente Manuale.
- Manuale di conservazione di Enerj, capitolo 8.8, Allegato n. 8 [Cap.9.8] al presente Manuale.

5.3 Gestione del pacchetto di distribuzione

Si rimanda a:

- Manuale di conservazione di POSTEL, capitolo 7.5 Allegato n. 6 [Cap.9.6] al presente manuale.
- Manuale di conservazione di UNIMATICA, capitolo F.5, Allegato n. 7 [Cap.9.7] al presente manuale.
- Manuale di conservazione di Enerj, capitolo 8.6, Allegato n. 8 [Cap.9.8] al presente manuale.

5.3.1 Modalità di esibizione

Si rimanda a:

- Manuale di conservazione di POSTEL, capitolo 7.6 Allegato n. 6 [Cap.9.6] al presente manuale.
- Manuale di conservazione di UNIMATICA, capitolo G.1, Allegato n. 7 [Cap.9.7] al presente manuale.
- Manuale di conservazione di Enerj, capitolo 8.6, Allegato n. 8 [Cap.9.8] al presente manuale.

5.3.2 Produzione di duplicati

Si rimanda a:

- Manuale di conservazione di POSTEL, capitolo 7.7 Allegato n. 6 [Cap.9.6] al presente manuale.
- Manuale di conservazione di UNIMATICA, capitolo G.2, Allegato n. 7 [Cap.9.7] al presente manuale.
- Manuale di conservazione di Enerj, capitolo 8.7, Allegato n. 8 [Cap.9.8] al presente manuale.

5.4 Monitoraggio e risoluzione delle anomalie

Si rimanda a:

- Manuale di conservazione di POSTEL, capitolo 9, Allegato n. 6 [Cap.9.6] al presente Manuale, in cui sono definite le specifiche operative e le modalità di interazione per la gestione delle anomalie e per il monitoraggio.
- Manuale di conservazione di UNIMATICA, capitolo J, Allegato n. 7 [Cap.9.7] al presente Manuale.
- Manuale di conservazione di Enerj, capitolo 10.4, Allegato n. 8 [Cap.9.8] al presente manuale.

6 Descrizione del sistema di Conservazione

6.1 Componenti logiche

Si rimanda a:

- Manuale di conservazione di POSTEL, capitolo 8.1, Allegato n. 6 [Cap.9.6] al presente manuale.
- Manuale di conservazione di UNIMATICA, capitoli H e H.1, Allegato n. 7 [Cap.9.7] al presente manuale.
- Manuale di conservazione di Enerj, capitolo 9.1, Allegato n. 8 [Cap.9.8] al presente manuale.

6.2 Componenti fisiche

Si rimanda a:

- Manuale di conservazione di POSTEL, capitolo 8.2, Allegato n. 6 [Cap.9.6] al presente manuale.
- Manuale di conservazione di UNIMATICA, capitoli H e H.1, Allegato n. 7 [Cap.9.7] al presente manuale.
- Manuale di conservazione di Enerj, capitolo 9.3, Allegato n. 8 [Cap.9.8] al presente manuale.

6.3 Componenti tecnologiche

Si rimanda a:

- Manuale di conservazione di POSTEL, capitolo 8.2, Allegato n. 6 [Cap.9.6] al presente manuale.
- Manuale di conservazione di UNIMATICA, capitoli H e H.1, Allegato n. 7 [Cap.9.7] al presente manuale.
- Manuale di conservazione di Enerj, capitolo 9.2, Allegato n. 8 [Cap.9.8] al presente manuale.

6.4 Procedure di gestione del sistema

Si rimanda a:

- Manuale di conservazione di POSTEL, capitolo 8.4, Allegato n. 6 [Cap.9.6] al presente manuale.
- Manuale di conservazione di UNIMATICA, capitolo I, Allegato n. 7 [Cap.9.7] al presente manuale.
- Manuale di conservazione di Enerj, capitolo 9.4, Allegato n. 8 [Cap.9.8] al presente manuale.

6.5 Evoluzione del sistema

Si rimanda a:

- Manuale di conservazione di POSTEL, capitolo 8.4, Allegato n. 6 [Cap.9.6] al presente manuale.

- Manuale di conservazione di UNIMATICA, capitolo I.2, Allegato n. 7 [Cap.9.7] al presente manuale.
- Manuale di conservazione di Enerj, capitolo 9.4, Allegato n. 8 [Cap.9.8] al presente manuale.

6.6 Monitoraggio e controlli

Si rimanda a:

- Manuale di conservazione di POSTEL, capitolo 9, Allegato n. 6 [Cap.9.6] al presente manuale.
- Manuale di conservazione di UNIMATICA, capitolo J, Allegato n. 7 [Cap.9.7] al presente manuale.
- Manuale di conservazione di Enerj, capitolo 10, Allegato n. 8 [Cap.9.8] al presente manuale.

7 Strategie adottate a garanzia della conservazione

7.1 Misure a garanzia della interoperabilità

Si rimanda a:

- Manuale di conservazione di POSTEL, capitolo 7.9, Allegato n. 6 [Cap.9.6] al presente manuale.
- Manuale di conservazione di UNIMATICA, capitolo G, Allegato n. 7 [Cap.9.7] al presente manuale.
- Manuale di conservazione di Enerj, capitolo 8.9, Allegato n. 8 [Cap.9.8] al presente manuale.

8 Trattamento dei dati personali

Il Responsabile del trattamento dei dati ha il compito di tutela delle informazioni contenute nei documenti da conservare; tale ruolo viene svolto sia dal Produttore che dal Conservatore nelle forme previste dalla normativa in materia di protezione dei dati personali (Regolamento generale per la protezione dei dati personali n. 2016/679 (General Data Protection Regulation o GDPR e dal Codice della Privacy 2020.

9 Allegati

9.1 Normativa di riferimento

Decreto Legislativo 13 dicembre 2017, n. 217, Disposizioni integrative e correttive al decreto legislativo 26 agosto 2016, n. 179, concernente modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche

Decreto Legislativo 26 agosto 2016, n. 179, Modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'art. 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche

Decreto Legislativo 12 maggio 2016, n. 90, Completamento della riforma della struttura del bilancio dello Stato, in attuazione dell'art. 40, comma 1, della legge 31 dicembre 2009, n. 196

Direttiva dell'Unione Europea (UE) 2016/680 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativa alla Protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

Regolamento dell'Unione Europea (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).

Decreto Legislativo 7 gennaio 2016, n. 2, Attuazione della direttiva 2014/60/UE relativa alla restituzione dei beni culturali usciti illecitamente dal territorio di uno Stato membro e che modifica il regolamento (UE) n. 1024/2012.

Risoluzione dell'Agenzia delle Entrate 25 settembre 2015, n.81/E, Interpello - ART. 11, legge 27 luglio 2000, n. 212 – Comunicazione del luogo di conservazione in modalità elettronica dei documenti rilevanti ai fini tributari, art. 5 D.M. 17 giugno 2014.

Decreto Legislativo 5 agosto 2015, n. 127, Trasmissione telematica delle operazioni IVA e di controllo delle cessioni di beni effettuate attraverso distributori automatici, in attuazione dell'art. 9, comma 1, lettere d) e g),

della legge 11 marzo 2014, n. 23.

Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014, Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli artt. 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

Circolare dell'Agenzia delle Entrate 24 giugno 2014, n. 18/E, *IVA. Ulteriori istruzioni in tema di fatturazione.*

Decreto del Ministro dell'Economia e delle Finanze 17 giugno 2014, Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - art. 21, comma 5, del decreto legislativo n. 82/2005.

Circolare dell'Agenzia per l'Italia Digitale - 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'art. 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.

Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013, Regole tecniche in materia di Sistema di conservazione ai sensi degli artt. 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

Decreto del Ministro dell'Economia e delle Finanze 3 aprile 2013, n. 55, Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'art. 1, commi da 209 a 213, della legge 24 dicembre 2007, n. 244.

Decreto del Presidente del Consiglio dei Ministri 21 marzo 2013, Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni.

Decreto Legge 22 giugno 2012, n. 83, convertito con Legge 7 agosto 2012, n. 134, *Misure urgenti per la crescita del Paese.*

Decreto Legislativo 7 marzo 2005, n. 82, *Codice dell'amministrazione digitale.*

Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68 Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'art. 27 della legge 16 gennaio 2003, n. 3

Decreto Legislativo 22 gennaio 2004, n. 42, Codice dei beni culturali e del paesaggio, ai sensi dell'art. 10 della legge 6 luglio 2002, n. 137.

Decreto Legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali.

Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.

Decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000, Regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica 20 ottobre 1998, n. 428.

Legge 7 agosto 1990, n. 241, Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.

9.1.1 Istruzioni, linee guida e documentazione informativa

Linee guida dell'Agenzia per l'Italia Digitale – AgID settembre 2020, Linee Guida sulla formazione, gestione e conservazione dei documenti informatici

Istruzioni dell'Agenzia per l'Italia Digitale – AgID marzo 2015, Produzione e conservazione del registro giornaliero di protocollo.

Linee guida dell'Agenzia per l'Italia Digitale – AgID dicembre 2015, *Linee guida sulla conservazione dei documenti informatici.*

Linee guida dell'Agenzia per l'Italia Digitale – AgID 26 aprile 2016, Linee Guida per la sicurezza ICT delle Pubbliche Amministrazioni – Misure minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del Presidente del Consiglio dei Ministri 1° agosto 2015).

European Commission, working party on the protection of individuals with regard to the processing of personal data set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, *Guidelines on Data Protection Officers ('DPOs') Adopted on 13 December 2016.*

European Commission, working party on the protection of individuals with regard to the processing of personal data set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, *Guidelines on the right to data portability Adopted on 13 December 2016.*

Linee guida del Garante per la protezione dei dati personali 2 marzo 2011, n. 088 del registro dei provvedimenti, Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web.

Linee guida del Garante per la protezione dei dati personali, 4 aprile 2013, n. 161 del registro dei provvedimenti, Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach).

Linee guida del Garante per la protezione dei dati personali, 15 maggio 2014 n. 243 del registro dei provvedimenti, Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati.

Scheda informativa del Garante per la protezione dei dati personali, 17 marzo 2016, Scheda informativa sulla figura del Responsabile della protezione dei dati personali (Data Protection Officer).

Guida informativa del Garante per la protezione dei dati personali, giugno 2016, Prima guida informativa al Regolamento europeo 2016/679 in materia di protezione dei dati personali.

9.1.2 Standard di riferimento

Per la conservazione digitale l'importanza degli standard nasce dal problema dell'interoperabilità e questo per diverse ragioni:

- l'utilizzo di una risorsa digitale presuppone la capacità di decodificarne e restituirne correttamente il contenuto ed è necessario poter interpretare correttamente i metadati associati alla risorsa;
- i soggetti produttori e i soggetti beneficiari agiscono a distanza di spazio e di tempo, e dunque non è possibile assumere che possano fare affidamento sulle stesse risorse tecnologiche (sistemi di elaborazione ed applicazioni software);
- durante il processo di conservazione, la risorsa digitale passa potenzialmente attraverso diversi cambi di custodia, viene cioè scambiata tra diversi Sistemi di conservazione e affinché tali Sistemi possano colloquiare correttamente occorre che la loro struttura ed il loro modo di operare osservi regole precise, note e condivise.

Se poi ci si pone il problema di verificare e certificare la qualità del processo di conservazione, ciò può concretamente essere fatto solo con riferimento a schemi architetturali e organizzativi noti e concordati: gli standard. Essi descrivono in dettaglio, a seconda dei casi, il formato delle risorse, la struttura ed il significato dei metadati associati alle risorse, l'organizzazione dei sistemi di archiviazione e conservazione e le modalità con cui si scambiano pacchetti informativi.

Gli standard vengono emessi da organismi nazionali od internazionali di riconosciuta autorevolezza, in primis l'ISO (International Standard Organization), al termine di un iter di approvazione spesso lungo e complesso, ma comunque rigoroso. Ed è appunto ciò che conferisce loro il ruolo di insostituibile punto di riferimento.

Raggruppamento dei principali standard di interesse nel settore della conservazione digitale:

9.1.2.1 Metadati

- LoC-DLF METS:2001 – Metadata Encoding and Transmission Standard.
- NLZ Preservation metadata:2003 – National Library of New Zealand Metadata - Standards Framework – Metadata Implementation Schema.
- OCLC-RLG PREMIS:2005/2008 – PREMIS Data Dictionary for Preservation *Metadata*.
- ISO 23081-1/3:2011 – Information and documentation – Metadata for records.

9.1.2.2 Archivi digitali

- ISO 15489-1/2: 2001 – Information and documentation – Records management.
- DoD 5015.02-STD:2007 – Design Criteria Standard for Electronic Records Management Software Applications.
- EU-DML Forum MoReq2:2008 – Model Requirements for the Management of Electronic
- Records.
- ICA guidelines: 2008 – Principles and Functional Requirements for Records in Electronic Office Environments.
- ISO 16175-1/3:2010 – Information and documentation – Principles and functional requirements for records in electronic office environments.
- EU-DML Forum MoReq2010: 2011 – Modular Requirements for Records Systems.

9.1.2.3 Depositi di conservazione

- ISO/TR 18492: 2005 – Long-term preservation of electronic document-based information.
- ISO 14721:2005/2012 – Space data and information transfer systems – Open archival information system (OAIS) Reference model.
- ISO 16363:2012 - Audit and certification of trustworthy digital repositories.
- ISO 16919:2014 - Space data and information transfer systems - Requirements

for bodies providing audit and certification of candidate trustworthy digital repositories.

9.2 Glossario dei termini e degli acronimi

Glossario dei termini e degli acronimi

Allegato 1 al documento "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*".

Indice

Sommario

Indice 2
CAPITOLO 1 4
Premessa 4
1.1 Scopo e campo di applicazione del documento 4
1.2 Glossario dei termini 4
1.3 Glossario degli Acronimi 14

Questo allegato è parte integrante al testo delle linee guida sulla *Formazione, gestione e conservazione dei documenti informatici*.

CAPITOLO 1

Premessa

1.3 Scopo e campo di applicazione del documento

Lo scopo del presente allegato è il seguente:

- esplicitare il significato dei termini maggiormente utilizzati nel documento *linea guida sulla formazione, gestione e conservazione dei documenti informatici*, che necessitano una spiegazione.

1.4 Glossario dei termini

TERMINE	DEFINIZIONE
Accesso	Operazione che consente di prendere visione dei documenti informatici.
Affidabilità	Caratteristica che, con riferimento a un sistema di gestione documentale o conservazione, esprime il livello di fiducia che l'utente ripone nel sistema stesso, mentre con riferimento al documento informatico esprime la credibilità e l'accuratezza della rappresentazione di atti e fatti in esso contenuta.
Aggregazione documentale informatica	Insieme di documenti informatici o insieme di fascicoli informatici riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente.
Archivio	Complesso dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività.
Archivio informatico	Archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche.

TERMINE	DEFINIZIONE
Area Organizzativa Omogenea	Un insieme di funzioni e di uffici individuati dall'ente al fine di gestire i documenti in modo unitario e coordinato, secondo quanto disposto dall'art. 50 comma 4 del D.P.R. 28 dicembre 2000, n. 445. Essa rappresenta il canale ufficiale per l'invio di istanze e l'avvio di procedimenti amministrativi.
Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.
Autenticità	Caratteristica in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto un oggetto è autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze.
Certificazione	Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi.
Classificazione	Attività di organizzazione di tutti i documenti secondo uno schema costituito da un insieme di voci articolate in modo gerarchico e che individuano, in astratto, le funzioni, competenze, attività e/o materie del soggetto produttore.
Cloud della PA	Ambiente virtuale che consente alle Pubbliche Amministrazioni di erogare servizi digitali ai cittadini e alle imprese nel rispetto di requisiti minimi di sicurezza e affidabilità.
Codec	Algoritmo di codifica e decodifica che consente di generare flussi binari, eventualmente imbustarli in un file o in un *wrapper* (codifica), così come di estrarli da esso (decodifica).
Conservatore	Soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici.
Conservazione	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo

TERMINE	DEFINIZIONE
	adottato, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti
Convenzioni di denominazione del file	Insieme di regole sintattiche che definisce il nome dei file all'interno di un filesystem o pacchetto.
Coordinatore della Gestione Documentale	Soggetto responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 nei casi di amministrazioni che abbiano istituito più AOO.
Destinatario	Soggetto o sistema al quale il documento informatico è indirizzato.
Digest	Vedi Impronta crittografica.
Documento amministrativo informatico	Ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa
Documento elettronico	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva
Documento informatico	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Duplicato informatico	Vedi art. 1, comma 1, lett) i quinquies del CAD.
eSeal	Vedi sigillo elettronico.
Esibizione	operazione che consente di visualizzare un documento conservato
eSignature	Vedi firma elettronica.
Estratto di documento informatico	Parte del documento tratto dal documento originale
Estratto per riassunto di documento informatico	Documento nel quale si attestano in maniera sintetica fatti, stati o qualità desunti da documenti informatici.

TERMINE	DEFINIZIONE
Estrazione statica dei dati	Estrazione di informazioni utili da grandi quantità di dati (es. database, datawarehouse ecc...), attraverso metodi automatici o semi-automatici
Evidenza informatica	Sequenza finita di *bit* che può essere elaborata da una procedura informatica.
Fascicolo informatico	Aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento.
File	Insieme di informazioni, dati o comandi logicamente correlati, raccolti sotto un unico nome e registrati, per mezzo di un programma di elaborazione o di scrittura, nella memoria di un computer.
File container	Vedi Formato contenitore.
File wrapper	Vedi Formato contenitore.
File-manifesto	File che contiene metadati riferiti ad un file o ad un pacchetto di file.
Filesystem	Sistema di gestione dei file, strutturato mediante una o più gerarchie ad albero, che determina le modalità di assegnazione dei nomi, memorizzazione e organizzazione all'interno di uno storage.
Firma elettronica	Vedi articolo 3 del Regolamento eIDAS.
Firma elettronica avanzata	Vedi articoli 3 e 26 del Regolamento eIDAS.
Firma elettronica qualificata	Vedi articolo 3 del Regolamento eIDAS.
Flusso (binario)	Sequenza di bit prodotta in un intervallo temporale finito e continuativo che ha un'origine precisa ma di cui potrebbe non essere predeterminato il suo istante di interruzione.
Formato contenitore	Formato di file progettato per consentire l'inclusione ("imbustamento" o *wrapping*), in uno stesso file, di una o più

TERMINE	DEFINIZIONE
	evidenze informatiche soggette a differenti tipi di codifica e al quale possono essere associati specifici metadati.
Formato del documento informatico	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
Formato "deprecato"	Formato in passato considerato ufficiale il cui uso è attualmente sconsigliato a favore di una versione più recente.
Funzioni aggiuntive del protocollo informatico	Nel sistema di protocollo informatico, componenti supplementari rispetto a quelle minime, necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni.
Funzioni minime del protocollo informatico	Componenti del sistema di protocollo informatico che rispettano i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445.
Funzione di *hash* crittografica	Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o *digest* (vedi) in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
Gestione Documentale	Processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta, uso, selezione e conservazione dei documenti.
hash	Termine inglese usato, impropriamente, come sinonimo d'uso di "impronta crittografica" o "*digest*" (vedi).
Identificativo univoco	Sequenza di numeri o caratteri alfanumerici associata in modo univoco e persistente ad un'entità all'interno di uno specifico ambito di applicazione.
Impronta crittografica	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di *hash* crittografica a un'evidenza informatica.

TERMINE	DEFINIZIONE
Integrità	Caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità.
Interoperabilità	Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi.
Leggibilità	Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica.
Manuale di conservazione	Documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture.
Manuale di gestione	Documento informatico che descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.
Metadati	Dati associati a un o documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017.
Naming convention	Vedi Convenzioni di denominazione
Oggetto di conservazione	Oggetto digitale versato in un sistema di conservazione.
Oggetto digitale	Oggetto informativo digitale, che può assumere varie forme tra le quali quelle di documento informatico, fascicolo informatico, aggregazione documentale informatica o archivio informatico.

TERMINE	DEFINIZIONE
Pacchetto di archiviazione	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel manuale di conservazione.
Pacchetto di distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione.
Pacchetto di file (*file package*)	Insieme finito di più file (possibilmente organizzati in una struttura di sottoalbero all'interno di un filesystem) che costituiscono, collettivamente oltre che individualmente, un contenuto informativo unitario e auto-consistente.
Pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione.
Pacchetto informativo	Contenitore logico che racchiude uno o più oggetti di conservazione con i relativi metadati, oppure anche i soli metadati riferiti agli oggetti di conservazione.
Path	Percorso (*vedi*).
Pathname	Concatenazione ordinata del percorso di un file e del suo nome.
Percorso	Informazioni relative alla localizzazione virtuale del file all'interno del filesystem espressa come concatenazione ordinata del nome dei nodi del percorso.
Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi.
Piano della sicurezza del sistema di gestione Informatica dei documenti	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi.
Piano di classificazione (Titolario)	Struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata.

TERMINE	DEFINIZIONE
Piano di conservazione	Documento, allegato al manuale di gestione e integrato con il sistema di classificazione, in cui sono definiti i criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445.
Piano di organizzazione delle aggregazioni documentali	Strumento integrato con il sistema di classificazione a partire dai livelli gerarchici inferiori di quest'ultimo e finalizzato a individuare le tipologie di aggregazioni documentali (tipologie di serie e tipologie di fascicoli) che devono essere prodotte e gestite in rapporto ai procedimenti e attività in cui si declinano le funzioni svolte dall'ente
Piano generale della sicurezza	Documento che pianifica le attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza.
Presa in carico	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione e, in caso di affidamento del servizio all'esterno, dagli accordi stipulati tra il titolare dell'oggetto di conservazione e il responsabile del servizio di conservazione.
Processo	Insieme di attività correlate o interagenti che trasformano elementi in ingresso in elementi in uscita.
Produttore dei PdV	Persona fisica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con il responsabile della gestione documentale.
qSeal	Sigillo elettronico qualificato, come da art. 35 del Regolamento eIDAS.
qSignature	Firma elettronica qualificata, come da art. 25 del Regolamento eIDAS.
Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.

TERMINE	DEFINIZIONE
Registro di protocollo	Registro informatico ove sono memorizzate le informazioni prescritte dalla normativa per tutti i documenti ricevuti e spediti da un ente e per tutti i documenti informatici dell'ente stesso.
Registro particolare	Registro informatico individuato da una pubblica amministrazione per la memorizzazione delle informazioni relative a documenti soggetti a registrazione particolare.
Regolamento eIDAS	electronic IDentification Authentication and Signature, Regolamento (UE) № 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
Repertorio	Registro su cui vengono annotati con un numero progressivo i fascicoli secondo l'ordine cronologico in cui si costituiscono all'interno delle suddivisioni del piano di classificazione.
Responsabile dei sistemi informativi per la conservazione	Soggetto che coordina i sistemi informativi all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID.
Responsabile del servizio di conservazione	soggetto che coordina il processo di conservazione all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Responsabile della conservazione	Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.
Responsabile della funzione archivistica di conservazione	soggetto che coordina il processo di conservazione dal punto di vista archivistico all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Responsabile della gestione documentale	Soggetto responsabile della gestione del sistema documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445.

TERMINE	DEFINIZIONE
Responsabile della protezione dei dati	Persona con conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, in grado di assolvere i compiti di cui all'articolo 39 del Regolamento (UE) 2016/679.
Responsabile della sicurezza dei sistemi di conservazione	soggetto che assicura il rispetto dei requisiti di sicurezza all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	soggetto che assicura lo sviluppo e la manutenzione del sistema all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Riferimento temporale	Insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC).
Riversamento	Procedura mediante la quale uno o più documenti informatici sono convertiti da un formato di file (ovvero di busta, ovvero di pacchetto di file) ad un altro, lasciandone invariato il contenuto per quanto possibilmente permesso dalle caratteristiche tecniche del formato (ovvero dei formati) dei file e delle codifiche di destinazione.
Scarto	Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico-culturale.
Serie	Raggruppamento di documenti con caratteristiche omogenee (vedi anche aggregazione documentale informatica).
***Sidecar* (file)**	File-manifesto (*vedi*).
Sigillo elettronico	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi.
Sistema di conservazione	Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, comma 1, del CAD.
Sistema di gestione informatica dei documenti	Insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle organizzazioni per la gestione dei documenti. Nell'ambito

TERMINE	DEFINIZIONE
	della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445
Timeline	Linea temporale virtuale su cui sono disposti degli eventi relativi ad un sistema informativo o a un documento informatico. Costituiscono esempi molto diversi di *timeline* un file di log di sistema, un flusso multimediale contenente essenze audio\video sincronizzate.
Titolare dell'oggetto di conservazione	Soggetto produttore degli oggetti di conservazione.
Trasferimento	Passaggio di custodia dei documenti da una persona o un ente ad un'altra persona o un altro ente.
TUDA	Testo Unico della Documentazione Amministrativa, Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni e integrazioni.
Ufficio	Riferito ad un'area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico.
Utente abilitato	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.
Versamento	Passaggio di custodia, di proprietà e/o di responsabilità dei documenti. Nel caso di un organo giudiziario e amministrativo dello Stato operazione con la quale il responsabile della conservazione trasferisce agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali.

1.5 Glossario degli Acronimi

ACRONIMO	DEFINIZIONE
AGID	Agenzia per l'Italia digitale

ACRONIMO	DEFINIZIONE
AOO	Area Organizzativa Omogenea
CAD	Codice dell'Amministrazione Digitale - Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni.
eIDAS	Regolamento (UE) № 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
FEA	Vedi firma elettronica avanzata.
FEQ	Vedi firma elettronica qualifica.
GDPR	Regolamento (UE) № 679/2016 del Parlamento Europeo e del Consiglio, del 27 aprile 2016 ("*General Data Protection Regulation*"), 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.
PdA (AiP)	Pacchetto di Archiviazione.
PdD (DiP)	Pacchetto di Distribuzione.
PdV (SiP)	Pacchetto di Versamento.
UOR	Unità Organizzativa Responsabile

9.3 Elenco delle AOO e UOR

L'Agenzia Spaziale Italiana costituisce un'unica Area Organizzativa Omogenea (AOO).

Elenco UOR dell'AOO Agenzia Spaziale Italiana

- CENTRO DI GEODESIA SPAZIALE -CGS DI MATERA
- DIREZIONE COORDINAMENTO AMMINISTRATIVO
- DIREZIONE COORDINAMENTO TECNICO SCIENTIFICO
- SEGRETERIA DI PRESIDENZA
- SERVIZIO DI PREVENZIONE E PROTEZIONE
- STRUTTURA DI MISURAZIONE DELLE PERFORMANCE
- UFFICIO PROCEDIMENTI DISCIPLINARI
- UNITA' AFFARI LEGALI
- UNITA' ATTIVITA' DI FORMAZIONE
- UNITA' AMMINISTRAZIONE CONTABILITA' E FINANZA
- UNITA' CONSERVAZIONE E STATISTICA
- UNITA' CONTRATTI
- UNITA' DI RICERCA SCIENTIFICA
- UNITA' ESPLORAZIONE E OSSERVAZIONE DELL'UNIVERSO
- UNITA' GESTIONE E VALORIZZAZIONE RISORSE UMANE
- UNITA' INFRASTRUTTURE E SISTEMI INFORMATIVI
- UNITA' INNOVAZIONE E TRASFERIMENTO DELLE TECNOLOGIE
- UNITA' LANCIATORI TRASPORTO SPAZIALE E PROGRAMMA PRORA
- UNITA' MICROGRAVITA' E VOLO UMANO
- UNITA' OSSERVAZIONE DELLA TERRA
- UNITA' QUALITA' E PROCESSI
- UNITA' RELAZIONI ESTERNE E URP
- UNITA' RELAZIONI INTERNAZIONALI
- UNITA' SICUREZZA
- UNITA' STRATEGIE E POLITICA INDUSTRIALE
- UNITA' SUPPORTO ORGANI E PARTECIPATE
- UNITA' SUPPORTO TECNICO-GESTIONALE ALLA DIREZIONE GENERALE
- UNITA' TECNICA DI PRESIDENZA
- UNITA' TECNOLOGIE E INGEGNERIA
- UNITA' TELECOMUNICAZIONI E NAVIGAZIONE

9.4 Elenco delle tipologie documentarie soggette a conservazione, soluzione di conservazione scelta e periodicità di invio in conservazione

Tipologia documentale	Descrizione	Tempo di conservazione	Periodicità invio in conservazione
Registri	Registro giornaliero protocollo; registri annuali degli atti	Piano di conservazione	Annuale
Atti	Delibere CdA, decreti Presidente, decreti DG, Decreti DOR, Decreti COA, Determine Responsabile Delegato, Delibere Commissario Straordinario, Decreti Amministratore Straordinario, Buste paga Ordini di servizio, disposizioni organizzative; Documenti interni, PEC, Fatture	Piano di conservazione	Annuale
Mandati	L'intera serie	Piano di conservazione	Annuale
Protocolli	L'intera serie	Piano di conservazione	Annuale

9.5 Ruoli e Responsabilità

9.5.1 Figure interne (facenti capo al produttore)

9.5.1.1 RC – Responsabile della conservazione

Al momento della redazione del presente atto il ruolo è ricoperto dalla dott.ssa Daniela Scialdoni, giusta decreto Direttoriale n. 477 del 2 agosto 2019. La delega può essere conferita esclusivamente a personale assegnato all'unità Conservazione e Statistica.

9.5.1.2 RGD – Responsabile della gestione documentale

Al momento della redazione del presente atto il ruolo è ricoperto dalla dott.ssa Daniela Scialdoni, giusta decreto Direttoriale n. 477 del 2 agosto 2019. La delega può essere conferita esclusivamente a personale assegnato all'unità Conservazione e Statistica.

9.5.1.3 DPO - Responsabile per la Protezione dei Dati Personali (Data protection officer)

Al momento della redazione del presente atto la figura del DPO è ricoperta dall'Avv. Franco Angelo Ferraro (esterno all'ASI)

9.5.1.4 RSI – Responsabile sistemi informativi e Responsabile della sicurezza

Il responsabile dei servizi informativi è il Responsabile dell'Unità Organizzativa Infrastrutture e Sistemi Informativi.
Al momento della redazione del presente atto il ruolo è ricoperto dall'ing Bruno Tribioli.
Il responsabile della sicurezza è il Responsabile dell'Unità Sicurezza; Al momento della redazione del presente atto il ruolo è ricoperto dall'Ing. Franco Marucci

9.5.1.5 RTD - Responsabile per la transizione digitale Ex art. 17 comma 1 e 1 sexies del CAD.

Al momento della redazione del presente atto la figura del *Responsabile per la transizione digitale è da nominare.*

9.5.1.6 TT – Titolare trattamento dati personali -Ex art. 4 comma 1, lettera F) Codice Privacy.

Al momento della redazione del presente il titolare è il Presidente dell'ASI, ing. Giorgio Saccoccia.

9.5.1.7 RTDP – Responsabile trattamento dati personali

Al momento della redazione del presente atto l'organigramma privacy è in aggiornamento.

9.5.2 Figure esterne (facenti capo al servizio di conservazione in outsourcing)

Si rimanda a:

- Manuale di conservazione di POSTEL, capitolo 4.1, Allegato n. 6 [Cap.9.6] al presente manuale.
- Manuale di conservazione di UNIMATICA, capitolo D.1, Allegato n. 7 [Cap.9.7] al presente manuale.
- Manuale di conservazione di Enerj, capitolo 5.2, Allegato n. 8 [Cap.9.8] al presente manuale.

9.6 Manuale del Conservatore Postel

Manuale di Conservazione di Postel SpA

Emissione del documento

Azione	Data	Nominativo	Funzione
Redazione	07/09/2017	Luigi Fatica	Tecnologie dell'Informazione
Verifica	06/09/2017	Valerio Cristofaro	Supporto clienti e qualità
Approvazione	06/09/2017	Marco Bonanni	Tecnologie dell'Informazione

Registro delle versioni

Versione	Data	Paragrafi Modificati e Motivazione
1.1	16/10/2014	Integrazione manuale per l'accreditamento
1.2	09/07/2015	Aggiornamento Paragrafo 'Struttura organizzativa' e 'Profili professionali'
1.3	21/09/2015	Aggiornamento standard di riferimento e terminologia
1.4	25/01/2016	Aggiornamento template secondo l'indice AgID
1.5	09/03/2016	Aggiunta alle figure presenti "testo alternativo"
1.6	06/09/2017	Aggiornamento a livello organizzativo

INDICE

1. SCOPO ED AMBITO DI APPLICAZIONE ---- 4
1.1. Trasparenza ---- 5
2. TERMINOLOGIA ---- 6
2.1. Glossario ---- 6
2.2. Acronimi ---- 8
3. NORMATIVA E STANDARD DI RIFERIMENTO ---- 9
3.1. Normativa di riferimento ---- 9
3.2. Procedure interne di riferimento ---- 10
3.3. Standard di riferimento ---- 10
4. RUOLI E RESPONSABILITA' ---- 11
4.1. Storia dei responsabili del servizio di conservazione ---- 14
5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE ---- 14
5.1. Organigramma ---- 14
5.2. Strutture organizzative ---- 15
6. OGGETTI SOTTOPOSTI A CONSERVAZIONE ---- 17
6.1. Oggetti conservati ---- 17
6.2. Pacchetto di versamento ---- 17
6.3. Pacchetto di archiviazione ---- 19
6.4. Pacchetto di distribuzione ---- 21
6.5. Tipologie documentali ---- 21
6.5.1. Fattura elettronica ---- 21
6.5.2. Libri contabili ---- 23
6.5.3. Registri assicurativi ---- 23
6.5.4. Libro Unico del Lavoro ---- 24
6.5.5. Assegni bancari ---- 25
7. IL PROCESSO DI CONSERVAZIONE ---- 26
7.1. Modalità di acquisizione dei pacchetti di versamento ---- 27
7.2. Verifiche sui pacchetti di versamento ---- 27
7.3. Accettazione dei pacchetti di versamento e generazione del relativo rapporto di versamento ---- 28
7.4. Rifiuto dei pacchetti di versamento e generazione del relativo rapporto di versamento --- 28
7.5. Preparazione e gestione del pacchetto di archiviazione ---- 28
7.6. Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione a norma ---- 29
7.7. Produzione di duplicati e descrizione dell'eventuale intervento del pubblico ufficiale ----- 30
7.8. Scarto dei pacchetti di archiviazione ---- 30
7.9. Predisposizione di misure e garanzia dell'interoperabilità e trasferibilità ad altri conservatori ---- 31
8. IL SISTEMA DI CONSERVAZIONE ---- 31
8.1. Componenti logiche ---- 31

8.1.1. Front-end ---- 31
8.1.2. Back-end ---- 31
8.2. Componenti tecnologiche ---- 32
8.3. Componenti fisiche ---- 32
8.4. Procedure di gestione ed evoluzione ---- 33
9. MONITORAGGIO E CONTROLLI ---- 35
9.1. Procedure di monitoraggio ---- 35
9.2. Verifica dell'integrità e leggibilità degli archivi ---- 35
9.3. Soluzioni adottate in caso di anomalie ---- 36

1. SCOPO ED AMBITO DI APPLICAZIONE

Il presente documento è il Manuale di Conservazione di Postel SpA (società del Gruppo Poste Italiane), ai sensi del Codice dell'Amministrazione Digitale e del DPCM 3 dicembre 2013.

Descrive le strutture organizzative coinvolte nell'erogazione del servizio di conservazione, il processo attraverso il quale è possibile conservare a norma i documenti informatici, le architetture e le infrastrutture utilizzate, nonché le misure di sicurezza adottate ed i controlli effettuati al fine di garantire un servizio efficace ed efficiente nei confronti dei propri clienti.

Qualora siano previste personalizzazioni del servizio di conservazione, il presente Manuale sarà corredato dall'Allegato "Specificità del contratto", nel quale saranno riportate le specificità in merito ai contratti stipulati con i propri clienti (a titolo di esempio, personalizzazioni dei metadati/ formati di conservazione, modalità di trasmissione dei documenti, esibizione, ecc.).

Ai sensi di quanto previsto dal Codice dell'Amministrazione Digitale e DPCM 3 dicembre 2013, il responsabile della conservazione, appartenente alla struttura organizzativa dell'ente produttore, può decidere sotto la propria responsabilità ed autonomia di affidare il processo di conservazione ad uno o più soggetti, pubblici o privati, anche accreditati presso l'AgID. Il soggetto al quale è affidato il processo di conservazione assume il ruolo di responsabile del servizio di conservazione e del trattamento dei dati personali (il ruolo di Titolare del trattamento dei dati personali rimane in capo alla Società di appartenenza dell'ente produttore).

Conformemente a quanto appena riportato, Postel, conservatore accreditato presso l'Agenzia per l'Italia Digitale, assume il ruolo di responsabile del servizio di conservazione e responsabile del trattamento dei dati personali. Il servizio è rivolto a tutti quei soggetti, pubblici e privati, che intendono esternalizzare il processo di conservazione dei documenti informatici.

Ovviamente, il processo di conservazione è proprio di ciascuna organizzazione: ad esempio, soprattutto per le pubbliche amministrazioni, è necessario ragionare nell'ottica di una conservazione nel lungo periodo (nella maggior parte dei casi, i documenti amministrativi informatici devono essere conservati per oltre 20 anni a chiusura del relativo procedimento amministrativo); inoltre, devono richiedere il permesso alla Soprintendenza archivistica (ai sensi di quanto esplicitamente dichiarato dal Ministero per i beni e le attività culturali e del turismo) qualora decidessero di esternalizzare il processo di conservazione dei propri archivi.

In relazione a quanto appena riportato ed in linea con i requisiti di qualità e sicurezza del sistema di conservazione definiti da AgID, Postel offre un servizio con livelli di qualità e sicurezza elevati, garantendo l'integrità e leggibilità del proprio archivio conservato, non solo nel breve ma anche nel lungo periodo. Particolare attenzione si ripone a tutti quei cambiamenti normativi e tecnologici che potrebbero comportare modifiche al sistema di conservazione: è fondamentale per Postel offrire un servizio conforme alle normative vigenti e basato su tecnologie atte a garantire un elevato livello di sicurezza ed affidabilità dei dati/ documenti trattati.

Si riportano, di seguito, i documenti contrattuali con i quali è regolato il servizio di conservazione di Postel:

- Proposta economica. All'interno è riportato anche l'atto di affidamento, attraverso il quale è formalizzato l'affidamento a Postel del processo di conservazione e stabilisce espressamente quali attività di fatto vengono assunte da Postel e quali rimangano a carico dell'affidatario;
- Descrizione del servizio;
- Allegati tecnici;
- Manuale della conservazione, depositato sul sito dell'AgID;
- Condizioni Generali di Contratto;
- Specificità del contratto. Allegato al manuale della conservazione, nel caso in cui il cliente richieda personalizzazioni del servizio di conservazione offerto da Postel e/ o la conservazione a norma di ulteriori tipologie documentali non riportare nel presente documento.

Torna al sommario

1.1. Trasparenza

Fondamentale per tutti gli enti, pubblici e privati, che erogano servizi nei confronti di altre società e cittadini, è il principio di trasparenza (dal latino *trans parere* ovvero far apparire, lasciar vedere, lasciar conoscere).

Postel, in relazione a suddetto principio e, in relazione al servizio di conservazione di documenti informatici offerto, garantisce la trasparenza mediante:

- Certificazione dei propri processi. Sul sito di Postel, sono rese pubbliche tutte le certificazioni conseguite, ovvero:
  - ISO/ IEC 27001:2013 "Sistema di gestione della sicurezza delle informazioni";
  - ISO 20000-1:2011 "Sistema di gestione della tecnologia dell'informazione";
  - ISO 22301:2012 "Sistema di gestione della business continuity";
  - ISO 9001:2008 "Sistema di gestione per la qualità dell'organizzazione".
- Audit periodici eseguiti sia da personale competente interno alla Società che da enti di certificazione accreditati da ACCREDIA;
- Assessment e riesami periodici, anche e soprattutto a seguito di cambiamenti normativi e/ o tecnologici;
- Pubblicazione del presente documento sul sito istituzionale dell'Agenzia per l'Italia Digitale.

  È possibile inoltre richiedere ulteriori documenti ed informazioni relativi al servizio di conservazione offerto, contattando le specifiche funzioni indicate nel sito di Postel.

Torna al sommario

2. TERMINOLOGIA

2.1. Glossario

Termine	Definizione
Aggregazione documentale informatica	Aggregazione di documenti informatici o fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura/ forma dei documenti o in relazione all'oggetto/ materia o in relazione alle funzioni dell'ente.
Certificatore/ Certification Authority	Soggetto che presta servizio di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime.
Conservazione	Processo che permette di conservare i documenti in modalità informatica a norma di legge e che risponde a quanto stabilito nel DPCM 3 dicembre 2013.
Content Addressed Storage	Sistema di memorizzazione delle informazioni basato sul contenuto delle stesse e non sull'indirizzo della posizione del sistema in cui esse sono memorizzate.
Documento analogico	Documento formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta (documenti cartacei), come le immagini su film (pellicole mediche, microfiche, microfilm), come le magnetizzazioni su nastro (cassette e nastri magnetici audio e video).
Documento informatico	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
Documento informatico statico ed immodificabile	Documento informatico il quale contenuto risulti non alterabile durante le fasi di accesso e conservazione, nonché immutabile nel tempo; a tal fine, non deve contenere macroistruzioni o codice eseguibile, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati.
Documento originale unico	Documento analogico per il quale permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione digitale, la sua conformità all'originale deve essere autenticata da un notaio/ pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico.
Documento originale non unico	Documento per il quale è possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi.
Fascicolo informatico	Aggregazione strutturata ed univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento.
Firma digitale	Particolare tipologia di firma elettronica qualificata, basata su un sistema di chiavi asimmetriche crittografiche, una privata ed una pubblica correlate tra loro, che permettono al Titolare mediante la chiave privata e al destinatario tramite la chiave pubblica, di rendere manifesta e verificare la provenienza ed integrità del documento sottoscritto digitalmente.
Funzione di hash	Funzione matematica che genera, a partire da una evidenza informatica, un'impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti. Postel utilizza come algoritmo di riferimento lo SHA-256.

Hardware Security Module	Insieme di hardware e software che realizza dispositivi sicuri per la generazione delle firme in grado di gestire in modo sicuro una o più coppie di chiavi crittografiche.
Impronta	Sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'utilizzo di un'opportuna funzione di hash.
Marca temporale	Riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo (opponibile ai terzi).
Metadati	Insieme di dati associati ad un documento informatico (fascicolo o aggregazione documentale informatica), per identificarlo e descriverne il contesto, contenuto e struttura, nonché per permetterne la gestione nel tempo all'interno del sistema di conservazione.
Network Time Protocol	Protocollo utilizzato per sincronizzare gli orologi dei computer all'interno di una rete.
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.
Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.
Responsabile della conservazione	Soggetto a cui sono attribuite le funzioni, adempimenti, attività e responsabilità relative al processo di conservazione.
Responsabile del servizio di conservazione	Soggetto pubblico o privato al quale il responsabile della conservazione affida l'intero (o parte) del processo di conservazione.
Riferimento temporale	Evidenza informatica contenente la data/ ora che viene associata ad uno o più documenti informatici.
Time Stamping Authority	Terza parte fidata che emette i certificati di marca temporale nel rispetto delle norme vigenti.
Time Stamping Service	Servizio di marca temporale che emette marche temporali nel rispetto delle norme vigenti.
Universal Time Coordinated	Fuso orario di riferimento da cui tutti gli altri fusi orari del mondo sono calcolati.
Utente	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/ o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.
Pacchetto informativo	Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare.
Pacchetto di versamento	Pacchetto informativo inviato dal soggetto produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione.
Pacchetto di archiviazione	Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del DPCM 3 Dicembre 2013 e secondo le modalità riportate nel manuale di conservazione.
Pacchetto di distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta.

Torna al sommario

2.2. Acronimi

Acronimo	Descrizione
AGID	Agenzia per l'Italia Digitale
CA	Certification Authority
CAD	Codice dell'Amministrazione Digitale
CAS	Content Addressed Storage
D.LGS	Decreto legislativo
DM	Decreto Ministeriale
DPCM	Decreto del Presidente del Consiglio dei Ministri
DPR	Decreto del Presidente della Repubblica
HSM	Hardware Security Module
MEF	Ministero dell'Economia e delle Finanza
NTP	Network Time Protocol
PA	Pubblica Amministrazione
PdV	Pacchetto di versamento
PdA	Pacchetto di archiviazione
PdD	Pacchetto di distribuzione
PU	Pubblico Ufficiale
RdV	Rapporto di versamento
SdC	Sistema di conservazione
SCQ	Supporto Clienti e Qualità
TI	Tecnologie dell'Informazione
TSA	Time Stamping Authority
TSS	Time Stamping Service
TU	Testo Unico
UTC	Universal Coordinated Time

Torna al sommario

3. NORMATIVA E STANDARD DI RIFERIMENTO

3.1. Normativa di riferimento

- *Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445* - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (La norma è stata per la maggior parte sostituita dal Codice dell'amministrazione digitale in vigore dal 1° gennaio 2006).
- *Decreto Legislativo del 7 marzo 2005, n. 82 e s.m.i.* - Codice dell'amministrazione digitale.
- *Decreto Legislativo 30 giugno 2003, n. 196* - Codice in materia di protezione dei dati personali.
- *Decreto Legislativo 20 febbraio 2004, n. 52* - Attuazione della direttiva 2001/115/CE che semplifica ed armonizza le modalità di fatturazione in materia di I.V.A.
- *Decreto Legislativo del 22 gennaio 2004, n. 42 e s.m.i. - Codice dei Beni Culturali e del Paesaggio.*
- *Decreto ministeriale 9 luglio 2008* - Modalità di tenuta e conservazione del libro unico del lavoro e disciplina del relativo regime transitorio.
- *Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014* - Regole tecniche per la formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici.
- *Decreto del Presidente del Consiglio dei Ministri 3 Dicembre 2013* - Regole tecniche in materia di sistema di conservazione.
- *Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013* - Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali.
- *Decreto del Ministero dell'Economia e delle Finanze 17 giugno 2014* - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di supporto.
- *Decreto del Presidente del Consiglio dei Ministri 21 Marzo 2013* – Documenti originali unici.
- *Decreto del Ministero dell'Economia e delle Finanze 3 ottobre 2014, n. 205* - Regolamento recante presentazione al pagamento in forma elettronica degli assegni bancari e circolari.
- *Decreto 7 marzo 2008* - Individuazione del gestore del Sistema di Interscambio della fatturazione elettronica nonché delle relative attribuzioni e competenze.
- *Decreto 3 aprile 2013* - Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche.
- *Codice Civile, articolo 2215 bis* - Documentazione informatica.
- *Legge del 7 agosto 1990, n. 241 e s.m.i.* - Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.
- *Circolare del Ministero del Lavoro 21 agosto 2008, n. 20* - Istruzioni operative del Ministero del Lavoro sulla tenuta del libro Unico del Lavoro.
- *Circolare AGID del 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.
- *Regolamento ISVAP 14 ottobre 2008, n. 27* - Tenuta dei registri assicurativi in modalità elettronica.
- *Regolamento 22 marzo 2016 Banca d'Italia* - Regolamento ex art. 8, comma 7, lettera e del decreto-legge 13 maggio 2011, n. 70, convertito dalla legge 12 luglio 2011, n. 106.

Torna al sommario

3.2. Procedure interne di riferimento

1) PRC_TI_763_GR “Service & software development and maintenance”.
2) PRC_TI_765_GR “Infrastructure design and operations”.
3) PRC_TI_814_ GR “Gestione Change Request e Service Request”.
4) PRC_TI_773_GR “Maintain & Improve”.
5) PRC_TI_868_GR “Piano di gestione dei servizi IT”.
6) PRC_TI_766_GR “Patch e Configuration Management”.
7) IST_SCQ_597_GR “Interventi di annullamento su delivery GED”.

Torna al sommario

3.3. Standard di riferimento

- **ISO 14721:2012 OAIS** (Open Archival Information System), Sistema informativo aperto per l’archiviazione.
- **ISO/ IEC 27001:2013** (Information technology - Security technology - Security techniques - Information security management systems – Requirements), Requisiti di un ISMS (Information Security Management System).
- **ETSI TS 101 533-1 V1.3.1 (2012-04)** (Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management), Requisiti per realizzare e gestire sistemi sicuri ed 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.
- **UNI ISO 15489-1:2006** (Information and documentation - Records management - Part 1: General, Informazione e documentazione), Gestione dei documenti di archivio - Principi generali sul record management.
- **UNI ISO 15489-2:2007** (Information and documentation - Records management - Part 2: Guideline, Informazione e documentazione), Gestione dei documenti di archivio - Linee guida sul record management.
- **ISO/ TS 23081-1:2006** (Managing metadata for records - Part 1: Principles), Quadro di riferimento per lo sviluppo di un sistema di metadati per la gestione documentale.

- **ISO/ TS 23081-2:2007** (Managing metadata for records - Part 2: Conceptual and implementation issues), Guida pratica per l'implementazione.

Torna al sommario

4. RUOLI E RESPONSABILITA'

In linea con quanto riportato nel documento pubblicato dall'AgID "Profili professionali", nel quali sono indicati i profili professionali peculiari che devono essere presenti nella struttura organizzativa del soggetto pubblico o privato accreditato, si riportano, di seguito, le figure ed i relativi ruoli all'interno di Postel coinvolte nel processo di conservazione digitale.

Ruolo	Nominativo	Attività di competenza	Periodo nel ruolo	Funzione/ Struttura/ Gruppo
Responsabile del servizio di conservazione	Valerio Cristofaro	Definizione ed 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. Verifica della 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.	2012 - oggi	Supporto clienti e qualità/ Assistenza tecnica
Responsabile della funzione archivistica	Valerio Cristofaro	Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore dei documenti da conservare, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni	2010 - oggi	Supporto clienti e qualità/ Assistenza tecnica

		documentali trasferiti, di esibizione, accesso e fruizione dell'archivio conservato. Definizione del set di metadati di conservazione da associare a ciascuna tipologia documentale ed ai fascicoli informatici. Monitoraggio del processo di conservazione ed analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione. Collaborazione con l'ente produttore ai fini del trasferimento in conservazione dei documenti, della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.		
Responsabile della sicurezza dei sistemi per la conservazione	Maurizio Sabbioni	Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, normative e politiche e procedure interne di sicurezza. Segnalazione delle eventuali difformità al responsabile del servizio di conservazione ed individuazione/ pianificazione delle necessarie azioni correttive	2010 - oggi	Tecnologie dell'informazione/ Architetture, infrastrutture e sicurezza ICT/ Networking e sicurezza ICT
Responsabile del trattamento dei dati personali	Fabio Cestola	Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali. Garanzia che il trattamento dei dati affidati dai Clienti avviene nel rispetto delle istruzioni impartite dal Titolare del	2016 - oggi	Tecnologie dell'informazione

		trattamento dei dati personali, con garanzia di sicurezza e riservatezza		
Responsabile dei sistemi informativi per la conservazione	Alfredo Sarrantonio	Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione. Monitoraggio del mantenimento dei livelli di servizio concordati con l'ente produttore. Segnalazione delle eventuali difformità degli SLA al responsabile del servizio di conservazione ed individuazione/ 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.	2015 - oggi	Tecnologie dell'informazione/ Architetture, infrastrutture e sicurezza ICT/ Architetture
Responsabile sviluppo e manutenzione del sistema della conservazione	Maria Teresa Muratore	Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione. Pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione. Monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione. Interfaccia con l'ente produttore relativamente alle modalità di	2013 - oggi	Tecnologie dell'informazione/ Software factory/ Factory GED

		trasferimento dei documenti e fascicoli informatici in merito ai formati da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche. Gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.		

Torna al sommario

4.1. Storia dei responsabili del servizio di conservazione

Responsabile del servizio di conservazione	Periodo nel ruolo
Valerio Cristofaro	18/12/2012 - oggi
Ulisse Del Gallo Roccagiovine	23/03/2011 – 17/12/2012
Valerio Cristofaro	1/04/2010 – 22/03/2011
Fabrizio Mancini	2/01/2010 – 31/03/2010

Torna al sommario

5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1. Organigramma

Di seguito, le strutture organizzative di Postel principalmente coinvolte nelle attività proprie del servizio di conservazione:

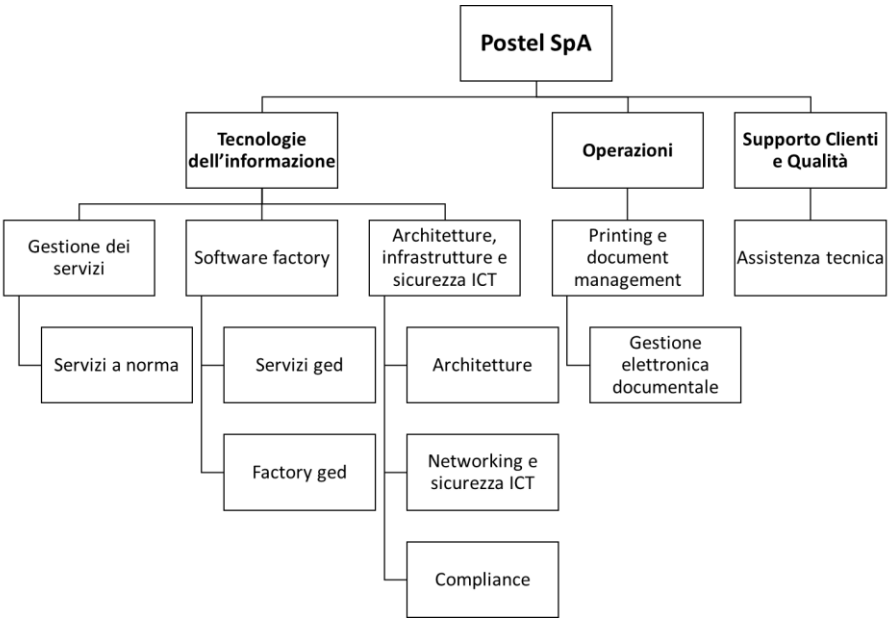


Figura 1 - Organigramma delle principali strutture coinvolte nel servizio di conservazione digitale

Torna al sommario

5.2. Strutture organizzative

Nella tabella seguente una sintesi delle responsabilità in relazione alle principali strutture organizzative coinvolte nelle attività proprie del servizio di conservazione.

Struttura Attività	Servizi a norma	Servizi ged	Factory ged	Architetture	Networking e sicurezza ICT	Compliance	Gestione elettronica documentale	Assistenza tecnica
Attivazione del servizio di conservazione	**R-E-V**							**R**
Acquisizione, verifica e gestione dei PdV presi in carico	**R-E-V**							**R**
Generazione del RdV	**R-E-V**							**R**
Preparazione e gestione del PdA	**R-E-V**							**R**
Preparazione e gestione del PdD	**R-E-V**							**R**

Preparazione e gestione dei duplicati	**V**						**R-E**	**R**
Scarto dei PdA	**R-E-V**							**R**
Chiusura del servizio di conservazione al termine di un contratto	**R-E-V**							**R**
Conduzione e manutenzione del SdC	**E-V**							**R**
Monitoraggio del SdC	**R-V**			**E**				
Change management	**R-V**	**E**	**E**		**V**	**V**		
Verifica periodica della conformità alla normativa vigente e standard di riferimento	**R-E**					**V**		
[R=Responsabile; E=Esegue; V=Verifica]								

Le persone interne al gruppo Servizi a norma, in relazione alle attività sopra indicate, sono nominate, tramite documento formale di nomina, Amministratori di sistema del SdC ed incaricati al trattamento dei dati personali e sensibili trattati all'interno del sistema.

Le persone interne al gruppo Gestione elettronica documentale, in relazione all'attività di produzione di duplicati informatici mediante la masterizzazione su DVD, in formato ISO, dei documenti conservati, sono nominate, tramite documento di nomina formale, incaricati al trattamento dei dati personali e sensibili.

Le attività eventualmente affidate ai singoli soggetti sono definite nell'ordine di servizio che regolamenta il rapporto tra Postel ed i dipendenti.

Ogni dipendente svolge solamente le attività per le quali ha raggiunto un comprovato livello di competenza e/ o esperienza tale da consentire un adeguato livello di autonomia, pur sotto la costante supervisione del diretto superiore gerarchico e/ o del responsabile del servizio di conservazione.

Torna al sommario

6. OGGETTI SOTTOPOSTI A CONSERVAZIONE

6.1. Oggetti conservati

Gli oggetti sottoposti a conservazione possono essere:

- Documenti informatici;
- Documenti amministrativi informatici;
- Fascicoli informatici o aggregazioni documentali informatiche.

In linea con quanto descritto nel modello OAIS, tutti gli oggetti versati nel SdC sono gestiti in forma di pacchetti informativi. Ai sensi del DPCM 3 dicembre 2013, il pacchetto informativo si distingue in:

- Pacchetto di Versamento (PdV). Pacchetto informativo con il quale il soggetto produttore invia al SdC gli oggetti da sottoporre in conservazione.
- Pacchetto di Archiviazione (PdA). Pacchetto informativo con il quale il SdC aggrega e conserva gli oggetti.
- Pacchetto di Distribuzione (PdD). Pacchetto informativo inviato dal SdC all'utente che fa richiesta di esibizione del documento conservato.

Torna al sommario

6.2. Pacchetto di versamento

Il pacchetto di versamento è il pacchetto informativo inviato dal soggetto produttore al SdC. Deve contenere (con riferimento al modello OAIS) i documenti da conservare, i metadati che permettono di ricercare gli stessi all'interno del SdC e le informazioni relative al soggetto produttore autenticato al sistema di trasmissione.

Per quanto concerne i metadati, le informazioni da associare a ciascun PdV sono definite in fase contrattuale e configurate all'interno SdC di Postel per ciascuna classe documentale definita con il soggetto produttore (in relazione alla tipologia documentale); con riferimento a quanto disposto dall'allegato 5 del DPCM 3 dicembre 2013, i metadati minimi da associare ad un documento informatico sono:

- Identificativo univoco del documento;
- Soggetto produttore;
- Oggetto;
- Data di chiusura;
- Destinatario;
- Impronta.

Per quanto riguarda, invece, i documenti amministrativi informatici, il set minimo di metadati è quello previsto in fase di registrazione di protocollo, ovvero:

- Numero di protocollo (numero composto da 7 cifre che si rinnova ogni anno solare);

- Data di protocollo;
- Codice identificativo della PA;
- Codice identificativo dell'area organizzativa omogenea (AOO);
- Codice identificativo del registro di protocollo;
- Impronta.

In relazione ai fascicoli amministrativi informatici ed aggregazioni documentali informatiche, il set minimo di metadati è:

- Identificativo del fascicolo/ aggregazione documentale;
- Codice identificativo della PA titolare del procedimento;
- Codice identificativo delle eventuali altre PA coinvolte nel procedimento;
- Oggetto del procedimento;
- Responsabile del procedimento amministrativo;
- Elenco dei documenti presenti nel fascicolo/ aggregazione documentale.

Per quanto concerne i formati accettati dal SdC di Postel, si fa riferimento all'allegato 2 del DPCM 3 dicembre 2013 (formati idonei alla conservazione), ovvero:

Formato	Proprietario	Estensione	Tipo	Aperto	Standard
PDF PDF/ A	Adobe System	.pdf	Application/ pdf	Si	ISO 32000-1
PDF/ A	Adobe System	.pdf	Application/ pdf	Si	ISO 19005-1:2005 (vers. PDF 1.4) ISO 19005-2:2011 (vers. PDF 1.7)
TIFF	Adobe	.tiff	Image/ tiff	No	ISO 12639 (TIFF/ IT) ISO 12234 (TIFF/ EP)
JPG e JPEG 2000	Joint Photographic Experts Group	.jpg, .jpeg, .jp2	Image/ jpeg	Si	ISO/ IEC 10918:1 ISO/ IEC 15444-1
OOXML	Microsoft	.docx, .xlxs, .pptx	MIME	Si	ISO/ IEC DIS 29500:2008
ODF	OASIS	.ods, .odp, .odg, .odb	Application/ vnd.oasis.opendocument.text	Si	ISO/ IEC 26300:2006 UNI CEI ISO/ IEC 26300
XML	W3C	.xml	Application/ xml text/ xml	Si	
TXT		.txt	ASCII, UTF-8, UNICODE	Si	ISO 646 RFC 3629 ISO/ IEC 10646

Pec/ mail		.eml	MIME	No	RFC 2822/ MIME

Rimane salva la possibilità di utilizzare ulteriori formati rispetto a quelli sopra riportati, sempre concordati in fase contrattuale, purché sia adeguatamente descritta la relativa motivazione e siano rispettate le caratteristiche di: apertura, sicurezza, diffusione, portabilità, supporto allo sviluppo e funzionalità.
Con particolare riferimento a quelle tipologie documentali che richiedono un periodo di conservazione a lungo termine (a titolo di esempio, superiore ai 20 anni), è opportuno privilegiare quei formati che permettono di garantire maggiormente le caratteristiche di immodificabilità, integrità e leggibilità nel lungo periodo (ad esempio, il formato PDF/ A). A tal proposito, è sempre possibile far riferimento all'allegato 2 del DPCM 3 dicembre 2013.

Il dettaglio in termini di modalità di trasmissione, metadati, formati, verifiche effettuate su ciascun PdV, ecc., è riportato nel documento "Specificità del Pacchetto e Rapporto di versamento"; per quanto riguarda le eventuali personalizzazioni rispetto al servizio offerto da Postel, sono riportate nel documento "Specificità del contratto" rilasciato al soggetto produttore al termine della stipula del contratto di servizio.
Torna al sommario

6.3. Pacchetto di archiviazione

Come espressamente richiesto dal DPCM 3 dicembre 2013, ogni PdV viene trasformato in un pacchetto di archiviazione (PdA) secondo lo standard UNI Sincro 11386 (specifiche riportante anche nell'allegato 4 dello stesso DPCM).
Il PdA è costituito dai seguenti file:

- Lista dei documenti conservati all'interno del PdA. Tale lista può essere un sovra-insieme o un sotto-insieme dei documenti presenti nel PdV iniziale;
- File indice del PdA (IPdA). Suddetto file rispetta la struttura UNI Sincro e contiene le seguenti informazioni:
  - Informazioni generali relative all'IPdA;
  - Informazioni relative al PdA;
  - Indicazione di uno o più raggruppamenti di uno o più file che sono contenuti nel PdA;
  - Informazioni relative al processo di produzione del PdA.

Di seguito, se ne riporta un esempio:

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
<ns1:IdCs1:url="http://www.uni.com/U3011/sincro/"ns1:version="1.0" xmlns:ns1="http://www.uni.com/U3011/sincro/">
        <ns1:SelfDescription>
                <ns1:ID ns1:scheme="SCN">improntaDisco438_13.xml</ns1:ID>
                <ns1:CreatingApplication>
                        <ns1:Name>CoD</ns1:Name>
                        <ns1:Version>3.0.10</ns1:Version>
                        <ns1:Producer>Postel S.p.A</ns1:Producer>
```

```
                </ns1:CreatingApplication>
        </ns1:SelfDescription>
        <ns1:VdC>
                <ns1:ID ns1:scheme="SCN">438_13</ns1:ID>
                <ns1:MoreInfo ns1:XMLScheme="IDX/index.xsd">
                        <ns1:ExternalMetadata ns1:format="text/xml">
                                <ns1:ID ns1:scheme="SCN">indexDisco438_13.xml</ns1:ID>
                                <ns1:Path>IDX/indexDisco438_13.xml</ns1:Path>
                                <ns1:Hashns1:function="SHA-
                        256">CA8C15B33A98AF453C8DEC3B3E0AF91A55479AB753DFDD372A4F7BDE98685
                        292</ns1:Hash>
                        </ns1:ExternalMetadata>
                </ns1:MoreInfo>
        </ns1:VdC>
        <ns1:FileGroup>
                <ns1:File ns1:format="image/tiff" ns1:extension="tiff" ns1:encoding="binary">
                        <ns1:ID ns1:scheme="SCN">F1600001371000009</ns1:ID>
                        <ns1:Path>DOC/F1600001371000009_60314481906.tiff</ns1:Path>
                        <ns1:Hashns1:function="SHA-
                256">7BC468C7A0CFB340A4836F52DFA083E74077AEF2BB73C23940C21E8353B48E8C</ns1:
                Hash>
                </ns1:File>
        </ns1:FileGroup>
        <ns1:Process>
                <ns1:Agentns1:role="PreservationManager"ns1:otherRole=""ns1:type="organization">
                        <ns1:AgentName>
                                <ns1:FormalName>Postel S.p.A</ns1:FormalName>
                        </ns1:AgentName>
                </ns1:Agent>
                <ns1:TimeReference>
                        <ns1:DetachedTimestampns1:format="application/timestamp-reply"
                ns1:encoding="binary"ns1:normal="2016-11-
                14T17:09:05.865+01:00">improntaDisco438_13.xml.tsr</ns1:DetachedTimestamp>
                </ns1:TimeReference>
        </ns1:Process>
</ns1:IdC>
```

- File degli indici in formato xml, richiamato all'interno dell'IPdA. Di seguito un esempio:

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
<DOCUMENT_CLASS company_name="Z0000001" class_name="INPS_CART_SEZ_i">
        <DOCUMENT>
                <INDEX id="ID" value="  "/>
                <INDEX id="FILE_NAME" value="  "/>
                <INDEX id="DENOMINAZIONE" value="  "/>
                <INDEX id="DATA" value="  "/>
                <INDEX id="OGGETTO" value="  "/>
        </DOCUMENT>
<DOCUMENT>
```

- File IPdA in formato xml firmato digitalmente dal responsabile del servizio di conservazione;
- File IPdA in formato xml marcato temporalmente. La marca temporale apposta su questo file attesta l'esatto momento di congelamento di tutti i documenti in esso contenuti.

Torna al sommario

6.4. Pacchetto di distribuzione

Il servizio di conservazione offerto da Postel, in linea con quanto riportato nel DPCM 3 dicembre 2013, permette l'esibizione a norma di tutti i documenti conservati all'interno del proprio sistema.
A seguito di una richiesta di esibizione da parte di un utente opportunatamente profilato, il SdC, a partire dal PdA, crea il PdD.
Il PdD è quel pacchetto informativo che permette di visualizzare un determinato documento conservato all'interno del SdC unitamente ad una serie di informazioni che permettono di verificarne l'integrità, e validità della firma apposta sul PdA da parte del responsabile del servizio di conservazione.
Nel dettaglio, il PdD creato dal SdC di Postel, contiene:

- File IPdA nei 3 formati previsti: .xml, .xml.p7m (firmato digitalmente) e .xml.p7m.tsr (firmato digitalmente e marcato temporalmente);
- File degli indici in formato xml di ciascun documento presente nel PdA.
- Documento per il quale l'utente ha richiesto l'esibizione a norma.

È possibile pertanto verificare che il documento esibito sia presente all'interno dell'IPdA, calcolarne l'impronta e confrontarla con quella riportata nel suddetto indice (verifica integrità), nonché verificare la validità del certificato di firma e marca temporale.

Ai fini dell'interoperabilità degli oggetti conservati tra i sistemi di conservazione ed ai sensi del DPCM 3 dicembre 2013, la produzione dei PdD coincide con quella dei PdA.

Torna al sommario

6.5. Tipologie documentali

6.5.1. Fattura elettronica

Il DMEF 17 giugno 2014 armonizza le disposizione di legge di natura tributaria sulla conservazione con le regole tecniche vigenti (DPCM 3 dicembre 2013) di attuazione del CAD, in materia di sistema di conservazione. In particolare, i documenti informatici rilevanti ai fini tributari/ fiscali, e quindi anche le fatture elettroniche, devono avere le seguenti caratteristiche:

- Immodificabilità;
- Integrità ed Autenticità (garantita, ad esempio, dalla sottoscrizione con firma digitale e riferimento temporale);
- Leggibilità;

- Ordine cronologico e non soluzione di continuità per ciascun periodo d'imposta (in fase di conservazione).

La scelta dei formati per la conservazione deve essere, quindi, strumentale a che il documento assuma le caratteristiche sopra indicate; è pertanto opportuno fare riferimento all'Allegato 2 del DPCM 3 dicembre 2013, che fornisce indicazioni sui formati più idonei per la conservazione dei documenti informatici.

Con particolare riferimento alle fatture elettroniche, la Legge 24 dicembre 2007, n. 244, art. 1, commi da 209 a 213, introduce l'obbligo di fatturazione elettronica nei confronti della PA. Si istituisce il Sistema di Interscambio (SdI), gestito dall'Agenzia delle Entrate, quale punto di passaggio obbligato per le fatture elettroniche destinate alla PA. Con il DMEF 3 aprile 2013, n. 55, sono stabilite le regole tecniche per l'emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alla PA.
Infine, ai sensi dell'art. 2 del D.lgs. 52/ 2004, le fatture elettroniche trasmesse o ricevute in forma elettronica sono archiviate (conservate) nella stessa forma; le fatture elettroniche consegnate o spedite in copia sotto forma cartacea possono essere archiviate (conservate) in forma elettronica.
La trasmissione elettronica è possibile solo in caso di preventivo accordo tra le parti, posto che il cessionario (o committente) sia in possesso degli strumenti tecnici alla ricezione del documento informatico (Circolare 45/ E dell'Agenzia delle Entrate 19 ottobre 2005). Ciò comporta la possibilità, laddove non vi sia il consenso o comportamento concludente del ricevente, che vi sia una fattura elettronica solo per l'emittente, il quale procede alla sua generazione in formato elettronico (con firma digitale e riferimento temporale) ed alla sua successiva conservazione digitale; per il ricevente rimane una normale fattura cartacea.
Ai sensi di quanto indicato nel DMEF 17 giugno 2014, le fatture elettroniche, in qualità di documenti informatici rilevanti ai fini tributari/ fiscali, devono essere versate all'interno del SdC entro il termine di 3 mesi dalla presentazione annuale.

A fronte delle disposizioni regolamentari sopra citate, Postel, in qualità di responsabile del servizio di conservazione, provvede:

- Alla conservazione delle fatture elettroniche per conto dell'emittente - lato attivo;
- Alla conservazione delle fatture elettroniche per conto del ricevente - lato passivo;
- In caso di fatture spedite in copia cartacea, prima alla loro dematerializzazione e poi alla loro successiva conservazione digitale.
- Alla conservazione delle fatture elettroniche e delle relative notifiche del SdI, sia lato fornitore che PA, nel caso di fatturazione elettronica nei confronti della PA.

In linea con quanto indicato nell'Allegato 2 del DPCM 3 dicembre 2013, Postel utilizza come formati quelli indicati dalla normativa di settore (ad es. PDF, PDF/ A, xmlPA) e come metadati (compresivi di quelli obbligatori richiesti dal DMEF 17 Giugno 2014):

- Denominazione o Nome e Cognome;
- Codice Fiscale o Partita IVA;

- Data emissione (lato attivo);
- Data registrazione (lato passivo);
- Numero documento (lato attivo)
- Numero registrazione (lato passivo).

Le fatture elettroniche sono conservate da Postel all'interno del proprio SdC per un periodo pari a 10 anni (art. 2220 del Codice Civile).

Torna al sommario

6.5.2. Libri contabili

Con riferimento all'articolo 2215 bis del Codice Civile, i libri contabili, la cui tenuta è obbligatoria per disposizioni di legge, possono essere formati e tenuti con strumenti informatici; gli obblighi di numerazione progressiva e vidimazione previsti dalla legge, sono assolti mediante apposizione, almeno una volta all'anno, della marca temporale e firma digitale dell'imprenditore o di altro soggetto dal medesimo delegato.

In particolare, è possibile assolvere ai suddetti obblighi entro i termini previsti in materia di conservazione digitale (DMEF 17 Giugno 2014), ovvero:

- Entro 3 mesi dalla presentazione della dichiarazione annuale, per assolvere agli obblighi di numerazione progressiva e vidimazione, l'imprenditore (o suo delegato) deve apporre la propria firma digitale e marca temporale sul libro prodotto;
- In un secondo momento, ma sempre entro il termine annuale stabilito, ai fini della chiusura del processo di conservazione, il responsabile della conservazione deve apporre la propria firma digitale e marca temporale sul PdA.

In linea con quanto indicato nel DMEF 17 giugno 2014, Postel utilizza come formato per la conservazione dei libri contabili il PDF/ A e come metadati le chiavi di indicizzazione richieste dal medesimo Decreto. Sono eventualmente aggiunti ulteriori metadati in relazione alla specifica tipologia di libro contabile (libro giornale, libro IVA, ecc.).

I libri contabili sono conservati nel SdC di Postel per un periodo pari a 10 anni (ai sensi dell'art. 2220 del Codice Civile).

Torna al sommario

6.5.3. Registri assicurativi

Con il Regolamento 14 ottobre 2008 n. 27, l'Isvap ha riconosciuto piena validità giuridica e fiscale alla tenuta digitalizzata di registri e documenti obbligatori per le compagnie assicurative, ivi compresi i contratti di assicurazione e riassicurazione.

Nello specifico, l'articolo 4 disciplina le modalità di compilazione dei registri assicurativi introducendo la possibilità di formare gli stessi su supporti informatici nel rispetto di quanto stabilito dal CAD e dalle relative regole tecniche. L'articolo 5, comma 4, aggiunge: la cadenza per la conservazione dei registri

formati su supporto informatico è trimestrale. Per quanto riguarda il periodo di conservazione, il comma successivo richiama il termine decennale, prevedendo, al contempo, un termine ventennale per il registro dei contratti Ramo Vita. Fermi restando gli obblighi di conservazione previsti al comma 4, si è previsto, al comma 6, che le imprese dispongano delle informazioni contenute nei registri assicurativi in basi di dati che consentano l'estrazione e l'elaborazione elettronica delle informazioni anche relative a più registri, in modo da facilitare i controlli interni ed esterni all'impresa.

Pertanto, coordinando suddetto regolamento con il DPCM 3 dicembre 2013 e DMEF 17 giugno 2014, il flusso corretto per la formazione, tenuta e conservazione dei bollati è il seguente:

- L'assicurazione forma il documento secondo le proprie procedure;
- Il regolamento Isvap prevede la conservazione trimestrale del libro; la trimestralità, in mancanza dell'indicazione di un momento iniziale da cui far decorrere i tre mesi, può coincidere con la trimestralità solare: ad esempio, 31 marzo, 30 giugno, 30 settembre, 31 dicembre.
- La porzione trimestrale del libro deve arrivare in conservazione firmata digitalmente dal soggetto produttore e marcata temporalmente.

Con riferimento a quanto sopra riportato, Postel provvede alla conservazione trimestrale dei registri assicurativi informatici e registri assicurativi cartacei dematerializzati. Come formato di conservazione è utilizzato il PDF e, di seguito, i metadati associati alla tipologia documentale in oggetto:

- Denominazione;
- Partita IVA;
- Mese;
- Anno;
- Progressivo.

I registri assicurativi sono conservati nel SdC di Postel per un periodo pari a 10 anni; i registri dei contratti Ramo Vita per un periodo di 20 anni.

Torna al sommario

6.5.4. Libro Unico del Lavoro

Dal 1° gennaio 2009 il datore di lavoro è obbligato alla tenuta del Libro Unico del Lavoro (LUL), in sostituzione di tutti i libri obbligatori (con esclusione del libro infortuni) che lo stesso doveva istituire ai sensi della normativa previgente. Il Decreto del 9 luglio 2008 e la Circolare n. 20 del 2008 individuano le modalità di tenuta e conservazione del LUL. In particolare, la tenuta e conservazione del LUL può essere effettuata mediante l'utilizzo di supporti magnetici o ad elaborazione automatica dei dati, garantendone la consultazione in ogni momento, l'inalterabilità ed integrità dei dati, nonché la sequenzialità cronologica delle operazioni eseguite, nel rispetto delle regole tecniche disciplinate dal DPCM 3 dicembre 2013. Tali sistemi sono sottratti ad obblighi di vidimazione ed autorizzazione, previa apposita comunicazione scritta, anche a mezzo fax o e-mail, alla direzione provinciale del lavoro competente per territorio, prima della messa in uso, con indicazione dettagliata delle caratteristiche tecniche del sistema adottato. Con specifico riferimento alla modalità di tenuta su supporti magnetici, è importante precisare che i documenti

informatici che compongono il LUL devono avere la forma di documenti statici non modificabili e devono essere emessi, al fine di garantirne l'attestazione della data, l'autenticità ed integrità, con l'apposizione del riferimento temporale e della sottoscrizione elettronica. Possono essere memorizzati su qualsiasi tipo di supporto di cui sia garantita la leggibilità nel tempo, purché rimanga sempre assicurato l'ordine cronologico e non vi sia soluzione di continuità per ciascun periodo di paga. Il libro unico del lavoro su supporto magnetico deve essere reso leggibile e, a richiesta, disponibile su supporto cartaceo o informatico (formato PDF), in caso di verifiche, controlli o ispezioni. Devono essere versati nel sistema di conservazione entro la fine del mese successivo alla loro registrazione, garantendo le seguenti funzioni di ricerca: Cognome, Nome, Codice Fiscale del lavoratore, Data ed associazioni logiche di tali dati. Il datore di lavoro ha l'obbligo di conservare il libro unico del lavoro per la durata di cinque anni dalla data dell'ultima registrazione e di custodirlo nel rispetto del D.lgs. 30 giugno 2003, n. 196, in materia di protezione dei dati personali.

Il Libro Unico del Lavoro può essere conservato presso la sede legale del datore di lavoro; in alternativa, l'impresa può scegliere di tenere il LUL anche presso una sede diversa dalla sede legale. In ogni caso ciò che conta, sotto un profilo di rispetto sostanziale della normativa, è che il datore di lavoro affidatario del Libro Unico sia in condizione di poter esibire le scritture e la documentazione senza poter opporre alcuna eccezione relativa alla sede liberamente prescelta.

Postel, in qualità di responsabile del servizio di conservazione, provvede a conservare il LUL in formato PDF, per cinque anni, associando allo stesso i seguenti metadati:

- Nome del lavoratore;
- Cognome del lavoratore;
- Codice Fiscale del lavoratore;
- Denominazione della società;
- Partita Iva della società;
- Mese di riferimento;
- Anno di riferimento;

ed associazioni logiche dei dati sopra indicati.

Torna al sommario

6.5.5. Assegni bancari

Il DMEF 3 Ottobre 2014, n. 205 ed il Regolamento 22 Marzo 2016 della Banca d'Italia, consentono alle Istituzioni Bancarie di presentare al pagamento gli assegni bancari e circolari in formato elettronico, permettendone, così, una loro successiva conservazione digitale.

Con particolare riferimento al processo di conservazione, l'attività è a carico del negoziatore. Nel dettaglio, il negoziatore è tenuto a conservare (per il tempo previsto dalla legge):

- L'immagine dell'assegno (sottoscritto digitalmente dallo stesso al fine di attestarne la conformità all'originale cartaceo);
- Documento di protesto/ constatazione equivalente (inviati dal trattario/ emittente);

- Documento di non protestabilità (inviato dal trattario/ emittente).
- Contestualmente alla conservazione digitale, il negoziatore deve conservare l'assegno in formato analogico per 6 mesi a partire dalla presentazione al pagamento.

Postel, ai sensi di quanto stabilito dal sopra citato Regolamento (per il quale l'attività di conservazione può essere esternalizzata a terze parti), si pone come responsabile del servizio di conservazione per conto della Banca Negoziatrice. Nel dettaglio, garantisce la conservazione dell'immagine dell'assegno, documento di protesto e non protestabilità, assicurandone la ricerca almeno per le seguenti chiavi di indicizzazione:

- Dati identificativi dell'assegno:
  - Identificativo negoziatore (codice ABI_codice CAB);
  - Identificativo trattario/ emittente (codice ABI_codice CAB);
  - Importo;
  - Data emissione;
  - Numero assegno;
  - Nome beneficiario.
- Tipologia:
  - Immagine assegno;
  - Protesto/ constatazione equivalente;
  - Documento di non protestabilità.

I documenti sopra indicati sono conservati nel SdC di Postel per un periodo pari a 10 anni (ai sensi dell'art. 119 del TU bancario).

Torna al sommario

7. IL PROCESSO DI CONSERVAZIONE

Il processo di conservazione definito da Postel individua le principali fasi riportate nel DPCM 3 dicembre 2013, descritte nei successivi paragrafi.

Di seguito, una sintesi del processo di conservazione:

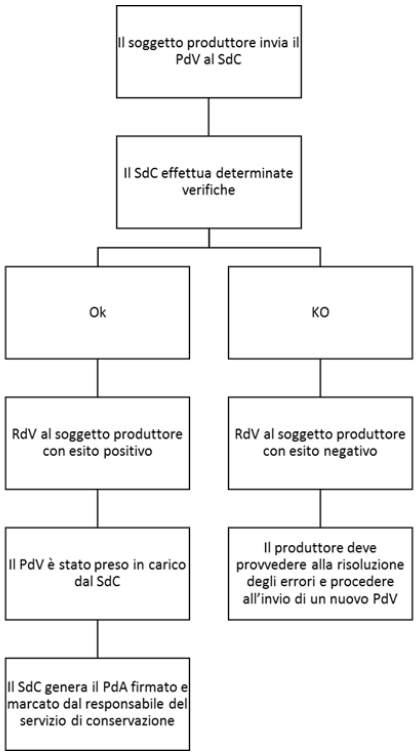


Figura 2 - Processo di conservazione digitale

Torna al sommario

7.1. Modalità di acquisizione dei pacchetti di versamento

La prima fase del processo di conservazione è l'acquisizione del pacchetto di versamento da parte del SdC.

La trasmissione del PdV da parte del produttore avviene mediante l'utilizzo di un canale sicuro definito in sede contrattuale rispetto ai canali messi a disposizione da Postel, e secondo le indicazioni fornite nel documento "Specificità del Pacchetto e Rapporto di versamento".

In relazione al canale di trasmissione, il soggetto produttore avrà modo di verificare l'effettivo invio ed accettazione da parte di Postel del pacchetto inviato, mediante la ricezione di apposite ricevute.

Una volta accettato, il PdV è veicolato direttamente al SdC di Postel.

Torna al sommario

7.2. Verifiche sui pacchetti di versamento

Una volta ricevuto il PdV, il SdC effettua le verifiche necessarie per poter prendere in carico e poi conservare lo stesso pacchetto ricevuto. Nel documento "Specificità del Pacchetto e rapporto di versamento", è presente una descrizione dettagliata delle verifiche effettuate dal SdC; qualora il soggetto produttore richieda particolari controlli, gli stessi saranno dettagliatamente descritti nel documento "Specificità del contratto".

In termini generali, sono effettuate le seguenti verifiche:

- Validazione statica. Durante questa fase vengono effettuati dei controlli sulla correttezza strutturale del PdV, ovvero: file non corrotto, completo e strutturato correttamente.
- Verifica Dinamica. Superata la fase di validazione statica, il PdV passa nella fase di validazione dinamica, nella quale è sottoposto ad una serie di controlli sia a livello di pacchetto che di singolo documento.

Torna al sommario

7.3. Accettazione dei pacchetti di versamento e generazione del relativo rapporto di versamento

Se non è riscontrato alcun errore nelle fasi di validazione statica e dinamica, il SdC genera in automatico un rapporto di versamento con esito positivo, con lo scopo di attestare l'effettiva presa in carico da parte del SdC del PdV ricevuto. Il RdV è messo a disposizione del cliente mediante il canale definito in fase contrattuale.

La struttura del RdV generato dal SdC di Postel, dettagliatamente descritta del documento "Specificità del Pacchetto e Rapporto di versamento", è conforme a quanto indicato nel DPCM 3 dicembre 2013, ovvero:

- Identificato in maniera univoca all'interno del SdC;
- Contiene un riferimento temporale relativo al tempo UTC e l'impronta del relativo PdV.

Torna al sommario

7.4. Rifiuto dei pacchetti di versamento e generazione del relativo rapporto di versamento

Nel caso di errori riscontrati in fase di validazione statica/ dinamica, il PdV viene messo in stato di errore ed annullato. L'elaborazione si arresta e viene generato in automatico un rapporto di versamento contenente le tipologie di errori riscontrate, messo a disposizione del cliente mediante il canale definito in fase contrattuale.

Per poter proseguire con il processo di conservazione il soggetto produttore dovrà provvedere alla risoluzione degli errori e procedere con l'invio di un nuovo pacchetto corretto.

Torna al sommario

7.5. Preparazione e gestione del pacchetto di archiviazione

Una volta inviato il RdV con esito positivo al soggetto produttore, attestante l'effettiva presa in carico da parte del sistema del pacchetto ricevuto, si provvede alla creazione del PdA.

Il SdC di Postel genera il PdA in linea con quanto richiesto dalla normativa vigente.

Nel dettaglio, il SdC genera:

- Il file IPdA in formato UNI Sincro (i documenti sono raggruppati secondo criteri di omogeneità condivisi con il soggetto produttore);

- Il file dei metadati relativi ai documenti presenti nel PdA. Suddetto file è richiamato all'interno dell'IPdA nella sezione MoreInfo (ExternalMetadati) nelle informazioni relative al PdA.
- Il file contenete tutti i documenti presenti nel PdA;
- Il file IPdA firmato digitalmente dal responsabile del servizio di conservazione;
- Il file IPdA marcato temporalmente.

Per quanto concerne la firma digitale e marca temporale, Postel richiede il servizio di firma digitale e marca temporale ad CA e TSA accredite presso AgID.

Torna al sommario

7.6. Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione a norma

Conformemente a quanto indicato del DPCM 3 dicembre 2013, il servizio di conservazione offerto da Postel permette l'esibizione a norma dei documenti conservati qualora un utente opportunatamente profilato ne faccia richiesta. Nel dettaglio, il servizio permette l'esibizione a norma mediante le 2 seguenti modalità:

- Direttamente dal portale di conservazione. L'utente può richiedere, tramite interfaccia web, l'esibizione di un determinato documento cliccando sull'apposita icona;
- Produzione di supporti di memorizzazione rimovibili (DVD) in formato ISO.

In entrambi i casi, il processo di esibizione a norma permette di estrarre un documento di cui sia stato completato il processo di conservazione (è stato generato il PdA) attraverso la generazione del pacchetto di distribuzione. A supporto dell'interoperabilità dei documenti conservati tra diversi sistemi di conservazione, il PdD è prodotto in modalità analoga al PdA ed è reso disponibile congiuntamente al documento per il quale è stato richiesto il processo di esibizione.

Per ogni PdD, l'utente ha la possibilità di visualizzare:

- Il documento per il quale è stata richiesta l'esibizione a norma;
- Il file con l'impronta del documento;
- L'IPdA firmato digitalmente;
- L'IPdA marcato temporalmente;
- Il file dei metadati.

Inoltre, è possibile visualizzare le informazioni relative alla marca temporale ed al certificato relativo alla firma digitale (e verificarne la validità).

Non è possibile utilizzare le caselle di posta elettronica certificata per la trasmissione dei PdD a seguito di una richiesta di esibizione da parte dell'utente (conseguentemente, non sono previste specifiche procedure per le quali al termine della trasmissione si procede con la cancellazione delle copie inviate).

Torna al sommario

7.7. Produzione di duplicati e descrizione dell'eventuale intervento del pubblico ufficiale

Ai sensi del CAD e DPCM 13 novembre 2014, il duplicato informatico è un documento informatico ottenuto mediante la memorizzazione sullo stesso dispositivo o su supporti differenti, della medesima sequenza di valori binari del documento informatico originario.
Con riferimento a quanto appena descritto, il SdC di Postel permette la produzione di duplicati informatici, su richiesta dell'utente, attraverso il processo di masterizzazione del documento informatico conservato su supporto di memorizzazione rimovibile (DVD). Il duplicato informatico così prodotto ha la medesima valenza giuridica e probatoria del documento informatico conservato all'interno del SdC di Postel.

Mentre, la copia informatica, ai sensi del CAD e DPCM 13 novembre 2014, è quel documento informatico avente lo stesso contenuto del documento informatico originale ma differente sequenza di valori binari.
Postel, offre il servizio di produzione di copie informatiche nella fase precedente alla conservazione: in fase contrattuale, il soggetto produttore può richiedere a Postel di produrre copie informatiche dei documenti dallo stesso prodotti per adeguarli ad un formato idoneo alla conservazione oppure per motivi di leggibilità in caso di successive attività di esibizione. Qualora si renda necessario l'intervento del PU per attestare la conformità della copia prodotta all'originale informatico, sarà a cura del soggetto produttore gestire suddetta attività di attestazione.
Torna al sommario

7.8. Scarto dei pacchetti di archiviazione

Ai sensi di quanto definito nel DPCM 3 dicembre 2013, il processo di conservazione deve prevedere l'attività di scarto dei PdA all'interno del proprio sistema, nel momento in cui risulti cessato il termine di conservazione previsto dalla normativa e/ o in fase contrattuale, dandone informativa al soggetto produttore.
In termini generali, a cadenze definite, il SdC di Postel, tramite apposita funzionalità, produce una lista di pre-scarto relativa ai PdA prossimi alla scadenza. Suddetta lista contiene i PdA proposti per lo scarto ed il riferimento di tutti i documenti presenti all'interno del pacchetto. La lista di pre-scarto è messa a disposizione del soggetto produttore mediante il medesimo canale definito in fase contrattuale.
Il produttore deve validare la lista di pre-scarto e restituirla a Postel mediante il servizio di Assistenza Tecnica. Ricevuto il riscontro, Postel procede con quanto richiesto dal soggetto produttore.
Nel caso di archivi pubblici o privati di particolare interesse culturale, lo scarto dei documenti conservati deve avvenire previa autorizzazione della Sovrintendenza archivistica (ai sensi di quanto dichiarato dal Ministero dei beni e delle attività culturali e del turismo). Conseguentemente, il soggetto produttore deve far validare la lista di pre-scarto, messa a disposizione da Postel, alla Sovrintendenza archivistica e solo dopo aver ricevuto il nulla-osta da parte della stessa può trasmettere a Postel quanto definito.

Il SdC di Postel prevede anche la possibilità di annullare una PdV contenuto in un PdA conservato all'interno del sistema. In termini generali, il soggetto produttore dovrà fornire l'identificativo del PdV da

annullare e l'eventuale nuovo PdV da inserire; tale identificativo dovrà essere comunicato al gruppo Servizi a norma, il quale dovrà individuare il PdA contenente l'identificativo, procedere con la creazione di un nuovo PdA contenete i PdV presenti nel vecchio PdA e l'eventuale nuovo PdV fornito dal produttore. Per un maggior dettaglio, si rimanda alla procedura Postel IST_SCQ_597_GR "Interventi di annullamento su delivery GED".

Torna al sommario

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

Al fine di garantire un servizio efficiente ed a norma di legge, si è reso fondamentale definire, fin dalla fase di progettazione, un SdC conforme alle normative vigenti, definendo specifici requisiti in funzione, anche e soprattutto, alle tipologie documentali ed all'interoperabilità trai i sistemi di conservazione.

Con particolare riferimento al concetto di interoperabilità, l'obiettivo è quello di rispondere alla necessità di sviluppare e mantenere nel tempo un sistema stabile e capace di interfacciarsi con altri sistemi di conservazione. Ciò è garantito soprattutto dalla conformità dell'IPdA allo standard UNI Sincro. Suddetto standard ha proprio l'obiettivo di definire la struttura dell'insieme dei dati a supporto del processo di conservazione, individuando gli elementi informativi necessari alla creazione di un file di indice, descrivendone sia la semantica sia l'articolazione, in maniera tale da consentire agli operatori del settore di utilizzare una struttura dati condivisa e raggiungere un soddisfacente grado d'interoperabilità nei processi di migrazione.

Torna al sommario

8. IL SISTEMA DI CONSERVAZIONE

8.1. Componenti logiche

8.1.1. Front-end

Nel front-end, a seconda del profilo utente che effettua il login (utente interno/ esterno), è possibile:

- Configurare nuove utenze e classi documentali;
- Gestire i PdA;
- Monitorare le lavorazioni dei pacchetti informativi;
- Gestire le lavorazioni bloccate;
- Richiedere l'esibizione a norma dei documenti conservati.

Torna al sommario

8.1.2. Back-end

Nel back-end sono installati e configurati tutti i processi di business che implementano il motore di conservazione, ossia che permettono, a partire dai documenti ricevuti dal soggetto produttore di eseguire

tutte le fasi del processo di conservazione in conformità al DPCM 3 dicembre 2013. Più precisamente, a livello di business il SdC si presenta nel seguente modo:

- Moduli software sviluppati in modalità web services;
- Moduli di comunicazione con l'applicazione web.

Torna al sommario

8.2. Componenti tecnologiche

Il servizio di conservazione di Postel è implementato da una applicazione software appositamente sviluppata, in un'architettura distribuita su più livelli. È integrato nativamente nel Sistema di Gestione Documentale Integrata di Postel e ne estende i servizi con funzionalità di stoccaggio digitale; può essere integrato da sistemi di gestione documentali terzi tramite esposizione di apposite web service.

È erogato in modalità ASP (Application Service Provider) secondo uno schema di Business Process Outsourcing (BPO); tale modalità consente al soggetto produttore/ utente di accedere ai servizi di conservazione su un sistema gestito da Postel e fisicamente posto nei locali di quest'ultima. Il servizio è accessibile dall'apposita URL di rete: il produttore/ utente richiama i servizi di conservazione secondo le modalità definite da Postel ed indicate in fase contrattuale.

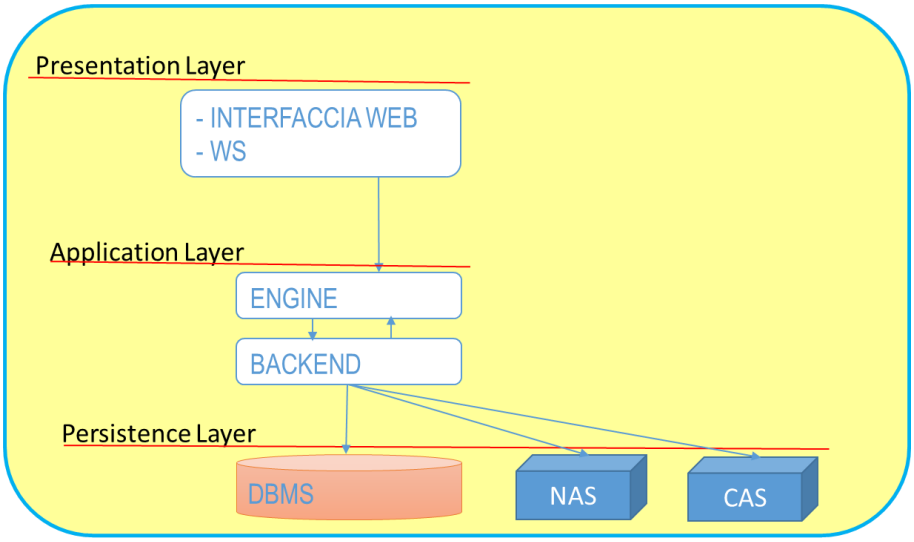


Figura 3 - Architettura tecnologica del sistema di conservazione

Torna al sommario

8.3. Componenti fisiche

L'infrastruttura fisica di supporto al servizio di conservazione è suddivisa in due siti:

- Il sito primario di produzione, dove risiede il SdC. È situato presso il data center di Pomezia, di proprietà di Telecom Italia; suddetto data center è certificato ISO 27001 ed è dotato di sistemi

evoluti di controllo degli accessi interni ed esterni, di rilevamento allagamenti/ incendi e di continuità elettronica. L'indirizzo è il seguente:

Telecom Italia
SS 148 Pontina Km. 29.100
00048, Pomezia

- Il sito secondario di produzione, attivato tempestivamente in caso di disastri o calamità naturali del sito primario, secondo apposita procedura di disaster recovery. Le caratteristiche del data center secondario sono del tutto assimilabili a quelle di quello primario e consentono l'erogazione del servizio di conservazione nel caso di impossibilità del sito primario. È situato all'interno del comune di Torino, presso il data center di proprietà di Poste Italiane. L'indirizzo è il seguente:

Poste Italiane
Corso Tazzoli, 235
10137 Torino (TO)

Entrambi i siti sono situati in territorio nazionale ad una distanza geografica di circa 550 Km.
Torna al sommario

8.4. Procedure di gestione ed evoluzione

Indispensabile per l'erogazione del servizio di conservazione è il continuo monitoraggio, riesamina delle funzionalità del SdC ed aggiornamento dello stesso rispetto alle normative vigenti. L'obiettivo è quello di garantire un architettura stabile ed affidabile, con elevati livelli di sicurezza e qualità.
In questo scenario, risulta fondamentale la corretta applicazione del processo di change management al servizio/ sistema di conservazione definito all'interno di Postel.
Nel dettaglio, il processo di change management è regolato da una serie di procedure, quali, ad esempio:

- PRC_TI_763_GR "Service & software development and maintenance", mira ad introdurre i controlli relativi all'Information Security fin dalle fasi di sviluppo, test e collaudo fino a quelle di esercizio e mantenimento di un determinato servizio/ sistema;
- PRC_TI_765_GR "Infrastructure design and operations", definisce il processo attraverso il quale è possibile realizzare un nuovo progetto, servizio, sistema, ecc., all'interno dell'infrastruttura tecnologica, garantendo, al contempo, un elevato livello di sicurezza di tutte le componenti infrastrutturali;
- PRC_TI_814_ GR "Gestione Change Request e Service Request", definisce tutte le possibili situazione che possono portare all'avanzamento di una richiesta di cambiamento e tutte le azioni/ attività necessarie per realizzarle;

- PRC_TI_773_GR “Maintain & Improve”, mira a ridurre i rischi legati al change management ed a garantire un miglioramento continuo dell’efficacia/ efficienza dei processi di sicurezza di Postel;
- PRC_TI_868_GR “Piano di gestione dei servizi IT”, individua le possibili tipologie di richieste di cambiamento e, in relazione a ciascuna, l’iter da seguire per la loro effettiva messa in produzione.

Con riferimento al sistema/ servizio di conservazione, tra le possibili richieste di cambiamento è possibile individuare:

- Cambiamenti legati a nuove attività progettuali;
- Cambiamenti derivanti da particolari richieste da parte dei clienti (se, ovviamente, ritenute utili per il SdC);
- Richieste di cambiamento a seguito di correttive/ evolutive del SdC, con lo scopo di migliorare il sistema in termini di efficacia, efficienza, semplicità e fruibilità;
- Richieste di cambiamento legate a malfunzionamenti del sistema, che potrebbero impattare sulla corretta erogazione del servizio di conservazione.

Coerentemente con quanto richiesto dalle procedure Postel, il processo di cambiamento deve essere necessariamente a carico delle persone coinvolte nel SdC competenti in relazione alla tipologia di cambiamento richiesta. Tale valutazione viene effettuata sulla base del gruppo di appartenenza delle singole persone potenzialmente coinvolte e, quindi, sul ruolo ricoperto dalle stesse.

Il processo di cambiamento è applicato sia al personale interno a Postel, che ad eventuali fornitori/ outsourcer. Anche in questo caso, in maniera analoga a quanto previsto per il personale interno, si rende necessaria una comunicazione formale (ad esempio, tramite mail) dei cambiamenti effettuati (con le relative motivazioni sottostanti) ai fornitori/ outsourcer; viceversa, eventuali fornitori/ outsourcer devono informare tempestivamente Postel, tramite comunicazione formale, di eventuali modifiche ai processi critici del SdC gestiti dagli stessi.

Contestualmente al processo di cambiamento, è indispensabile monitorare la vulnerabilità del sistema; in linea con le procedure Postel PRC_TI_765_GR “Infrastructure design and operations” e PRC_TI_766_GR “Patch e Configuration Management”, sono periodicamente svolte attività di patch, vulnerability e penetration test al SdC; è prevista, inoltre, la possibilità, nel caso si renda necessaria, di ripristinare la versione precedente del software o comunque ritornare alla situazione iniziale, mediante apposita procedura di rollback.

Sono inoltre definiti e programmati audit interni per stabilire se il processo di conservazione e le relative procedure siano efficacemente realizzati. La struttura di Compliance pianifica, almeno una volta all’anno (e comunque ogni qualvolta si renda necessario) un audit al SdC anche e soprattutto in termini di conformità agli standard e normative di riferimento. A titolo di esempio, in fase di verifica, sono esaminati i processi di conservazione (devono essere conformi alle certificazioni degli standard conseguite da

Postel), sono effettuati controlli a campione rispetto ai formati utilizzati per la conservazione ed ai log generati durante le fasi di conservazione. I risultati dell'audit sono riportati in apposito verbale, nel quale sono indicate anche le azioni necessarie qualora siano riscontrate non conformità. Il suddetto verbale, verrà considerato nel successivo audit.

Torna al sommario

9. MONITORAGGIO E CONTROLLI

9.1. Procedure di monitoraggio

Il responsabile del servizio di conservazione, con riferimento a quanto indicato nel DPCM 3 dicembre 2013, effettua il monitoraggio periodico del SdC, fondamentale ai fini di una corretta ed efficiente erogazione del servizio di conservazione.

In termini generali, il processo di monitoraggio (dettagliatamente descritto nella Procedura di monitoraggio del sistema di conservazione), individua una serie di attività che permettono di monitorare costantemente:

- Le componenti funzionali (infrastruttura) del SdC, tramite apposite sonde;
- Tutte le fasi relative al processo di conservazione, dalla presa in carico del PdV alla sua effettiva conservazione.

Torna al sommario

9.2. Verifica dell'integrità e leggibilità degli archivi

Ai sensi di quanto indicato nel DPCM 3 dicembre 2013, il responsabile del servizio di conservazione deve verificare periodicamente, con cadenza non superiore ai 5 anni, l'integrità e leggibilità dei documenti conservati nel proprio SdC, al fine di garantirne integrità, immodificabilità e leggibilità del contenuto nel breve e lungo periodo. Assicurare la leggibilità ed usabilità dei documenti conservati nel proprio archivio digitale è un requisito fondamentale per chi svolge attività di conservazione digitale.

Rispetto a quanto sopra riportato, Postel provvede a verificare l'integrità dei documenti sia nella fase precedente alla conservazione sia durante il periodo di conservazione a norma.

Nel primo caso, viene verificato che il documento sia rimasto integro durante la fase di trasmissione, dal soggetto produttore al SdC: tale verifica viene effettuata mediante il calcolo dell'impronta del documento trasmesso e successivo confronto della stessa con quella inviata (come metadato) dal soggetto produttore.

Nel secondo caso, Postel verifica periodicamente, almeno ogni 5 anni, l'integrità dei documenti conservati all'interno del proprio sistema.

In termini generali, la verifica d'integrità viene effettuata mediante l'estrazione di un campione di documenti dallo storage di conservazione. Per la selezione del campione, in relazione a tutte le tipologie documentali configurate per ciascun cliente, sono estratti e sottoposti a verifica il 5% del totale dei documenti. Per tutti i documenti così selezionati:

- È calcolata l'impronta (tramite la funzione di hash) di ogni singolo documento e verificato che la stessa corrisponda a quella riportata all'interno del PdA.

Al termine della verifica sono prodotti appositi verbali/ report; in caso di esito negativo, il gruppo Servizi a norma provvede ad aprire un incident con impatto alto ed a valutare la causa che ha generato la corruzione in termini di integrità del documento/ i. A seguito dell'analisi, si procede con le seguenti fasi:

- Recupero della copia di sicurezza del documento danneggiato;
- Creazione di un nuovo PdA con tutti i documenti integri e la copia di sicurezza del documento corrotto;
- Update dei puntamenti al nuovo PdA sul database dei documenti conservati, in modo tale che il processo di esibizione (compresa la masterizzazione) sia sempre possibile.

Per quanto concerne la leggibilità del proprio archivio conservato, Postel ha provveduto all'implementazione di un visualizzatore unico relativo a tutti i formati idonei alla conservazione (riportati nell'allegato 2 del DPCM 3 dicembre 2013) e gestiti all'interno del SdC (opportunatamente aggiornati rispetto agli standard/ normativa vigente). A ciascun documento conservato è associato un metadato di sistema che permette di collegare il documento in oggetto all'ultima versione del visualizzatore.

In termini generali, Postel attesta e garantisce la leggibilità dei propri documenti conservati estraendo, almeno ogni 5 anni, un campione di PdA mediante il seguente criterio:

- PdA con un periodo di conservazione superiore ai 3 anni;
- PdA non sottoposti alla verifica di leggibilità da più di 3 anni

e verificando che i documenti in essi contenuti siano leggibili, tramite l'utilizzo del visualizzatore.

Al termine del processo, sono generati appositi verbali nei quali si attesta l'effettiva leggibilità dei documenti presenti nei PdA estratti a campione.

Torna al sommario

9.3. Soluzioni adottate in caso di anomalie

Postel è impegnata nel continuo perfezionamento ed aggiornamento del SdC, in modo da individuare preventivamente ogni potenziale causa di incidente e provvedere alla sua tempestiva risoluzione, evitando il blocco del sistema o danneggiamento dei documenti in esso contenuti.

Qualora si verificasse un incidente di sistema o processo, le operazioni di ripristino seguono una procedura definita e documentata all'interno del Sistema di Gestione della Sicurezza delle Informazioni (SGSI), certificato ISO 27001:2013.

Per ogni incidente con impatto sugli SLA normativi, è redatto un verbale di evento anomalo, nel quale sono anche indicate le contromisure adottate; il documento è versato all'interno del SdC.

Torna al sommario

9.7 Manuale del Conservatore UNIMATICA

MANUALE DELLA CONSERVAZIONE



SISTEMA DI GESTIONE PER LA QUALITÀ - DQ_07.03

INDICE

EMISSIONE DEL DOCUMENTO **4**

REGISTRO DELLE VERSIONI **5**

A SCOPO E AMBITO DEL DOCUMENTO **6**

A.1 TRATTAMENTO DEI DATI PERSONALI 6

B NORMATIVA E STANDARD DI RIFERIMENTO **8**

B.1 RIFERIMENTI NORMATIVI 8

B.2 STANDARD 10

C GLOSSARIO **11**

D. COMPITI E RESPONSABILITÀ DELLA CONSERVAZIONE **16**

D.1 RUOLI E RESPONSABILITÀ 16

E. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE **20**

E.1 ORGANIGRAMMA 20

E.2 STRUTTURE ORGANIZZATIVE 20

F. OGGETTI SOTTOPOSTI A CONSERVAZIONE **23**

F.1 METADATI 23

F.1.1 Metadati minimi del documento informatico 24

F.1.2 Metadati minimi del documento informatico avente rilevanza tributaria 25

F.1.3 Metadati minimi del fascicolo informatico o dell'aggregazione documentale informatica 29

F.2 FORMATI 31

F.3 STRUTTURA DATI DEL PACCHETTO DI VERSAMENTO 33

F.4 STRUTTURA DATI DEL PACCHETTO DI ARCHIVIAZIONE 38

F.5 STRUTTURA DATI DEL PACCHETTO DI DISTRIBUZIONE 42

G IL PROCESSO DI EROGAZIONE DEL SERVIZIO **44**

G.1 IL PROCESSO DI CONSERVAZIONE 44

G.2 PRODUZIONE DI DUPLICATI E COPIE INFORMATICHE 49

G.3 SCARTO DEI PACCHETTI DI ARCHIVIAZIONE 50

H LA SERVER FARM DI UNIMATICA **51**

H.1 UNISTORAGE – IL SISTEMA PER LA CONSERVAZIONE 52

I PROCEDURE DI GESTIONE E DI EVOLUZONE **54**

I.1 MISURE DI SICUREZZA LOGICA 54
I.1.1 Gestione utenze 54
I.1.2 Gestione sistemi di protezione 55
I.1.3 Gestione degli incidenti di sicurezza 55
I,1.4 Gestione dei backup e Disaster Recovery 56
I.1.5 Gestione dei supporti di memorizzazione 57
I.2 PROCEDURE DI EVOLUZIONE E CHANGE MANAGEMENT 57
J MONITORAGGIO E CONTROLLI 59
J.1 AUDIT INTERNI E VERIFICA DELLINTEGRITÀ DEGLI ARCHIVI 59
J.2 GESTIONE DELLE ANOMALIE 60
J.3 REPORTISTICA DI SERVIZIO 62
APPENDICE A 64

Emissione del documento

Redatto da:	Roberta Rosatone (nome, cognome, qualifica)	Data	14/01/2015
Verificato da:	Andrea Anghinolfi (nome, cognome, qualifica)	Data	19/01/2015
Approvato da:	Silvano Ghedini (nome, cognome, qualifica)	Data	17/02/2015

Registro delle versioni

Revisione	Data	Motivo Revisione	Redatto da	Approvato da
1.0	03/10/2009	Emissione	Andrea Anghinolfi	Silvano Ghedini
2.0	12/02/2010	Aggiornamento funzionalità	Andrea Anghinolfi	Silvano Ghedini
3.0	20/06/2010	Aggiornamento funzionalità	Andrea Anghinolfi	Silvano Ghedini
4.0	28/09/2010	Aggiornamento funzionalità	Andrea Anghinolfi	Silvano Ghedini
5.0	15/10/2010	Aggiornamento funzionalità	Andrea Anghinolfi	Silvano Ghedini
6.0	10/02/2011	Modifica gestione anomalie – Ampliamento funzionalità Unistorage	Andrea Anghinolfi	Silvano Ghedini
7.0	20/05/2011	Aggiornamento composizione societaria Unimatica	Andrea Anghinolfi	Silvano Ghedini
8.0	30/11/2012	Aggiornamento Data Center	Andrea Anghinolfi	Silvano Ghedini
8.1	11/12/2012	Personalizzazioni	Andrea Anghinolfi	Silvano Ghedini
8.2	20/06/2013	Aggiornamento compiti e responsabilità della conservazione	Sabina Falcinelli	Andrea Anghinolfi
8.3	04/07/2013	Aggiornamento normative	Sabina Falcinelli	Andrea Anghinolfi
8.4	05/02/2014	Aggiornamento normative	Sabina Falcinelli	Andrea Anghinolfi
8.5	11/02/2014	Aggiornamento Data Center	Sabina Falcinelli	Andrea Anghinolfi
8.6	05/03/2014	Adeguamento normative	Sabina Falcinelli	Andrea Anghinolfi
8.7	17/02/2015	Adeguamento DPCM 03/12/2013	Roberta Rosatone	Silvano Ghedini

A. Scopo e ambito del documento

Il presente documento costituisce il Manuale della conservazione fornito da UNIMATICA S.p.A. allo scopo di illustrare la struttura del sistema di conservazione descrivendo analiticamente gli oggetti sottoposti a conservazione, il processo di conservazione e le componenti logiche, tecnologiche e fisiche relative al suo funzionamento. Delinea, inoltre, i soggetti che sono coinvolti nelle attività e nei processi di conservazione i quali hanno la responsabilità del sistema.

Il Manuale della conservazione unitamente alla Scheda Cliente predisposta da UNIMATICA S.p.A. al fine di personalizzare il rapporto contrattuale con il Cliente Soggetto produttore (da ora in poi Soggetto produttore) costituiscono parte integrante del contratto di fornitura del servizio e garantiscono ai propri clienti la disponibilità nel tempo di documenti integri, autentici, legalmente validi e facilmente consultabili.

Ogni Soggetto produttore avrà accesso diretto al Manuale della conservazione, disponibile in formato PDF/A, dal portale messo a disposizione da UNIMATICA S.p.A., nell'apposita sezione di Help.

A.1 Trattamento dei dati personali

Ai sensi e per gli effetti dell'articolo 29 del D. Lgs. 30 giugno 2003 n. 196, relativamente e limitatamente ai trattamenti riguardanti la conservazione degli oggetti digitali affidati a UNIMATICA S.p.A., a partire dalla data di sottoscrizione del contratto, il Soggetto produttore affida a UNIMATICA S.p.A. i seguenti compiti e impartisce le seguenti istruzioni per il trattamento dei dati cui UNIMATICA S.p.A. deve attenersi:

1. Il trattamento dei dati in questione sarà da UNIMATICA S.p.A. effettuato esclusivamente per lo svolgimento del servizio di che trattasi, in modo lecito e secondo correttezza, attenendosi alle prescrizioni della normativa sulla protezione dei dati personali nonché alle previsioni della presente delega o successivamente concordate tra le parti; è fatto esplicito divieto di diffondere o comunicare i dati in questione a soggetti che siano estranei all'esecuzione del trattamento.
2. UNIMATICA S.p.A. in particolare dovrà:
   a) effettuare tutte le operazioni in termini di mansioni, definendo regole e modelli di comportamento che assicurino la riservatezza e il rispetto del divieto di comunicazione e diffusione dei dati ai quali si ha accesso;
   b) incaricare per iscritto i soggetti che abbiano le caratteristiche di Responsabili di Sistema e di Amministratori di Sistema, tenerne l'elenco aggiornato a disposizione del Soggetto produttore e fornirne eventualmente copia a semplice richiesta dello stesso;
   c) comunicare prontamente al Soggetto produttore i dati relativi a Società terze cui eventualmente si intendano affidare, in tutto o in parte, le attività in premessa, a seguito di accordi di subappalto e previa autorizzazione del Soggetto produttore stesso, affinché questi provveda alla conseguente Nomina a Responsabile del trattamento dati personali anche nei confronti delle Società subappaltanti;
   d) adottare, se del caso, idonee misure di sicurezza in aggiunta a quelle già previste, in modo da ridurre al minimo i rischi di distruzione e perdita, anche accidentale dei dati/documenti stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

e) informare immediatamente il Soggetto produttore di qualsiasi richiesta o comunicazione da parte dell'Autorità Garante e/o Giudiziaria, per concordare congiuntamente l'evasione delle stesse;
f) collaborare con il Soggetto produttore per l'attuazione delle prescrizioni eventualmente impartite dal Garante;
g) comunicare al Soggetto produttore qualsiasi accadimento che possa compromettere il corretto trattamento dei dati personali.

3. Il trattamento dei dati deve intendersi effettuato sotto la vigilanza del Soggetto produttore il quale, in ogni momento e con congruo preavviso, potrà operare controlli e impartire eventuali ulteriori specifiche istruzioni per il suo svolgimento, nonché chiederne la cessazione se imposta dalla necessità di adempiere a divieti od obblighi di legge, ovvero a provvedimenti dell'Autorità Garante e/o Giudiziaria.

L'autorizzazione al trattamento dei dati personali e sensibili avrà la medesima validità ed efficacia della durata della conservazione legale dei documenti, stabilita dalla normativa.

B. Normativa e standard di riferimento

Il sistema di conservazione sviluppato da UNIMATICA S.p.A. è conforme alla normativa e agli standard elencati nei successivi paragrafi.

B.1 Riferimenti normativi

Notazione abbreviate	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], art. 2215 bis – Documentazione informatica.
L. 7 agosto 1990, n. 241	Legge 7 agosto 1990, n. 241, e successive modificazioni e integrazioni. Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.
D.P.R. 28 dicembre 2000, n. 445	Disposizioni legislative in materia di documentazione amministrativa - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.
AIPA, Circolare 7 maggio 2001, n. 28	Standard, modalità di trasmissione, formato e definizione dei tipi di informazioni minime ed accessorie comunemente scambiate tra le pubbliche amministrazioni e associate ai documenti protocollati e successive revisioni.
D. Lgs. 30 giugno 2003, n. 196 (codice sulla privacy)	D. lgs. 30 giugno 2003, n. 196, e successive modificazioni e integrazioni. Codice in materia di protezione dei dati personali.
DPCM 13 gennaio 2004	Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici.
D. Lgs. 22 gennaio 2004, n. 42 (codice dei beni culturali)	D. lgs. 22 gennaio 2004, n. 42, e successive modificazioni e integrazioni. Codice dei beni culturali e del paesaggio ai sensi dell'articolo 10 della Legge 6 luglio 2002, n. 137.
MEF, Decreto 23 gennaio 2004	Ministero dell'Economia e delle Finanze, decreto 23 gennaio 2004, recante le modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di supporto. Disposizioni in vigore solo per i documenti già conservati al momento dell'entrata in vigore del nuovo decreto ministeriale 27 giugno 2014 Strumenti per favorire la cessione dei crediti certificati.
D. Lgs. 20 febbraio 2004, n. 52	Attuazione della direttiva 2001/115/CE che semplifica ed armonizzale modalità di fatturazione in materia di IVA.
DPR 2 marzo 2004, n. 117	Regolamento concernente la diffusione della carta nazionale dei servizi, a norma dell'articolo 27, comma 8, lettera b), della legge 16 gennaio 2003, n. 3.
DPR 11 febbraio 2005, n. 68	Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della Legge 16 gennaio 2003, n. 3.
Codice dell'amministrazione digitale (CAD)	D. lgs. 7 marzo 2005, n. 82, e successive modificazioni e integrazioni. Codice dell'amministrazione digitale.
Agenzia delle Entrate, Circolare 19 ottobre 2005, n. 45	Circolare esplicativa della fattura elettronica.
Circolare 6 dicembre 2006, n. 36/E	Chiarimenti sull'applicazione del Decreto 23 gennaio, 2004.
DPMC 30 marzo 2009	Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici.

Delibera CNIPA, n. 45 21 maggio 2009	Regole per il riconoscimento e verifica del documento informatico.
DPCM 10 febbraio 2010	Fissazione del termine che autorizza l'autocertificazione circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza.
Determinazione DigitPA n. 69 del 28 luglio 2010	Modifica alla Delibera n. 45/2009.
Provvedimento 25 ottobre 2010	Agenzia delle Entrate: provvedimento attuativo della comunicazione dell'impronta relativa ai documenti informatici rilevanti ai fini tributari.
D. lgs. 30 dicembre 2010, n. 235	Modifiche e integrazioni al decreto legislativo 7 marzo 2005, n. 82 "NUOVO CAD".
DPCM 22 febbraio 2013	Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli art. 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71.
DPCM 3 dicembre 2013	Regole tecniche in materia di sistema di conservazione ai sensi degli artt. 20, 23ter, 43, 44, 44bis e 71 del CAD di cui al Dlgs 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'art. 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.
Decreto MEF 17 giugno 2014	Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005.
il Regolamento UE n. 910/2014	eIDAS Regulation - Identification and trusted services for electronic transactions in the internal market.

B.2 Standard

Sigla	Titolo standard
ISO 14721:2012 OAIS	Open Archival Information System – Sistema informativo aperto per l'archiviazione.
ISO/IEC 27001	Information technology – Security techniques – Information security management systems – Requirements. - Requisiti di un ISMS (Information Security Management System).
ETSI TS 101 533-1 v1.3.1 (2012-04)	Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part. 1: Requirements for Implementation and Management. – Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.
ETSI TR 101 533-2 v1.3.1 (2012-04)	Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part. 2: Guidelines for Assessors. – Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.
UNI 11386:2010	Standard SInCRO – Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.
ISO 15836:2009	Information and documentation – The Dublin Core metadata element set. – Sistema di metadata del Dublin Core

C. Glossario e acronimi

Termine	Definizione
Accesso	Operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici.
Accreditamento	Riconoscimento, da parte dell'Agenzia per l'Italia digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione.
AE	Agenzia dell'Entrate.
AES	Advanced Encryption Standard.
Affidabilità	Caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico.
AgID	Agenzia per l'Italia Digitale.
AIPA	Autorità per l'Informatica nella Pubblica Amministrazione.
AM	Application Management
ANORC	Associazione Nazionale per Operatori e Responsabili per la Conservazione digitale.
AOO	Area Organizzativa Omogenea.
Apertura (formato)	Conforme a specifiche pubbliche, cioè disponibili a chiunque abbia interesse ad utilizzare quel formato.
Archivio	Complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un Soggetto produttore durante lo svolgimento dell'attività.
Archivio informatico	Archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico.
Area organizzativa omogenea	Un insieme di funzioni e di strutture, individuate dall'Amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445.
ASP	Application Service Provider.
Autenticità	Caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico.
Base di dati	Collezione di dati registrati e correlati tra loro.
BGP	Border Gateway Protocol.
CA	Certification Authority.
CAD	Codice dell'Amministrazione Digitale.
CD	Compact Disk.
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione.
Comunità di riferimento	Comunità di riferimento: il sottoinsieme degli utenti in grado di comprendere autonomamente l'informazione archiviata nella forma in cui è conservata e resa disponibile dall'OAIS.
Conservazione	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in

	relazione al modello organizzativo adottato e descritto nel Manuale della conservazione.
CRL	Certificate Revocation List.
DC	Data Center.
Destinatario	Identifica il soggetto/sistema al quale il documento informatico è indirizzato.
Diffusione (formato)	Estensione dell'impiego di uno specifico formato per la formazione e la gestione dei documenti informatici.
D.lgs	Decreto Legislativo.
DM	Decreto Ministeriale.
DMZ	Demilitarized zone
DPCM	Decreto del Presidente del Consiglio dei Ministri.
DPR	Decreto del Presidente della Repubblica.
DR	Disaster Recovery.
Duplicazione dei documenti informatici	Produzione di duplicati informatici.
DVD	Digital Versatile Disk.
Extrainfo	Elemento che consente di introdurre metadati soggettivi relativi all'IdPA liberamente definiti con un proprio schema.
Esibizione	Operazione che consente di visualizzare un documento conservato e di ottenerne copia.
ETSI	European Telecommunications Standards Institut.
Formato	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
FTP	File Transfer Protocol.
Generazione automatica di documento informatico	Formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni.
GB	Gigabyte.
Hash	Funzione matematica univoca ed unidirezionale (cioè non può essere invertita), che trasforma un testo di qualunque lunghezza (input) in testo di lunghezza fissa (output) relativamente limitata.
HSM	Hardware Security Module.
HTMLS	Linguaggio di markup per la strutturazione delle pagine web, e da Ottobre 2014 pubblicato come W3C Recommendation.
IDC	Internet Data Centre.
Java J2EE	Java 2 Enterprise Edition.
JBOSS	Java Bean Open Source Server.
Identificativo univoco	Sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione.
IDS	Intrusion Detection System.
IdPA	Indice del Pacchetto di Archiviazione.
IEC	International Electrotechnical Commission.
Immodificabilità	Caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso.
Impronta	La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash.

Insieme minimo di metadati del documento informatico	Complesso dei metadati, la cui struttura è descritta nell'allegato 5 del DPCM 3 dicembre 2013 Regole tecniche in materia di sistema di conservazione, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta.
Integrità	Insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato.
Interoperabilità	Capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi.
IPS	Intrusion Prevention System.
ISMS	Information Security Management System.
ISO	International Organization for Standardizations.
Leggibilità	Insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti.
Log di sistema	Registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati.
Manuale della conservazione	Strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 del DPCM 3 dicembre 2013 Regole tecniche in materia di sistemi conservazione.
Massimario di selezione	Strumento che consente di coordinare razionalmente lo scarto archivistico (cioè la destinazione al macero) dei documenti prodotti dagli enti pubblici e dagli organi centrali e periferici dello Stato. Il massimario riproduce l'elenco delle partizioni (categorie) e sottopartizioni del titolario con una descrizione più o meno dettagliata delle competenze cui ciascuna partizione si riferisce e della natura dei relativi documenti; indica per ciascuna partizione quali documenti debbano essere conservati permanentemente (e quindi versati dopo quarant'anni dall'esaurimento degli affari nei competenti Archivi di Stato) e quali invece possono essere destinati al macero dopo cinque anni, dopo dieci anni, dopo venti anni, ecc.
MEF	Ministero dell'Economia e della Finanza.
Memorizzazione	Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici.
Metadati	Insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 del presente decreto.
NFS	Network File System.
OAIS	Open Archival Information System.
ORM	Object Relational Mapping.
OTRS	Open-source Ticket Request System.
Pacchetto di archiviazione	Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del presente decreto e secondo le modalità riportate nel Manuale della conservazione.
Pacchetto di distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta.

Pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel Manuale della conservazione.
Pacchetto informativo	Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare.
PdA	Pacchetto di Archiviazione.
PdD	Pacchetto di Distribuzione.
PdV	Pacchetto di Versamento.
Piano della sicurezza del sistema conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza.
Piano di conservazione	Strumento, integrato con il sistema di classificazione per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445.
Portabilità	Facilità con cui i formati possano essere usati su piattaforme diverse, sia dal punto di vista dell'hardware che del software, inteso come sistema operativo. Di fatto è indotta dall'impiego fedele di standard documentati e accessibili.
Presa in carico	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal Manuale della conservazione.
Processo di conservazione	Insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 10 delle regole tecniche del sistema di conservazione.
RAM	Random Access Memory.
Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.
Responsabile della conservazione	Soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 del DPCM Regole tecniche in materia di sistema di conservazione.
Responsabile del trattamento dei dati	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.
Responsabile della sicurezza	Soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza.
Riferimento temporale	Informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento.
RDBMS	Relational DataBase Management System.
RdV	Rapporto di Versamento.
RFA	Responsabile della Funzione Archivistica.
RSC	Responsabile del Servizio di Conservazione.
RSI	Responsabile dei Sistemi Informativi.
RSM	Responsabile della Sviluppo e Manutenzione.
RSSI	Responsabile della Sicurezza dei Sistemi.
RTD	Responsabile per il Trattamento dei Dati personali.
SaaS	Software-as-a-Service.

Scarto	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale.
SFPT	Simple File Transfert Protocol.
SINcRO	Supporto all'interoperabilità nella Conservazione e nel Recupero degli Oggetti Digitali.
Sistema di conservazione	Sistema di conservazione dei documenti informatici di cui all'articolo 44 del CAD.
Sistema di gestione informatica di documenti	Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445; per i privati è il sistema che consente la tenuta di un documento informatico.
SLA	Service Level Agreement.
SOA	Service-Oriented Architecture.
Soggetto 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.
Supporto allo sviluppo (formato)	Modalità con cui si mettono a disposizione le risorse necessarie alla manutenzione e sviluppo del formato e i prodotti informatici che lo gestiscono (organismi preposti alla definizione di specifiche tecniche e standard, società, comunità di sviluppatori, ecc.).
TSM	Tivoli Storage Manager.
Unistorage	Applicazione della società Unimatica per la gestione dei Servizi di Conservazione a Norma dei documenti digitali, sia Autentica che Sostititutiva.
URL	Uniform Resource Locator.
URN	Uniform Resource Name.
USB	Universal Serial Bus.
Utente	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.
VPN	Virtual Private Network.
VTL	Virtual Tape Library.
WS	Web Service.
XML	Extensible Markup Language.
XSD	XML Schema Definition.

D. Compiti e responsabilità della conservazione

Ragione sociale	**UNIMATICA S.p.A.**
Codice Fiscale/Partita IVA:	02098391200
Sede legale ed operativa:	Via Cristoforo Colombo, 21 – 40131 Bologna

UNIMATICA S.p.A. utilizza personale altamente specializzato e formato sulle problematiche legate alla conservazione e all'archiviazione digitale.

Tale personale è inoltre costantemente aggiornato sulle nuove normative e sugli aspetti tecnologici, attraverso la consultazione della documentazione, messa a disposizione dall'azienda, e la partecipazione ad appositi corsi di approfondimento, interni ed esterni.

L'impegno e l'attenzione di tutta l'azienda sulla tematica specifica ed i risultati raggiunti nel corso degli anni di attività hanno permesso ad UNIMATICA S.p.A. di ottenere l'iscrizione quale socio sostenitore presso l'associazione ANORC (Associazione Nazionale per Operatori e Responsabili della Conservazione Digitale).

D.1 Ruoli e responsabilità

L'art. 6, c.1 del DPCM 3 dicembre 2013 individua all'interno della struttura organizzativa del sistema di conservazione i ruoli di:

- Soggetto produttore,
- Responsabile della Conservazione,
- Utente.

Il **Soggetto produttore** è la persona fisica o giuridica che permette la produzione dei Pacchetti di Versamento[1] ed è il responsabile del trasferimento di questi dal proprio sistema di gestione documentale al sistema di conservazione UNIMATICA S.p.A. Per l'intera durata del contratto, il Soggetto produttore resterà il titolare degli oggetti documentali versati.

Il **Responsabile della Conservazione** viene nominato dal Soggetto produttore. In accordo con il Responsabile del trattamento dei dati personali, con il Responsabile della sicurezza e con il Responsabile dei sistemi informativi definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia di documenti da conservare, in conformità alla normativa vigente. Il Responsabile della conservazione, tramite specifico contratto, affida al Responsabile del servizio di conservazione di UNIMATICA S.p.A. le attività di gestione e la supervisione dei processi del sistema di conservazione. In particolare, il Responsabile del servizio di conservazione si occuperà di:

- definire le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente;

[1] Traduzione di Submission Information Package dal Modello OAIS Open Archival Information Standard che individua nel sistema di archiviazione tre diversi tipi di aggregazioni documentali: Submission Information Package (SIP), Archival Information Package (AIP) e Dissemination Information Package (DIP).

- gestire il processo di conservazione e di garantirne nel tempo la conformità alla normativa vigente;
- generare il Rapporto di Versamento, secondo le modalità previste dal Manuale della conservazione;
- generare e sottoscrivere il Pacchetto[2] di Distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal Manuale della conservazione;
- effettuare il monitoraggio della corretta funzionalità del sistema di conservazione;
- assicurare la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
- al fine di garantire la conservazione e l'accesso ai documenti informatici, adottare misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; occuparsi, inoltre di adottare analoghe misure con riguardo all'obsolescenza dei formati;
- provvedere alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal Manuale della conservazione;
- adottare le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12 delle Regole tecniche in materia di sistemi di conservazione;
- assicurare la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
- assicurare agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
- provvedere, per gli organi giudiziari e amministrativi dello Stato, al versamento dei documenti conservati all'archivio centrale dello Stato e agli archivi di Stato secondo quanto previsto dalle norme vigenti;
- predisporre il Manuale della conservazione di cui all'art. 8 delle Regole tecniche in materia di sistemi di conservazione e curare l'aggiornamento periodico di questo in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Il **Responsabile del servizio di conservazione**, quindi, si occupa di definire e attuare le politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione e di definire le caratteristiche e i requisiti del sistema di conservazione in conformità alla normativa vigente. Garantisce una corretta erogazione del servizio di conservazione all'ente produttore e gestisce le convenzioni, definisce gli aspetti tecnico-operativi e la validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.

Nominativo	Periodo nel ruolo
Silvano Ghedini	Dal 2004 ad oggi

Silvano Ghedini, Responsabile del servizio di conservazione di UNIMATICA S.p.A., nello svolgere le attività del processo di conservazione, ha delegato l'esercizio complessivo di queste a:

[2] Traduzione di Dissemination Information Package dal Modello OAIS Open Archival Information Standard che individua nel sistema di archiviazione tre diversi tipi di aggregazioni documentali: Submission Information Package (SIP), Archival Information Package (AIP) e Dissemination Information Package (DIP).

Nominativo Delegato Responsabile del Servizio di conservazione	Periodo di delega
Andrea Anghinolfi	01/2009 ad oggi

L'Utente è la persona, l'ente o il sistema che interagisce con i servizi del sistema di conservazione allo scopo di usufruire degli oggetti conservati di suo interesse. Gli Utenti costituiscono la comunità di riferimento individuata nel modello OAIS, sulla base della quale il sistema di conservazione struttura le modalità di esibizione.

All'interno della struttura organizzativa del sistema di conservazione, così come specificato nella circolare dell'Agenzia per l'Italia Digitale n. 65 del 10 aprile 2014, in particolare nel documento "Profili professionali", si individuano le seguenti figure responsabili coinvolte nel servizio:

Responsabile sicurezza dei sistemi per la conservazione. Si occupa di monitorare e rispettare i requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza. In caso di eventuali difformità si occupa di segnalarle al Responsabile del servizio di conservazione e, quindi, individua e pianifica le necessarie azioni correttive.

Nominativo	Periodo nel ruolo
Massimo Ortensi	Dal 2001 ad oggi

Responsabile della funzione archivistica di conservazione. Si occupa di definire e gestire il processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato. Definisce, inoltre, il set di metadati di conservazione dei documenti e dei fascicoli informatici. Monitora il processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema. Collabora con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.

Nominativo	Periodo nel ruolo
Sabina Falcinelli	Dal 2012 ad oggi

Responsabile del trattamento dei dati personali. Si occupa di garantire il rispetto delle vigenti disposizioni in materia di trattamento dei dati personali. Garantisce, inoltre che il trattamento dei dati affidati dai Soggetti produttore avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.

Nominativo	Periodo nel ruolo
Silvano Ghedini	Dal 2004 ad oggi

Responsabile dei sistemi informativi per la conservazione. Si occupa di gestire l'esercizio delle componenti hardware e software del sistema di conservazione. E monitora il mantenimento dei livelli di servizio (SLA) concordati con il Soggetto produttore. Segnala le eventuali difformità degli SLA al Responsabile del servizio di conservazione e individua e pianifica le necessarie azioni correttive. Si occupa di pianificazione lo sviluppo delle infrastrutture tecnologiche del sistema di conservazione e verifica i livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.

Nominativo	Periodo nel ruolo
Andrea Anghinolfi	Dal 2008 ad oggi

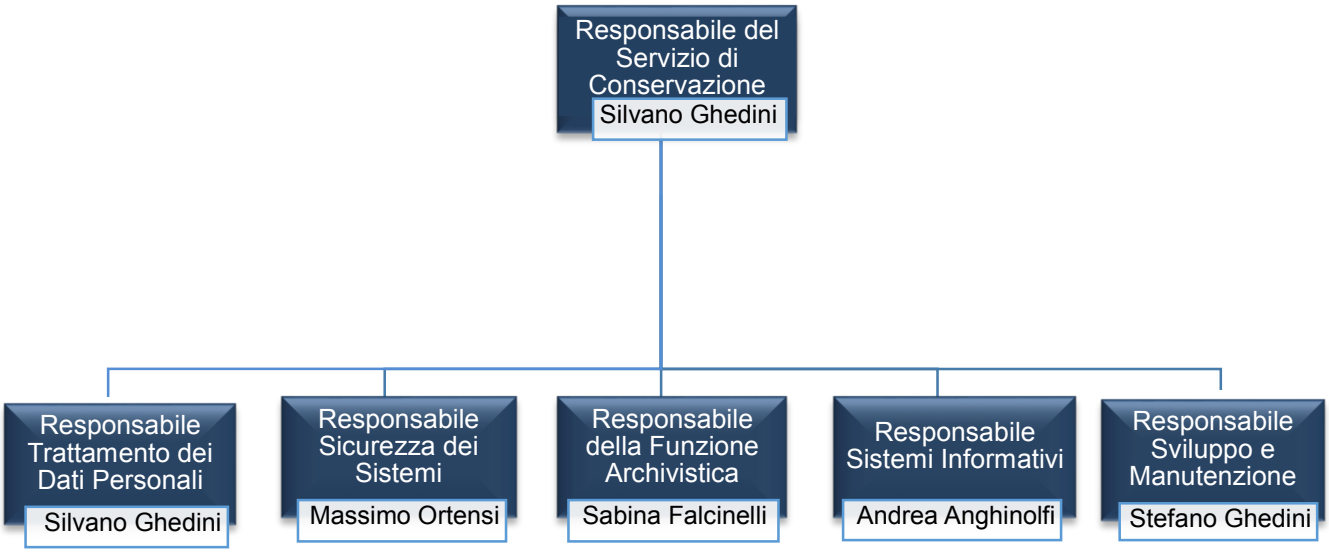
Responsabile sviluppo e manutenzione del sistema di conservazione. Si occupa di coordinare lo sviluppo e la manutenzione delle componenti hardware e software del sistema di conservazione. Pianifica e monitora i progetti di sviluppo del sistema di conservazione. Monitora inoltre gli SLA relativi alla manutenzione del sistema di conservazione. Si occupa di interfacciarsi con il Soggetto produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche. Gestisce, inoltre lo sviluppo di siti web e portali connessi al servizio di conservazione.

Nominativo	Periodo nel ruolo
Stefano Ghedini	Dal 2008 ad oggi

E. Struttura organizzativa per il servizio di conservazione

Il presente capitolo ha lo scopo di illustrare la struttura organizzativa del settore conservazione di UNIMATICA S.p.A. L' espletamento di un processo di conservazione prevede una serie di complesse attività, pertanto la società si avvale di personale altamente qualificato e con esperienza decennale. Si riporta di seguito l'organigramma della struttura organizzativa e una sintetica descrizione[3] delle funzioni e delle responsabilità che intervengono nel processo di conservazione.

E.1 Organigramma



E.2 Strutture organizzative

Nel presente paragrafo vengono descritte sinteticamente le fasi principali del processo di conservazione e le attività di gestione dei sistemi informativi, individuando per ciascuna di queste le figure che ne assumono le responsabilità.

Attività proprie di ciascun contratto di servizio			
Fase	Attività	Descrizione	Responsabilità
1	Attivazione del servizio di conservazione (a seguito della sottoscrizione del contratto).	Il Soggetto produttore invia una richiesta di attivazione del servizio che avviene in seguito alla compilazione del modulo "Change Request" dove vengono dichiarati dettagli degli oggetti da conservare, come: dimensioni, frequenza invio, ecc.	RSC RTD RFA RSM

[3] La descrizione dettagliata del processo di conservazione è riportata nel capitolo G.

2	Acquisizione, verifica e gestione dei Pacchetti di versamento e generazione del Rapporto di versamento.	Sui PdV vengono effettuate verifiche circa l'identificazione certa del soggetto, la firma digitale, formati e metadati. In caso di verifiche andate a buon fine viene generato il RdV, altrimenti viene generata la Comunicazione delle anomalie.	RSC RFA
3	Preparazione e gestione dei Pacchetti di archiviazione[4].	Gli oggetti versati vengono trasformati in PdA, i quali dovranno contenere, oltre agli oggetti da conservare, l'IdPA[5] formato secondo le regole dello standard SInCRO. L'IdPA viene sottoscritto con firma digitale dal RSC e viene marcato temporalmente.	RSC RFA
4	Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta.	I PdD, vengono creati in base alle richieste dell'Utente. Possono essere visualizzati mediante WS o, se richiesto, tramite memorizzazione su supporto ottico.	RSC RFA RTD
5	Scarto dei pacchetti di archiviazione	Sette mesi prima della scadenza del contratto UNIMATICA contatta il Soggetto produttore il quale in caso di rescissione del contratto comunicherà in forma scritta la decisione. UNIMATICA eliminerà fisicamente i PdA. Per i PdA provenienti da enti pubblici o da archivi privati per i quali è stato dichiarato l'interesse culturale si terrà conto dei massimari di scarto di questi e della decisione ultima della Soprintendenza archivistica.	RSC RTD
6	Chiusura del servizio di conservazione (al termine di un contratto)	Il Soggetto produttore comunicherà ad UNIMATICA, nei tempi previsti dal manuale, la rescissione del contratto.	RSC RTD

Attività proprie di gestione dei sistemi informativi			
Fase	Attività	Descrizione	Responsabilità
1	Conduzione e manutenzione del sistema di conservazione	Le attività di manutenzione vengono svolte sia sui processi che sulle strutture hardware e software e viene condotta una quotidiana verifica delle attività sulle infrastrutture parallelamente ad una pianificazione delle eventuali procedure	RSM RSSI

[4] Traduzione di Archival Information Package dal Modello OAIS Open Archival Information Standard che individua nel sistema di archiviazione tre diversi tipi di Pacchetti: Submission Information Package (SIP), Archival Information Package (AIP) e Dissemination Information Package (DIP).
[5] Indice del pacchetto di archiviazione.

		straordinarie da condurre in caso di anomalie.	
2	Monitoraggio del sistema di conservazione	Viene effettuato il monitoraggio del sistema di Log che consente la registrazione degli accessi e degli eventi (operazioni). Tra le attività di monitoraggio rientrano anche la verifica dell'integrità degli archivi e la gestione delle anomalie.	RSC RFA RSSI
3	Change management	Vengono definite politiche, priorità e tempistiche dell'adeguamento all'evoluzione tecnologica affinché il sistema di conservazione possa garantire nel tempo integrità, disponibilità e sicurezza.	RFA RSI
4	Verifica periodica di conformità a normativa e standard di riferimento	La conformità a normativa e standard è costantemente monitorata ed eventualmente aggiornata grazie al lavoro di supervisione svolto dal RSC.	RSC RSSI

Legenda	
RSC	Responsabile del Servizio di Conservazione
RSSI	Responsabile Sicurezza dei Sistemi Informativi per la Conservazione
RFA	Responsabile Funzione Archivistica per la Conservazione
RTD	Responsabile Trattamento Dati Personali
RSI	Responsabile Sistemi Informativi per la Conservazione
RSM	Responsabile Sviluppo e Manutenzione del Sistema di Conservazione

F. Oggetti sottoposti a conservazione

UNIMATICA S.p.A. mediante UniStorage, il prodotto applicativo descritto nel capitolo H, utilizzato per la gestione del processo di conservazione e sviluppato integralmente dalla società, è in grado di gestire diverse tipologie di documenti, relativi a diversi ambiti applicativi, quali:

- Documenti e disposizioni in ingresso e in uscita
- Documenti di sportello bancario
- Contratti ed allegati
- Fatture attive e Fatture passive
- Libri e registri sociali
- Libri e registri contabili
- Libri e registri assicurativi
- Libretto unico del lavoro (LUL)
- Assegni
- Mandati di pagamento e Reversali d'incasso
- Ricevute e quietanze di pagamento
- Delibere, determine, atti e provvedimenti
- Referti, Cartelle cliniche, Immagini diagnostiche

In accordo con il Soggetto produttore, UNIMATICA S.p.A. si riserva la facoltà di accettare anche documenti non menzionati nel suddetto elenco. L'indicazione di tali documenti, compresa la gestione di questi, verranno indicati nella Scheda Cliente allegata al Manuale della conservazione e al contratto stipulato con il Soggetto produttore.

UNIMATICA S.p.A. accetta e conserva solo documenti digitali. Il sistema di conservazione permette l'acquisizione sia di documenti firmati digitalmente, sia di documenti non firmati. Entrambe le tipologie subiscono il medesimo trattamento eccezion fatta in fase di controllo[6] quando tra le verifiche non verrà effettuata quella sulla firma per i documenti dei quali è stato dichiarato non essere firmati. Con l'ausilio del Responsabile del servizio di conservazione, è il Soggetto produttore a definire nella Scheda cliente allegata al Manuale della conservazione le modalità di trattamento dei documenti firmati o non firmati.

F.1 Metadati

Come previsto dall'art. 3, c. 1 del Decreto della Presidenza del Consiglio dei Ministri 3 dicembre 2013 Regole tecniche in materia di sistema di conservazione, il sistema di conservazione assicura dalla presa in carico dal Soggetto produttore fino all'eventuale scarto, la conservazione tramite l'adozione di regole, procedure e tecnologie degli oggetti in esso conservati, garantendone oltre all'autenticità, all'integrità, all'affidabilità e alla leggibilità anche la reperibilità. Al fine di rendere agevole ed efficiente la ricerca di un documento, di un fascicolo, o di un'aggregazione documentale informatica conservati è necessario individuare dei metadati, ovvero un insieme di dati da associare all'oggetto informatico o al fascicolo informatico che ne descrivano il contenuto e lo identifichino all'interno del sistema.
UNIMATICA S.p.A., in piena conformità con le Regole tecniche, individua un insieme minimo di metadati.

[6] Le verifiche effettuate sui documenti ricevuti sono descritte al capitolo G, Fase 2.

In particolare:

- un set di metadati minimi del documento informatico,
- un set di metadati minimi del documento informatico avente rilevanza tributaria,
- un set di metadati minimi del fascicolo informatico o dell'aggregazione documentale informatica.

F.1.1 Metadati minimi del documento informatico

Di seguito vengono elencati i metadati minimi del documento informatico:

1. **Identificativo:** è una sequenza di max. 20 caratteri alfanumerici associati in maniera univoca e persistente al documento informatico così da garantirne l'identificazione. Il Dublin Core Metadata Element Set[7] raccomanda di identificare la risorsa per mezzo di una sequenza di caratteri alfabetici o numerici secondo un sistema di identificazione formalmente definito. Esempi di tali sistemi di identificazione includono l'Uniform Resource Identifier (URL) (incluso l'Uniform Resource Locator (URN)), il Digital Object Identifier (DOI) e l'International Standard Book Number (ISBN)**.**

Valori ammessi	Tipo dato
Come da Sistema di identificazione formalmente definito	Alfanumerico 20 caratteri

2. **Data di chiusura:** indica la data di creazione del documento informatico, ovvero il momento in cui tale documento è reso immodificabile.

Valori ammessi	Tipo dato
Data	Formato yyyy/mm/dd

3. **Oggetto:** riassume sinteticamente il contenuto del documento informatico e può contenere un riassunto analitico, un indice o una rappresentazione grafica del contenuto.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

4. **Soggetto produttore:** colui che ha la responsabilità della produzione del documento informatico.

Valori ammessi	Tipo dato
Nome: testo libero	Alfanumerico 40 caratteri
Cognome: testo libero	Alfanumerico 40 caratteri

[7] Il Dublin Core Metadata si propone come uno standard di descrizione delle risorse in formato elettronico ed è costituito da 15 elementi descrittivi: titolo, autore o creatore, soggetto e parole chiave, descrizione, editore, altro responsabile, data, tipo di risorsa, formato, identificatore della risorsa, lingua, fonte, relazione, copertura e diritti.

Codice fiscale: codice fiscale	Alfanumerico 16 caratteri

5. **Destinatario:** colui che ha la responsabilità della ricezione del documento.

Valori ammessi	Tipo dato
Nome: testo libero	Alfanumerico 40 caratteri
Cognome: testo libero	Alfanumerico 40 caratteri
Codice fiscale: codice fiscale (Obbligatorio, se disponibile)	Alfanumerico 16 caratteri

Nella Scheda Cliente predisposta da UNIMATICA S.p.A. allegata al Manuale della conservazione e al contratto, è possibile personalizzare i set di metadati in base alle esigenze del Soggetto produttore e alle diverse tipologie documentali conservate. In un'apposita tabella il cliente specificherà i metadati di proprio interesse.

F.1.2 Metadati minimi del documento informatico aventi rilevanza tributaria

I metadati minimi dei documenti informatici con rilevanza tributaria, laddove tali informazioni siano obbligatoriamente previste[8], sono i seguenti:

- per i documenti fiscali di tipo Fattura i metadati obbligatori per il ciclo attivo sono:

1. **Partita IVA emittente:** partita iva dell'emittente.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

2. **Numero documento:** stringa che identifica il numero della fattura.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico255 caratteri

[8] Rif. Art. 3 del Decreto del Ministero Economia e Finanza del 17 giugno 2014 - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005.

3. **Data documento**

Valori ammessi	Tipo dato
Data	Formato yyyy/mm/dd hh:mm:ss

4. **Partita IVA cliente:** partita IVA del cliente.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico255 caratteri

5. **Codice fiscale cliente:** codice fiscale del cliente.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico255 caratteri

6. **Nome Cliente:** nome cliente della fattura in caso di persona fisica.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico255 caratteri

7. **Cognome Cliente:** cognome cliente della fattura in caso di persona fisica.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico255 caratteri

8. **Denominazione:** denominazione in caso di persona giuridica.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico255 caratteri

9. **Valuta:** valuta importo fatture “EUR”.

Valori ammessi	Tipo dato
Valore fisso “EUR”	Alfanumerico 255 caratteri

10. **Totale fattura:** importo totale della fattura.

Valori aammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

UNIMATICA S.p.A., nella Scheda Cliente allegata al Manuale della conservazione, predispone anche i seguenti metadati facoltativi:

- **Totale tasse**

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

- **Data scadenza:** data scadenza documento.

Valori ammessi	Tipo dato
Data	Formato yyyy/mm/dd hh:mm:ss

- **Codice cliente**

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

- **ID documento_sistema:** identificativo del cliente.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

- Per i documenti fiscali di tipo Fattura i metadati obbligatori per il ciclo passivo sono:

1. **Partita IVA emittente:** partita iva dell'emittente.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

2. **Numero documento:** stringa che identifica il numero della fattura.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

3. **Data documento**

Valori ammessi	Tipo dato
Data	Formato yyyy/mm/dd hh:mm:ss

4. **Partita IVA fornitore:** partita IVA del fornitore.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

5. **Codice fiscale fornitore:** codice fiscale del fornitore.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

6. **Nome fornitore:** nome fornitore della fattura in caso di persona fisica.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

7. **Cognome fornitore:** cognome fornitore della fattura in caso di persona fisica.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

8. **Denominazione:** denominazione in caso di persona giuridica.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

9. **Valuta:** valuta importo fatture, valore fisso “EUR”.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

10. **Totale fattura:** importo totale della fattura.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

UNIMATICA S.p.A., nella Scheda Cliente allegata al Manuale della conservazione predispone anche i seguenti metadati facoltativi:

- **Totale tasse**

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

- **Data scadenza:** data scadenza documento.

Valori ammessi	Tipo dato
Data	Data yyyy/mm/dd hh:mm:ss

- **Codice cliente**

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

- **ID documento_sistema:** identificativo del cliente.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

Si riporta di seguito un estratto di xml:

```
<Profilo>
    <Metadato Chiave="Categoria">REGISTRO IVA ACQUISTI</Metadato>
    <Metadato Chiave="Azienda">Anagrafica</Metadato>
    <Metadato Chiave="C.F.">c.f. </Metadato>
    <Metadato Chiave="Partita IVA">p.iva</Metadato>
    <Metadato Chiave="Oggetto">Oggetto del documento</Metadato>
</Profilo>
```

Nei casi in cui tali metadati non siano ricavabili da particolari tipologie di documenti informatici aventi rilevanza tributaria, nell'apposita Scheda Cliente allegata al Manuale della conservazione il Soggetto produttore potrà indicare i metadati individuabili dal documento come specificato nell' all'art. 3, comma1, lettera b) del Decreto del 17 giugno 2014 - Min. Economia e Finanze, Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005.

F.1.3 Metadati minimi del fascicolo informatico o dell'aggregazione documentale informatica

I metadati minimi dei fascicoli o delle aggregazioni documentali per i versamenti effettuati dalle pubbliche amministrazioni sono:

1. **Identificativo**: Identificativo univoco e persistente è una sequenza di caratteri alfanumerici associata in modo univoco e permanente al fascicolo o aggregazione documentale informatica in modo da consentirne l'identificazione. Dublin Core raccomanda di identificare il documento per mezzo di una sequenza di caratteri alfabetici o numerici secondo un sistema di identificazione formalmente definito. Esempi di tali sistemi di identificazione includono l'Uniform Resource Identifier (URI), il Digital Object Identifier (DOI) e l'International Standard Book Number (ISBN).

Valori ammessi	Tipo dato
Come da sistema di identificazione formalmente definito	Alfanumerico 20 caratteri

2. **Amministrazione titolare**: Amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo.

Valori ammessi	Tipo dato
Vedi specifiche Codice IPA	Codice IPA

3. **Amministrazioni partecipanti**: Amministrazioni che partecipano all'Iter del procedimento.

Valori ammessi	Tipo dato
Vedi specifiche Codice IPA	Codice IPA

4. **Responsabile del procedimento**:

Valori ammessi	Tipo dato
Nome: testo libero	Alfanumerico 40 caratteri
Cognome: testo libero	Alfanumerico 40 caratteri
Codice fiscale: codice fiscale	Alfanumerico 16 caratteri

5. **Oggetto**: Oggetto, metadato funzionale a riassumere brevemente il contenuto del documento o comunque a chiarirne la natura. Dublin Core prevede l'analoga proprietà "Description" che può includere ma non è limitata solo a: un riassunto analitico, un indice, un riferimento al contenuto di una rappresentazione grafica o un testo libero del contenuto.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

6. **Documento**: Elenco degli identificativi dei documenti contenuti nel fascicolo che ne consentono la reperibilità.

Valori ammessi	Tipo dato
Identificativo del documento così come definito agli articoli 9 e 19 delle regole tecniche per il protocollo informatico di cui al D.P.C.M. 31 ottobre 2000 e descritti nella Circolare AIPA del 7 maggio 2001, n. 28.	Alfanumerico 100 caratteri

I Metadati minimi dei fascicoli o delle aggregazioni documentali informatiche per i versamenti effettuati dai soggetti privati sono:

1. **Denominazione cliente**: Ragione sociale del Soggetto produttore.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

2. **Identificativo cliente**: sequenza alfanumerica di caratteri associati in maniera univoca e permanente al fascicolo o all'aggregazione documentale informatica in modo da consentirne l'identificazione.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

3. **Oggetto:** Oggetto del fascicolo o dell'aggregazione documentale informatica.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

4. **Data**: Data di presa in carico da parte di UNMATICA S.p.A. del fascicolo o dell'aggregazione documentale informatica.

Valori ammessi	Tipo dato
Data	Formato yyyy/mm/dd hh:mm:ss

5. **Partita IVA**: Partita IVA del Soggetto produttore.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

6. Codice fiscale cliente: Codice fiscale del Soggetto produttore.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

F.2 Formati

UNIMATICA S.p.A., in conformità all'allegato 2 al Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 Regole tecniche in materia di sistema di conservazione, accetta formati che maggiormente garantiscano i principi di interoperabilità tra sistemi di conservazione. Al fine di assicurare una corretta gestione degli oggetti conservati è opportuno che i formati assicurino le seguenti caratteristiche[9]:

- apertura,
- sicurezza,
- portabilità,
- funzionalità,
- supporto allo sviluppo,
- diffusione.

[9] Per maggiori dettagli circa le spiegazioni di tali caratteristiche fare riferimento all'allegato 2 al DPCM 3 dicembre 2013 Regole tecniche in materia di conservazione.

Di seguito viene riportato un breve elenco dei formati più diffusi accettati da UNIMATICA S.p.A. e i relativi dettagli esplicativi.

Formato	Estensione	Tipo MIME	Formato aperto	Specifiche tecniche	Ultima Versione
Portable Document Format	.pdf	application/pdf	si	Pubbliche	1.7
Joint Photographic Experts Group	.jpg .jpeg	image/jpeg	si	Pubbliche	2009
Extensible Markup Language	.xml	application/xml, text/xml	si	Pubbliche	
Office Open XML (OOXML)	.docx .xlsx .pptx		si	Pubbliche	1.1
Tagged Image File Format	.tiff	image/tiff	no	Pubbliche	TIFF 6.0 del 1992 TIFF Supplement 2 del 2002
Open Document Format	.ods .odp .odg .odb	application/vnd.oasis .opendocument.text	si	Pubbliche	1.0
Zip	.zip	application/zip	si	Pubbliche	3.0
Digital Imaging and Communications in Medicine	.dicom	image/x-dicom		Pubbliche	
Health Level-7	.hl7	application/edi-hl7			

In accordo con il Soggetto produttore, UNIMATICA S.p.A. si riserva la facoltà di accettare anche formati non menzionati nell'elenco delle Regole Tecniche ma che il Soggetto produttore ritiene di dover conservare. L'indicazione di tali formati, compresa la gestione di questi, verranno indicati nella Scheda Cliente allegata al Manuale della conservazione e al contratto stipulato con il Soggetto produttore.

Alla ricezione del documento il sistema, attraverso l'uso di una libreria WAZFORMAT, la cui procedura utilizzerà un metodo di indagine diretta con tecniche euristiche, riconosce il formato controllando il valore descritto nel magic number.
Questo passaggio permette di associare il formato al documento per garantirne la corretta visualizzazione e quindi leggibilità utilizzando gli opportuni i visualizzatori.

F.3 Struttura dati del Pacchetto di versamento

UNIMATICA S.p.A. mediante il prodotto applicativo UniStorage, con la supervisione del Responsabile del servizio di conservazione permette un duplice iter per la ricezione dei Pacchetti di Versamento: ricezione dei file tramite canale File Transfert Protocol e ricezione tramite sistema Web service.

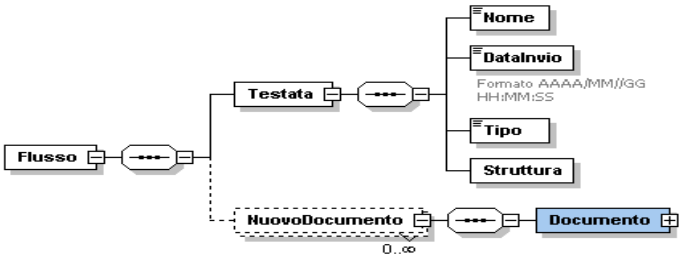
- La ricezione mediante File Transfert Protocol prevede l'upload del Pacchetto di versamento composto da un file indice e da un insieme di file, in formato .zip.

Si riporta di seguito lo schema xml della struttura dati di un Pacchetto di versamento

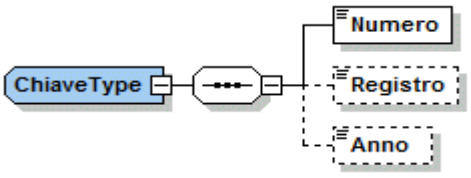
```
<?xml version="1.0" encoding="utf-8"?>
<Flusso>
  <Testata>
    <Nome>xxxxxxxxxxxxxxx</Nome>
    <DataInvio>yyyy/mm/dd 00.00.00</DataInvio>
    <Tipo>xxxxxxxxxxxxxxxx</Tipo>
    <Struttura>xxxxx</Struttura>
  </Testata>
  <NuovoDocumento>
    <Documento>
      <Chiave>
        <Numero>XXXXXXXXXXXXXXXXXXXXXXXX</Numero>
        <Registro />
        <Anno />
      </Chiave>
      <Proprieta>
        <TipoDocumento>xxxxxx</TipoDocumento>
        <Data>yyyy/mm/dd 00:00:00</Data>
        <IdSistemaMittente>xxxxxxxxxxxxxxxxxx</IdSistemaMittente>
      </Proprieta>
      <File>
        <Hash Algoritmo="SHA1" Codifica="B64">xxxxxxxxxxxxxx</Hash>
        <Path>XXXXXXXXXXXXXXXXXXXXXXX.pdf</Path>
      </File>
      <Profilo>
        <Metadato Chiave="COD_SOC">xx</Metadato>
        <Metadato Chiave="COD_UO">xxxx</Metadato>
        <Metadato Chiave="COD_SPORTELLO">xxxx</Metadato>
        <Metadato Chiave="WORKSTATION">xxxxxx</Metadato>
        <Metadato Chiave="OPERATORE">xxxxxxxx</Metadato>
        <Metadato Chiave="COD_RAPPORTO">xxxxxxxx</Metadato>
        <Metadato Chiave="NDG">xxxxxxxx</Metadato>
        <Metadato Chiave="NOME">xxxxxxxx</Metadato>
        <Metadato Chiave="COGNOME">xxxxxxxx</Metadato>
        <Metadato Chiave="IMPORTO">xxxxxx</Metadato>
        <Metadato Chiave="COD_ADESIONE">xxx</Metadato>
        <Metadato Chiave="FG_ANNULLO">x</Metadato>
        <Metadato Chiave="EMAIL_CLIENTE">xxxxxx</Metadato>
        <Metadato Chiave="TRANSAZIONE">xxxxx</Metadato>
```

```
        <Metadato Chiave="DATA_CONTABILE">yyyy/mm/dd
00:00:00</Metadato>
        <Metadato Chiave="DATA_CREAZIONE">yyyy/mm/dd
00:00:00</Metadato>
        <Metadato Chiave="DATA_FIRMA">yyyy/mm/dd
00:00:00</Metadato>
        <Metadato Chiave="VERSIONE">x</Metadato>
      </Profilo>
      <Referenze />
    </Documento>
  </NuovoDocumento>
</Flusso>
```

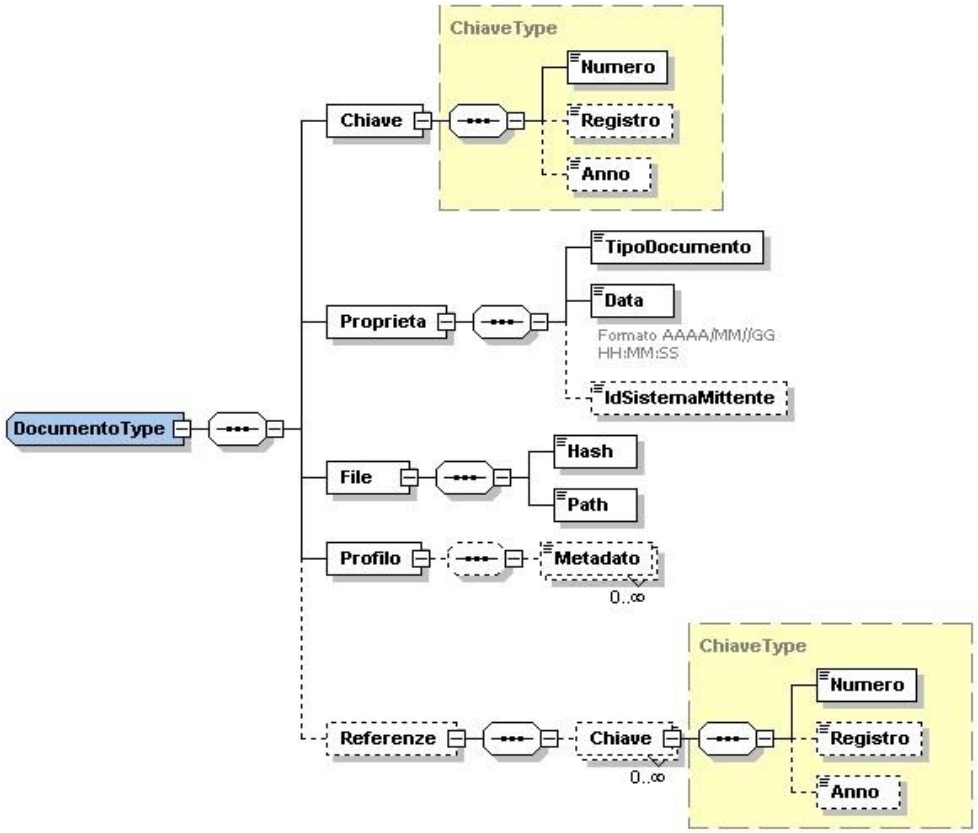
Dove il nodo *Flusso* contiene un solo nodo Testata e una serie di nodi di tipo NuovoDocumento,



i nodi di tipo *Chiave* forniscono un identificativo univoco dei documenti,



il nodo *Documento* contiene tutti gli elementi per la sua descrizione.



Per maggiori dettagli circa la struttura dei Pacchetti di versamento, fare riferimento al documento FlussiConservazione_ver 1.7

- La ricezione tramite Sistema Web Service è possibile da qualsiasi piattaforma che permetta di eseguire e ricevere chiamate Web Service conformi allo standard WS-I Basic Profile 1.0. Con questo servizio il sistema di conservazione riceve singoli documenti ed eventuali allegati, ne verifica la firma digitale se presente e ne gestisce la conservazione autentica.

Si riporta di seguito lo schema xml della struttura dati di un Pacchetto di versamento

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
       <soapenv:Body>
              <ConsegnaAnticipata
xmlns="http://anticipati.versamenti.service.unirepo.unimaticaspa.it/">
                     <Documento xmlns="">
                            <chiave>
                                   <proprieta>
                                          <chiave>NUMERO</chiave>
                                          <valore>xx</valore>
                                   </proprieta>
                                   <proprieta>
                                          <chiave>ANNO</chiave>
                                          <valore>xxxx</valore>
```

```
                        </proprieta>
                        <proprieta>
                              <chiave>CLASSIFICAZIONE</chiave>
                              <valore>xxxxxx</valore>
                        </proprieta>
                  </chiave>

                  <allegati>
                        <proprieta>
                              <chiave>tipo_allegato</chiave>
                              <valore>GENERICO</valore>
                        </proprieta>
                        <proprieta>
                              <chiave>chiave_allegato</chiave>
                              <valore>prova_allegato_1</valore>
                        </proprieta>
                        <versioneOriginale>
                              <proprieta>
                                    <chiave>formato_versione</chiave>
                                    <valore>xml firmato tipo1</valore>
                              </proprieta>
                                    <parti>
                                    <proprieta>

<chiave>formato_parte</chiave>
                                                <valore>xxx</valore>
                                    </proprieta>
                                    <proprieta>
                                          <chiave>numero_parte</chiave>
                                          <valore>x</valore>
                                    </proprieta>
                                    <files>
                                          <dati></dati>
                                                <proprieta>

<chiave>ordinePresentazione</chiave>
                                                      <valore>x</valore>
                                                </proprieta>
                                          <proprieta>
                                                <chiave>formato_file</chiave>
                                                <valore>xxx</valore>
                                                </proprieta>
                                                <proprieta>

<chiave>nomeFile</chiave>

<valore>ConsegnaAnticipataAllegatoFileAllegato.pdf.p7m</valore>
                                                </proprieta>
                                          <proprieta>

<chiave>id_cliente</chiave>

<valore>Test_Consegna_Anticipata_Allegato_ALLEGATO</valore>
                                                </proprieta>
                                    </files>
                                    </parti>
                        </versioneOriginale>
                  </allegati>


                  <proprieta>
                        <chiave>tipo_documento</chiave>
                        <valore>xxxxxxxx</valore>
                  </proprieta>
```

```
                        <proprieta>
                              <chiave>forza_conservazione</chiave>
                              <valore>xxxxx</valore>
                        </proprieta>
                        <proprieta>
                              <chiave>forza_accettazione</chiave>
                              <valore>xxxxx</valore>
                        </proprieta>
                        <profiloArchivistico>
                              <proprieta>
                                    <chiave>Contraente</chiave>
                                    <valore>xxxxxxxxxx</valore>
                              </proprieta>
                              <proprieta>
                                    <chiave>Codice Rivenditore</chiave>
                                    <valore>xxxxxxx</valore>
                              </proprieta>
                              <proprieta>
                                    <chiave>Numero Contratto</chiave>
                                    <valore>xxxxxxxxx</valore>
                              </proprieta>
                              <proprieta>
                                    <chiave>Data Effetto</chiave>
                                    <valore>xxxxxxx</valore>
                              </proprieta>

                              <proprieta>
                                    <chiave>Codice Fiscale</chiave>
                                    <valore>xxxxxxxxxxxxxx</valore>
                              </proprieta>
                              <proprieta>
                                    <chiave>Scadenza</chiave>
                                    <valore>xxxxxxxxx</valore>
                              </proprieta>
                        </profiloArchivistico>

                        <versioneOriginale>
                              <parti>
                                    <files>
                                          <dati></dati>
                                           <documento>
                  <xop:Include href="consensi.pdf.p7m"
xmlns:xop="http://www.w3.org/2004/08/xop/include">
                                                                  </xop:Include>
                  </documento>
                                          <proprieta>

      <chiave>ordine_presentazione</chiave>
                                                <valore>0</valore>
                                          </proprieta>
                                          <proprieta>
                                                <chiave>nome_file</chiave>
                                                <valore>Consenso.pdf.p7m</valore>
                                          </proprieta>
                                          <proprieta>
                                                <chiave>id_cliente</chiave>
                                                <valore>xxx</valore>
                                          </proprieta>
                                          <proprieta>
                                                <chiave>formato_file</chiave>
                                                <valore>xxxxx</valore>
                                          </proprieta>
                                    </files>
                                    <proprieta>
```

```
                                        <chiave>formato_parte</chiave>
                                        <valore>xxxxxx</valore>
                                  </proprieta>
                                  <proprieta>
                                        <chiave>numero_parte</chiave>
                                        <valore>x</valore>
                                  </proprieta>
                            </parti>
                            <proprieta>
                                  <chiave>formato_versione</chiave>
                                  <valore>xxxxxx</valore>
                            </proprieta>
                      </versioneOriginale>
                </Documento>
                <Proprieta xmlns="">
                      <item>
                            <chiave>FAMILY</chiave>
                            <valore>xxxxxxxxxx</valore>
                      </item>
                      <item>
                            <chiave>ORGANIZZAZIONE</chiave>
                            <valore>xxxxxxxxxxxx</valore>
                      </item>
                      <item>
                            <chiave>STRUTTURA</chiave>
                            <valore>xxxxxxxxxxx</valore>
                      </item>
                      <item>
                            <chiave>USER_ID</chiave>
                            <valore>xxxxxxxxxxxx</valore>
                      </item>
                </Proprieta>

          </ConsegnaAnticipata>
    </soapenv:Body>
</soapenv:Envelope>
```

Per ulteriori precisazioni circa la ricezione degli oggetti digitali tramite Sistema Web Service si rimanda al documento “Specifiche del servizio web per la consegna anticipata di documenti nel Sistema di conservazione”.

F.4 Struttura dati del Pacchetto di archiviazione

Terminato il processo di acquisizione dei Pacchetti di versamento, il prodotto applicativo UniStorage sotto la supervisione del Responsabile del servizio di conservazione e del Responsabile della funzione archivistica provvede alla creazione dei Pacchetti di archiviazione e dell’Indice del pacchetto di archiviazione previsto dallo standard UNI 11386:2010 SInCRO – Supporto all’interoperabilità nella conservazione e nel recupero degli oggetti digitali.
I Pacchetti di archiviazione contengono[10]:

- l’oggetto o gli oggetti da conservare;
- l’Indice del Pacchetto di archiviazione, formato secondo le regole dettate dallo Standard UNI 11386:2010 SInCRO – Supporto all’Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali, è composto da:

[10] Sono elencate le caratteristiche indicate nell’allegato 4 al DPCM 3 dicembre 2013 Regole tecniche in materia di sistema di conservazione.

- il nodo **Self Description** contiene gli elementi:
    - **ID**: identificatore dell'Indice del pacchetto di archiviazione;
    - **CreatingApplication**: riferimento all'applicazione che ha creato tale indice. Può assumere tre valori: Name, Producer e Version;
    - **SourceIdc**: eventuali riferimenti ad altri Indici di pacchetti di archiviazione dai quali deriva il presente;
- il **nodo VdC**, con informazioni relative al Pacchetto di archiviazione, contiene gli elementi:
    - **ID**: identificatore del Pacchetto di archiviazione;
    - **SourceVdc**: eventuali riferimenti a ad altri Pacchetti di archiviazione dai quali deriva il presente;
    - **VdcGroup**: informazioni relative ad un'eventuale tipologia/aggregazione di natura logica o fisica cui il Pacchetto di Archiviazione appartiene;
    - **MoreInfo**: permette l'introduzione di metadati soggettivi relativi all'Indice del pacchetto di archiviazione individuati dal Soggetto produttore e indicati con un proprio schema nella Scheda cliente allegata al Manuale della conservazione al Contratto.
- Il nodo **FileGroup**, che comprende indicazione di uno o più raggruppamenti di uno o più file contenuti nel Pacchetto di archiviazione, è composto dai seguenti elementi:
    - **Label**: identificativo univoco descrive il documento, lo identificano mediante il numero del documento, l'anno, il registro e il tipo di documento;
    - **File**: descrizione di ogni file facente parte integrante del documento mediante
        - ID inteso come identificatore del documento,
        - Hash calcolato da UniStorage,
        - PreviousHash, se presente, corrisponde all'impronta calcolata dal cliente,
        - MoreInfo, che riporta informazioni sulle operazioni di controllo in base ai criteri scelti dal cliente nella fase di configurazione del servizio;
    - **MoreInfo**: permette l'introduzione di metadati soggettivi relativi ai raggruppamenti di file inclusi nel Pacchetto di archiviazione.
- Il nodo **Process** con le informazioni sul processo di conservazione del Pacchetto di archiviazione, ovvero:
    - **Agent**: indicazione del nome e del ruolo dei soggetti che intervengono nel processo di produzione dei Pacchetti di archiviazione;
    - **TimeReference**: riferimento temporale adottato;

- **LawAndRegulation**: indicazione dei riferimenti tecnici e normativi ai quali ci si è attenuti per la realizzazione del processo di produzione dei Pacchetti di archiviazione;

- **MoreInfo**: permetta l'introduzione di metadati soggettivi relativi all'Indice del pacchetto di archiviazione individuati dal Soggetto produttore e indicati con un proprio schema nella Scheda cliente allegata al Manuale della conservazione al Contratto.

Si riporta di seguito lo schema xml dell'Indice del Pacchetto di archiviazione:

```
<?xml version="1.0" encoding="UTF-8"?>
<sincro:IdC xmlns:sincro="http://www.uni.com/U3011/sincro/"
xmlns:unimatica="http://www.unimaticaspa.it/unimatica-SinCRO/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.uni.com/U3011/sincro/IdC.xsd
http://www.unimaticaspa.it/unimatica-SinCRO/TagUnimatica.xsd"
sincro:url="http://www.uni.com/U3011/sincro/" sincro:version="1.0">
  <sincro:SelfDescription>
    <sincro:ID sincro:scheme="local">Marca-blocco_497170_1168_FIRMATI_VALIDI_2014-150112-
051727-106773032</sincro:ID>
    <sincro:CreatingApplication>
      <sincro:Name>Unistorage</sincro:Name>
      <sincro:Version>3.1.41</sincro:Version>
      <sincro:Producer>Unimatica SPA</sincro:Producer>
    </sincro:CreatingApplication>
  </sincro:SelfDescription>
  <sincro:VdC>
    <sincro:ID sincro:scheme="local">497170</sincro:ID>
    <sincro:VdCGroup>
      <sincro:Label>xxxxx</sincro:Label>
      <sincro:ID sincro:scheme="local">1168</sincro:ID>
      <sincro:Description>xxxxxx</sincro:Description>
    </sincro:VdCGroup>
    <sincro:MoreInfo sincro:XMLScheme="http://www.unimaticaspa.it/unimatica-
SinCRO/TagUnimatica.xsd">
      <sincro:EmbeddedMetadata>
        <unimatica:UnimaticaInfo>
          <unimatica:VdCInfo>
            <unimatica:Lista-Crl>
              <unimatica:Crl>
                <unimatica:Issuer>xxxxxxxxxxx</unimatica:Issuer>
                <unimatica:Crl-Number>xxxxxxx</unimatica:Crl-Number>
                <unimatica:File-Name>xxxxxxxx</unimatica:File-Name>
                <unimatica:Progressivo>xxxx</unimatica:Progressivo>
              </unimatica:Crl>
              <unimatica:Crl>
                <unimatica:Issuer>xxxxxxxxxx</unimatica:Issuer>
                <unimatica:Crl-Number>xxxx</unimatica:Crl-Number>
                <unimatica:File-Name>xxxxxx</unimatica:File-Name>
                <unimatica:Progressivo>x</unimatica:Progressivo>
              </unimatica:Crl>
            </unimatica:Lista-Crl>
            <unimatica:Lista-Certificati-Trusted>
              <unimatica:Certificato-Trusted>
                <unimatica:Issuer>xxxxxxxxxxx</unimatica:Issuer>
                <unimatica:Serial>xxxxxxxxxx</unimatica:Serial>
                <unimatica:File-Name>xxxxxx</unimatica:File-Name>
                <unimatica:Progressivo>x</unimatica:Progressivo>
              </unimatica:Certificato-Trusted>
```

```
            </unimatica:Lista-Certificati-Trusted>
          </unimatica:VdCInfo>
        </unimatica:UnimaticaInfo>
      </sincro:EmbeddedMetadata>
    </sincro:MoreInfo>
  </sincro:VdC>
  <sincro:FileGroup>
    <sincro:Label>xxxxxxxxxxx</sincro:Label>
    <sincro:File sincro:encoding="base64" sincro:extension="XML.P7M"
sincro:format="application/octet-stream">
      <sincro:ID>xxxxxxxxxxxx</sincro:ID>
      <sincro:Hash sincro:function="SHA-1">rMBhWqRKsvXhvF1W8LUpGlmlksI=</sincro:Hash>
      <sincro:MoreInfo sincro:XMLScheme="http://www.unimaticaspa.it/unimatica-
SinCRO/TagUnimatica.xsd">
        <sincro:EmbeddedMetadata>
          <unimatica:UnimaticaInfo>
            <unimatica:FileInfo>
              <unimatica:Forza-Accettazione>xx</unimatica:Forza-Accettazione>
              <unimatica:Forza-Conservazione>xx</unimatica:Forza-Conservazione>
              <unimatica:Urn>xxxxxxx</unimatica:Urn>
              <unimatica:Esito-File>
                <unimatica:Valore>xxxxxxx</unimatica:Valore>
                <unimatica:Codice>xxxx</unimatica:Codice>
              </unimatica:Esito-File>
              <unimatica:Firme>
                <unimatica:Firma>
                  <unimatica:Codice-Fiscale>xxxxxx</unimatica:Codice-Fiscale>
                  <unimatica:Nome>xxxxx</unimatica:Nome>
                  <unimatica:Cognome>xxxxx</unimatica:Cognome>
                  <unimatica:Esito-Firma>
                    <unimatica:Valore>xxxxxxx</unimatica:Valore>
                    <unimatica:Codice>xxx</unimatica:Codice>
                    <unimatica:Revoca>xx</unimatica:Revoca>
                    <unimatica:Validita-Temporale>xx</unimatica:Validita-Temporale>
                  </unimatica:Esito-Firma>
                  <unimatica:Verifiche>
                    <unimatica:Esito-Verifica unimatica:tipo-verifica="Conservazione"
unimatica:verifica-alla-data="2015-01-12T05:17:28.000">
                      <unimatica:Controllo-Struttura-
Firma>xxxxxxxxxxx</unimatica:Controllo-Struttura-Firma>
                      <unimatica:Controllo-
Crittografico>xxxxxxxxxxxxxxxxxxx</unimatica:Controllo-Crittografico>
                      <unimatica:Controllo-
Certificato>xxxxxxxxxxxxxxxxxx</unimatica:Controllo-Certificato>
                      <unimatica:Controllo-Catena-
Trusted>xxxxxxxxxxxxxxxxx</unimatica:Controllo-Catena-Trusted>
                      <unimatica:Controllo-Certificate-Revocation-
List>xxxxxxxxxx</unimatica:Controllo-Certificate-Revocation-List>
                      <unimatica:Crl-Progressivo>x</unimatica:Crl-Progressivo>
                    </unimatica:Esito-Verifica>
                    <unimatica:Esito-Verifica unimatica:tipo-verifica="Chiusura-Blocco"
unimatica:verifica-alla-data="2015-01-12T05:17:28.000">
                      <unimatica:Controllo-Struttura-
Firma>xxxxxxxxxxxxxxxxx</unimatica:Controllo-Struttura-Firma>
                      <unimatica:Controllo-
Crittografico>xxxxxxxxxxxxxxxxx</unimatica:Controllo-Crittografico>
                      <unimatica:Controllo-
Certificato>xxxxxxxxxxxxx</unimatica:Controllo-Certificato>
                      <unimatica:Controllo-Catena-
Trusted>xxxxxxxxxxxxxx</unimatica:Controllo-Catena-Trusted>
                      <unimatica:Controllo-Certificate-Revocation-
List>xxxxxxxxxxx</unimatica:Controllo-Certificate-Revocation-List>
                      <unimatica:Crl-Progressivo>x</unimatica:Crl-Progressivo>
                    </unimatica:Esito-Verifica>
```

```
                  </unimatica:Verifiche>
                  <unimatica:Certificato-Trusted-Progressivo>x</unimatica:Certificato-
Trusted-Progressivo>
                </unimatica:Firma>
              </unimatica:Firme>
            </unimatica:FileInfo>
          </unimatica:UnimaticaInfo>
        </sincro:EmbeddedMetadata>
      </sincro:MoreInfo>
    </sincro:File>
  </sincro:FileGroup>
  <sincro:Process>
    <sincro:Agent sincro:type="organization" sincro:role="PreservationManager">
      <sincro:AgentName>
        <sincro:FormalName>Unimatica SPA</sincro:FormalName>
      </sincro:AgentName>
      <sincro:Agent_ID sincro:scheme="TaxCode">xxxxxxx</sincro:Agent_ID>
    </sincro:Agent>
    <sincro:TimeReference>
      <sincro:AttachedTimeStamp sincro:normal="2015-01-12T08:35:10+01:00"/>
    </sincro:TimeReference>
    <sincro:MoreInfo sincro:XMLScheme="http://www.unimaticaspa.it/unimatica-
SinCRO/TagUnimatica.xsd">
      <sincro:EmbeddedMetadata>
        <unimatica:UnimaticaInfo>
          <unimatica:ProcessInfo>
            <unimatica:Blocca-Crl-Scadute unimatica:time="0">xx</unimatica:Blocca-Crl-
Scadute>
            <unimatica:Catena-Trust>si</unimatica:Catena-Trust>
            <unimatica:Certificato-Valido>xx</unimatica:Certificato-Valido>
            <unimatica:Controllo-Crl>si</unimatica:Controllo-Crl>
            <unimatica:Verifica-Crittografica>xx</unimatica:Verifica-Crittografica>
            <unimatica:Verifica-Timestamp>si</unimatica:Verifica-Timestamp>
          </unimatica:ProcessInfo>
        </unimatica:UnimaticaInfo>
      </sincro:EmbeddedMetadata>
    </sincro:MoreInfo>
  </sincro:Process>
</sincro:IdC>
```

F.5 Struttura dati del Pacchetto di distribuzione

La produzione di Pacchetti di distribuzione avviene in seguito alla richiesta da parte dell'Utente.

L'esibizione del materiale di interesse avviene mediante memorizzazione su supporto ottico. La descrizione dettagliata delle procedure è indicata nel successivo capitolo, Fase 6.
I Pacchetti di distribuzione coincidono con i Pacchetti di archiviazione, come previsto delle Regole tecniche in materia di sistemi di conservazione, ma saranno corredati di informazioni aggiuntive necessarie per la creazione dei DVD, CD, ecc. nel caso di richiesta di esibizione da parte dell'Utente.

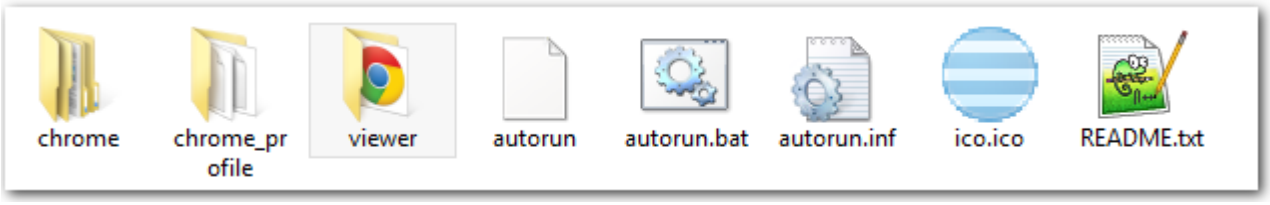
UniStorage consente la produzione di supporti rimovibili che possono essere forniti all'Utente.
In ogni supporto vengono trasferiti dei Pacchetti di distribuzione chiamati "Registrazioni", contenenti sia gli oggetti che l'insieme delle evidenze di conservazione.
La registrazione generata è auto-esplicativa, intendendo con questo che i dati sono affiancati da indici e informazioni di riferimento tali da poter permettere la comprensione del contenuto anche da programmi esterni al sistema di conservazione.

La registrazione è contenuta in una directory, il cui nome contiene un'indicazione del blocco dei documenti e data/ora dell'inizio della creazione della registrazione stessa.

Contenuto della directory della registrazione:

- file README.txt
- file autorun
- icona
- directory chrome
- directory chrome_profile
- directory viewer

I vari Pacchetti di distribuzione a seconda delle dimensioni possono venire raggruppati in volumi auto consultanti, la struttura dei volumi è la seguente:

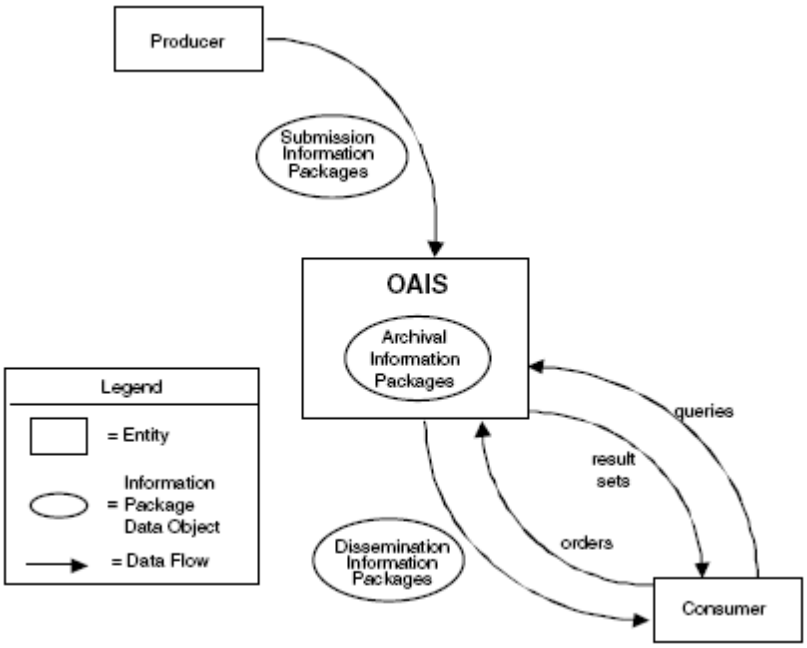


All'interno della directory viewer avremo una directory contenente i documenti suddivisi per Pacchetti. Questi volumi sono auto consultanti e permettono la ricerca dei documenti conservati, i metadati associati e le marche di conservazione.

G. Il processo di erogazione del servizio di conservazione

Il processo di conservazione eseguito da UNIMATICA S.p.A. adotta il modello standard OAIS - Open Archival Information System[11] che definisce concetti e funzionalità degli archivi digitali. Lo schema seguente illustra brevemente gli aspetti principali di un generico processo di conservazione: il Soggetto produttore invia il Pacchetto di versamento, di cui ha piena responsabilità, al Soggetto conservatore il quale provvede a trasformarlo in Pacchetto di archiviazione. Ai fini dell'esibizione e della distribuzione richiesti dalla comunità di riferimento[12], il Soggetto conservatore provvederà a creare i Pacchetti di distribuzione così che venga garantita la corretta visualizzazione di questi.
Il sistema di conservazione di UNIMATICA S.p.A., in caso di acquisizione del servizio da parte di un altro Soggetto conservatore è in grado di gestire la presa in carico di Pacchetti di versamento coincidenti con i Pacchetti di archiviazione. Per assicurare, inoltre, interoperabilità e trasferibilità ad altri conservatori in caso di chiusura del contratto per scelta del Soggetto produttore, UNIMATICA S.p.A. crea Pacchetti di distribuzione coincidenti con quelli di archiviazione, così come indicato all'art. 9, comma 1, lettera h) delle Regole tecniche in materia di sistema di conservazione.

Figura 1 Modello OAIS



G.1 Il processo di conservazione

Il servizio offerto da UNIMATICA S.p.A. ad ogni Soggetto produttore viene avviato al termine di un processo di attivazione che segue questi fasi fondamentali:

[11] L'Open Archival Information System è lo standard ISO per la conservazione a lungo termine di archivi digitali.
[12] Comunità di riferimento: il sottoinsieme degli utenti in grado di comprendere autonomamente l'informazione archiviata nella forma in cui è conservata e resa disponibile dall'OAIS

1. condivisione di informazioni tecniche di richiesta configurazione e invio dei Pacchetti di versamento;
2. verifiche sui Pacchetti di versamento e sugli oggetti in esso contenuti;
3. accettazione dei Pacchetti di versamento e generazione del Rapporto di versamento di presa in carico;
4. rifiuto dei Pacchetti di versamento e modalità di comunicazione delle anomalie;
5. preparazione e gestione del Pacchetto di archiviazione;
6. preparazione e gestione del Pacchetto di distribuzione ai fini dell'esibizione;

Ognuno degli step sopra indicati viene eseguito per ogni tipologia di configurazione richiesta.
Di seguito vengono dettagliate le fasi:

Fase 1: Condivisione informazioni tecniche di richiesta configurazione e invio dei Pacchetti di versamento.
In questa fase il Soggetto produttore veicola al Responsabile del servizio di conservazione, al Responsabile per il trattamento dei dati personali e al Responsabile della funzione archivistica la richiesta di attivazione del servizio per l'invio di Pacchetti di versamento. Le tre figure responsabili sopracitate, con l'ausilio del Responsabile dello sviluppo e della manutenzione, incaricato di curare l'interfaccia con il Soggetto produttore relativamente alle modalità di trasferimento dei documenti, valuteranno la domanda di acquisizione del servizio affinché venga accertato che i requisiti del Soggetto produttore siano compatibili con le policy di UNIMATICA S.p.A.

L'attivazione del servizio avviene attraverso la compilazione del Modulo 'Change Request'. In particolare, tale modulo deve essere compilato con le seguenti informazioni:

- ragione sociale;
- indirizzo;
- partita iva;
- e-mail;
- oggetti documentali gestiti;
- interoperabilità tra sistema del Soggetto produttore e sistema di conservazione;
- tipo di protocollo da utilizzare per lo scambio dei Pacchetti.

Per ogni Pacchetto di versamento dichiarato dal Soggetto produttore, è indispensabile definire:

- i volumi in termini di numero documenti annui previsti da gestire e spazio di occupazione previsto per i dati da Conservare (GB);
- la dimensione massima del Pacchetto di versamento;
- la frequenza di invio dei Pacchetti;
- l'eventuale richiesta di invio di supporti ottici (DVD) di conservazione con la definizione della relativa frequenza.

Il Responsabile del servizio di conservazione, valuterà in accordo con il Responsabile del trattamento dei dati, con il Responsabile della funzione archivistica e con il Responsabile dello sviluppo e della manutenzione la domanda di acquisizione del servizio collaborando con il Soggetto produttore guidandolo nella compilazione della domanda per l'attivazione del servizio.

Il Responsabile del servizio di conservazione e il Responsabile della funzione archivistica una volta ricevuta la richiesta, si impegnano a valutarne l'impatto stimando la data di evasione e fornendo al Soggetto produttore una pianificazione delle fasi successive. Se la richiesta di configurazione implica un aggravio di costi, verrà fornita parallelamente al Soggetto produttore la quotazione economica dell'attività redatta dal Referente Commerciale di UNIMATICA S.p.A.

L'acquisizione dei Pacchetti di versamento avviene mediante due canali: tramite File Transfert Protocol e tramite canale Web service descritti dettagliatamente nel paragrafo F.3.

Ad ogni attivazione verranno consegnate le credenziali per accedere all'applicativo web reso disponibile da UNIMATICA S.p.A., in base ai dati presenti nella Scheda cliente. Tale accesso garantirà la piena esibizione dei Pacchetti di distribuzione.

Fase 2: Verifiche sui Pacchetti di versamento e sugli oggetti in esso contenuti.
I parametri gestionali del Pacchetto di versamento vengono verificati e messi a punto dal Responsabile del servizio di conservazione e dal Responsabile della funzione archivistica in accordo con il Soggetto produttore. Le verifiche effettuate sui Pacchetti di versamento sono le seguenti:

- **identificazione certa del Soggetto produttore**;

- verifica della **firma digitale** mediante un controllo crittografico dell'integrità del documento e della validità formale della firma stessa. In un secondo momento viene verificata l'identità del sottoscrittore. Se una chiave privata sia stata usata in una firma è verificabile, mediante processo crittografico, con la corrispondente chiave "pubblica". Le chiavi pubbliche sono riportate nei "certificati di firma digitale", documenti digitali anch'essi, che definiscono anche i dati d'identità del sottoscrittore. I certificati sono a loro volta firmati da una autorità di certificazione emittente (C.A. - Certification Authority). In generale si risalirà la catena di certificazione fino a raggiungere un "certificato fidato", ovvero pubblicamente noto. Tra le evidenze informatiche che UNIMATICA S.p.A. conserva ci sono, per ogni Pacchetto, tutti i certificati a vario modo coinvolti nelle catene di certificazione necessarie alle verifiche di firma digitale. Questo consente di costituire un insieme "auto-contenuto" di evidenze che possono essere verificate anche a posteriori. Si può anche verificare il caso che l'autorità emittente non sia direttamente un'autorità pubblicamente nota, ma che esista una "catena di certificazione" (trust chain) per cui l'autorità di un certificato vada a sua volta identificata risalendo ad un'autorità terza.

- verifica che i **formati** degli oggetti da conservare siano conformi con quanto dichiarato nel modulo 'Change Request' e nell'allegato 2 al Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 Regole tecniche in materia di sistema di conservazione e dichiarati nel presente Manuale;

- verifica che i **metadati** siano conformi con i set minimi dichiarati nel modulo 'Change Request' e nell'allegato 5 al Decreto della Presidenza del Consiglio dei Ministri 3 dicembre 2013 Regole tecniche in materia di sistema di conservazione e dichiarati nel presente Manuale.

Fase 3: Accettazione dei Pacchetti di versamento e generazione del Rapporto di versamento di presa in carico.

L'esito positivo delle verifiche effettuate sui Pacchetti di versamento viene registrato in un Rapporto di versamento di presa in carico. Il Rapporto conterrà un'impronta del file originale comprensivo di algoritmo con la quale tale impronta viene calcolata (hash) e un riferimento temporale certificato che costituisce evidenza dell'esistenza e dell'esatta composizione del Rapporto collegato all'istante indicato (Tcons).
Apponendo un timestamp al Rapporto di versamento, lo si "sigilla" e contemporaneamente si fissa il riferimento temporale. Tale procedimento costituisce un riferimento temporale certificato per il Rapporto di versamento.
Il Rapporto di versamento attesta la corretta esecuzione del processo di immissione dei Pacchetti, ha la funzione di raccogliere evidenze indirette di tutti i documenti del Pacchetto e garantisce due principali funzioni:

- la possibilità di provare l'integrità dei dati di ogni file contenuto nel pacchetto,
- di permettere il controllo dell'integrità per ogni file in modo separato, senza creare un'interdipendenza tra i file ai fini dell'esibizione e del controllo.

Il Rapporto di versamento è un file in formato XML che riporta, per ognuno dei file inclusi nel Pacchetto, alcune informazioni tra cui un "URN" (unified resource name) e un "hash". L'URN è una stringa univoca che identifica l'oggetto digitale, mentre l'hash è un'impronta del documento, ovvero una sequenza di bit che può essere ricavata dal file in modo ripetibile e standardizzato e che garantisce una corrispondenza esatta col contenuto originale (in modo pratico possiamo dire di avere la garanzia che a due file differenti corrispondono sempre due impronte distinte).

La modalità di conservazione mediante Rapporto di versamento permette di verificare l'integrità di ogni singolo file, a prescindere da tutti gli altri file conservati nello stesso pacchetto. Infatti sarà sufficiente essere in possesso di un file "candidato" e conoscere il suo URN identificativo per poter eseguire la funzione di hash e confrontare l'impronta ricalcolata con la stringa riportata nel Rapporto.
In questa fase vengono associate all'indice tutte le evidenze di autenticità delle firme digitali che verranno verificate all'istante del riferimento temporale:

- i certificati di firma di tutte le firme presenti nel Pacchetto di versamento,
- tutti i certificati appartenenti alle catene di certificazione (trusting chain),
- le liste di revoca dei singoli certificati (CRL).

Il Rapporto di versamento viene conservato all'interno del sistema garantendone l'ininterrotta custodia e la non modificabilità.

Fase 4: Rifiuto dei Pacchetti di versamento e modalità di comunicazione delle anomalie.
Le verifiche effettuate sui Pacchetti di versamento possono risultare negative. Nei casi in cui anche solo su uno dei controlli indicati nella fase 2 si dovesse riscontrare una mancanza o non corrispondenza di informazioni viene generato un file di Comunicazione delle anomalie che verrà comunicato mediante un file di esito al Soggetto produttore. Tale Comunicazione comprenderà i dettagli delle verifiche eseguite sui Pacchetti di versamento comprensive delle precisazioni sulle anomalie. Le anomalie, in relazione a quanto descritto nella fase 2, possono essere identificate nella mancata corrispondenza di ciò che viene versato a quanto dichiarato dal Soggetto produttore nella Scheda cliente in termini di firma digitale, formati e metadati.

Sulla Comunicazione delle anomalie verrà apposto un riferimento temporale e conservata così come viene conservato il Rapporto di versamento.

Fase 5: **Preparazione e gestione dei Pacchetti di archiviazione.**

I Pacchetti versati in UniStorage, con la supervisione del Responsabile del servizio di conservazione e del Responsabile della funzione archivistica vengono raggruppati in Pacchetti di archiviazione. Questi pacchetti vengono assemblati dal sistema nei tempi e con i criteri di raggruppamento scelti e concordati con il Soggetto produttore, indicati nella Scheda Cliente (ad es. Pacchetti di archiviazione per tipologie documentali o in base alla cadenza temporale di consegna).
Il processo di costruzione dei Pacchetti di archiviazione, così come previsto dallo standard SInCRO UNI 11386:2010 – Supporto all'interoperabilità nella conservazione e nel recupero degli oggetti digitali, avviene con le seguenti modalità:

- individuazione dei documenti destinati a far parte del Pacchetto di archiviazione sulla base dei criteri scelti. Tali criteri vengono concordati con il cliente e sono definiti nella Scheda Cliente allegata al Manuale della conservazione e si possono basare sia su caratteristiche legate allo stato del documento, sia su sui metadati minimi indicati nell'allegato 5 al Decreto del presidente del consiglio dei ministri Regole tecniche in materia di sistemi di conservazione. Un esempio del primo tipo di caratteristiche può essere lo stato della firma: firmato valido, non firmato, firmato invalido;
- i Pacchetti di archiviazione vengono chiusi in seguito a due tipi di regole:
  - automatiche: impediscono ad un documento di scadere una volta inserito in un Pacchetto di archiviazione. Questa tipologia di regole ha la precedenza su quelle descritte nel punto successivo, le quali riguardano la dimensione massima del Pacchetto di archiviazione e il tempo limite oltre il quale un Pacchetto di archiviazione deve essere forzatamente chiuso,
  - attuate dal Responsabile del servizio di Conservazione in accordo con il Soggetto produttore: definite nella Scheda Cliente allegata al Manuale della conservazione.

Nei casi in cui i Pacchetti di archiviazione contengano referti sanitari, questi vengono crittografati mediante crittografia simmetrica con chiave AES a 1024 bit.
I Pacchetti di archiviazione vengono sottoscritti con firma digitale dal Responsabile del servizio di conservazione e marcati temporalmente.
La sottoscrizione dei Pacchetti di archiviazione effettuata da UNIMATICA S.p.A. attesta esclusivamente la corretta esecuzione del processo di conservazione secondo la normativa vigente in materia di conservazione. UNIMATICA S.p.A. non è responsabile dell'errato contenuto informativo degli oggetti versati.

Fase 6: **Preparazione e gestione dei Pacchetti di distribuzione ai fini dell'esibizione**.
La gestione dei Pacchetti di distribuzione fa capo al Responsabile del Servizio di Conservazione, al Responsabile della Funzione archivistica e al Responsabile del trattamento dei dati personali.

La produzione di Pacchetti di distribuzione avviene in seguito alla richiesta da parte dell'Utente, così come indicato all'art. 9, c.1, lett. h). Tali Pacchetti, però, posso differire nei casi in cui l'utente richiede l'esibizione tramite supporto ottico in quanto questo dovrà necessariamente contenere elementi utili all'avvio del supporto e alla visualizzazione dei contenuti informativi.

UniStorage, prevedendo la conservazione dei Pacchetti di archiviazione firmati, implementa un formato di composizione delle marche tale da permettere l'esibizione probatoria di un singolo documento. Quindi, ogni singolo file può essere esibito insieme ai suoi metadati, registrati nel data base, e alle sue prove di conservazione in maniera assolutamente INDIPENDENTE dagli altri documenti.
UNIMATICA S.p.A. permette l'accesso ai Pacchetti di distribuzione esclusivamente agli utenti autorizzati. I livelli di accesso vengono definiti in base alle esigenze delle richieste effettuate,

rendendo disponibile soltanto il materiale richiesto grazie all'utilizzo di filtri predefiniti che selezionano i canali previsti per la visualizzazione di un determinato pacchetto.

È possibile visualizzare i documenti tramite duplice canale:

- via web: i Soggetti produttori titolari dei documenti potranno ricercare e visualizzare tutti i documenti conservati direttamente sul portale di UNIMATICA S.p.A. attraverso l'apposita funzionalità. L'accesso avviene tramite il portale al quale è demandata la sicurezza e la gestione della sessione. I documenti saranno disponibili per l'esibizione on-line per tutto il periodo di conservazione. La descrizione di dettaglio dell'interfaccia web per le richieste di esibizione dei documenti è contenuta nell'allegato 'Manuale dell'interfaccia web'. Vengono inoltre resi disponibili servizi web (Web Services) per le eventuali integrazioni con i portali dei Soggetti produttori.
- copia del documento su supporto ottico. La descrizione dettagliata circa la visualizzazione dei Pacchetti di distribuzione mediante supporto ottico è presente nel paragrafo F.5.

La struttura architetturale di UniStorage consente di definire diversi livelli operativi e garantisce che ciascuna Azienda/Ente, Area Organizzativa, Agenzia, Ufficio, Dipartimento, ecc. possa accedere solo ed esclusivamente ai suoi documenti, in base alle credenziali e alle politiche di accesso attivate.

G.2 Produzione di duplicati e copie informatiche

Con la richiesta da parte dell'utente di esibizione dei Pacchetti di distribuzione mediante supporto ottico, viene generata una copia autentica del documento, conforme all'originale. Per i dettagli sulla modalità di richiesta di esibizione dei Pacchetti di distribuzione, fare riferimento al paragrafo F.5 e al capitolo G, fase 6.

Nei casi in cui, come previsto dall'art. 23-bis, c. 2 del Codice dell'Amministrazione Digitale[13] il Soggetto produttore richieda la presenza di un pubblico ufficiale, UNIMATICA S.p.A. garantirà tale presenza mettendo a disposizione tutte le necessarie risorse che serviranno all'espletamento delle attività, rimandando in ogni caso la scelta al Soggetto produttore al quale saranno addebitate le spese.

Inoltre, in caso di adeguamento del formato dovuto all'evoluzione tecnologica verranno rispettate tutte le procedure elencate nell'Allegato 'Infrastrutture' del presente Manuale. Anche in questo caso, l'eventuale presenza del pubblico ufficiale per l'attestazione di conformità, sarà garantita in seguito alla richiesta del Soggetto produttore a cui vengono attribuiti i costi di gestione.

[13] "Le copie e gli estratti informatici del documento informatico, se prodotti in conformità alle vigenti regole tecniche di cui all'articolo 71, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale, in tutti le sue componenti, è attestata da un pubblico ufficiale a ciò autorizzato o se la conformità non è espressamente disconosciuta. Resta fermo, ove previsto, l'obbligo di conservazione dell'originale informatico."

G.3 Scarto dei Pacchetti di archiviazione

Sette mesi prima della scadenza del periodo di conservazione dei documenti, UNIMATICA S.p.A. comunica al Soggetto produttore, in modalità certa, che in assenza di ulteriori comunicazioni, trascorsi i termini previsti, provvederà alla cancellazione dei documenti.
In caso di proroga della conservazione, UNIMATICA S.p.A. rinnova la marca temporale sui documenti per il periodo richiesto (uno o più anni).

Lo scarto dei Pacchetti di archiviazione in caso di pacchetti versati da Pubbliche amministrazioni avviene previa autorizzazione della Soprintendenza archivistica così come prevede la normativa vigente in materia.
I tempi di scarto vengono dettati dal Soggetto produttore mediane il proprio Massimario di selezione.
Il Soggetto produttore è tenuto a compilare un lista del materiale che intende scartare e a sottoporre tale lista alla Soprintendenza archivistica competente la quale rilascerà il nulla osta alla procedura di scarto.
UNIMATICA S.p.A. permette al Soggetto produttore l'accesso diretto ai Pacchetti mediante un'apposita interfaccia attraverso la quale potrà selezionare direttamente i Pacchetti che intende scartare. Come prova di tale processo, UNIMATICA S.p.A. rilascerà un rapporto di scarto che verrà firmato dal Soggetto produttore e controfirmato da UNIMATICA e sul quale verrà apposta una marca temporale così da provare quali Pacchetti siano stati scartati. Il rapporto di scarto viene conservato all'interno del sistema UniStorage.

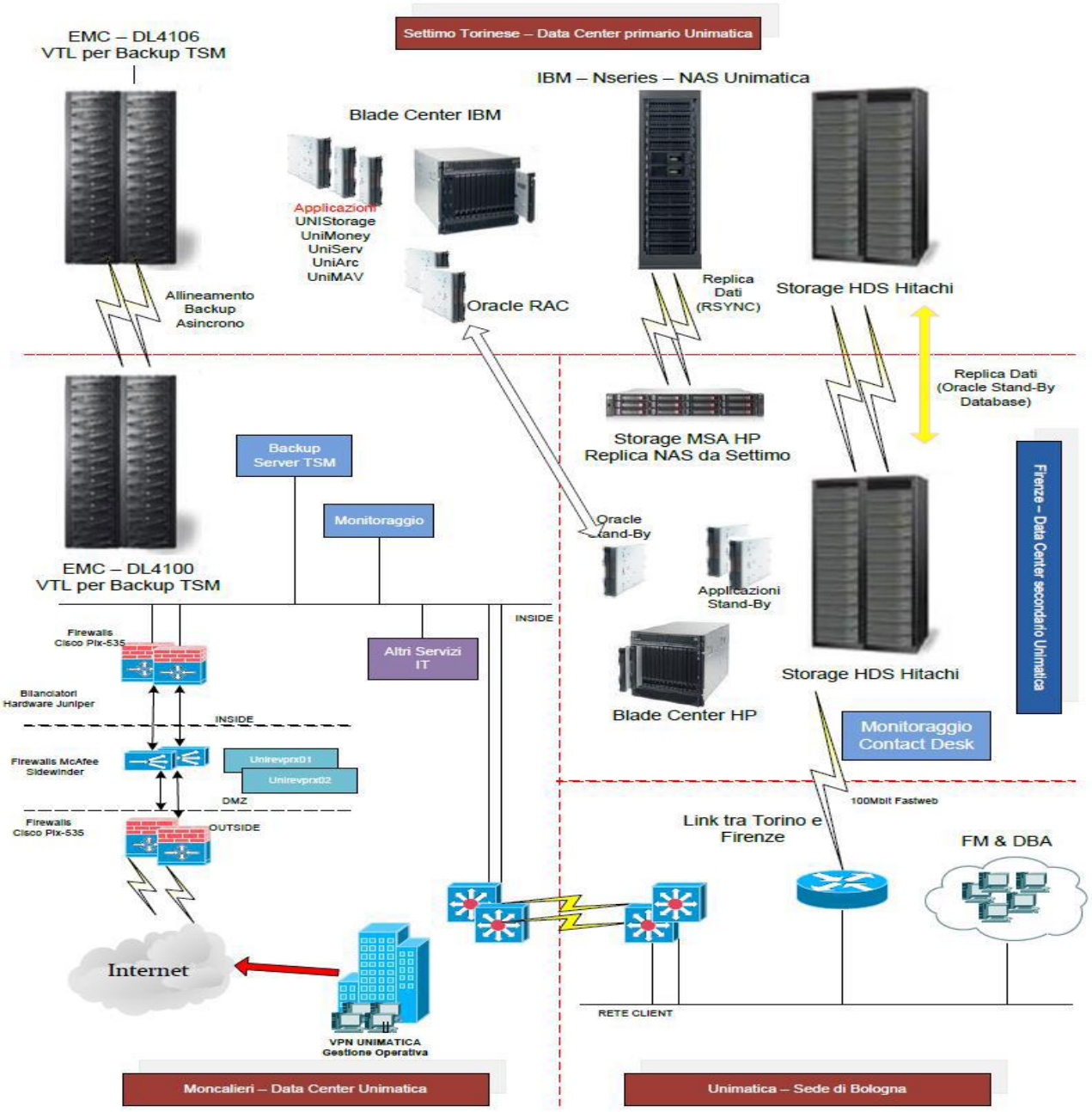
L'intervento della Soprintendenza archivistica è previsto anche nel caso di archivi privati per i quali è stato dichiarato l'interesse culturale, secondo quanto disposto dall'art. 21, comma 1, lettera d del Codice dei beni culturali (D. Lgs. 22 gennaio 2004, n. 42).

Una volta rilasciato il rapporto di scarto, verranno fisicamente eliminati i Pacchetti e le relative prove di conservazione.

H. La server farm di Unimatica

Dal punto di vista infrastrutturale, i data center dai quali UNIMATICA S.p.A. eroga i propri servizi consentono di offrire un servizio di alta qualità in termini di continuità e affidabilità. Tale qualità deriva dalle caratteristiche progettuali che hanno contraddistinto la realizzazione dei Data Center, con criteri focalizzati sempre sull'obiettivo di fornire le massime garanzie di sicurezza, disponibilità e continuità, sia per quanto riguarda l'erogazione di energia elettrica, sia attraverso un opportuno condizionamento climatico, sia attraverso un adeguato meccanismo di sicurezza fisica (impianto antincendio e sorveglianza con allarmi 24x7), sia attraverso la ridondanza architetturale dei sistemi, delle infrastrutture di rete e delle connessioni verso l'esterno.

Lo schema seguente rappresenta l'implementazione hardware/software dell'architettura di conservazione presso i siti di Settimo Torinese e Firenze, nei quali sono allocati i data center, rispettivamente Primario e Secondario:



H.1 UniStorage - Il sistema per la conservazione

Il sistema software utilizzato per la gestione del processo di conservazione legale dei documenti digitali è costituito dal prodotto applicativo UniStorage.
UniStorage, sviluppato internamente e totalmente da UNIMATICA S.p.A., è un sistema integrato e completo per la conservazione dei documenti digitali che viene fornito in modalità Outsourcing/ASP/SaaS congiuntamente a tutti i servizi di gestione e supporto correlati, oppure in modalità pacchetto applicativo, installando le applicazioni presso il Data Center del Soggetto produttore.

I servizi offerti, oltre che di tipo applicativo e tecnologico, comprendono tutto il necessario supporto normativo, organizzativo e contrattuale (deleghe, privacy, ecc.).

UniStorage esegue la conservazione nel tempo dei documenti sottoscritti con firma digitale e rispetta il Decreto del Presidente del consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5 *-bis*, 23 *-ter* , comma 4, 43, commi 1 e 3, 44 , 44 *-bis* e 71, comma 1, del Codice dell'amministrazione digitale di cui al Decreto legislativo n. 82 del 2005 e presenta le seguente caratteristiche generali:

- completezza - presenza di qualsiasi documento emesso
- robustezza - garanzia di consistenza dei dati inseriti
- sicurezza - protezione dalla manipolazione non autorizzata dei dati
- affidabilità - indipendenza dai guasti dell'hardware
- chiarezza - facilità di consultazione secondo diversi criteri di ricerca

garantendo:

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

Il sistema è progettato per partizionare in maniera opportuna i dati gestiti al fine di garantire la separazione per contesto organizzativo e la consistenza dei dati. Il partizionamento opera tra i dati di Aziende diverse o di diversi dipartimenti o uffici afferenti ad una stessa Azienda (Aree Organizzative Omogenee). I Pacchetti versati provenienti anche da flussi diversi di conservazione, vengono mantenuti separati tramite una chiave primaria che li identifica, fin dal loro ingresso in conservazione, come appartenenti ad una data AOO e non ad un'altra. Il sistema di partizionamento è direttamente collegato al sistema di controllo degli accessi e tracciatura, viene quindi garantita la riservatezza dei dati presenti in archivio.
UniStorage è una applicazione Web a tre livelli (desktop, application e database) e utilizzabile da posti di lavoro dotati di sistema operativo Windows o Linux, per mezzo di browser standard quali ad esempio Internet Explorer vers. 11 o superiore, Mozilla Firefox 3.6 o superiore, Google Chrome 11.0.696.7 o superiore, Apple Safari 5.0.5 o superiore. Per le postazioni che dovranno operare sulle funzionalità di firma è necessario che localmente siano attivi i driver del dispositivo di firma (lettore, smart card o token USB di firma, tablet per la firma grafometrica, ecc.), oppure che sia utilizzato un dispositivo HSM (Hardware Security Module) raggiungibile via rete.

Il servizio in outsourcing ASP del servizio di conservazione dei documenti digitali prodotti ed inviati dal Soggetto produttore prevede lo svolgimento da parte di UNIMATICA S.p.A., dietro apposita nomina e delega da parte del Soggetto produttore, delle funzioni e responsabilità di conservazione dei documenti.

La descrizione dettagliata delle componenti logiche, tecnologiche e fisiche è riportata nel documento "Infrastruttura" allegato al Manuale della conservazione.

I. Procedure di gestione e di evoluzione

A coordinare la gestione del sistema, l'aggiornamento di questo e le procedure di adeguamento all'evoluzione tecnologica è la figura del Responsabile sviluppo e manutenzione che esegue una costante attività di controllo dell'attività di conservazione in conformità agli standard di qualità e sicurezza ISO 9001 e ISO 27001.
Affinché venga garantito un controllo totale sul sistema e un buon funzionamento di questo, le attività di manutenzione vengono svolte sia sui processi che sulle strutture hardware e software e viene condotta una quotidiana verifica delle attività sulle infrastrutture parallelamente ad una pianificazione delle eventuali procedure straordinarie da condurre in caso di anomalie.

I.1 Misure di sicurezza logica

Il presente paragrafo ha l'obiettivo di descrivere le misure di sicurezza adottate per l'erogazione del Servizio e per la protezione dei dati che fanno riferimento al Piano per la sicurezza del sistema di conservazione di UNIMATICA S.p.A. In particolare, verranno descritte:

- la gestione utenze,
- la gestione sistemi di protezione,
- la gestione degli incidenti di sicurezza,
- la gestione dei backup,
- la gestione dei supporti di memorizzazione.

I.1.1 Gestione utenze

La policy di riferimento per la gestione delle utenze applicative e di sistema adottata da UNIMATICA S.p.A. prevede che le utenze siano rilasciate da un ente (o persona) differente dall'ente o persona che le utilizzerà.
Nell'ambito del servizio di conservazione, le utenze applicative e di sistema sono gestite secondo i criteri che seguono le misure minime di sicurezza di cui all'allegato B del D. Lgs 196/2003, in ottemperanza alla policy di UNIMATICA S.p.A.:

- Utilizzo di password complesse definite secondo i seguenti criteri:
  - la password non deve essere visibile in fase di inserimento nelle sessioni di login e sia criptata all'interno del Data Base;
  - la password:
    - deve avere una lunghezza compresa fra 8 e 25caratteri,
    - non può contenere il nome dell'utente,
    - non può contenere il cognome dell'utente,
    - non può contenere l'username dell'utente,
    - non può contenere il nome dell'utente invertito,
    - non può contenere il cognome dell'utente invertito,
    - non può contenere l'username invertito,
    - non può' contenere porzioni della data di nascita,
    - non può' contenere due (o più) caratteri uguali consecutivi,
    - non può' essere una delle ultime 5 utilizzate;

- La scadenza della password è configurabile attraverso un parametro;
- il sistema deve forzare l'utente a cambiare la password al primo utilizzo;
- il sistema deve avvertire l'utente della necessità di rinnovare la password;
- l'utenza deve essere disabilitata in seguito a ripetuti tentativi di accesso non andati a buon fine;

- Applicazione del principio 'segregation of duty' nel rilascio delle credenziali (utente, password e profilo), vale a dire separazione tra chi rilascia e chi utilizza le credenziali di accesso ai dati;
- Applicazione del principio 'need to know' nel rilascio dei profili, vale a dire rilascio dei soli diritti per eseguire le attività di competenza;
- Assegnazione ad ogni utente di credenziali (user e password) personali, uniche e non assegnabili ad altri utenti;
- Revisione periodica degli utenti e dei relativi profili.

I.1.2 Gestione sistemi di protezione

Net Security
La realizzazione logica della rete è fatta secondo i seguenti criteri :

- controllo degli accessi e dei flussi realizzato tramite firewall in cross-mode (doppio Cisco Pix-535) ed utilizzo di software IP Tables per il port e IP filtering;
- filtro sui flussi di traffico da/per Internet costituito da sistemi McAfee Sidewinder ridondati, che effettuano deep packet inspection e forniscono funzionalità di firewall applicativo (livello 7 OSI);
- segregazione della rete e suddivisione della medesima in differenti porzioni dedicate alla rete di Back End dati per i server contenenti i data base, alla rete di Front End per la parte di presentazione, alla rete di gestione per l'amministrazione (funzione di supporto tecnico) della piattaforma;

Gli accessi alla rete sono segregati a livello di porte ed indirizzi IP. Gli accessi agli apparati di rete sono sottoposti a misure rigide di controllo e sono consentiti solamente agli amministratori della medesima.

IDS e IPS
Allo scopo di evitare che eventuali malintenzionati possano forzare le protezioni presenti per accedere in maniera illecita a dati riservati, la barriera di firewall applicativi fornisce anche un costante monitoraggio contro accessi non autorizzati tramite funzionalità IPS (Intrusion Prevention System).

I.1.3 Gestione degli incidenti di sicurezza

Gli incidenti di sicurezza (e più in generale tutti gli incidenti che avvengono) sono segnalati al servizio Service Desk aziendale tramite uno strumento elettronico di Help Desk (OTRS - Open-source Ticket Request System). Obbiettivo del servizio di Service Desk è:

- ripristinare la normale operatività del servizio (processo di produzione) il più rapidamente possibile, minimizzando l'impatto negativo sull'operatività, nel rispetto degli SLA concordati;
- soddisfare le richieste dei Soggetti produttori nell'ambito dell'utilizzo dell'infrastruttura tecnologica in ambiente di produzione;
- identificare le corrette modalità di escalation verso i livelli superiori del management.

Gli addetti del servizio Service Desk, prendono in carico le richieste e, in base ad una valutazione della gravità, seguendo la procedura di incident management definita, possono decidere di:

- gestire e risolvere direttamente il problema e chiudere la richiesta;
- scalare il problema al supporto tecnico di 2° livello e seguirne lo sviluppo;
- in caso di incidente grave (disastro) attivare l'unità di crisi preposta, tramite chiamata telefonica al Responsabile della sicurezza dei sistemi , che coordina le azioni di comunicazione e operative.

Ogni attività di questo tipo è tracciata in modo da poter evidenziare tempi di risposta, tempi e modalità di risoluzione, autori della risoluzione.
Nel caso specifico di incidenti di sicurezza viene eseguita una analisi sul tipo di incidente e viene deciso se:

- archiviare il fatto per successive statistiche;
- eseguire analisi più approfondite (forensic analisys) con coinvolgimento del Responsabile della sicurezza dei sistemi;
- attivare enti giuridici di controllo (autorità sulla privacy, polizia postale).

I.1.4 Gestione dei backup e Disaster Recovery

Il sistema di backup è organizzato in differenti modalità in relazione alle informazioni da salvare:
le funzionalità di Backup e Restore dei dati e delle configurazioni, sono state implementate utilizzando il software Tivoli Storage Manager (TSM), il cui client è stato installato su tutti i sistemi virtuali. Il server TSM utilizza la piattaforma Storage EMC-DL4100, costituita da due librerie di nastri virtuali (Virtual Tape Library) sul sito di Settimo Torinese e Moncalieri.
La funzionalità di backup sulla base dati è stata implementata utilizzando Oracle RMAN, con cadenza giornaliera e settimanale.

Vengono effettuate le seguenti policy di salvataggio:

- Backup Full settimanale e incrementale giornaliero (utilizzando RMAN)
- Copia mensile con retention 1 anno
- Copia annuale

- il salvataggio dei documenti su CDROM con consegna al Soggetto produttore, può essere eseguito su richiesta;
- il salvataggio dell'applicazione sia server che client è realizzato su supporto fisico esterno (Data tape o CDROM) per eseguire una rapida reinstallazione in caso di necessità;

- i supporti di backup hanno rotazione con frequenza settimanale.

Per le attività di salvataggio si eseguono i seguenti controlli:

- monitoraggio e controllo dei log-files dei risultati dei salvataggi (con frequenza quotidiana);
- ripristino periodico a campione dei dati;
- controllo della validità e della funzionalità (leggibilità) dei supporti.

I servizi di conservazione di Unimatica sono erogati tramite un Data Center Primario ed un Data Center Secondario che svolge il compito di Backup Remoto e di Disaster Recovery (D/R), al fine di garantire gli opportuni livelli di continuità del servizio.
I due Data Center hanno una distanza fra loro superiore a 300 Km. e la disponibilità di servizio è H24 per entrambi.
Il Data Center secondario permette di usufruire dei servizi in Produzione anche in caso di indisponibilità del Data Center Primario.
Per questo servizio Unimatica definisce con il Cliente il livello dei parametri che caratterizzano il servizio di D/R e di continuità operativa.

- Recovery Point Objective (RPO)
  Rappresenta il massimo tempo che intercorre tra la produzione di un dato sul sito primario e la sua messa in sicurezza (ad esempio attraverso backup) e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di disastro e che devono essere successivamente ripresi.
- Recovery Time Objective (RTO)
  È il tempo necessario per il pieno recupero dell'operatività di un sistema e del relativo processo organizzativo.

I.1.5 Gestione dei supporti di memorizzazione

La gestione dei supporti di memorizzazione, ove richiesti, segue i seguenti criteri:

- i media di memorizzazione elettronica sono correttamente etichettati in modo da fornire le seguenti informazioni: tipologia del media, tecnica della scrittura, data delle scrittura, contenuto. Per tecnica della scrittura si intende il formato in cui il media è stato preparato, nel nostro caso formato ISO, dipendentemente dal tipo supporto (CD o DVD);
- in caso di media che vengano riutilizzati per altri dati, essi vengono preventivamente riformattati tramite le tecniche di formattazione a basso livello, allo scopo di evitare che le informazioni ed i dati in essi contenuti possano essere presi e divulgati a soggetti non autorizzati;
- nel caso in cui i dati registrati sui media non più utilizzati non possano essere definitivamente cancellati si procede alla distruzione del media stesso, impedendone quindi il riutilizzo;
- i media sui quali sono eseguiti i salvataggi aziendali sono conservati in una sede differente rispetto a quella dove sono le strumentazioni cui i salvataggi si riferiscono ed in un luogo non accessibile se non al personale autorizzato,
- periodicamente è eseguita una verifica dei media e della disponibilità degli strumenti di accesso ai medesimi. In caso che per qualche media sia verificata la non disponibilità (anche prevista nel breve futuro) degli strumenti di accesso a qualche media si procede allo svecchiamento dei media tramite riversamento del loro contenuto in altro media.

I.2 Procedure di evoluzione e Change management

I cambiamenti che vengono apportati al sistema di conservazione di UNIMATICA S.p.A. risultano essere il prodotto di un'adeguata corrispondenza alle procedure di evoluzione tecnologica sia sulle strutture hardware sia su quelle software. Il Responsabile della funzione archivistica e il Responsabile dei sistemi informativi definiscono politiche, priorità e tempistiche affinché vengano garantite nel tempo integrità, disponibilità e sicurezza.

In caso di disservizi causati da problematiche riscontrate durante il processo di aggiornamento, è possibile effettuare il ripristino delle versioni precedenti così da assicurare il corretto e continuo svolgimento delle attività.

Il Responsabile del servizio di conservazione e il Responsabile della sicurezza dei sistemi informativi periodicamente si occuperanno di aggiornare la normativa e gli standard di riferimento in base all'evoluzione di questi.
La dettagliata descrizione delle procedure di evoluzione è riportata nel paragrafo 3.2.2 del documento "Piano della sicurezza del sistema di conservazione".

J. Monitoraggio e controlli

L'attività di monitoraggio e controllo viene portata avanti dal Responsabile della sicurezza dei sistemi e dal Responsabile della funzione archivistica, in accordo con il Responsabile del sistema di conservazione. Tale attività è finalizzata alla rilevazione di eventi di sicurezza, identificabili come stati che indicano il mancato rispetto delle politiche di sicurezza, che possano costituire una possibile fonte di rischio per il sistema di conservazione. Nello specifico gli obiettivi delle attività di monitoraggio sono la valutazione del livello del rischio associato agli eventi di sicurezza e la gestione di tali eventi, mediante strumenti come i Report dei controlli, agendo per il contenimento e/o eliminazione delle cause.

Gli eventi di sicurezza sono monitorati tramite il sistema di Log che consente la registrazione degli accessi e degli eventi (operazioni). Il sistema di Log è organizzato per registrare eventi ai vari livelli di astrazione della piattaforma:

- log del sistema operativo (incluso file system) atto ad identificare ingressi, anomalie ed errori;
- log del Data Base atti ad identificare ingressi, anomalie ed errori;
- log dei sistemi di rete (firewall e router) atti ad identificare ingressi, anomalie ed errori;
- log delle applicazioni software utilizzate (realizzati con vista a livello di singolo utente) atti ad identificare ingressi, principali attività svolte dagli utenti, sequenze del processo, accessi ai dati.

I log file degli applicativi contengono almeno le seguenti informazioni:

- utente che ha eseguito l'operazione;
- data e ora dell'operazione;
- operazione eseguita.

I file di log non sono modificabili o eliminabili da parte degli Utenti che usano il sistema (che non dispongono dei diritti di accesso).
I log di sistema sono analizzati da parte dei sistemisti qualora si rendesse necessaria un'indagine a seguito di un malfunzionamento del sistema.
La dettagliata descrizione dei processi relativi alle attività di monitoraggio e controlli è riportata nel documento "Piano della sicurezza del sistema di conservazione", capitolo 3.
I log vengono successivamente inviati in conservazione per mantenere traccia delle comunicazioni tra Soggetto produttore e sistema di conservazione.

J.1 Audit interni e Verifica dell'integrità degli archivi

Le verifiche ispettive interne vengono pianificate dal Responsabile sviluppo e manutenzione del sistema di conservazione, dal Responsabile sicurezza dei sistemi per la conservazione in accordo con il Responsabile del servizio di conservazione tenendo conto dello stato e dell'importanza dei processi e delle aree oggetto di verifica, nonché dei risultati delle precedenti verifiche. La frequenza con la quale vengono disposte le verifiche ispettive interne è almeno annuale. Al termine delle verifiche viene predisposto il relativo verbale di verifica.
I verbali di verifica possono essere consultati dal Soggetto produttore facendo richiesta al Responsabile del sistema di conservazione e al Responsabile sviluppo e manutenzione.
La scelta del personale verificatore viene fatta in modo da garantire obiettività ed imparzialità nel processo di verifica.

Il libro delle comunicazioni e dei verbali delle verifiche periodiche allegato al Manuale, che UNIMATICA S.p.A. mantiene aggiornato, tiene traccia di:

- verifiche periodiche sullo stato di conservazione dei supporti di memorizzazione, tendenti a verificare con l'ausilio di software appropriati, lo stato di conservazione dei supporti di memorizzazione e a ricercare eventuali difetti,
- verifiche periodiche sui documenti conservati, tendenti a verificare periodicamente, con cadenza non superiore a cinque anni, l'effettiva integrità dei documenti stessi. La procedura che gestisce il processo di conservazione presenta delle funzionalità di controllo massivo dei dati conservati: tali tipologie di controllo consistono nell'impostare/configurare a livello informatico la periodicità dei controlli da effettuare; attualmente, il sistema è configurato per verificare giornalmente un milione di documenti, eseguendo controlli a rotazione su documenti diversi. L'applicazione informatica che gestisce il processo di conservazione, effettua un check automatico loggando per ogni Pacchetto conservato, la data/ora in cui è stata eseguita l'ultima verifica di integrità. Il sistema segnala eventuali difettosità sulla console di sistema. Nel caso ciò si verifichi le figure responsabili competenti dovranno preoccuparsi di recuperare la copia di backup ed effettuarne immediatamente la duplicazione. Tale verifica viene eseguita sia sui dati contenuti nell'archivio digitale on-line (sito primario) che sui dati presenti nell'archivio digitale in Disaster Recovery (sito secondario).

Il "libro delle comunicazioni e dei verbali delle verifiche periodiche" contiene le seguenti informazioni:

- variazioni Famiglie documentali oggetto di conservazione
- variazioni normative
- registro delle variazioni di ruoli e funzioni dei soggetti coinvolti nel processo di conservazione
- registro delle variazioni del processo di conservazione
- registro delle comunicazioni all'Agenzia delle Entrate
- registro delle edizioni del Manuale della conservazione
- scadenziario delle comunicazioni
- registro delle comunicazioni effettuate
- registro delle modifiche all'archivio
- registro delle anomalie
- registro dei riversamenti diretti o sostitutivi
- piano delle verifiche
- registro delle verifiche ispettive
- registro dei documenti distrutti

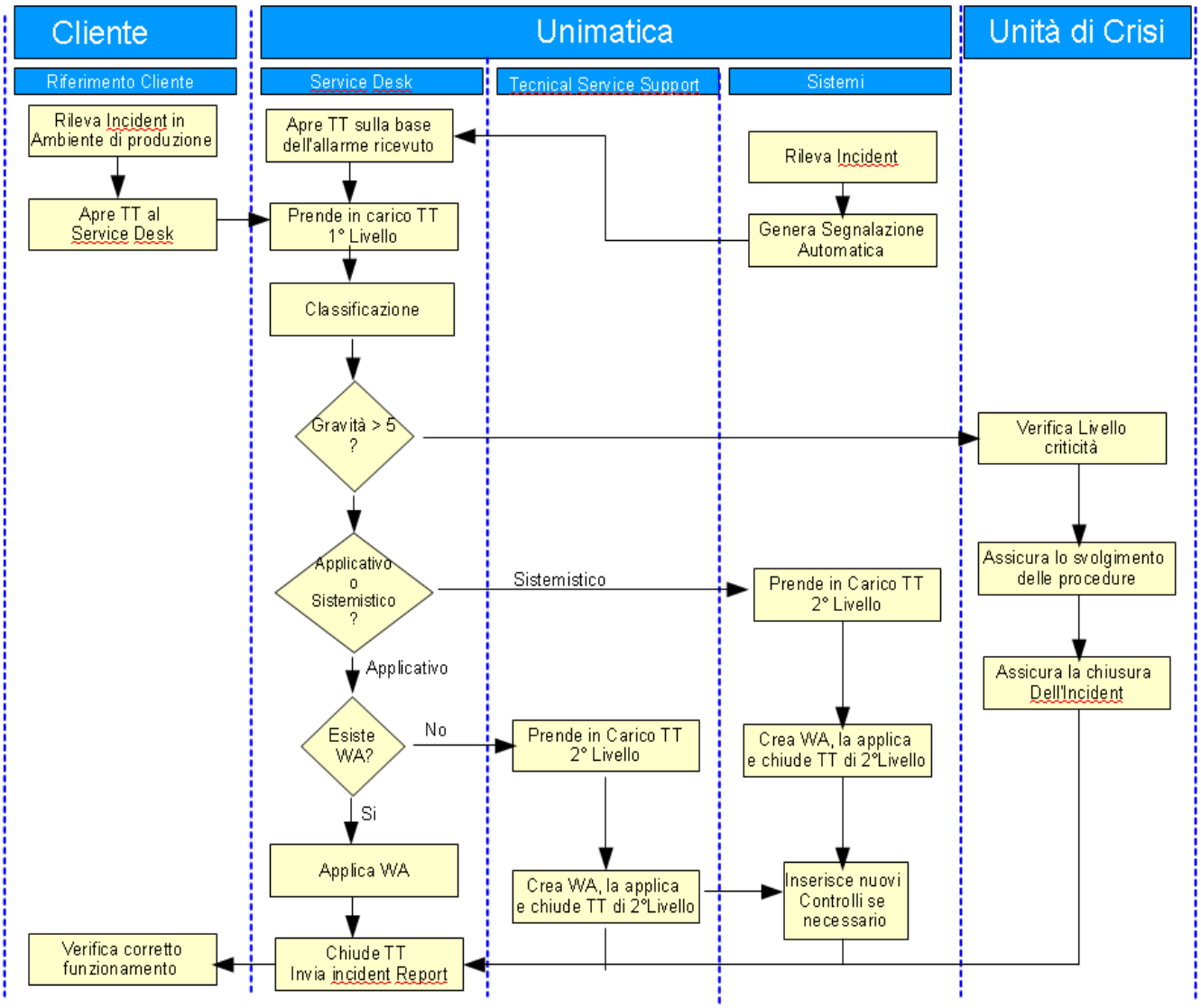
J.2 Gestione delle anomalie

UNIMATICA S.p.A. gestisce le anomalie attraverso l'utilizzo di due funzioni aziendali che fanno parte del settore tecnico di UNIMATICA: il Service desk e l'AM Settore conservazione e Settore sistemi.
Le suddette funzioni garantiscono la gestione di tutte le anomalie relative al servizio di Conservazione assicurando due tipologie di interventi:

- interventi **reattivi** a fronte delle segnalazioni degli utenti;

- Interventi **proattivi** a fronte di generazioni spontanee di eventi e segnalazioni generati dai sistemi di monitoraggio infrastrutturale e applicativo.

Le anomalie sono gestite attraverso l'utilizzo del processo di Incident Management di UNIMATICA, il cui processo è rappresentato dal seguente schema funzionale:



Di seguito vengono descritti gli step del processo più significativi:

1. apertura e presa in carico della segnalazione al Service Desk UNIMATICA;
2. classificazione dell'Incident secondo il livello di criticità, macrotipologia e livello di competenza IT;
3. implementazione workaround, soluzione Incident;
4. compilazione Incident Report.

Fase 1:
il Service Desk UNIMATICA prende in carico la segnalazione dell'incident, che può provenire dal Soggetto produttore o dai sistemi, tracciandolo sul sistema di Trouble Ticketing e verificando se sono correlabili eventi di Tipo Critical segnalati in quel momento.

Fase 2:
Il Service Desk classifica l'incident secondo i parametri di criticità segnalati e/o rilevati secondo l'area di competenza e verifica la possibilità di applicare autonomamente il workaround necessario per risolvere l'Incident.

Fase 3:
Nel caso in cui esista un workaround da applicare, il Service Desk UNIMATICA la applica, notifica la soluzione dell'incident all'utente che ha segnalato l'anomalia attendendo la conferma relativa alla soluzione applicata.
Nel caso in cui non esista un workaround applicabile, il Service Desk UNIMATICA inoltra il problema al secondo livello specialistico, sia esso applicativo (Service Support) o infrastrutturale (Sistemi). Il Secondo livello specialistico definisce il workaround necessario e lo implementa notificando la chiusura dell'intervento al Service Desk UNIMATICA.
Il Secondo livello specialistico valuta se è necessario implementare nuove sonde di monitoraggio in Control Room, in caso affermativo le implementa e le rende operative.

Fase 4:
Al termine dell'intervento viene fornito un Incident Report contenente questo set minimo di informazioni:

- Data/Ora Segnalazione Anomalia;
- Descrizione dell'anomalia Segnalata;
- Data/Ora Presa in Carico Anomalia;
- Descrizione problema tecnico rilevato;
- Data/Ora Chiusura Anomalia;
- Tipo di WA Applicata (se di 1° o 2° Livello) e descrizione WA;
- Necessità di implementare una soluzione definitiva (Si/No);
- Descrizione Soluzione Definitiva;
- Tempi di implementazione.

J.3 Reportistica di servizio

Il sistema di conservazione UniStorage gestisce un sistema di tracciatura nel quale vengono registrati tutti i singoli eventi che riguardano sia la gestione dei Pacchetti, dalla fase di versamento a quella di distribuzione, sia i singoli documenti. Questa tracciatura, costruita per implementare un "forensic log", è in un formato rigido e non disabilitabile. La tracciatura è prerequisito indispensabile per l'esecuzione delle operazioni.
Nel dettaglio, il sistema di log prevede la registrazione di informazioni relative alle diverse funzioni del processo di conservazione per tutte le fasi descritte nel capitolo G.

La reportistica di servizio che UNIMATICA gestisce è di due Tipologie:

1. Reportistica relativa al processo di Conservazione,

2. Reportistica del servizio di Supporto Utente (Service Desk e AM Settore conservazione e Settore sistemi).

Tipologia 1:
vengono prodotti periodicamente i seguenti report:

- Report Consuntivo Pacchetti di archiviazione,
- Report Excel che fornisce la lista dei Pacchetti di archiviazione e che comprende questo set Minimo di informazioni:
    1. Ragione Sociale Cliente;
    2. Numero documenti conservati e spazio occupato nel periodo totali e per tipologia di documento;
    3. Numero documenti conservati e spazio occupato totali e per tipologia di documento.

Tipologia 2:
viene prodotto un report di Servizio che fornirà le seguenti evidenze:

- Numero Incident Segnalati
- Media Tempo di presa in carico Incident
- Media Tempo di chiusura Incident
- Numero Service Request
- Media Tempo di presa in Carico Service Request
- Media Tempo di Chiusura Service Request

Periodicità: Semestrale

Appendice A

Allegati al Manuale della conservazione:

- Allegato ‘Infrastrutture’.

Specificità del contratto e documenti di riferimento:

- Scheda Cliente.
- FlussiConservazione_ver 1.7
- Specifiche del servizio web per la consegna anticipata di documenti nel Sistema di conservazione.
- ‘Manuale dell’interfaccia web'.
- ‘Libro delle comunicazioni e dei verbali delle verifiche periodiche’.

9.8 Manuale del Conservatore Enerj

Manuale di Conservazione

di Enerj S.r.l.

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	24/09/2015	Ferdinando Auletta	*Responsabile del Servizio di Conservazione*
Verifica	24/09/2015	Silvano Artioli	*Responsabile della Sicurezza del Sistema di Conservazione*
Approvazione	24/09/2015	Giovanni Auletta	*Direzione*

REGISTRO DELLE VERSIONI

Num. versione	Data emissione	Modifiche apportate
1	Settembre 2005	Stesura
2	Febbraio 2006	Aggiornamento
3	Ottobre 2006	Aggiornamento
4	Marzo 2007	Aggiornamento
5	Novembre 2008	Aggiornamento
6	Marzo 2009	Aggiornamento
7	Marzo 2010	Aggiornamento
8	Marzo 2013	Aggiornamento
9	Novembre 2014	Aggiornamento
10	Febbraio 2015	Aggiornamento
11	Settembre 2015	Aggiornamento per accreditamento AGID

INDICE DEL DOCUMENTO

1 INTRODUZIONE 5
2 SCOPO E AMBITO DEL DOCUMENTO 6
2.1 Specificità di contratto 6
3 TERMINOLOGIA 7
3.1 GLOSSARIO 7
3.2 ACRONIMI 15
4 NORMATIVA E STANDARD DI RIFERIMENTO 18
4.1 Normativa inerente per la conservazione - Legislazione Italiana 18
4.2 Altre normative 19
4.3 Standard tecnici internazionali di riferimento 20
4.3.1 ISO/IEC 20
4.3.2 ETSI (European Telecommunications Standards Institute) 20
4.3.3 OAIS (Open Archival Information System) 21
5 RUOLI E RESPONSABILITÀ 22
5.1 Ruoli esterni al SdC 22
5.1.1 Produttore 22
5.1.2 Fruitore 22
5.1.3 Certification Authority e fornitori di servizi di Firma Digitale 22
5.1.4 Time Stamping Authority 22
5.2 Ruoli interni al SdC 22
5.2.1 Responsabile del Servizio di Conservazione (RSC) 22
5.2.2 Responsabile della sicurezza dei sistemi per la conservazione (RQS) 23
5.2.3 Responsabile funzione archivistica di conservazione (RFA) 23
5.2.4 Responsabile del Trattamento dei Dati personali (DIR) 23
5.2.5 Responsabile sistemi informatici per la conservazione (RSI) 24
5.2.6 Responsabile sviluppo e manutenzione del sistema (RSM) 24
6 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE 26
6.1 Organigramma 26
6.2 Strutture organizzative 26
6.2.1 Attività proprie di ciascun contratto di servizio di conservazione 26
6.2.2 Attività proprie di gestione dei sistemi informativi 27

7 OGGETTI SOTTOPOSTI A CONSERVAZIONE 29
7.1 Oggetti conservati 29
7.2 Formati 30
7.3 Pacchetto di versamento 31
7.4 Pacchetto di archiviazione 33
7.5 Pacchetto di distribuzione 37
8 IL PROCESSO DI CONSERVAZIONE 39
8.1 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico 40
8.2 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti 40
8.3 Accettazione dei pacchetti di versamento e generazione del rapporto di versamento e di presa in carico 41
8.4 Rifiuto dei PdV e modalità di comunicazione delle anomalie 43
8.5 Preparazione e gestione del PdA 43
8.6 Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione 44
8.7 Produzione di duplicati e copie informatiche ed eventuale intervento del pubblico ufficiale nei casi previsti 47
8.7.1 Produzione di duplicati informatici 47
8.7.2 Produzione di copie informatiche/analogiche ed estratti di documenti informatici 47
8.7.3 Produzione di copie informatiche di documenti analogici 48
8.8 Scarto dei pacchetti di archiviazione 48
8.9 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori 48
8.10 Conservazione delle comunicazioni intercorrenti tra il SdC e i fruitori del servizio di conservazione. 49
9 IL SISTEMA DI CONSERVAZIONE 50
9.1 Componenti Logiche 50
9.2 Componenti Tecnologiche 51
9.3 Componenti Fisiche 52
9.4 Procedure di gestione e di evoluzione 54
9.4.1 Conduzione e manutenzione del sistema di conservazione 54
9.4.2 Gestione e conservazione dei log 54
9.4.3 Change management 55
9.4.4 Verifica periodica di conformità a normativa e standard di riferimento 55
10 MONITORAGGIO E CONTROLLI 56
10.1 Procedure di monitoraggio applicativo 56

10.2 Procedure di monitoraggio infrastrutturale 56
10.3 Verifica dell'integrità degli archivi 56
10.4 Soluzioni adottate in caso di anomalie 58
10.5 Sicurezza del SdC 58

1 INTRODUZIONE

Enerj, società operante nel settore informatico dal 2005, progetta, sviluppa e distribuisce piattaforme software per la gestione degli archivi informatici, l'archiviazione documentale e la conservazione digitale a norma di legge.

Nell'ambito della gestione delle proprie attività peculiari, Enerj eroga un servizio di conservazione digitale rivolto alle organizzazione pubbliche e private.

Allo scopo di garantire il livello massimo di qualità dei servizi e dei prodotti distribuiti, Enerj ha implementato un sistema di gestione della qualità e della sicurezza delle informazioni, ottenendo le certificazioni:

- ISO/IEC 27001:2013
- UNI EN ISO 9001:2008

dall'ente CSQA (accreditato da Accredia) per le seguenti attività:

"Progettazione, sviluppo e distribuzione di software e servizi informatici; attività di assistenza alla clientela, erogazione di archiviazione e conservazione digitale, di gestione elettronica di documenti e di fatturazione elettronica per enti pubblici e privati".

2 SCOPO E AMBITO DEL DOCUMENTO

Il Manuale di Conservazione di Enerj (di seguito MdC) è un documento informatico redatto al fine di documentare il Sistema di Conservazione (SdC):

- dei documenti informatici, prodotti dai Clienti di Enerj nel corso della gestione della propria attività e dell'erogazione dei propri servizi di gestione degli archivi informatici;
- di altri documenti informatici che, per qualsiasi altra ragione, Enerj ritenga opportuno gestire tramite il sistema documentato dal presente manuale.

Il MdC è redatto inoltre al fine di documentare le modalità e le tempistiche adottate nella gestione dei processi di conservazione dei documenti informatici che ne consentono il mantenimento del valore legale (civile e fiscale) in base a quanto previsto dal panorama normativo vigente.

Il sistema assicura la conservazione dei documenti informatici garantendone il mantenimento delle caratteristiche di autenticità, integrità, intelligibilità, affidabilità, reperibilità e interoperabilità.

Il presente documento sostituisce le versioni precedenti.

2.1 Specificità di contratto

Il MdC descrive il funzionamento delle componenti generali del Sistema di Conservazione (SdC) implementato e gestito da Enerj. Il MdC non ha al suo interno componenti personalizzate o specifiche per singolo cliente. Ogni aspetto particolare del servizio di conservazione quale ad esempio, i documenti coinvolti, metadati scelti per l'archiviazione dei documenti, formati dei documenti, modalità di trasferimento e riferimenti presso il cliente, viene concordato e descritto nel Contratto di Servizio di Conservazione e nello Schema di conservazione (MCD01).

Torna al sommario

3 TERMINOLOGIA

3.1 GLOSSARIO

Preliminarmente si conviene di attribuire, ai termini tecnici utilizzati nel testo che segue, il significato di cui:

- all’art. 1, comma 1 del Decreto Legislativo n. 82 del 7 marzo 2005 (Codice dell'Amministrazione Digitale) e successive modifiche;
- all'art. 1 del Decreto del Presidente del Consiglio dei Ministri del 30 marzo 2009.
- all'Allegato: Regole tecniche in materia di documento informatico e gestione documentale, protocollo informatico e conservazione di documenti informatici: "Glossario e Definizioni" del Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013.

L'intera struttura e tutti i contenuti del manuale sono redatti sulla base dei modelli, della terminologia e delle indicazioni fornite dall'Agenzia per l'Italia Digitale.

Di seguito si riporta in ordine alfabetico il Glossario dei termini e Acronimi ricorrenti nel testo o comunque giudicati significativi in relazione alla materia trattata.

TERMINE	DEFINIZIONE
accesso	operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici
accreditamento	riconoscimento, da parte dell'Agenzia per l'Italia Digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione
affidabilità	caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico
archivio	complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività
archivio informatico	archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico
attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico
autenticità	caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico
base di dati	collezione di dati registrati e correlati tra loro

certificatore accreditato	soggetto, pubblico o privato, riconosciuti dall' Agenzia per l'Italia Digitale che emettono certificati qualificati (per la firma digitale) e certificati di autenticazione (per le carte nazionali dei servizi).
ciclo di gestione	arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo
conservatore accreditato	soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia Digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, dall'Agenzia per l'Italia Digitale
conservazione	insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione
Contratto di Servizio	Documento contrattuale stipulato tra il Cliente (Produttore) ed Enerj (Conservatore) che contiene la descrizione analitica del servizio. Gli accordi di dettaglio sono riportati negli specifici allegati
destinatario	identifica il soggetto/sistema al quale il documento informatico è indirizzato
duplicazione dei documenti informatici	produzione di duplicati informatici
esibizione	operazione che consente di visualizzare un documento conservato e di ottenerne copia
evidenza informatica	una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica

fascicolo informatico	aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del CAD.
formato	modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
funzione di *hash*	una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
generazione automatica di documento informatico	formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni
Hardware Security Module	dispositivi per la gestione sicura delle firme digitali che ne velocizzano l'apposizione e ne permettono la completa gestione in remoto
identificativo univoco	sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione

immodificabilità	caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso
impronta	la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di *hash*
insieme minimo di metadati del documento informatico	complesso dei metadati, la cui struttura è descritta nell'allegato 5 del DPCM 3 dicembre 2013, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta
integrità	insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato
interoperabilità	capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi
JDoc	Software proprietario di Enerj di gestione elettronica dell'archivio informatico
leggibilità	insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti
log di sistema	registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati

Manuale della Sicurezza del Sistema Informativo	documento interno che descrive le attività, le caratteristiche tecniche e procedurali del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio
marca temporale	Riferimento temporale rilasciato da un certificatore accreditato che garantisce data e ora certa
memorizzazione	processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici
metadati	insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 del DPCM 3 dicembre 2013
pacchetto di archiviazione	pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del DPCM 3 dicembre 2013
pacchetto di distribuzione	pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta
pacchetto di versamento	pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel Manuale di Conservazione

pacchetto informativo	contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare
piano della sicurezza del sistema di conservazione	documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza
presa in carico	accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione
processo di conservazione	insieme delle attività finalizzate alla conservazione dei documenti informatici
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 il responsabile della gestione documentale
rapporto di versamento	documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore

registro di protocollo	registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti
responsabile della conservazione	soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 delle regole tecniche del sistema di conservazione
responsabile del trattamento dei dati	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali
riferimento temporale	informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento
scarto	operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale
Schema di Conservazione	modulo interno personalizzato per ogni Cliente contenente la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione
sistema di conservazione	sistema di conservazione dei documenti informatici
sistema di gestione informatica dei documenti	sistema che consente la tenuta di un documento informatico come ad esempio il software di Enerj JDoc

staticità	caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione
utente	persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse

3.2 ACRONIMI

ACRONIMO	DEFINIZIONE
AGID	Agenzia per l'Italia Digitale
CAD	Codice dell'Amministrazione Digitale
DIR	Direzione aziendale
DPCM	Decreto del Presidente del Consiglio dei Ministri del 03 dicembre 2013
FTP (e FTPS)	File Transfer Protocol - Protocollo informatico di trasmissione di informazioni tra mittenti e destinatari, FTPS è il medesimo protocollo ulteriormente implementato con appositi criteri informatici allo scopo di aumentarne il livello sicurezza.
HSM	Hardware Security Module
IPdA	Indice del pacchetto di archiviazione
ISMS	Information Security Management System - Sistema di gestione della qualità e della sicurezza delle informazioni di Enerj

MdC	Manuale di Conservazione
MSI	Manuale della Sicurezza del Sistema Informativo
OAIS	Open Archival Information System
PBK	Piano di Backup
PCO	Piano di Continuità Operativa del Business e Disaster Recovery
PCD	Procedura di Gestione della Conservazione
PGC	Procedura di Gestione Clienti e Assistenza
PdA	Pacchetto di Archiviazione
PdD	Pacchetto di Distribuzione
PdV	Pacchetto di Versamento
RCM	Responsabile gestione Commerciale, Comunicazione e Marketing
RDA	Responsabile Direzione Amministrativa e contabile
RDT	Responsabile Direzione Tecnica
RFA	Responsabile della Funzione Archivistica
RGC	Responsabile Gestione dei Clienti e assistenza
RGP	Responsabile Gestione del Personale

RQS	Responsabile della sicurezza dei sistemi per la conservazione
RSC	Responsabile Servizio di Conservazione
RSI	Responsabile dei sistemi informativi per la conservazione
RSM	Responsabile sviluppo Software e Manutenzione
SdC	Sistema di Conservazione
SLA	Service Level Agreement

4 NORMATIVA E STANDARD DI RIFERIMENTO

Di seguito è riportata la principale normativa di riferimento per l'attività di conservazione a livello nazionale.

Alla data l'elenco dei principali riferimenti normativi italiani in materia, ordinati secondo il criterio della gerarchia delle fonti, è riportato di seguito.

4.1 Normativa inerente per la conservazione - Legislazione Italiana

- **Codice Civile –** "Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica.";
- **Legge 7 agosto 1990, n. 241 e s.m.i.** – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- **Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i.** – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- **Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i.** – Codice dei Beni Culturali e del Paesaggio;
- **Decreto Legislativo 11 febbraio 2005 n. 68** . Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3;
- **Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i.** – Codice dell'amministrazione digitale (CAD);
- **Decreto del 2 novembre 2005** - Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata (Gazzetta Ufficiale n. 266 del 15-11-2005) del Ministro per l'Innovazione e le Tecnologie;
- **Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009** - Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici;
- **Deliberazione Cnipa del 21 maggio 2009, n. 45** (come modificata dalla determinazione dirigenziale DigitPA n. 69/2010). Regole per la creazione dei certificati di firma e di marca che quelle per il loro utilizzo, riconoscimento e verifica;

- **Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013** – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
- **Decreto del Presidente del Consiglio dei Ministri 21 marzo 2013** - Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni;
- **Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013** - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- **Circolare AGID 10 aprile 2014, n. 65** - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.
- **Decreto del Ministero dell'Economia e delle Finanze 17 giugno 2014** - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005.

4.2 Altre normative

- **Decreto Legislativo 1 settembre 1993 n.385** - "Testo unico delle leggi in materia bancaria e creditizia";
- **Decreto Legislativo 6 settembre 2005, n. 206** - Codice del consumo, a norma dell'articolo 7 della legge 29 luglio 2003, n. 229;
- **Decreto Legislativo 9 aprile 2008, n. 81** - Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro;
- **Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i.** – Codice in materia di protezione dei dati personali;

- **Legge 22.04.1941 n° 633 , G.U. 16.07.1941 e s.m.i.** - Legge sul diritto d'autore.

4.3 Standard tecnici internazionali di riferimento

4.3.1 ISO/IEC

- **UNI EN ISO 9000:2005** - Sistemi di gestione per la qualità - Fondamenti e vocabolario;
- **UNI EN ISO 9001:2008 -** Sistemi di gestione per la qualità - Requisiti;
- **UNI EN ISO 9004:2009 -** Gestire un'organizzazione per il successo durevole: L'approccio della gestione per la qualità;
- **UNI EN ISO 19011:2012 -** Linee guida per audit di sistemi di gestione;
- **ISO 14721:2012 -** Space data and information transfer systems - Open archival information system (OAIS) - Reference model; Sistema informativo aperto per l'archiviazione;
- **UNI ISO 31000:2010 -** Gestione del rischio - Principi e linee guida;
- **ISO/IEC 27000:2012 -** Overview and vocabulary;
- **ISO/IEC 27001:2013 -** Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- **ISO/IEC 27002:2013 -** Code of practice for information security controls;
- **ISO/IEC 27005:2011 -** Information technology -- Security techniques -- Information security risk management;
- **UNI ISO 15489-1:2006** - Informazione e documentazione - Gestione dei documenti di archivio - Principi generali sul record management;
- **UNI ISO 15489-2:2007** - Informazione e documentazione - Gestione dei documenti di archivio - Linee Guida sul record management;
- **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.

4.3.2 ETSI (European Telecommunications Standards Institute)

- **ETSI TS 101 533-1 V1.3.1 (2012-04)** Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni
- **ETSI TR 101 533-2 V1.3.1 (2012-04) -** Electronic Signatures and

Infrastructures (ESI); Data Preservation Systems Security; Part 2: Guidelines for Assessors; Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni

- **ETSI GS ISI 001-1 V1.1.1 (2013-04) -** Information Security Indicators (ISI); Indicators (INC); Part 1: A full set of operation al indicators for organizations to use to benchmark their security posture;
- **ETSI GS ISI 001-2 V1.1.1 (2013-04) -** Information Security Indicators (ISI);Indicators (INC); Part 2: Guide to select operational indicators based on the full set given in part 1;
- **ETSI GS ISI 002 V1.1.1 (2013-04) -** Information Security Indicators (ISI); Event Model A security event classification model and taxonomy;
- **ETSI GS ISI 003 V1.1.2 (2014-06) –** Information Security Indicators (ISI); Key Performance Security Indicators (KPSI) to evaluate the maturity of security event detection;
- **ETSI GS ISI 004 V1.1.1 (2013-12) -** Information Security Indicators (ISI); Guidelines for event detection implementation.

4.3.3 OAIS (Open Archival Information System)

- Consultative Committee for Space Data Systems (CCSDS – Audit and Certification of Trustworthy Digital Repositories – Recommended Practice – CCSDS 652.0-M-2 - 2012;
- Consultative Committee for Space Data Systems (CCSDS – Reference Model for an Open Archival Information System (OAIS).

Torna al sommario

5 RUOLI E RESPONSABILITÀ

5.1 Ruoli esterni al SdC

5.1.1 Produttore

È il Cliente che, avvalendosi dei servizi di gestione degli archivi informatici erogati da Enerj, conferisce al SdC i documenti informatici (di cui è titolare) da conservare elettronicamente.

5.1.2 Fruitore

Il ruolo del Fruitore del SdC è ricoperto dai soggetti che, opportunamente autorizzati, accedono al SdC ottenendo uno o più Pacchetti di Distribuzione (PdD).

5.1.3 Certification Authority e fornitori di servizi di Firma Digitale

I certificati crittografici utilizzati nel processo di firma sono certificati rilasciati da Certificatori accreditati dall'AGID.

Il dispositivo HSM deputato alle operazioni di firma è conforme al D.P.C.M. 22 febbraio 2013 e viene mantenuto in un Data Center, sito presso il Certificatore Accreditato, con certificazioni ISO 27001:2005, ISO 9001:2008, ISO 14001:2004, OHSAS 18001:2007.

5.1.4 Time Stamping Authority

Le marche temporali utilizzate nel processo di apposizione del riferimento temporale sono rilasciate da Certificatori accreditati dall'AGID.

5.2 Ruoli interni al SdC

Per motivi di riservatezza il nominativo ed i riferimenti dei soggetti riportati nelle sezioni che seguono sono omessi dal presente manuale e sono esclusivamente indicati nel Contratto di Servizio nel quale sono anche presenti le attività affidate al Responsabile del Servizio di Conservazione, i periodi di permanenza negli incarichi riferiti ai diversi profili e le eventuali deleghe.

5.2.1 Responsabile del Servizio di Conservazione (RSC)

Il RSC è individuato, all'interno dell'organigramma di Enerj, come Responsabile dei Servizi di gestione dell'archivio informatico e conservazione ed è incaricato delle seguenti funzioni:

- Definisce e attua le politiche complessive del sistema di conservazione, nonché il governo della gestione del sistema di conservazione;

- Definisce le caratteristiche e i requisiti del sistema di conservazione in conformità alla normativa vigente;
- Assicura la corretta erogazione del servizio di conservazione all'ente produttore;
- Gestisce le convenzioni, definisce gli aspetti tecnico-operativi e valida i disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.

5.2.2 Responsabile della sicurezza dei sistemi per la conservazione (RQS)

- Definisce le politiche di rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza;
- Segnala le eventuali difformità a RSC, individua e pianifica le necessarie azioni correttive.

5.2.3 Responsabile funzione archivistica di conservazione (RFA)

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

5.2.4 Responsabile del Trattamento dei Dati personali (DIR)

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

5.2.5 Responsabile sistemi informatici per la conservazione (RSI)

- Gestisce l'esercizio delle componenti hardware e software del sistema di conservazione;
- Monitora il mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore;
- Segnala le eventuali difformità degli SLA al RSC e individua e pianifica le necessarie azioni correttive;
- Pianifica lo sviluppo delle infrastrutture tecnologiche del sistema di conservazione;
- Controlla e verifica i livelli di servizio erogati da terzi e segnala le eventuali difformità al RSC.

5.2.6 Responsabile sviluppo e manutenzione del sistema (RSM)

- Coordina lo sviluppo e la manutenzione delle componenti hardware e software del sistema di conservazione;
- Pianifica e monitora i progetti di sviluppo del sistema di conservazione;
- Monitora gli SLA relativi alla manutenzione del sistema di conservazione;
- Si interfaccia con il produttore in relazione alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche;
- Gestisce lo sviluppo degli applicativi software connessi al servizio di conservazione.

Di seguito vengono riportati i nominativi attualmente in carica.

Ruolo	**Nominativo in carica**
Responsabile del Servizio di Conservazione (RSC)	Auletta Ferdinando
Responsabile della sicurezza dei sistemi per la conservazione (RQS)	Artioli Silvano
Responsabile funzione archivistica di conservazione (RFA)	Auletta Ferdinando
Responsabile del Trattamento dei Dati personali (DIR)	Auletta Giovanni

Ruolo	Nominativo in carica
Responsabile sistemi informatici per la conservazione (RSI)	Recchia Mauro
Responsabile sviluppo e manutenzione del sistema (RSM)	Zanella Stefano

Torna al sommario

6 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

6.1 Organigramma

Le strutture organizzative coinvolte nel servizio di conservazione sono illustrate nell'organigramma (ALL01) allegato.

6.2 Strutture organizzative

Di seguito si descrivono le strutture organizzative che intervengono nelle principali funzioni che riguardano il servizio di conservazione, in particolare si specificano, per ogni attività svolta dalle strutture, le relative figure di riferimento.

6.2.1 Attività proprie di ciascun contratto di servizio di conservazione

Attività	Figura di riferimento	Strutture organizzative interagenti
Attivazione del servizio di conservazione (a seguito della sottoscrizione di un contratto)	RGC	Gestione commerciale, comunicazione e marketing Gestione clienti e assistenza Gestione della funzione archivistica Servizi di gestione dell'archivio informatico e conservazione
Acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento	RSC	Servizi di gestione dell'archivio informatico e conservazione Gestione clienti e assistenza
Preparazione e gestione del pacchetto di archiviazione	RSC	Servizi di gestione dell'archivio informatico e conservazione Gestione della funzione archivistica
Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta	RSC	Servizi di gestione dell'archivio informatico e conservazione Gestione clienti e assistenza Gestione sistemi informativi

Attività	Figura di riferimento	Strutture organizzative interagenti
Scarto dei pacchetti di archiviazione	RSC	Gestione della funzione archivistica Servizi di gestione dell'archivio informatico e conservazione
Chiusura del servizio di conservazione (al termine di un contratto)	RSC	Gestione clienti e assistenza Gestione commerciale, comunicazione e marketing Gestione della funzione archivistica Direzione amministrativa e contabile

6.2.2 Attività proprie di gestione dei sistemi informativi

Attività	Figura di riferimento	Strutture organizzative interagenti
Conduzione e manutenzione del sistema di conservazione	RSM	Gestione sviluppo software e manutenzione Gestione sistemi informativi Gestione della qualità e della sicurezza delle informazioni e dei sistemi
Monitoraggio del sistema di conservazione	RQS	Gestione della qualità e della sicurezza delle informazioni e dei sistemi Servizi di gestione dell'archivio informatico e conservazione Gestione della funzione archivistica Presidenza (Responsabile del trattamento dei dati personali)

Attività	Figura di riferimento	Strutture organizzative interagenti
Change management	RFA	Gestione della qualità e della sicurezza delle informazioni e dei sistemi Gestione della funzione archivistica Gestione clienti e assistenza Gestione commerciale, comunicazione e marketing Direzione tecnica
Verifica periodica di conformità a normativa e standard di riferimento	RQS	Gestione della qualità e della sicurezza delle informazioni e dei sistemi Gestione della funzione archivistica Direzione tecnica Presidenza (Responsabile del trattamento dei dati personali)

Torna al sommario

7 OGGETTI SOTTOPOSTI A CONSERVAZIONE

Nella presente sezione si descrivono le tipologie degli oggetti e dei pacchetti in essi contenuti sottoposti a conservazione.

7.1 Oggetti conservati

Il SdC acquisisce pacchetti informativi trasformandoli in PdA e conservandoli in linea con i requisiti della normativa.

Un pacchetto informativo può contenere qualsiasi tipologia di documento informatico, nonché una o più aggregazioni documentali informatiche. Di seguito si descrivono le principali aggregazioni gestite:

Tipologia documentale	Descrizione
Fatture elettroniche (in formato XML FatturaPA)	Fatture commerciali emesse e/o ricevute dalle Amministrazioni Pubbliche in formato FatturaPA.
Fatture clienti	Fatture commerciali attive (elettroniche ed analogiche) emesse da organizzazioni private e pubbliche fruitrici del servizio di conservazione.
Fatture fornitori	Fatture commerciali passive (elettroniche ed analogiche) ricevute da organizzazioni private e pubbliche fruitrici del servizio di conservazione.
Documenti di trasporto	Documenti emessi per giustificare il trasferimento di un materiale da cedente a cessionario attraverso il trasporto dello stesso, in base a quanto sancito dal Testo del D.P.R. 14 agosto 1996 n. 472. ("Regolamento di attuazione delle disposizioni contenute nell'art. 3, comma 147, lettera d), della legge 28 dicembre 1995, n. 549, relativamente alla soppressione dell'obbligo della bolla di accompagnamento delle merci viaggianti")
Libri contabili	Libri, registri, documenti e altre scritture contabili obbligatorie e/o richieste dalla natura e dalle dimensioni dell'impresa, quali (a titolo esemplificativo): libro giornale, libro inventari, piano dei conti, libro mastro, libro magazzino, registri iva, ecc....

Documenti di protocollo	Documenti afferenti al sistema di gestione del protocollo informatico nella Pubblica Amministrazione quali (a titolo esemplificativo): mail PEC, registro di protocollo.
Atti amministrativi	Documenti formati dalla Pubblica Amministrazione nella gestione ordinaria delle sua attività istituzionale, quali (a titolo esemplificativo): delibere di giunta, delibere di consiglio, determine, ordinanze, albo pretorio, contratti, ecc...
Mandati di pagamento e reversali informatici	Documenti di interscambio tra la Pubblica Amministrazione e l'Istituto Bancario gestore del Servizio di Tesoreria.

I metadati di ogni tipologia documentale sono definiti in modo parametrico attraverso il SdC per ogni singolo cliente e formalizzati nel Contratto di Servizio. Nella definizione dei metadati dei documenti aventi rilevanza fiscale si fa riferimento all'art. 3 del DMEF 17 giugno 2014.

Il set di metadati minimi associati ai documenti informatici è allineato con quanto definito dall'allegato 5 del DPCM.

7.2 Formati

Il SdC, in linea con quanto indicato nell'allegato 2 del DPCM, gestisce i documenti informatici mediante diversi formati di file tra i quali si indicano, di seguito, i principali:

Formato del file	Visualizzatore	Standard	Versione del formato	Sistema Operativo
PDF - PDF/A	Adobe Reader	ISO 32000-1 ISO 19005-1:2005 ISO 19005-1:2011	1.4 -1.7	Qualsiasi
XML	Browser internet o text editor	ISO 26300:2006	ND	Qualsiasi
EML	MS Outlook o Mozilla Thunderbird	RFC 5322	ND	Qualsiasi
Documento con firma digitale	Dike, ArubaSign.	CADES, XADES, PADES	ND	Qualsiasi

7.3 Pacchetto di versamento

Il PdV è il pacchetto informativo, inviato dal produttore al SdC, il cui formato e contenuto sono concordati con il soggetto produttore.

I PdV contengono insiemi informativi da sottoporre a conservazione e sono generati tramite:

- procedura automatizzata messa a disposizione dalla piattaforma JDoc;
- appositi web-services che consentono l'inserimento nel SdC;
- trasmissione telematica tramite canale sicuro;
- interfaccia web-based e mediante una azione di "upload" dei documenti informatici,
- altri software sviluppati da partner di Enerj

Il PdV, eventualmente integrato da ulteriori informazioni concordate con il cliente, viene trasferito dal produttore al soggetto conservatore Enerj tramite una apposita procedura informatica automatizzata che consente l'identificazione certa del soggetto, dell'ente o dell'amministrazione che ha formato e trasmesso il documento.

Le informazioni relative alle diverse tipologie di pacchetti di versamento trattati, sono descritte nel Contratto di Servizio e sono concordate specificamente con ciascun soggetto produttore.

A titolo di esempio riportiamo, di seguito, un tracciato XML di un PdV.

```
<?xml version="1.0" encoding="utf-8"?>
<IdC xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" p3:version="-" p3:url=""
p3:schemaLocation="-" xmlns:p3="http://www.uni.com/U3011/sincro/"
xmlns="http://www.uni.com/U3011/sincro/">
<p3:SelfDescription>
    <p3:ID p3:scheme="local">d170cb44-62b3-4084-87b2-d63642202588</p3:ID>
    <p3:CreatingApplication>
      <p3:Name>JDoc</p3:Name>
      <p3:Version>6.0.0.0</p3:Version>
      <p3:Producer>enerj s.r.l.</p3:Producer>
    </p3:CreatingApplication>
  </p3:SelfDescription>
  <p3:VdC>
    <p3:ID p3:scheme="local">36cfc425-d08e-4fc9-8bdc-5b3811c3de71</p3:ID>
  </p3:VdC>
  <p3:FileGroup>
    <p3:File p3:encoding="binary" p3:extension="p7m"
p3:format="application/p7m">
      <p3:ID p3:scheme="local">210b033f-e467-4289-8055-77f94a7c29a2</p3:ID>
      <p3:Path>./File/210b033f-e467-4289-8055-77f94a7c29a2.p7m</p3:Path>
      <p3:Hash p3:function="SHA-
256">4826a0a7634c2b96b4cfb1d6e1fc1aef21394791f46338d16d356aa1a9b410a</p3:Has
h>
      <p3:MoreInfo p3:XMLScheme="">
```

```
         <p3:ExternalMetadata p3:format="application/xml"
p3:encoding="binary">
               <p3:ID p3:scheme="local">0d3c702d-9e25-4b87-a7ce-
b87f413b29d4</p3:ID>
               <p3:Path>./Meta/0d3c702d-9e25-4b87-a7ce-
b87f413b29d4.xml</p3:Path>
               <p3:Hash p3:function="SHA-
256">48b849509eb8994cee42a233bf19063ecfec6a88b11c91517ff8d86663ba3809</p3:Ha
sh>
         </p3:ExternalMetadata>
      </p3:MoreInfo>
    </p3:File>
    <p3:File p3:encoding="binary" p3:extension="p7m"
p3:format="application/p7m">
      <p3:ID p3:scheme="local">d001c351-b862-440e-a5dc-490574244c98</p3:ID>
      <p3:Path>./File/d001c351-b862-440e-a5dc-490574244c98.p7m</p3:Path>
      <p3:Hash p3:function="SHA-
256">69eb58664b83234a804d231a117629673bbeb0b3f767e9b03897d1459e7fc758</p3:Ha
sh>
      <p3:MoreInfo p3:XMLScheme="">
         <p3:ExternalMetadata p3:format="application/xml"
p3:encoding="binary">
               <p3:ID p3:scheme="local">a477ebf5-df4f-4df9-adbc-
f85fc1b5e114</p3:ID>
               <p3:Path>./Meta/a477ebf5-df4f-4df9-adbc-
f85fc1b5e114.xml</p3:Path>
               <p3:Hash p3:function="SHA-
256">e3ee0413622956a9ccdeb9ef3e8edfc90808a4d2cae1d09e4a4de66f503c0a7d</p3:Ha
sh>
         </p3:ExternalMetadata>
      </p3:MoreInfo>
    </p3:File>
          <p3:File p3:encoding="binary" p3:extension="p7m"
p3:format="application/p7m">
      <p3:ID p3:scheme="local">a50e8671-fa15-47b6-b1d1-97a34a8a8316</p3:ID>
      <p3:Path>./File/a50e8671-fa15-47b6-b1d1-97a34a8a8316.p7m</p3:Path>
      <p3:Hash p3:function="SHA-
256">c2b1e05b9f7999fb00060cfe5adb371ec8844b65b923253834fbb040418f4203</p3:Ha
sh>
      <p3:MoreInfo p3:XMLScheme="">
         <p3:ExternalMetadata p3:format="application/xml"
p3:encoding="binary">
               <p3:ID p3:scheme="local">1b32e85b-58e2-432d-bd06-
5cda0b64e0a7</p3:ID>
               <p3:Path>./Meta/1b32e85b-58e2-432d-bd06-
5cda0b64e0a7.xml</p3:Path>
               <p3:Hash p3:function="SHA-
256">b16495efe3ad36832146bd18179d036d6129830c2988e78367e035c50ed26863</p3:Ha
sh>
         </p3:ExternalMetadata>
      </p3:MoreInfo>
    </p3:File>
  </p3:FileGroup>
  <p3:Process>
    <p3:Agent p3:type="organization" p3:role="OtherRole"
p3:otherRole="Producer">
      <p3:AgentName>
        <p3:FormalName>ESEMPIO S.p.A.</p3:FormalName>
```

```
      </p3:AgentName>
      <p3:Agent_ID
p3:scheme="VATRegistrationNumber">12345678910</p3:Agent_ID>
    </p3:Agent>
    <p3:TimeReference>
      <p3:AttachedTimeStamp>2015-06-
03T14:04:01.444+02:00</p3:AttachedTimeStamp>
    </p3:TimeReference>
  </p3:Process>
</IdC>
```

7.4 Pacchetto di archiviazione

Il PdA viene formato secondo le regole tecniche definite nella norma UNI 11386:2010 Standard SInCRO (Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti Digitali).

Le informazioni più rilevanti che il sistema di conservazione gestisce, in relazione ad ogni PdA prodotto, sono:

- Informazioni relative al cliente Produttore (Codice anagrafico, Ragione Sociale , Codice Fiscale, Partita IVA, ...);
- Identificativo univoco dell'IPdA generato automaticamente dal SdC;
- Informazioni sull'applicazione che ha generato il PdA (Produttore, nome e versione);
- Informazioni sui PdA contenuti nell'indice;
- Informazioni sui documenti (ID, Impronta di hash, formato, percorso);
- Informazioni relative al processo di conservazione (elementi identificativi del RSC);
- Informazioni relative alla data di produzione del pacchetto stesso (marca temporale);
- Informazioni relative alla firma digitale.
- Informazioni relative ai metadati dei documenti previste negli accordi specifici del Contratto del Servizio;
- Informazioni necessarie per il controllo ed il log delle operazioni relative al pacchetto stesso;

La norma definisce il contenuto del PdA in base alla tassonomia specificamente determinata dal DPCM e schematizzata come segue:

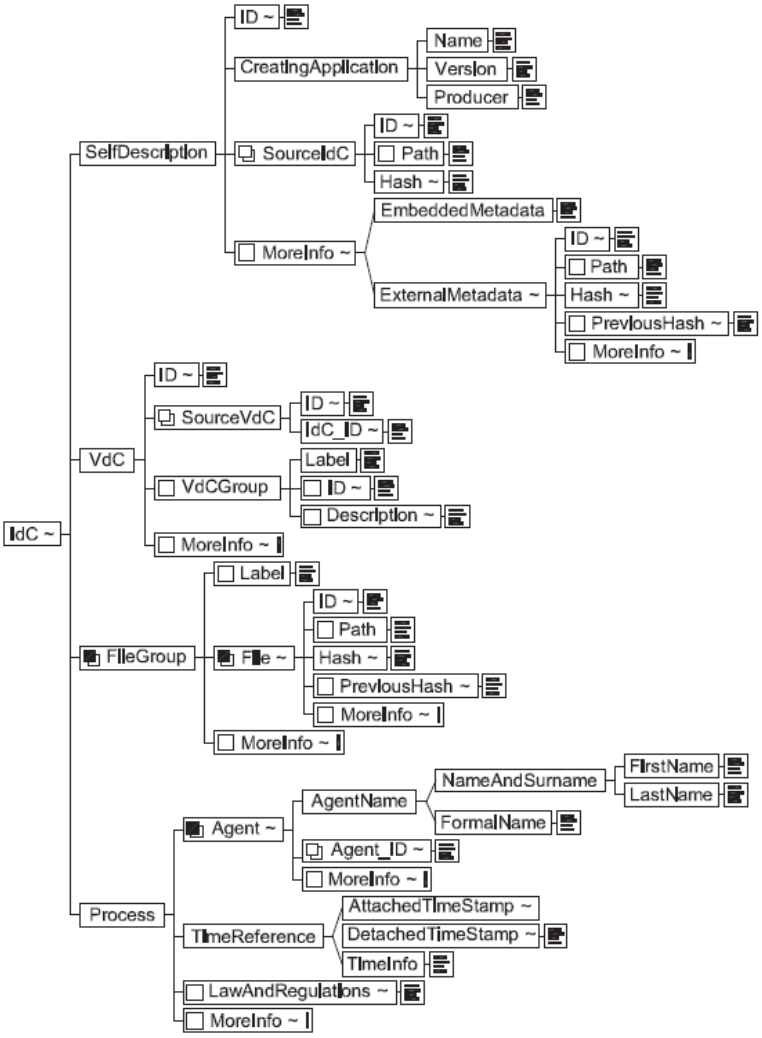


Figura 1 - Rappresentazione UML del contenuto del PdA

A titolo esemplificativo riportiamo, di seguito, un tracciato XML di un PdA.

```
<?xml version="1.0" encoding="utf-8"?>
<IdC xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" p3:version="-" p3:url=""
p3:schemaLocation="-" xmlns:p3="http://www.uni.com/U3011/sincro/"
xmlns="http://www.uni.com/U3011/sincro/">
  <p3:SelfDescription>
    <p3:ID p3:scheme="local">d170cb44-62b3-4084-87b2-d63642202588</p3:ID>
    <p3:CreatingApplication>
      <p3:Name>JDoc</p3:Name>
      <p3:Version>6.0.0.0</p3:Version>
      <p3:Producer>enerj s.r.l.</p3:Producer>
    </p3:CreatingApplication>
  </p3:SelfDescription>
  <p3:VdC>
```

```
    <p3:ID p3:scheme="local">36cfc425-d08e-4fc9-8bdc-5b3811c3de71</p3:ID>
  </p3:VdC>
  <p3:FileGroup>
    <p3:File p3:encoding="binary" p3:extension="p7m"
p3:format="application/p7m">
      <p3:ID p3:scheme="local">210b033f-e467-4289-8055-77f94a7c29a2</p3:ID>
      <p3:Path>./File/210b033f-e467-4289-8055-77f94a7c29a2.p7m</p3:Path>
      <p3:Hash p3:function="SHA-
256">4826a0a7634c2b96b4cfb1d6e1fc1aef21394791f46338d16d356aa1a9b2410a</p3:Ha
sh>
      <p3:MoreInfo p3:XMLScheme="">
         <p3:ExternalMetadata p3:format="application/xml"
p3:encoding="binary">
            <p3:ID p3:scheme="local">0d3c702d-9e25-4b87-a7ce-
b87f413b29d4</p3:ID>
            <p3:Path>./Meta/0d3c702d-9e25-4b87-a7ce-
b87f413b29d4.xml</p3:Path>
            <p3:Hash p3:function="SHA-
256">48b849509eb8994cee42a233bf19063ecfec6a88b11c91517ff8d86663ba3809</p3:Ha
sh>
         </p3:ExternalMetadata>
      </p3:MoreInfo>
    </p3:File>
    <p3:File p3:encoding="binary" p3:extension="p7m"
p3:format="application/p7m">

      <p3:ID p3:scheme="local">d001c351-b862-440e-a5dc-490574244c98</p3:ID>
      <p3:Path>./File/d001c351-b862-440e-a5dc-490574244c98.p7m</p3:Path>
      <p3:Hash p3:function="SHA-
256">69eb58664b83234a804d231a117629673bbeb0b3f767e9b03897d1459e7fc758</p3:Ha
sh>
      <p3:MoreInfo p3:XMLScheme="">
         <p3:ExternalMetadata p3:format="application/xml"
p3:encoding="binary">
            <p3:ID p3:scheme="local">a477ebf5-df4f-4df9-adbc-
f85fc1b5e114</p3:ID>
            <p3:Path>./Meta/a477ebf5-df4f-4df9-adbc-
f85fc1b5e114.xml</p3:Path>
            <p3:Hash p3:function="SHA-
256">e3ee0413622956a9ccdeb9ef3e8edfc90808a4d2cae1d09e4a4de66f503c0a7d</p3:Ha
sh>
         </p3:ExternalMetadata>
      </p3:MoreInfo>
    </p3:File>
          <p3:File p3:encoding="binary" p3:extension="p7m"
p3:format="application/p7m">
      <p3:ID p3:scheme="local">a50e8671-fa15-47b6-b1d1-97a34a8a8316</p3:ID>
      <p3:Path>./File/a50e8671-fa15-47b6-b1d1-97a34a8a8316.p7m</p3:Path>
      <p3:Hash p3:function="SHA-
256">c2b1e05b9f7999fb00060cfe5adb371ec8844b65b923253834fbb040418f4203</p3:Ha
sh>
      <p3:MoreInfo p3:XMLScheme="">
         <p3:ExternalMetadata p3:format="application/xml"
p3:encoding="binary">
            <p3:ID p3:scheme="local">1b32e85b-58e2-432d-bd06-
5cda0b64e0a7</p3:ID>
            <p3:Path>./Meta/1b32e85b-58e2-432d-bd06-
5cda0b64e0a7.xml</p3:Path>
```

```
            <p3:Hash p3:function="SHA-
256">b16495efe3ad36832146bd18179d036d6129830c2988e78367e035c50ed26863</p3:Ha
sh>
       </p3:ExternalMetadata>
      </p3:MoreInfo>
    </p3:File>
  </p3:FileGroup>
  <p3:Process>
    <p3:Agent p3:type="organization" p3:role="PreservationManager">
      <p3:AgentName>
        <p3:FormalName>enerj s.r.l.</p3:FormalName>
      </p3:AgentName>
      <p3:Agent_ID
p3:scheme="VATRegistrationNumber">03466010232</p3:Agent_ID>
    </p3:Agent>
    <p3:Agent p3:type="organization" p3:role="Delegate">
      <p3:AgentName>
        <p3:FormalName>enerj s.r.l.</p3:FormalName>
      </p3:AgentName>
      <p3:Agent_ID
p3:scheme="VATRegistrationNumber">03466010232</p3:Agent_ID>
    </p3:Agent>
    <p3:Agent p3:type="organization" p3:role="OtherRole"
p3:otherRole="Producer">
      <p3:AgentName>
        <p3:FormalName>ESEMPIO S.p.A.</p3:FormalName>
      </p3:AgentName>
      <p3:Agent_ID
p3:scheme="VATRegistrationNumber">12345678910</p3:Agent_ID>
    </p3:Agent>
    <p3:TimeReference>
      <p3:AttachedTimeStamp>2015-06-
03T14:04:01.444+02:00</p3:AttachedTimeStamp>
    </p3:TimeReference>
  </p3:Process>
</IdC>
```

Alla struttura del PdA citata in precedenza sono collegate ulteriori strutture, in formato XML, contenenti i metadati del documento, tramite i diversi elementi “MoreInfo” previsti nello standard SInCRO. Di seguito riportiamo un esempio di una struttura implementata per la conservazione delle fatture elettroniche alla PA.

```
<?xml version="1.0" encoding="utf-8"?>
<documento IDDocumento="210b033f-e467-4289-8055-77f94a7c29a2">
  <datachiusura>2015-01-13</datachiusura>
  <oggettodocumento>esempio</oggettodocumento>
  <soggettoproduttore>
    <nome>Mario</nome>
    <cognome>Rossi</cognome>
    <codicefiscale>esempioesempioes</codicefiscale>
  </soggettoproduttore>
  <destinatario>
    <nome>Nome responsabile PA destinataria</nome>
    <cognome>Cognome responsabile PA destinataria</cognome>
    <codicefiscale>esempioesempioes</codicefiscale>
  </destinatario>
    <ProgressivoInvio>0000069284</ProgressivoInvio>
```

```
        <NomeFile>IT03466010232_00I1U.xml</NomeFile>
        <DatiGeneraliDocumento>
         <TipoDocumento>TD01</TipoDocumento>
         <Data>2015-09-02</Data>
         <Numero>2015110727</Numero>
    </DatiGeneraliDocumento>
        <CessionarioCommittente>
         <CodiceFiscale>xxxxxx00988</CodiceFiscale>
         <PartitaIVA>ITxxxxxx00988</PartitaIVA>
         <Denominazione>Nome Pubblica Amministrazione</Denominazione>
        </CessionarioCommittente>
</documento>
```

7.5 Pacchetto di distribuzione

La richiesta di esibizione da parte del Cliente dei documenti conservati viene soddisfatta attraverso la generazione di un PdD.

Il PdD viene formato secondo le regole tecniche definite nello Standard SInCRO.

Il PdD ha una struttura analoga a quella del PdA ed include i riferimenti univoci ai PdA che sono stati estratti dal SdC.

Il PdD è corredato da ulteriori informazioni quali:

- Informazioni relative al cliente Produttore (Codice anagrafico, Ragione Sociale , Codice Fiscale, Partita IVA, ...);
- Identificativo univoco dell'PdD generato automaticamente dal SdC;
- Informazioni sull'applicazione che ha generato il PdD (Produttore, nome e versione);
- Informazioni sui PdA contenuti nel PdD;
- Informazioni sui documenti (ID, Impronta di hash, formato, percorso);
- le immagini in formato originale estratte dai PdA;
- Informazioni relative al processo di conservazione (elementi identificativi del RSC);
- Informazioni relative alla data di produzione del pacchetto stesso (marca temporale);
- Informazioni relative alla firma digitale.
- eventuali informazioni relative ai metadati dei documenti previste negli accordi specifici del Contratto del Servizio;
- Informazioni necessarie per il controllo ed il log delle operazioni relative al pacchetto stesso;

Le richieste di esibizione dei PdD sono accettate solamente se provenienti dai

soggetti autorizzati dal Cliente.

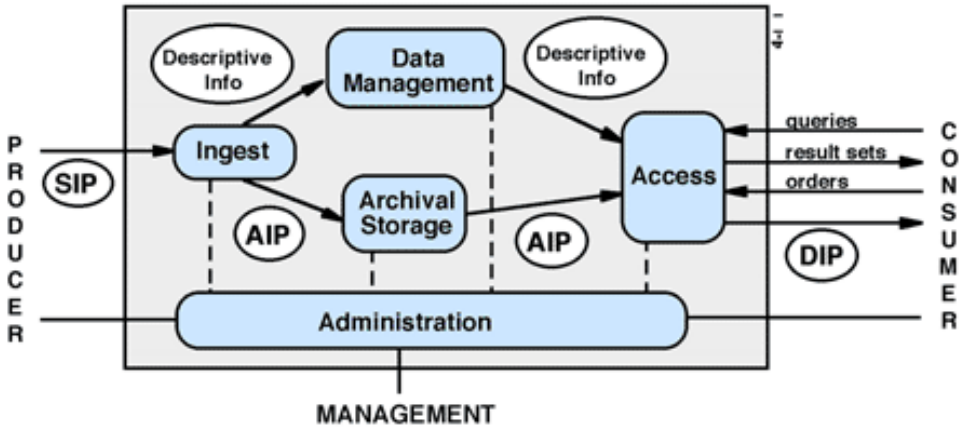
Torna al sommario

8 IL PROCESSO DI CONSERVAZIONE

Il processo di conservazione si esegue sulla base delle modalità previste dall' art. 9 del DPCM, e delle specifiche contenute nella Procedura di gestione della Conservazione Digitale (PCD) afferente al ISMS e dalle peculiarità presenti nei Contratti di Servizio.

Il processo di conservazione è realizzato sulla base del modello funzionale OAIS (Open Archival Information System) normato dallo standard ISO 14721:2003 a cui si è fatto riferimento. Il modello OAIS ha introdotto nella gestione degli archivi informatici i concetti fondamentali relativi alle modalità di transazione dei pacchetti informativi (PdV, PdA, PdD) contemplati e descritti nel presente manuale.

Nello schema che segue si evidenziano le modalità che regolano il flusso informativo di pacchetti informativi generati da un soggetto produttore (nello schema: *Producer*) sotto forma di PdV (nello schema: *SIP*) ad un SdC (nello schema: *management*) che lo trasforma in PdA (nello schema: *AIP*) e ne cura la conservazione ed il mantenimento nel tempo. Il SdC provvede anche a mettere a disposizione del soggetto fruitore (nello schema: *consumer*) il contenuto del PdA tramite opportune modalità di accesso (nello schema: *Access*) e sotto forma di PdD (nello schema *DIP*)



Schema 1 **- Modello funzionale OAIS**

8.1 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico

Le principali modalità di trasmissione del pacchetto di versamento sono:

- procedura automatizzata messa a disposizione dalla piattaforma JDoc;
- appositi web-services che consentono l'inserimento nel SdC;
- trasmissione telematica tramite canale sicuro;
- interfaccia web-based e mediante una azione di "upload" dei documenti informatici,
- altri software sviluppati da partner di Enerj

E' prevista anche l'integrazione con il servizio di fatturazione elettronica alla pubblica amministrazione di Enerj, qualora il fruitore sia anche utente di tale servizio. Tali documenti informatici da conservare sono già presenti nel sistema informativo Enerj, vengono pertanto generati dei pacchetti di versamento suddivisi per singolo cliente e periodo di competenza ed inviati al SdC.

Come dettagliato nel Manuale della Sicurezza del Sistema Informativo (MSI), tutti i canali FTP/HTTP di comunicazione instaurati con i Clienti sono cifrati per la protezione dei dati oggetto di transazione con il cliente. Il ripristino delle funzionalità del sistema in caso di corruzione o perdita dei dati è implementato e descritto nel Piano di Continuità Operativa del Business e Disaster Recovery (PCO). Per l'intero processo di acquisizione dei PdV, il SdC produce i log di sistema necessari alla tracciatura delle attività e delle operazioni svolte, così come descritto nella sezione dedicata al *Log Management* del Manuale della Sicurezza del Sistema Informativo (MSI).

8.2 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti

Il SdC, opera uno o più controlli sul contenuto del pacchetto di versamento ricevuto dal fruitore del servizio, per determinare la correttezza delle caratteristiche formali e dei documenti informatici e/o delle aggregazioni documentali informatiche afferenti al pacchetto stesso. Nelle sezioni successive, detti controlli sono ulteriormente approfonditi dal punto di vista procedurale.

Di seguito sono riportati alcuni tra gli automatismi più consueti implementati per il controllo e la verifica delle caratteristiche dei documenti relativi alle diverse aggregazioni documentali informatiche appartenenti all'archivio informatico del fruitore.

- **Identificazione certa del Produttore:** il sistema verifica l'identità del Produttore attraverso diverse modalita' in relazione alla disponibilità tecnica del cliente.
  Vengono verificate: le credenziali fornite ad esso, lo specifico canale sicuro di comunicazione messo a disposizione, il filtro sugli indirizzi internet, la codifica specifica del codice cliente attribuita ai dati che il Produttore invia in fase di Versamento.
- **Controlli di corretto trasferimento via rete internet:** dove previsto dalla parametrizzazione del SdC il trasferimento via rete internet il SdC verificata l'integrità dei documenti contenuti nei pacchetti di versamento, attraverso il confronto delle impronte di hash.
- **Controlli di formato:** il SdC verifica se i formati inviati dal produttore sono censiti e contrattualizzati nel periodo di competenza del servizio. I formati vengono verificati attraverso librerie e procedure software automatiche che effettuano un log completo delle operazioni effettuate. Per alcuni formati, dove possibile, viene anche controllata la correttezza dei dati.
- **Automatismi per la verifica della consistenza dei documenti presenti nel flusso:** il sistema verifica la presenza di tutti i dati e/o dei metadati dei documenti informatici che compongono l'archivio da sottoporre al procedimento di conservazione. L'utente del servizio ha a disposizione un insieme completo di informazioni e di riscontri utilizzabili in relazione ai dati di origine del flusso (sistema gestionali contabile, ERP, CRM, ecc…).
- **Verifica dell'omogeneità dei documenti:** dove previsto viene verificata la coerenza nella progressione numerica e temporale dei protocolli nonché la progressività dei protocolli rispetto all'ultima operazione di conservazione.
- **Verifica dei metadati minimi obbligatori:** il sistema verifica la presenza dei metadati minimi obbligatori per ogni specifici per ogni cliente e per ogni tipologia documentale, così come definito negli accordi specifici del Contratto di Servizio.

Ulteriori automatismi possono essere implementati su richiesta dell'organizzazione fruitrice ed in base alle esigenze delle stessa e sulla base degli accordi specifici del Contratto di Servizio.

I controlli e le verifiche implementabili sono descritti nella procedura di Gestione della Conservazione Digitale (PCD).

8.3 Accettazione dei pacchetti di versamento e generazione del rapporto di versamento e di presa in carico

L'accettazione del PdV da luogo alla generazione automatica del rapporto di versamento relativo ad uno o più pacchetti di versamento.

Il rapporto di versamento è strutturato secondo quanto previsto dalle regole tecniche (Art. 9, comma 1, lettere d) ed e) del DPCM ed è comprensivo dell'elenco dei pacchetti di versamento accettati.

Il SdC attribuisce un identificatore univoco a ciascun rapporto di versamento generato e la riferisce temporalmente (con riferimento al Tempo universale coordinato - UTC -).

Il rapporto di versamento include, a titolo non esaustivo, le seguenti informazioni:

- dati del Produttore
- dati dell'utente richiedente il versamento
- tipologie dei documenti
- formati dei documenti
- impronte dei documenti
- esiti dei controlli
- metadati del PdV
- riferimenti temporali

L'accettazione del PdV è subordinata ai controlli previsti dal SdC per il Cliente, le tipologie di documento oggetto di conservazione, i formati e quanto previsto al paragrafo 8.2. Tali controlli sono parametrizzati nel SdC stesso e sono parte integrante del Contratto di Servizio.

Nel rapporto di versamento sono elaborate e specificate le impronte, una o più, calcolate sull'intero contenuto del pacchetto di versamento, mediante procedura automatizzata.

Il SdC inoltra i rapporti di versamento al Produttore secondo diverse modalità in base a quanto espresso nel Contratto di Servizio. Le modalità utilizzate sono:

- trasmissione a mezzo mail,
- trasmissione a mezzo PEC,
- messa a disposizione tramite interfaccia web.

L' interfaccia web consente al Produttore di monitorare lo stato di tutti i PdV inviati al SdC e pertanto gestire anche eventuali errori risultanti dai controlli (vedasi paragrafo 8.4).

Tutti le informazioni inerenti alle operazioni eseguite dagli utenti e dai processi informatici relative ai PdV accettati dal Produttore al SdC vengono storicizzate su appositi log. Tra queste, a titolo non esaustivo, citiamo: data e ora di ogni singola

operazione, utente, processo informatico, codice cliente, tipo di operazione, metadati completi, identificativo univoco del PdV, informazioni di sicurezza.

8.4 Rifiuto dei PdV e modalità di comunicazione delle anomalie

In caso di esito negativo dei controlli e delle verifiche applicati sul PdV, il SdC genera una comunicazione di rifiuto, che viene riferita temporalmente e trasmessa al produttore.

Nella comunicazione sono indicate le anomalie presenti nel PdV che ne determinano il rifiuto, quali (a titolo esemplificativo e non esaustivo):

- Presenza di documenti informatici non integri o corrotti in fase di trasmissione;
- Incongruenze relative a errata numerazione di protocollo;
- Incongruenze relative alla consecutività temporale dei documenti informatici;
- Assenza dal PdV dei dati essenziali specificati nel Contratto di Servizio;
- Anomalie relative alla sicurezza dei dati.

La comunicazione viene inoltrata al produttore secondo diverse modalità in base a quanto espresso nel Contratto di Servizio. Le modalità utilizzate sono:

- trasmissione a mezzo mail,
- trasmissione a mezzo PEC,
- messa a disposizione tramite interfaccia web.

Tutti le informazioni inerenti le operazioni eseguite dagli utenti e dai processi informatici relative ai PdV rifiutati dal SdC vengono storicizzate su appositi log. Tra queste, a titolo non esaustivo, citiamo: data e ora di ogni singola operazione, utente, processo informatico, codice cliente, tipo di operazione, metadati completi, identificativo univoco del PdV, informazioni di sicurezza.

8.5 Preparazione e gestione del PdA

Mediante apposite procedure software del SdC, i PdV, opportunamente verificati e validati come descritto nelle sezioni precedenti, vengono trasformati in PdA e corredati delle ulteriori caratteristiche necessarie a soddisfare i requisiti previsti dalla normativa.

Qualora si rendano necessari interventi manuali da parte degli operatori del SdC di rettifica, integrazione di dati e metadati nei PdA, tali operazioni sono tracciate su appositi log che includono, a titolo non esaustivo, le seguenti informazioni: data e

ora di ogni singola operazione, utente/processo, codice cliente, tipo di operazione, metadati completi precedenti e successivi all'operazione, informazioni di sicurezza.

Le modalità di gestione degli interventi manuali da parte degli operatori del SdC sono documentati nella procedura PCD e prevedono l'utilizzo di apposita modulistica.

I PdA sono sottoscritti dal RSC e, ad essi, sono associate le relative marche temporali.

I PdA, così sottoposti al processo di conservazione digitale, sono custoditi, per i tempi previsti dalla normativa e dai Contratti di Servizio, nell'archivio informatico facente parte del SdC. Il sistema è implementato e sviluppato allo scopo di garantire e mantenere la disponibilità, la fruibilità, l'immodificabilità e l'autenticità dei documenti informatici in esso contenuti.

Le ulteriori informazioni peculiari contenute nel PdA, eventualmente concordate con il soggetto Produttore, sono definite nei Contratti di Servizio.

8.6 Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione

Il processo di preparazione del PdD è attivato dalla ricezione di una richiesta di esibizione da parte dell'utente. Il SdC si occupa di verificare che il profilo dell'utente che accede abbia le necessarie autorizzazioni per effettuare l'estrazione.

L'utente, guidato dal sistema, opera la selezione dei documenti informatici da estrarre. Il sistema, sulla base della selezione, compone la richiesta di esibizione che specifica quali documenti informatici comporranno il PdD.

Il sistema provvede quindi a confezionare il PdD contenente i documenti informatici oggetto della selezione ed i relativi IPdA.

I IPdA contengono le impronte dei documenti richiesti per consentire al fruitore la verifica autonoma e completa delle caratteristiche che determinano la corretta conservazione dei documenti.

Nel caso in cui si preveda l'utilizzo di supporti fisici rimovibili per la trasmissione dei pacchetti di distribuzione, si fa riferimento a quanto previsto nel Contratto di Servizio.

I supporti fisici non presentano riferimenti esterni che possano permettere l'identificazione dell'ente produttore, dei dati contenuti, della loro tipologia, ecc.

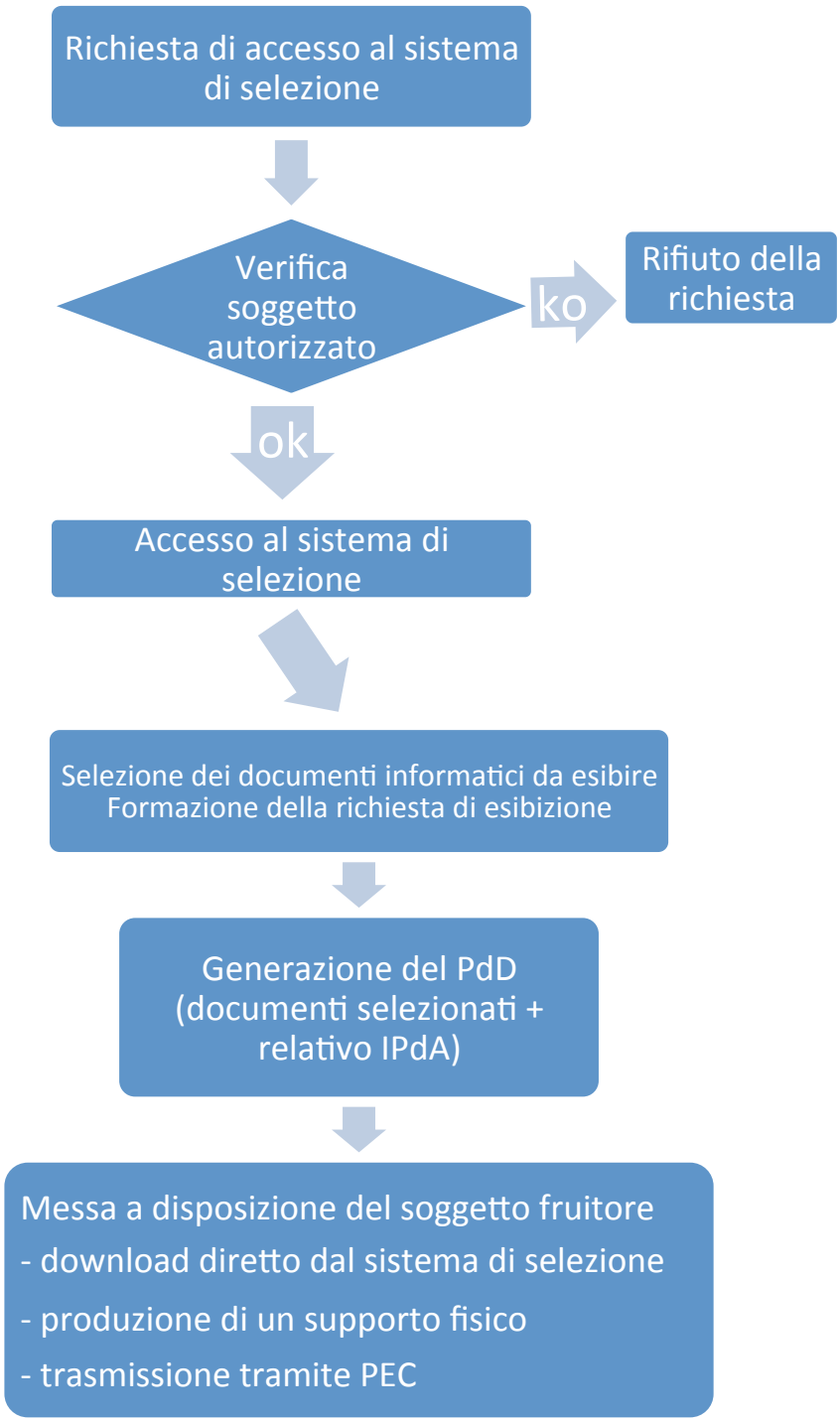
I supporti fisici sono trasportati a cura e responsabilità di personale Enerj o

incaricato da Enerj sulla base di specifici requisiti definiti dal RdC nella procedura PCD.

I dati richiesti sono crittografati con il certificato del destinatario prima della loro spedizione/trasmissione allo stesso.

Nel caso in cui i contratti di servizio implichino la consegna dei PdD via email, viene utilizzata la posta certificata per permettere di tracciare l'intera trasmissione e sono conservate le sole ricevute di invio e consegna.

Tutti le informazioni relative ai PdD richiesti, generati, esportati dal SdC vengono storicizzate su appositi log. Tra queste, a titolo non esaustivo, citiamo: data e ora di ogni singola operazione, utente/processo, codice cliente, tipo di operazione, metadati completi, informazioni di sicurezza.



Schema 2 - Processo di preparazione e gestione del PdD

8.7 Produzione di duplicati e copie informatiche ed eventuale intervento del pubblico ufficiale nei casi previsti

Il SdC di Enerj prevede specifiche procedure per la generazione e produzione di duplicati informatici e copie informatiche sulla base delle modalità definite dall'art. 22 del CAD.

8.7.1 Produzione di duplicati informatici

Il procedimento di produzione di duplicati informatici consente di ottenere dal SdC i duplicati informatici aventi il medesimo valore giuridico, ad ogni effetto di legge, dei documenti informatici dai quali sono tratti in conformità con le regole tecniche vigenti. I duplicati di documenti informatici hanno il medesimo contenuto e la medesima rappresentazione informatica degli originali dai quali sono tratti.

Il procedimento di produzione di duplicati si attiva automaticamente:

- ogni volta che il soggetto fruitore accede al sistema di selezione per ottenere uno o più PdD contenenti i documenti informatici di interesse;
- in occasione dei backup e delle repliche perpetrate sui PdA allo scopo di garantirne la permanenza dei requisiti essenziali di fruibilità e verificabilità;

8.7.2 Produzione di copie informatiche/analogiche ed estratti di documenti informatici

Il procedimento di produzione di copie informatiche ed estratti di documenti informatici consente di ottenere documenti aventi la stessa efficacia probatoria dei documenti informatici dai quali sono tratte. Le copie e gli estratti di documenti informatici hanno il medesimo contenuto degli originali da cui sono tratte ma diversa rappresentazione informatica.

Il procedimento di generazione di copie informatiche ed estratti viene di norma attivato:

- ogni qual volta sia richiesto dai soggetti fruitori e specificamente previsto dal Contratto di Servizio in relazione agli accordi;
- quando, per motivi legati all'evoluzione tecnologica e/o normativa, la rappresentazione informatica dei documenti originali non sia più fruibile dai sistemi di consultazione utilizzati e sia necessario adeguarne il formato.

Il procedimento di generazione di copie informatiche prevede la possibilità di richiedere l'intervento di un pubblico ufficiale allo scopo di attestare la conformità di queste con gli originali.

8.7.3 Produzione di copie informatiche di documenti analogici

Il procedimento di produzione di copie informatiche di documenti analogici consente di generare documenti informatici aventi la stessa efficacia probatoria degli originali analogici da cui sono tratti. Le modalità tecniche di ottenimento delle suddette copie sono costituite da procedure di digitalizzazione che avvengono tramite appositi dispositivi scanner o mediante procedure di rielaborazione delle informazioni che costituiscono i contenuti dei documenti analogici originali.

Il SdC di Enerj prevede espressamente la possibilità di conservare dette fattispecie documentali e le procedure di digitalizzazione utilizzate sono ampiamente descritte nelle procedure di Gestione della Digitalizzazione Interna (PDI) e Gestione della Digitalizzazione Esterna (PDO), afferenti al ISMS.

Le procedure di elaborazione di un documento analogico in informatico, menzionate al paragrafo precedente, sono invece gestite da un apposito modulo software del SdC.

Il procedimento di produzione di copie informatiche di documenti analogici viene attivato quando il soggetto fruitore conferisce al SdC documenti espressi su supporti analogici.

8.8 Scarto dei pacchetti di archiviazione

Il SdC di Enerj effettua lo scarto dei pacchetti di archiviazione sulla base di quanto espresso nei Contratti di Servizio. L'eliminazione dei pacchetti informativi scartati e delle eventuali relative informazioni a corredo viene eseguita tramite una procedura di distruzione sicura dei dati, in linea con la vigente normativa sulla sicurezza dei dati e privacy. Detta funzione è approfondita nella Piano della Sicurezza del Sistema di Conservazione (PDS) e nella Procedura di Conservazione Digitale (PCD).

Nel caso di archivi pubblici o privati di particolare interesse culturale, le procedure di scarto avvengono previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo. La gestione della richiesta di autorizzazione è a carico dell' Ente pubblico Produttore.

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

Enerj, al fine di garantire l'interoperabilità del proprio sistema di conservazione e la trasferibilità di archivi informatici ad altri eventuali soggetti conservatori ha predisposto le seguenti misure:

- Adozione conformemente a quanto determinato dallo standard SInCRO, di tracciati XML omogenei relativi ai PdD e PdA.
- Generazione di tracciati XML (conformi allo standard SInCRO) privi di informazioni non standardizzate e/o arbitrariamente definite da Enerj e/o ridondanti, salvo il caso in cui la presenza di esse sia espressamente richiesta dal fruitore del servizio e palesata nelle specificità contrattuali;
- Mantenimento, per i PdD, della medesima struttura di dati espressa dal DPCM per la configurazione dei PdA (vedasi paragrafi 7.4 e 7.5);
- Mantenimento di identità tra Indice IPdA del PdA ed il medesimo presente nel PdD;
- Gestione dei metadati dei documenti informatici esterna al PdA tramite la corretta valorizzazione della sezione <MoreInfo>.

Il SdC di Enerj è in grado di accettare il versamento di PdD prodotti da altri sistemi di conservazione se in formato standard SInCRO. Eventuali altri formati dovranno essere sottoposti ad analisi e valutazione tecnica prima dell'ingresso nel SdC allo scopo di programmare e svolgere le opportune attività volte all'adeguamento ai formati standard.

In caso di conclusione del Contratto di Servizio, Enerj si impegna a produrre i PdD, coincidenti con i PdA conservati per il fruitore del servizio, tramite i canali e nelle modalità definite negli specifici accordi contrattuali e previa sottoscrizione dei relativi verbali di consegna. Ove previsto dalla natura dei dati riprodotti, sarà effettuata la cifratura degli stessi e la comunicazione, con canale distinto, della relativa chiave per la decifratura e la fruizione esclusiva da parte del titolare dell'archivio.

8.10 Conservazione delle comunicazioni intercorrenti tra il SdC e i fruitori del servizio di conservazione.

Tutte le comunicazioni prodotte durante le transazioni di pacchetti informativi tra Enerj e il cliente (log applicativi, log di sistema, mail, mail pec) sono conservate mediante il SdC stesso.

Torna al sommario

9 IL SISTEMA DI CONSERVAZIONE

Il sistema di conservazione, di seguito descritto nelle sue modalità di accesso, utilizzo e protezione è composto da:

- Componenti Logiche e Tecnologiche: Informazioni e dati, prodotti / servizi di software installati presso Enerj e presso la Clientela
- Componenti Fisiche: architettura informatica aziendale in tutti le sue componenti hardware, reti (aziendali ed esterne),
- Procedure di gestione e di evoluzione: procedure di produzione del software aziendale e della sua manutenzione, procedure di conservazione, procedure di Audit, Riesame della Direzione.

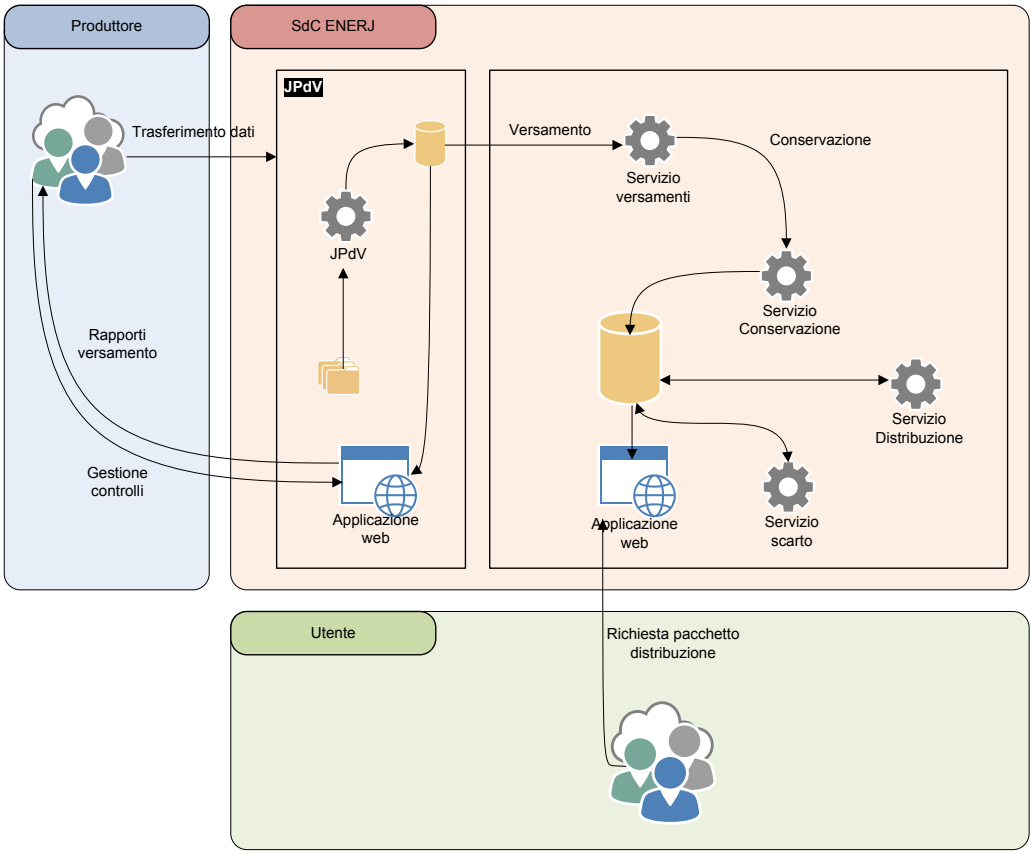
9.1 Componenti Logiche

Il SdC è composto dai seguenti oggetti:

- Produttore: effettuano il versamento dei nuovi PdV generati al SdC;
- JDoc che raccoglie e archivia i documenti inviati dal Produttore;
- JPdV: gestisce la generazione dei PdV effettuando tutte le azioni di monitoraggio e controllo previste nonché la generazione dei rapporti di versamento;
- Servizio Versamenti: prende in carico i PdV validati e gestisce l'inoltro al sistema di conservazione;
- Servizio Conservazione: gestisce la trasformazione da PdV a PdA utilizzando i servizi di firma digitale dei documenti implementati con tecnologia HSM presso una CA accreditata convenzionata con Enerj;
- Servizio Distribuzione: gestisce la ricerca dei documenti da parte degli Utenti abilitati e la generazione dei PdD è realizzata tramite JDoc;
- Servizio Scarto: gestisce lo scarto dei documenti in base a quanto previsto nelle specificità contrattuali;
- Utenti: fruiscono del SdC, accedendo alla piattaforma di front-end gestita tramite applicazioni web-based.

Tutte le funzionalità gestite dal sistema sono erogate in modalità di servizio. Un ulteriore elemento logico è costituito dall'ambiente di test e dall'ambiente di sviluppo che vengono gestiti in modo separato rispetto all'ambiente di produzione.

Lo schema riportato di seguito rappresenta l'architettura logico-funzionale del SdC.



Schema 3 - Schema delle componenti logiche del SdC

9.2 Componenti Tecnologiche

Enerj ha sviluppato una serie di moduli applicativi per l'implementazione del SdC tra cui si riportano i principali:

- **JDoc** Sistema di gestione dell'archivio informatico;
- **JCos** Sistema di gestione dei pacchetti informativi;
- **JSign** Modulo software di gestione della firma digitale e della marcatura temporale;
- **JView** Modulo software per la distribuzione e l'esibizione dei documenti informatici conservati.

L'elenco completo dei software implementati da Enerj e utilizzati nel SdC è contenuto negli inventari del software afferenti al ISMS (MCO04 - Inventario del software commerciale, MCO02 - Inventario del software proprietario).

9.3 Componenti Fisiche

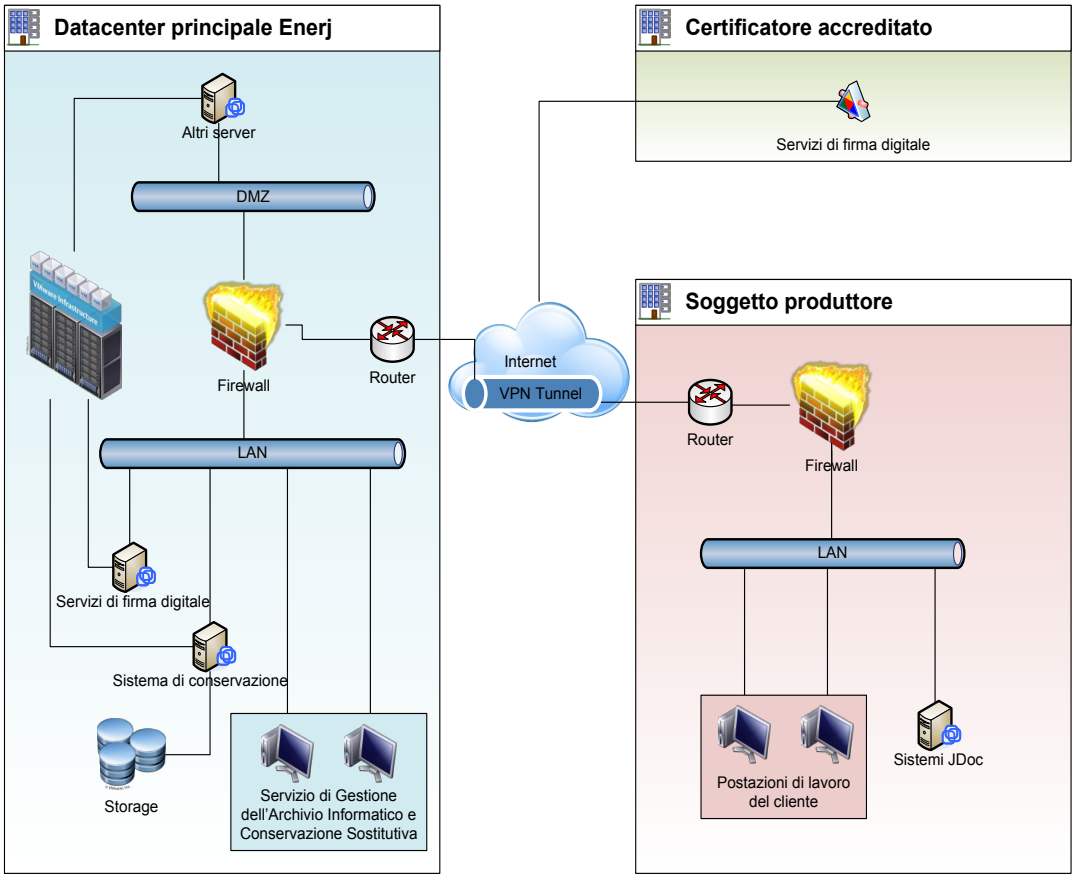
Le componenti fisiche utilizzate nell'infrastruttura di Enerj sono definite e descritte nel dettaglio nei seguenti documenti afferenti al ISMS:

- PDC - Procedura di Gestione del Datacenter
- MSI - Manuale della Sicurezza del Sistema Informativo
- MCO03 - Inventario delle attrezzature informatiche
- PCO - Piano della Continuità Operativa del business e Disaster Recovery
- PBK - Piano di Backup

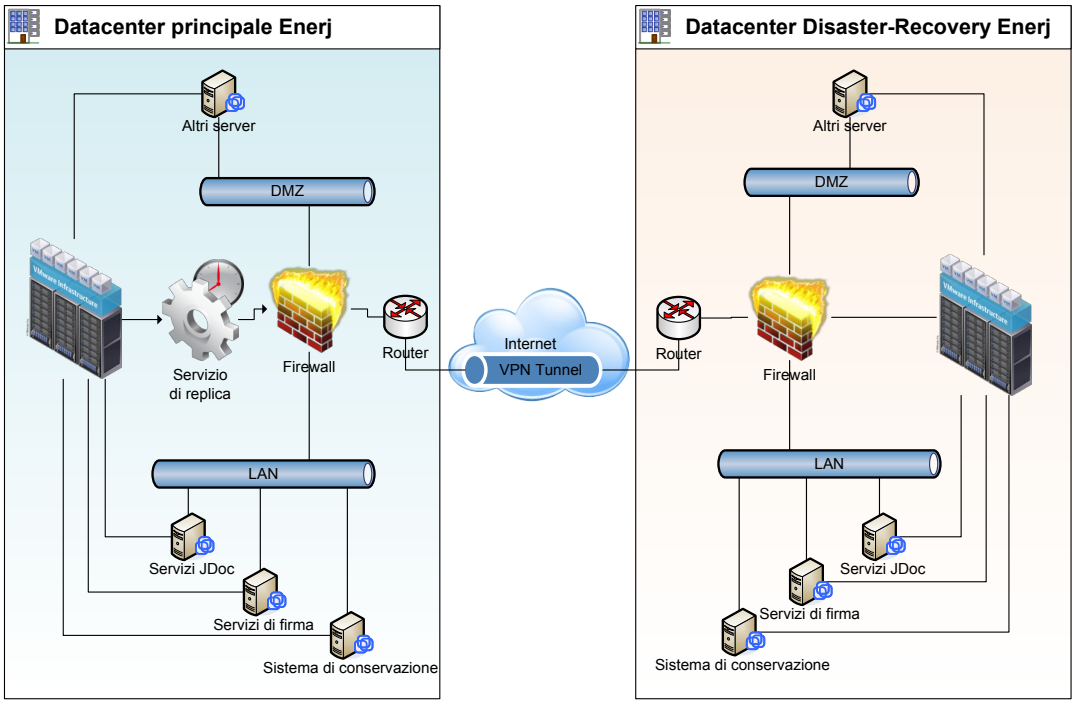
Il SdC si compone di due siti: uno primario situato presso la sede di Enerj ed uno secondario presso il sito di Disaster Recovery. I due datacenter sono connessi mediante una connessione sicura (VPN).

Gli HSM sono situati presso il datacenter del Certificatore accreditato convenzionato.

Di seguito si riporta lo schema dei siti di conservazione e delle connessioni tra i diversi siti con riferimento alle componenti fisiche e tecnologiche del SdC di Enerj.



Schema 4 - Schema e descrizione delle componenti fisiche presenti in ciascuno dei siti di conservazione.



Schema 5- Schema topologico che rappresenta del sistema di conservazione.

9.4 Procedure di gestione e di evoluzione

9.4.1 Conduzione e manutenzione del sistema di conservazione

In relazione alle componenti software di Enerj la procedura di Sviluppo e Manutenzione Software (PSS) descrive le modalità di aggiornamento degli applicativi software in relazione all'evoluzione normative, tecnologiche ed alle esigenze dei Clienti.

I componenti software implementati nel SdC sono sviluppati da una struttura aziendale dedicata.

9.4.2 Gestione e conservazione dei log

Il Sistema di "log management" di Enerj è descritto nel Manuale di Sicurezza del Sistema Informativo (MSI).

In particolare il sistema di "log management" del SdC traccia tutte le operazioni e le transazioni informatiche inerenti a:

- versamento di pacchetti informativi;
- trasformazioni di pacchetti informativi in PdA;

- conservazione dei PdA;
- comunicazioni ed esiti relativi ai pacchetti informativi scambiati con produttori e fruitori;
- gestione della firma digitale e della marcatura temporale;
- produzione e distribuzione dei PdD;
- controllo e verifica dei PdA;
- eventi di carattere sistemistico quali: accessi a risorse informatiche, incidenti di sicurezza, interruzione dell'operatività dei servizi, ecc...;
- accessi fisici ai locali.

9.4.3 Change management

L'evoluzione del SdC segue un percorso interno ad Enerj che prevede lo svolgimento di attività specifiche di presidio costante dell'allineamento del SdC all'evoluzione del panorama normativo vigente, nonché di ricerca e sviluppo, corredandole con la stesura e l'aggiornamento di appositi documenti, così come previsto nel ISMS, tra cui:

- riesame della direzione;
- moduli relativi allo sviluppo software;
- aggiornamento del presente manuale;
- aggiornamento del manuale della sicurezza del sistema informativo;
- aggiornamento del piano della sicurezza del SdC.

9.4.4 Verifica periodica di conformità a normativa e standard di riferimento

Enerj, nell'ambito della gestione del ISMS, ha previsto una specifica procedura di gestione degli audit (PGA) interni ed esterni, che assicura la persistenza della conformità del sistema alla normativa vigente ed agli standard di riferimento.

Torna al sommario

10 MONITORAGGIO E CONTROLLI

Enerj opera con l'obiettivo di mantenere, costantemente, il livello massimo di qualità e di sicurezza delle informazioni gestite tramite i propri servizi di conservazione digitale attraverso il monitoraggio delle applicazioni e delle infrastrutture. Si unisce al predetto obiettivo, la strategia di miglioramento continuo della qualità dei servizi, sostenendolo con investimenti di carattere tecnico e nella formazione delle risorse umane nel rispetto di quanto previsto dal DPCM art. 8, comma 2, lettera h.

10.1 Procedure di monitoraggio applicativo

Gli applicativi software del SdC producono i log delle transazioni dei pacchetti informativi (di cui alla sezione 9.4.2 del presente manuale), dall'elaborazione dei quali si traggono le informazioni necessarie per valutare nel tempo il mantenimento dell'efficacia del sistema, nonché dell'efficienza e della rispondenza dello stesso ai livelli di prestazioni previsti nei Contratti di Servizio.

La direzione, in sede di riesame, individua i conseguenti interventi sullo sviluppo e la manutenzione del software, sia gli investimenti necessari nell'infrastruttura tecnologica.

10.2 Procedure di monitoraggio infrastrutturale

L'infrastruttura tecnologica di Enerj è descritta nel Manuale della Sicurezza dei Sistemi Informativi (MSI) e relativi allegati. Il monitoraggio di tutti i dispositivi hardware quali apparati server, storage e networking, è effettuato tramite un'applicazione di terze parti. Inoltre Enerj è dotata di un contratto di Service Operation Center con un'azienda leader del settore.

Il monitoraggio mette a disposizione un cruscotto gestionale, interrogabile dall'amministratore del sistema, nonché dei report automatici.

10.3 Verifica dell'integrità degli archivi

Il SdC di Enerj prevede apposite procedure periodiche di controllo dell'integrità e leggibilità dei documenti conservati e della congruenza e completezza degli archivi. Le procedure sono descritte nel ISMS, in particolare:

- nel Manuale della Sicurezza dei Sistemi Informativi (MSI)
- nel Piano della Sicurezza del SdC (PDS)
- nella Procedura di Gestione degli Audit (PGA)
- nella Procedura di Analisi dei Rischi (PAR)
- nei verbali di verifica (moduli MCD)

In base al tipo di verifica la periodicità dei controlli può essere giornaliera, annuale e comunque non superiore ai cinque anni. Ulteriori procedure aggiuntive richieste dal soggetto Produttore possono essere descritte nel Contratto di Servizio.

Lo scopo dei sistemi di gestione della sicurezza implementati in Enerj è di evidenziare le eventuali vulnerabilità del sistema di tenuta degli archivi sottoposti a conservazione di Enerj, per potere migliorare costantemente il servizio dal punto di vista organizzativo e informatico, prevenendo possibili minacce e definendo un piano di intervento, in coerenza con il Sistema della Qualità interno e la procedura aziendale di miglioramento continuo.

I criteri di analisi e valutazione si basano sull'analisi oggettiva (condivisa dal management) delle vulnerabilità riscontrate (punti deboli, criticità), valutando l'effettiva probabilità di accadimento di un evento dannoso per gli stessi che limiti o comprometta la capacità operativa corrente, la prestazione dei servizi contrattualmente erogati alla clientela, il know-how aziendale, direttamente scaturenti dalla criticità riscontrata.

Tra i criteri utilizzati particolare rilievo assume l'analisi degli scenari basata sulla previsione e costruzione dei diversi accadimenti che si potrebbero verificare stimando gli eventuali rischi.

Qualora si renda necessario, Enerj è in grado attivare metodi adeguati per le opportune attività di test tese a provare la capacità del sistema di rispondere al verificarsi di eventi dannosi o potenzialmente rischiosi. Tra i test si riportano di seguito i principali:

- verifiche sull'integrità degli archivi conservati
- verifiche sulle copie di sicurezza dei dati
- security testing and evaluation (STE): strumenti comprendenti un'ampia gamma di tests sui sistemi;
- modalita' di sviluppo sicuro previste nelle procedure del Sistema della Qualità ISMS

Tutti le informazioni relative alle verifiche periodiche effettuate dal SdC vengono storicizzate su appositi log. Tra queste, a titolo non esaustivo, citiamo: data e ora di ogni singola operazione, utente/processo, codice cliente, tipo di operazione, esiti,

informazioni di sicurezza.

Sulla base delle risultanze dei test vengono intraprese da ENERJ le azioni preventive allo scopo di eliminare cause di potenziali non conformità prima ancora che le stesse si verifichino. Sono pertanto azioni preventive anche gli interventi di miglioramento.

Le procedure di audit definite nel Sistema della Qualità interno sono implementate allo scopo di individuare le azioni idonee a prevenire le potenziali cause di pregiudizio per l'integrità dei dati. Il personale dell'Area di gestione della Qualità e della Sicurezza dei dati e delle informazioni esamina, con frequenza almeno mensile o quando le condizioni lo rendano necessario, i risultati degli audit condotti (e le relative richieste di azione correttiva) e i documenti di registrazione che rappresentano la fonte principale di informazione relativamente ai processi ed alle attività aziendali. Oltre ai succitati documenti l'Area prende in considerazione anche tutte le comunicazioni formali o informali di tutte le funzioni organizzative in merito all'evidenza di situazioni carenti, inefficienze ed a proposte di miglioramento evinte dalle analisi dei rischi condotte.

La formalizzazione di azioni preventive avviene anche attraverso l'osservazione e l'analisi statistica dei dati e delle informazioni messe a disposizione dalla piattaforma CRM.

10.4 Soluzioni adottate in caso di anomalie

In caso di anomalie sono previste diverse soluzioni commisurate all'entità e alle caratteristiche dell'incidente. Nello specifico, la trattazione degli incidenti di sicurezza è documentata nel Manuale della Sicurezza del Sistema Informativo (MSI) afferente al sistema ISMS.

La gestione delle segnalazioni di anomalia relative al SdC pervenute ad Enerj dai Clienti sono documentate nella procedura Procedura Gestione Clienti e Assistenza (PGC).

10.5 Sicurezza del SdC

Il RSC approva il piano della sicurezza del SdC (PDS) e il RQS ne cura l'aggiornamento.

In relazione a quanto previsto nella procedura di analisi dei rischi (PAR) e relativi moduli (MAR) vengono periodicamente condotte le analisi dei rischi inerenti il SdC.

La continuità operativa del SdC è garantita dall'infrastruttura di backup e disaster recovery del datacenter di Enerj così come dettagliato nel Piano della Continuità

Operativa del Business e Disaster Recovery (PCO) e nel Piano di Backup (PBK).