

Manuale di Conservazione di Olsa Informatica

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	09/06/2016	Bernardino Cerocchi	<i>Responsabile della sicurezza dei sistemi per la conservazione</i>
		Giorgio Sabatini	<i>Responsabile della funzione archivistica</i>
Verifica	09/06/2016	Paolo Giulioni	<i>Responsabile del servizio di conservazione</i>
Approvazione	10/06/2016	Giampaolo Olivetti	<i>Legale Rappresentante</i>

REGISTRO DELLE VERSIONI

N° Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
1.9	15/11/2019	Aggiornamento §4 per revoca incarico di delegato del Responsabile dei Sistemi Informativi per la Conservazione e Responsabile della manutenzione del sistema di Conservazione	
1.8	02/05/2019	Aggiornamento §4 per revoca incarico di delegato del Responsabile della Sicurezza dei Sistemi per la Conservazione	
1.7	25/01/2019	Aggiornamento § 3.1 Normativa di riferimento; aggiornamento § 4 Ruoli e responsabilità, per nomina responsabile della Funzione Archivistica della conservazione; § 5.1 aggiornamento organigramma; § 7.1 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico; inserimento del § 10 Trattamento dei dati personali	
1.6	12/07/2018	Modifica § 7.1 per adeguamento a richieste AgID del 21/06/2018	

1.5	15/05/2018	Adeguamento alle richieste AgID pervenute in data 11/06/2018 – Aggiornamento Intestazione	
1.4	15/05/2018	Modifica § 4 e § 7.1 – Aggiornamento delegati	
1.3	03/04/2018	Inserimento Delegati	
1.2	10/06/2016	Adeguamento alle richieste AgID inviate in data 27/05/2016	
1.1	20/04/2016	Adeguamento alle richieste AgID inviate in data 23/03/2016	
1.0	24/02/2016	Prima emissione	

SOMMARIO

1. Scopo e ambito del documento.....	5
2. Terminologia (Glossario, Acronimi).....	7
3. Normativa e standard di riferimento	13
3.1. Normativa di riferimento.....	13
3.2. Standard di riferimento	14
4. Ruoli e responsabilità	15
5. Struttura organizzativa per il servizio di conservazione	21
5.1. Organigramma.....	21
5.2. Strutture organizzative	21
6. Oggetti sottoposti a conservazione	24
6.1. Oggetti conservati	24
6.2. Pacchetto di versamento	28
6.3. Pacchetto di archiviazione	30
6.4. Pacchetto di distribuzione	33
7. Il processo di conservazione.....	35
7.1. Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico	36
7.1.1. Acquisizione dei pacchetti di versamento dai soggetti produttori tramite Web Service e SFTP	37
7.1.2. Acquisizione dei pacchetti di versamento per conto dei soggetti privati.....	38
7.1.3. Struttura del file di indice	38
7.1.4. Trasferimento dei pacchetti di versamento tramite upload manuale	39
7.2. Verifiche effettuate sui pacchetti di versamento e sugli oggetti in esso contenuti	40
7.3. Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico	42
7.4. Rifiuto del pacchetto di versamento e modalità di comunicazione delle anomalie	43
7.5. Preparazione e gestione del pacchetto di archiviazione	45
7.6. Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione	46
7.7. Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti.	48
7.8. Scarto dei pacchetti di archiviazione	49
7.9. Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori	50

8. Il sistema di conservazione.....	52
8.1. Componenti logiche.....	53
8.1.1. Sistema di Versamento (SV)	54
8.1.2. Sistema di gestione dati (SGD)	56
8.1.3. Sistema di memorizzazione (SM)	56
8.1.4. Sistema di autenticazione e accesso (SAA)	56
8.1.5. Sistema di firma digitale	57
8.1.6. Sistema per l'apposizione della marca temporale	58
8.2. Componenti Tecnologiche	58
8.2.1. Componente Legal Archive®	58
8.2.2. Scalabilità sugli utenti	59
8.2.3. Componente database.....	59
8.2.4. Componente storage	60
8.3. Componenti fisiche.....	61
8.4. Procedure di gestione e di evoluzione	62
8.5. Log del sistema di conservazione.....	65
9. Monitoraggio e controlli.....	67
9.1. Procedure di monitoraggio	67
9.2. Verifica dell'integrità degli archivi	68
9.3. Soluzioni adottate in caso di anomalie	68
10. Trattamento dei dati personali	70

1. Scopo e ambito del documento

Il presente documento costituisce il manuale di conservazione di Olsa Informatica e ha lo scopo di descrivere il sistema di conservazione dei documenti informatici adottato dall'azienda. In particolare il presente manuale descrive il modello organizzativo della conservazione adottato e illustra nel dettaglio l'organizzazione della struttura che realizza il processo di conservazione, definendo i soggetti coinvolti e i ruoli svolti dagli stessi nel modello organizzativo di funzionamento dell'attività di conservazione.

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

Il software utilizzato per la gestione del processo di conservazione dei documenti informatici è Legal Archive[®]. Il sistema di conservazione ha come oggetto la realizzazione di un insieme di funzionalità atte a consentire la conservazione dei documenti informatici e a fornire un supporto alle figure coinvolte nel processo di conservazione.

Il presente manuale è così localizzato:

- una copia del manuale della conservazione è archiviata presso il soggetto produttore;
- una copia del manuale della conservazione è conservata a norma presso il soggetto conservatore.

Dati identificativi del soggetto conservatore

Denominazione	OLSA INFORMATICA S.p.A.
Indirizzo	Via dell'Industria, 18 – 04011 Aprilia (LT)
Legale Rappresentante	Giampaolo Olivetti
Referente tecnico cui rivolgersi in caso di problemi tecnico-operativi	Bernardino Cerocchi
E-mail del referente tecnico	d.cerocchi@olsainformatica.com
N° telefono/fax	+39 06 914841/91484227
Sito web istituzionale	www.olsainformatica.com
E-mail istituzionale	olsa@olsainformatica.com

Con il DPCM del 3 dicembre 2013 (G.U. n. 59 del 12 marzo 2014 – Suppl. Ordinario 20) sono state emanate le Regole tecniche in materia di sistema di conservazione dei documenti informatici, 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 CAD, in vigore dall'11 aprile 2014 (art. 14 comma 1).

Il manuale di conservazione secondo l'art. 8 DPCM 3 dicembre 2013 ha lo scopo di descrivere:

- L'organizzazione della struttura che realizza il processo di conservazione, definendo i soggetti coinvolti e i ruoli svolti dagli stessi;
- Il modello di funzionamento, la descrizione delle architetture e delle 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.

In merito alle tipologie degli oggetti sottoposti a conservazione e ai rapporti con i soggetti produttori, il presente manuale deve essere integrato con le Specifiche tecniche, documento allegato al Contratto di affidamento del servizio di conservazione, redatto con ogni soggetto produttore, che definisce le specifiche operative e le modalità di descrizione e di versamento nel sistema di conservazione digitale delle tipologie documentarie e aggregazioni documentali informatiche oggetto di conservazione.

Il presente manuale di conservazione è un documento informatico.

[Torna al sommario](#)

2. Terminologia (Glossario, Acronimi)

Le definizioni afferenti al processo di conservazione sono presenti nell'allegato 1 delle Regole tecniche (DPCM 3 dicembre 2013).

Indichiamo di seguito il *glossario* dei termini utilizzati nel presente documento:

Glossario dei termini	
TERMINE	DEFINIZIONE
<i>accesso</i>	Operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici.
<i>accreditamento</i>	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.
<i>affidabilità</i>	Caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico.
<i>aggregazione documentale informatica</i>	Aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente.
<i>allegato</i>	Documento che compone l'Unità documentaria per integrare le informazioni contenute nel documento principale. È redatto contestualmente o precedentemente al documento principale. La sua presenza è facoltativa.
<i>annesso</i>	Documento che compone l'Unità documentaria, generalmente prodotto e inserito nell'unità documentaria in un momento successivo a quello di creazione dell'Unità documentaria, per fornire ulteriori notizie e informazioni a corredo del Documento principale.
<i>application server</i>	Tipologia di server che fornisce l'infrastruttura e le funzionalità di supporto, sviluppo ed esecuzione di applicazioni nonché altri componenti server in un contesto distribuito. Si tratta di un complesso di servizi orientati alla realizzazione di applicazioni ad architettura multilivello ed enterprise, con alto grado di complessità, spesso orientate per il web (applicazioni web).
<i>archivio</i>	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.
<i>attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico</i>	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.
<i>autenticità</i>	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.

certificatore accreditato	Soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, dall' Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza.
ciclo di gestione	Arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo.
classificazione	Attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati.
cluster	Insieme di dispositivi di elaborazione connessi in maniera più o meno stretta che operano insieme in modo tale da poter essere considerati un unico sistema.
Codice	Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni.
comunità di riferimento	Un gruppo ben individuato di potenziali Utenti che dovrebbero essere in grado di comprendere un particolare insieme di informazioni. La Comunità di riferimento può essere composta da più comunità di Utenti [fonte: OAIS].
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.
contenuto informativo	L'insieme delle informazioni che costituisce l'obiettivo originario della conservazione. E' composto dall'Oggetto-dati e dalle Informazioni di rappresentazione [fonte: OAIS]
data center	Struttura utilizzata per ospitare computer e componenti associati quali dispositivi di telecomunicazioni e di storage, in generale con adeguati livelli di prestazioni e di sicurezza.
disaster recovery	Insieme delle misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi di business per imprese, associazioni o enti, a fronte di gravi emergenze che ne intacchino la regolare attività.
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 Codice.
file di indice	Indice dell'AIP: file XML che contiene tutti gli elementi del Pacchetto di archiviazione, derivati sia dalle informazioni contenute nel SIP (o nei SIP)

	trasmessi dal produttore, sia da quelle generate dal Sistema di conservazione nel corso del processo di conservazione.
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.
identificativo univoco	Sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione.
impronta	La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash.
informazioni descrittive	Descrivono il pacchetto informativo e consentono di ricercarlo nel sistema di conservazione. In base alle caratteristiche della tipologia di oggetto contenuto nel Pacchetto, tali informazioni possono essere un sottoinsieme di quelle presenti nel pacchetto informativo, possono coincidere o possono anche essere diverse.
informazioni sulla conservazione (PDI)	Informazioni necessarie a conservare il contenuto informativo e garantiscono che lo stesso sia chiaramente identificato e che sia chiarito il contesto in cui è stato creato. Sono costituite da metadati che definiscono la provenienza, il contesto, l'identificazione e l'integrità del Contenuto informativo oggetto della conservazione [fonte: OAIS].
Informazioni sulla rappresentazione	Informazioni che associano un Oggetto-dati a concetti più significativi.
informazioni sull'impacchettamento	Informazioni che consentono di mettere in relazione nel Sistema di conservazione, in modo stabile e persistente, il Contenuto informativo con le relative Informazioni sulla conservazione.
integrità	Insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato.
interoperabilità	Capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi.
leggibilità	Insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti.
log di sistema	Registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati.
manuale di conservazione	Strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 delle regole tecniche del sistema di conservazione.
marca temporale	Sequenza di caratteri che rappresentano una data e/o un orario per accertare l'effettivo avvenimento di un certo evento. La data è di solito presentata in un Formato compatibile, in modo che sia facile da comparare con un'altra per stabilirne l'ordine temporale. La pratica dell'applicazione di tale marca temporale è detto <i>timestamping</i> .

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 presente decreto e secondo le modalità riportate nel manuale di conservazione.
pacchetto di distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta.
pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione.
pacchetto informativo	Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare.
Piano della Sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza.
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.
presa in carico	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione.
processo di conservazione	Insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 10 delle regole tecniche del sistema di conservazione.
produttore	Persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale.
rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.
responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi	Dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al 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, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione.
responsabile della conservazione	Soggetto responsabile dell'insieme delle attività elencate nell'articolo 7, 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.
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
scarto	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale.
serie	Unità Archivistiche o Unità Documentarie ordinate secondo un sistema di classificazione o conservati insieme perché: <ul style="list-style-type: none"> - sono il risultato di un medesimo processo di sedimentazione o archiviazione o di una medesima attività; - appartengono ad una specifica tipologia documentaria; - a ragione di qualche altra relazione derivante dalle modalità della loro produzione, acquisizione o uso [fonte: ISAD].
sistema di classificazione	Strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata.
sistema di conservazione	Sistema di conservazione dei documenti informatici di cui all'articolo 44 del Codice.
sistema di gestione informatica dei 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.
Testo unico	Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni.
unità archivistica	Insieme organizzato di Unità documentarie o Documenti raggruppati dal produttore per le esigenze della sua attività corrente in base al comune riferimento allo stesso oggetto, attività o fatto giuridico. Può rappresentare una unità elementare di una Serie [fonte: ISAD].
unità documentaria	Aggregato logico costituito da uno più Documenti che sono considerati come un tutto unico. Costituisce l'unità elementare in cui è composto l'archivio.
versamento	Azione di trasferimento di SIP dal produttore al Sistema di conservazione.
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.

Indichiamo di seguito gli *acronimi* dei termini utilizzati nel presente documento:

- **AgID:** Agenzia per l'Italia Digitale
- **AIP:** Archival Information Package (Pacchetto di archiviazione)
- **CA:** Certification Authority
- **CAD:** Codice dell'Amministrazione Digitale

- **CRL:** Certificate Revocation List, è la lista dei certificati revocati o sospesi, ovvero lista di certificati che sono stati resi non validi prima della loro naturale scadenza
- **DIP:** Dissemination Information Package (Pacchetto di distribuzione)
- **HSM:** Hardware Security Module, è l'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
- **IdC:** Indice di conservazione realizzato secondo le specifiche dello standard UNI SInCRO
- **IPdA:** Indice del Pacchetto di Archiviazione
- **IR:** Informazioni sulla rappresentazione
- **IRse:** Informazioni sulla rappresentazione semantiche
- **IRsi:** Informazioni sulla rappresentazione sintattiche
- **ISO:** International Organization for Standardization
- **MAC:** Manutenzione correttiva e adeguativa
- **MEV:** Manutenzione evolutiva
- **OAIS:** Open Archival Information System
- **PDI:** Preservation description information (informazioni sulla conservazione)
- **PEC:** Posta Elettronica Certificata
- **SIP:** Submission Information Package (Pacchetto di versamento)
- **SMTP:** Simple Mail Transfer Protocol (SMTP) è il protocollo standard per la trasmissione via internet di e-mail
- **SNMP:** Simple Network Management Protocol
- **SP:** soggetto produttore
- **TSA:** Time Stamping Authority, è il soggetto che eroga la marca temporale
- **UNI SInCRO:** UNI 11386:2010 - Supporto all'Interoperabilità nella conservazione e nel Recupero degli oggetti digitali

[Torna al sommario](#)

3. Normativa e standard di riferimento

3.1. Normativa di riferimento

Il presente elenco riporta la normativa nazionale italiana di riferimento in ambito di conservazione dei documenti informatici.

- **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;
- **Legge n. 241 del 7 agosto 1990 e s.m.i.** - Norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- **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 Legislativo 22 gennaio 2004, n. 42, e successive modificazioni** - Codice dei beni culturali e del paesaggio;
- **Decreto Legislativo 7 marzo 2005, n. 82, e s.m.i.** - Codice dell'Amministrazione Digitale (CAD);
- **Deliberazione CNIPA 21 Maggio 2009, n. 45** - Regole per il riconoscimento e la verifica del documento informatico;
- **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;
- **Decreto Ministero Economia e 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. Pubblicato in G.U. n. 118 del 22 maggio 2013;
- **Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013** - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, comma 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 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 di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82;
- **Decreto Ministero Economia e Finanze 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;
- **Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014** - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.
- **REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO** del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché

alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

- **Decreto Legislativo 30/06/2003**, n 196 modificato dal D.lgs n. 101 del 10 agosto 2018.

[Torna al sommario](#)

3.2. Standard di riferimento

Così come richiesto dal DPCM 3 dicembre 2013, e nello specifico dall'allegato 3, di seguito si riportano gli standard per la conservazione dei documenti informatici:

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

[Torna al sommario](#)

4. Ruoli e responsabilità

Si elencano in questo capitolo i profili professionali e le diverse attività svolte dal gruppo di lavoro incaricato del servizio di conservazione dei documenti, così come individuati nel documento “Profili professionali” pubblicato da AgID.

Le procedure organizzative si basano sugli standard UNI EN ISO 27001:2013 e ISO 9001:2008.

La tabella di seguito riporta i dati identificativi dei soggetti responsabili:

Ruolo	Responsabile	Attività di competenza	Periodo nel ruolo
Responsabile del servizio di conservazione	Paolo Giulioni	<ul style="list-style-type: none"> - Definizione e attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione; - definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente; - corretta erogazione del servizio di conservazione all’ente produttore; - gestione delle convenzioni, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione. 	<p style="text-align: center;">Dal 22/06/2009 a oggi fino a revoca</p>
Responsabile della funzione archivistica di conservazione	Giulia Colombo	<ul style="list-style-type: none"> - Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell’ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; 	<p style="text-align: center;">Dal 25/01/2019 fino a revoca</p>

		<ul style="list-style-type: none"> - definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici; - monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione; - collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza. 	
<p>Responsabile della sicurezza dei sistemi per la conservazione</p>	<p>Bernardino Cerocchi</p>	<ul style="list-style-type: none"> - Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; - segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive. 	<p>Dal 22/06/2009 a oggi fino a revoca</p>
<p>Responsabile dei sistemi informativi per la conservazione</p>	<p>Andrea Reali</p>	<ul style="list-style-type: none"> - Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione; - monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore; - segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive; 	<p>Dal 22/06/2009 a oggi fino a revoca</p>

		<ul style="list-style-type: none"> - 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. 	
<p>Responsabile dello sviluppo e della manutenzione del sistema di conservazione</p>	<p>Bernardino Cerocchi</p>	<ul style="list-style-type: none"> - 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 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; - gestione dello sviluppo di siti web e portali connessi al servizio di conservazione. 	<p>Dal 22/06/2009 a oggi fino a revoca</p>
<p>Responsabile del trattamento dei dati personali</p>	<p>Andrea Reali</p>	<p>Il soggetto è delegato allo svolgimento delle seguenti attività nell'ambito del processo di conservazione nell'eventualità il responsabile sia impossibilitato a svolgere la mansione prevista (assenze prolungate, malattia ecc.):</p>	<p>Dal 30/03/2009 a oggi fino a revoca</p>

		<ul style="list-style-type: none"> - Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; - garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza. 	
--	--	---	--

La tabella di seguito riporta i dati identificativi dei soggetti delegati:

Ruolo	Delegato	Attività di competenza	Periodo di validità della delega
<i>Responsabile del servizio di conservazione</i>	Danilo Aloisi	<p>Il soggetto è delegato allo svolgimento delle seguenti attività nell'ambito del processo di conservazione nell'eventualità il responsabile sia impossibilitato a svolgere la mansione prevista (assenze prolungate, malattia ecc.):</p> <ul style="list-style-type: none"> - Definizione e attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione; - definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente; - corretta erogazione del servizio di conservazione all'ente produttore; - gestione delle convenzioni, definizione degli aspetti tecnico- 	<p style="text-align: center;">Dal 15/05/2018 a oggi fino a revoca</p>

		operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.	
Responsabile del trattamento dei dati personali	Bernardino Cerocchi	<p>Il soggetto è delegato allo svolgimento delle seguenti attività nell'ambito del processo di conservazione nell'eventualità il responsabile sia impossibilitato a svolgere la mansione prevista (assenze prolungate, malattia ecc.):</p> <ul style="list-style-type: none"> - Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; - garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza. 	<p>Dal 10/10/2016 ad oggi</p>

Cronologia dei responsabili del servizio di conservazione dei documenti informatici e loro delegati

Nome e Cognome	Funzione	Data nomina	Data Revoca
Riccardo Olivetti Legale Rappresentante	Responsabile del servizio di conservazione	//	22/06/2009
Paolo Giulioni	Responsabile del servizio di conservazione	22/06/2009	
Giorgio Sabatini	Responsabile della funzione archivistica di conservazione	22/06/2009	15/01/2019
Bernardino Cerocchi	Responsabile della sicurezza dei sistemi per la conservazione	22/06/2009	
Andrea Reali	Responsabile dei sistemi informativi per la conservazione	22/06/2009	

Bernardino Cerocchi	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	22/06/2009	
Andrea Reali	Responsabile per il trattamento dei dati personali	30/03/2009	
Bernardino Cerocchi	Delegato Responsabile del trattamento dei dati personali	10/10/2016	
Antonio Ferraiuolo	Delegato responsabile dei sistemi informativi per la conservazione	10/10/2016	04/11/2019
Antonio Ferraiuolo	Delegato responsabile della manutenzione del sistema di conservazione	10/10/2016	04/11/2019
Roberto D'Este	Delegato responsabile per la sicurezza dei sistemi informativi per la conservazione	10/10/2016	02/05/2019
Giorgio Sabatini	Delegato responsabile del Sistema di Conservazione	10/10/2016	15/05/2018
Ilaria Bortone	Delegato responsabile della Funzione Archivistica di conservazione	10/10/2016	30/11/2017
Giulia Colombo	Delegato Responsabile della Funzione Archivistica di conservazione	01/01/2018	25/01/2019
Danilo Aloisi	Delegato responsabile del Sistema di Conservazione	15/15/2018	
Giulia Colombo	Responsabile della funzione archivistica di conservazione	25/01/2019	

[Torna al sommario](#)

5. Struttura organizzativa per il servizio di conservazione

5.1. Organigramma

Si riporta di seguito l'organigramma della struttura coinvolta nel servizio di conservazione.

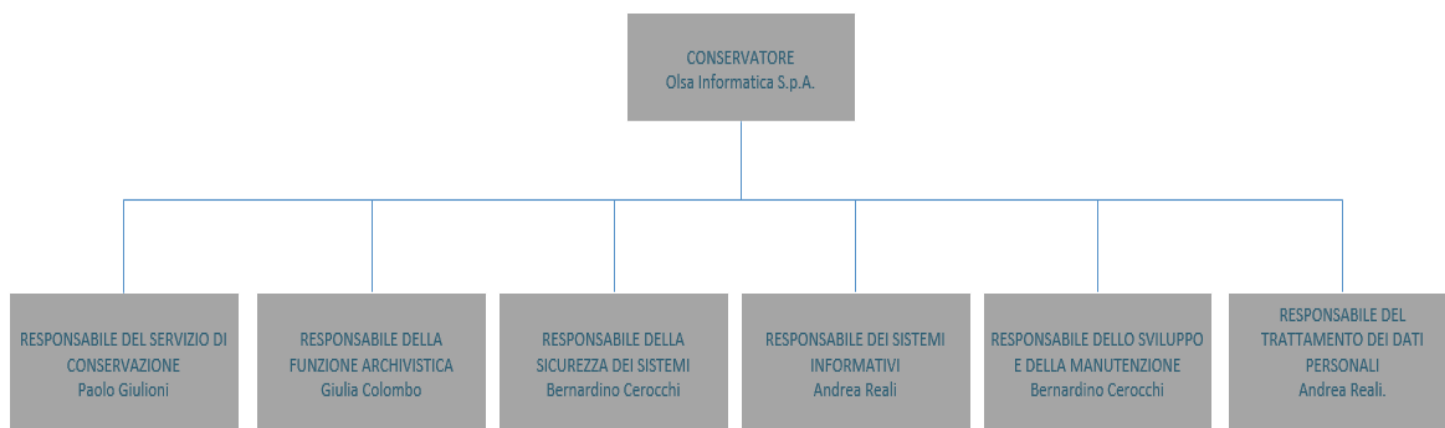


Figura 1: Organigramma di Olsa Informatica

[Torna al sommario](#)

5.2. Strutture organizzative

Olsa Informatica eroga servizi di conservazione utilizzando soluzioni tecnologiche che soddisfano i requisiti di alta affidabilità richiesti dalla normativa. Il modello organizzativo adottato dal soggetto conservatore è idoneo a gestire il servizio di conservazione in base a quanto stabilito dall'art. 5 comma 2 lettera b delle vigenti Regole tecniche (DPCM 3 dicembre 2013). Il sistema di conservazione opera secondo modelli organizzativi esplicitamente definiti che garantiscono la sua distinzione logica dal sistema di gestione documentale. Il modello organizzativo del soggetto conservatore è stato realizzato tenendo conto del modello OAIS (Open Archival Information System, certificato standard ISO 14721 nel 2003 e recentemente aggiornato in ISO 14721:2012), ovvero una struttura organizzata di persone e sistemi, che accetta la responsabilità di conservare l'informazione e di renderla disponibile per una comunità di riferimento.

Seguendo quanto indicato dalle Regole tecniche vigenti (vedi art. 6 comma 1 D.P.C.M. 3 dicembre 2013) e sulla base dello stesso modello OAIS, il sistema identifica i seguenti ruoli fondamentali all'interno del sistema di conservazione: produttore, utente, responsabile della conservazione.

Produttore: è una persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento (SIP) ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione, come indicato nelle vigenti Regole tecniche (Glossario, allegato 1 DPCM 3 dicembre 2013). Secondo lo standard OAIS, il produttore è il ruolo svolto dalle persone o dai sistemi client che forniscono le informazioni da conservare.

Il produttore si impegna a depositare i documenti informatici e le loro aggregazioni documentali informatiche nel sistema di conservazione, nei modi e nelle forme definite, garantendone l'autenticità e l'integrità nelle

fasi di produzione e di archiviazione corrente, effettuata nel rispetto delle norme sulla formazione e sui sistemi di gestione dei documenti informatici. In particolare, garantisce che il trasferimento dei documenti informatici venga realizzato utilizzando formati compatibili con la funzione di conservazione e rispondenti a quanto previsto dalla normativa vigente. Si impegna, inoltre, a depositare e mantenere aggiornati gli strumenti di ricerca e gestione archivistica elaborati a supporto della formazione dei documenti informatici e della tenuta degli archivi digitali. Il produttore ha accesso al sistema di conservazione direttamente dalla propria sede, tramite accesso da remoto.

Nelle Amministrazioni Pubbliche, tale figura si identifica con il responsabile della gestione documentale.

Utente: è una persona, ente o sistema che interagisce con i servizi di un sistema per la conservazione di documenti informatici al fine di acquisire le informazioni di interesse, come indicato nelle vigenti Regole tecniche (Glossario, allegato 1 DPCM 3 dicembre 2013). Tali informazioni vengono fornite dal sistema di conservazione secondo le modalità previste all'art. 10 del suddetto decreto.

L'utente richiede al sistema di conservazione l'accesso ai documenti informatici per acquisire le informazioni di interesse nei limiti previsti dalla legge. Il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, ai documenti informatici conservati e consente la produzione di un pacchetto di distribuzione (DIP) direttamente acquisibile dai soggetti autorizzati. In termini OAIS la comunità degli utenti può essere definita come comunità di riferimento.

Nelle Specifiche tecniche, allegato al Contratto di affidamento del servizio di conservazione, vengono indicati quei soggetti abilitati dal soggetto produttore che possono accedere ai documenti versati nel sistema di conservazione. L'abilitazione e l'autenticazione degli utenti avviene in base alle procedure di gestione utenze indicate nel Piano della sicurezza del sistema di conservazione e nel rispetto delle misure di sicurezza previste negli articoli 31-36 del D.Lgs. 30 giugno 2003, n. 196, in particolare di quelle indicate all'art. 34 comma 1, e dal Disciplinare tecnico di cui all'Allegato B del medesimo decreto.

Responsabile della conservazione: è il soggetto responsabile delle attività elencate nell'art. 7 comma 1 del DPCM 3 dicembre 2013. Il responsabile della conservazione opera d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei sistemi informativi, oltre che con il responsabile della gestione documentale, definendo le caratteristiche e i requisiti del sistema di conservazione in funzione alla tipologia di documenti da conservare, in conformità alla normativa vigente. Nelle Pubbliche Amministrazioni, il ruolo di responsabile della Conservazione può essere svolto dal responsabile della gestione documentale ovvero dal coordinatore della gestione documentale, ove nominato.

Secondo quanto previsto dall'art. 6 del suddetto decreto, il responsabile della conservazione, tramite specifico contratto, può affidare le attività di gestione e la supervisione del processo di conservazione a un soggetto pubblico o privato che svolge attività di conservazione, nella figura del Responsabile del servizio di conservazione, mediante contratto o convenzione di servizio.

Organismo di tutela e vigilanza (in riferimento alle Amministrazioni Pubbliche): il Ministero dei beni e delle attività culturali e del turismo (MiBACT), che esercita funzioni di tutela e vigilanza dei sistemi di conservazione degli archivi di enti pubblici e di enti privati dichiarati di notevole interesse storico, autorizza le operazioni di scarto e il trasferimento della documentazione conservata ai sensi del D.Lgs. 42/2004 (Codice dei beni culturali e del paesaggio).

La tutela e vigilanza sugli archivi di enti pubblici non statali è esercitata dal MiBACT, tramite le Soprintendenze archivistiche competenti per territorio.

"Lo spostamento, anche temporaneo, dei beni culturali", compresi gli Archivi storici e di deposito, è soggetto ad autorizzazione del Ministero (D.Lgs. 22 gen. 2004, n. 42, art. 21, c. 1, lettera b).

Anche "il trasferimento ad altre persone giuridiche di complessi organici di documentazione di archivi pubblici, nonché di archivi di soggetti giuridici privati", per i quali sia intervenuta la dichiarazione dell'interesse culturale ai sensi dell'articolo 13, rientra tra gli interventi soggetti ad autorizzazione del Ministero (D.Lgs. 22 gen. 2004, n. 42, art.21, c. 1, lettera e).

La disposizione si applica anche:

- all'affidamento a terzi dell'archivio (outsourcing);
- al trasferimento di archivi informatici ad altri soggetti giuridici, nell'ottica della conservazione permanente sia del documento sia del contesto archivistico.

La Soprintendenza può, in seguito a preavviso, effettuare ispezioni per accertare lo stato di conservazione e custodia degli archivi e può emettere prescrizioni per la tutela degli archivi.

In base alle Regole tecniche, i sistemi di conservazione delle Amministrazioni Pubbliche e i sistemi di conservazione dei conservatori accreditati sono soggetti anche alla vigilanza di AgID.

[Torna al sommario](#)

6. Oggetti sottoposti a conservazione

La rappresentazione degli oggetti sottoposti conservazione è parte integrante delle Specifiche tecniche (allegato al Contratto di affidamento del servizio di conservazione).

[Torna al sommario](#)

6.1. Oggetti conservati

Il sistema conserva documenti informatici, in particolare documenti amministrativi informatici, con i metadati ad essi associati e le loro aggregazioni documentali informatiche (aggregazioni), che includono i fascicoli informatici (fascicoli).

I documenti informatici e le loro aggregazioni di tipo fascicolo sono inviati in conservazione sotto forma di pacchetti di versamento (SIP), che contengono anche i relativi metadati.

Il sistema gestisce gli oggetti sottoposti a conservazione, distinti per ogni singolo soggetto produttore oppure per singole AOO (Aree Organizzative Omogenee), consentendo configurazioni e parametri adeguati ad ogni soggetto produttore, definiti sulla base degli accordi stipulati all'atto della sottoscrizione del Contratto di affidamento del servizio di conservazione.

Per mantenere nel sistema le informazioni relative alla struttura dell'archivio e al vincolo archivistico, le unità documentarie sono versate corredate da un set di metadati che include gli elementi identificativi e descrittivi del fascicolo, con riferimento alla voce di classificazione e all'eventuale articolazione in sottofascicoli. Inoltre è gestita la presenza di classificazioni, fascicoli e sottofascicoli e i collegamenti tra le diverse unità archivistiche e documentarie presenti nel sistema.

Le serie e i fascicoli possono essere versati nel sistema quando sono completi e dichiarati chiusi, descritti da un set di metadati che include obbligatoriamente, oltre alle informazioni di identificazione, classificazione e descrizione, anche il tempo di conservazione previsto. Nel caso delle serie, la chiusura può avvenire a cadenza annuale o comunque secondo una definizione temporale definita.

I documenti informatici (unità documentarie) e i fascicoli informatici, possono essere suddivisi secondo un piano di classificazione che identifica gruppi documentali omogenei per natura e/o funzione giuridica (titolo, classe, sottoclasse), modalità di registrazione o di produzione.

Le tipologie documentarie trattate e i loro specifici metadati e articolazioni, sono indicate nell'allegato di servizio concordato con ogni soggetto produttore e riportate nelle funzionalità di amministrazione del sistema.

L'unità documentaria rappresenta l'unità minima elementare di riferimento di cui è composto un archivio, pertanto rappresenta il riferimento principale per la costruzione dei pacchetti informativi secondo lo standard OAIS. Con riferimento a quanto indicato nello standard ISO 23081-2, l'unità documentaria rappresenta la più piccola "*unit of records*" individuabile e gestibile come una entità singola gestita nel sistema, anche se al suo interno contiene elementi come ad esempio un messaggio di posta elettronica con i suoi allegati. All'unità documentaria, e agli elementi che la compongono, sono associati set di metadati che li identificano e li descrivono, secondo le logiche e le articolazioni esposte nelle Specifiche tecniche descritte nel documento allegato al Contratto di affidamento del servizio di conservazione.

Coerentemente con quanto sopra riportato l'unità documentaria è pertanto logicamente strutturata su tre livelli: unità documentaria, documento, file.

Il sistema di conservazione utilizza come formati di conservazione quelli elencati al punto 5 dell'Allegato 2 alle Regole tecniche e, inoltre, è in grado di gestire, su richiesta del soggetto produttore, anche formati non compresi nel suddetto elenco ma che il soggetto produttore utilizza nei propri sistemi e che ritiene di dover conservare.

Tutti i formati gestiti sono elencati e descritti in un registro interno al sistema di conservazione "Registro dei Formati" in cui ogni formato è corredato da informazioni descrittive relative alla eventuale versione e al mime type.

Con ciascun soggetto produttore viene concordato un elenco di formati ammessi, che individua i formati che il sistema può accettare per ogni soggetto produttore e per ogni tipologia documentaria. L'elenco dei formati ammessi è riportato (e gestito) nelle funzionalità "Amministrazione strutture versanti" del sistema ed è aggiornato continuamente in base alle esigenze. Le modalità con cui si procede a tale aggiornamento sono concordate con ciascun soggetto produttore e riportate nelle Specifiche tecniche. Il sistema identifica i formati al momento della ricezione del SIP mediante l'analisi dei *magic number* o del contenuto del file, in modo tale da consentire l'individuazione dello specifico mime type. L'informazione sul formato è parte dei metadati dei componenti dell'unità documentaria e costituisce un elemento delle informazioni sulla rappresentazione.

Di seguito, viene fornito un riepilogo dei formati al momento ammessi per la conservazione, previsti nell'allegato 2 delle Regole tecniche, DPCM 13 novembre 2014.

Formato	Proprietario	Estensione	Tipo	Aperto	Standard
PDF - PDF/A	Adobe Systems http://www.adobe.com/	.pdf	application/pdf	Si	ISO 32000-1 (PDF); ISO 19005-1:2005 (vers. PDF 1.4); ISO 19005-2:2011 (vers. PDF 1.7)
TIFF	Aldus Corporation (acquisita Adobe)	.tif	image/tiff	No	ISO 12639 (TIFF/IT); ISO 12234 (TIFF/EP)
JPG e JPEG 2000	Joint Photographic Experts Group	.jpg, .jpeg, .jp2 (JPEG 2000)	image/jpeg	Si	ISO/IEC 10918:1 (JPG); ISO/IEC 15444-1 (JPEG 2000)
Office Open XML (OOXML)	Microsoft	.docx, .xlsx, .pptx	MIME	Si	ISO/IEC DIS 29500:2008
ODF Open Document Format	OASIS	.ods, .odp, .odg, .odb	application/vnd.oasis.opendocument.text	Si	ISO/IEC 26300:2006; UNI CEI ISO/IEC 26300
XML Extensible Markup Language	W3C	.xml	application/xml text/xml	Si	
TXT	-	.txt	ASCII, UTF-8, UNICODE	Si	ISO 646, RFC 3629, ISO/IEC 10646

PEC ed EMAIL	-	.eml	MIME	No	RFC 2822/MIME
--------------	---	------	------	----	---------------

Lo standard OAIS prevede che, ad ogni oggetto portato in conservazione, venga associato un insieme di informazioni (metadati) che ne permetta in futuro una facile reperibilità. In questo insieme di metadati troviamo le informazioni sulla rappresentazione (IR), classificabili in sintattiche (IRsi) e semantiche (IRse), il cui obiettivo è fornire tutte le informazioni necessarie per poter leggere ed interpretare la sequenza di bit dell'oggetto conservato. Inoltre, ad un sistema di conservazione che rispetti la normativa italiana, è richiesto il requisito di leggibilità degli oggetti dati, imposto dal comma 1 dell'art. 3 delle nuove Regole tecniche e dal comma 1 dell'art. 44 del Codice dell'Amministrazione Digitale.

Risulta necessario affrontare tre tematiche importanti:

- La prima riguarda “cosa” e “come” associare ad un oggetto conservato in merito alle informazioni sulla rappresentazione;
- La seconda si riferisce al “come” rispettare il requisito di leggibilità;
- La terza si riferisce a “cosa” e “come” fornire nel momento in cui quell'oggetto deve essere distribuito agli utenti.

Per soddisfare questi requisiti, prima di versare un qualsiasi oggetto digitale nel sistema di conservazione è necessario che il Responsabile del servizio di conservazione, in accordo con il soggetto produttore, proceda a conservare tutte le informazioni sulla rappresentazione necessarie alla consultazione di tale oggetto.

Classifichiamo quindi le informazioni sulla rappresentazione in:

- Strumenti per la leggibilità: tipicamente legati al formato dell'oggetto conservato.
- Informazioni sulla rappresentazione sintattica: tipicamente legate al formato dell'oggetto conservato.
- Informazioni sulla rappresentazione semantica: tipicamente legate alla descrizione archivistica dell'oggetto conservato.

Sebbene, le informazioni sulla rappresentazione sintattica (tipo 2) possano essere considerate le basi su cui poggiare le successive conservazioni di oggetti di uno specifico formato, poiché sono le informazioni necessarie a produrre/creare gli strumenti che ne permettono la leggibilità (tipo 1), resta fondamentale fornire fin dal principio, insieme all'oggetto conservato, gli strumenti necessari per poterlo leggere.

Concludendo, per soddisfare l'eventuale necessità di una disponibilità immediata dell'oggetto conservato, possiamo affermare che il sistema di conservazione deve avere almeno conservato gli strumenti per la leggibilità (visualizzatori) degli oggetti dati da conservare.

Si ritiene pertanto necessaria la capacità del software di generare, per ogni soggetto produttore, un insieme di descrizioni archivistiche “speciali” che permettano di conservare le tre tipologie di informazioni sulla rappresentazione.

Nel sistema di conservazione distinguiamo tre descrizioni archivistiche speciali:

1. Viewer: di tipologia “unità documentaria” con file di indice di tipo multi-indice.
2. Fascicolo: informazioni sulla rappresentazione di tipologia “fascicolo”.
3. Informazioni sulla rappresentazione di tipologia “unità documentaria” con file di indice di tipo indice singolo.

Le descrizioni archivistiche speciali sono descrizioni archivistiche prime, nel senso che gli oggetti digitali conservati non hanno nessuna associazione con informazioni sulla rappresentazione.

La prima è obbligatoria, e oltre ai classici metadati Dublin Core, permette di associare ad ogni documento informatico conservato (eseguibile del visualizzatore) la versione del visualizzatore, la lingua del visualizzatore e il sistema operativo di riferimento (versione, bit, lingua).

Le operazioni per il suo versamento possono essere effettuate sia attraverso un pacchetto di versamento (file di metadati di tipo multi indice) che manualmente da interfaccia web.

Dal punto di vista delle funzionalità invece si evidenziano i seguenti scenari:

- La conservazione di un nuovo “viewer” per un mime type già associato ad un Software precedente va in aggiunta.
- Sarà sempre possibile modificare il metadato “Data Fine” per un “Software” se non ci sono conservazioni successive alla “data fine” inserita.
- La modifica di un solo documento di un “fascicolo informazioni sulla rappresentazione” – nel caso in cui cambiano le specifiche di un formato file – prevede la ri-conservazione dell’intero fascicolo.

Le descrizioni archivistiche speciali sono di norma conservate per il conservatore ed ereditate da tutti gli altri SP. In generale l’ereditarietà delle Informazioni sulla rappresentazione si sviluppa come nel classico schema di ereditarietà:

soggetto produttore → soggetto produttore Padre → ... → soggetto produttore Padre → soggetto conservatore e Licenziatario.

Ad un oggetto digitale conservato viene associato un viewer sulla base delle seguenti:

- formato (mime type);
- eventuale versione del formato;
- versione dello strumento di visualizzazione;
- lingua dello strumento di visualizzazione;
- versione del sistema operativo.

Visto che questa n-pla permette di avere diversi strumenti per uno stesso mime type, il sistema di conservazione permette al Responsabile del servizio di conservazione di impostare, a livello di soggetto produttore e/o a livello di descrizione archivistica, quali siano gli strumenti che garantiscono la leggibilità nel lungo periodo di un documento in uno specifico formato da collegare all’atto della conservazione e restituire all’atto di esibizione.

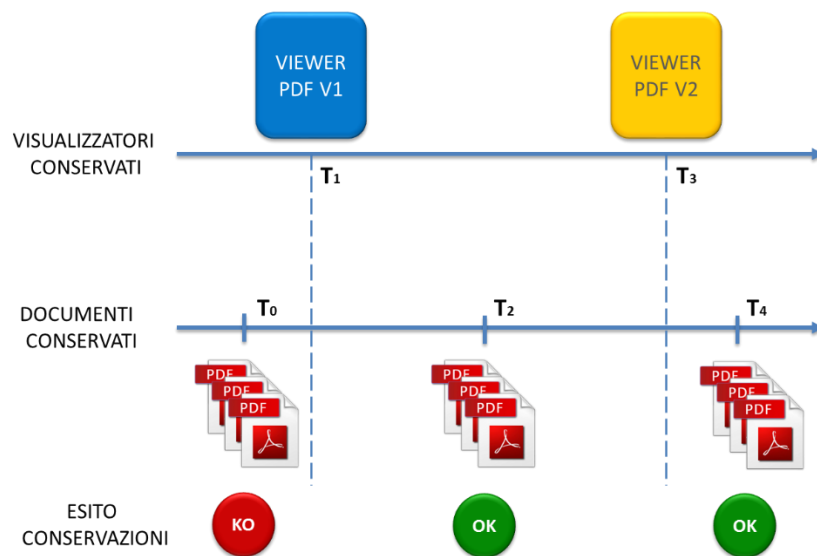


Figura 2: Gestione dell'aggiornamento del viewer

Per quanto riguarda le informazioni sulla rappresentazione sintattica, essendo legate al mime type e alla relativa versione come i viewer appena discussi, ogni oggetto in un pacchetto di archiviazione si riferisce ad uno o più link che permettono di risalire all'n-pla:

- formato (mime type);
- eventuale versione del formato.

Queste informazioni non si distinguono a livello di descrizione archivistica o soggetto produttore in quanto sono le specifiche internazionali sul formato in oggetto.

Per quanto riguarda le informazioni sulla rappresentazione semantica, essendo queste legate ad una particolare versione di una descrizione archivistica, sono tra loro riferite tramite chiave.

[Torna al sommario](#)

6.2. Pacchetto di versamento

Si tratta del pacchetto informativo inviato dal produttore al sistema di conservazione e oggetto dell'accordo stipulato in occasione del Contratto di affidamento del servizio di conservazione.

In termini di pacchetto di versamento, il Contratto di affidamento del servizio di conservazione è finalizzato alla definizione degli accordi che sanciscono le modalità di trasferimento dei pacchetti stessi, la loro tempistica di trasferimento, la loro costituzione e composizione e tutte le componenti informative di cui il sistema di conservazione necessita per creare degli AIP coerenti e bene strutturati.

Sulla base di quanto concordato nella fase di negoziazione iniziale, è possibile trasferire i pacchetti di versamento in maniera **automatizzata**, **semiautomatizzata** oppure **manuale**, da interfaccia web.

In questo sistema di conservazione possono essere trasferiti pacchetti di versamento conformi a quanto previsto dalle Regole tecniche: esso supporta SIP eventualmente accompagnati da IR nel formato definito nell'allegato 5 delle nuove Regole tecniche e nel formato CSV.

La fase relativa alla preparazione del pacchetto di versamento (SIP) e il conseguente invio al sistema di conservazione può avvenire in modi diversi, essendo dipendente fortemente dalla situazione specifica del

soggetto produttore e dagli accordi stipulati con il conservatore. Come anticipato, il sistema di conservazione dispone di tre modi per sottoporre un pacchetto di versamento:

1. **automatico** - via web service
2. **semiautomatico** - via file system
3. **manuale** - via interfaccia web mediante upload manuale dei documenti.

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

In condizioni generali il pacchetto di versamento, prodotto e trasferito dal produttore al sistema di conservazione, è costituito dall'insieme dei file che saranno oggetto di conservazione, accompagnati da un file detto file di indice o file dei metadati.

Il file di indice dovrà contenere i metadati per ricercare i documenti all'interno del sistema. Le informazioni sono concordate con il conservatore e configurate nel sistema di conservazione per ciascuna descrizione archivistica, nella stessa configurazione saranno anche implementate le regole di validazione dei metadati, concordate sempre con il conservatore. Come anticipato nel paragrafo precedente, il file di indice potrà essere un file in formato CSV o un file XML con tracciato definito nell'allegato 5 delle nuove Regole tecniche in materia di conservazione dei documenti informatici.

La struttura e la forma del file di indice dipendono sia dalla modalità di trasferimento, scelta tra le tre disponibili, sia dalla natura dei file che costituiscono il pacchetto e dalle eventuali relazioni tra gli stessi. Una volta che i Pacchetti di versamento sono stati acquisiti, questi vengono trasformati in pacchetti di archiviazione (AIP).

Nel sistema di conservazione di Olsa Informatica i metadati possono essere di vari tipi.

Ci si è attenuti all'allegato 5 del DPCM 3 Dicembre 2015 recante le Regole tecniche per il sistema di conservazione. In aggiunta ai metadati previsti al dal DPCM suddetto vengono gestiti i seguenti tipi:

- Stringa;
- Numero;
- Data;
- Dizionario (insieme finito di valori);
- Hash (SHA256 del file);
- Universal UID (per collegare il documento ad un eventuale documentale presente nel soggetto produttore);
- MIME Type (per poter poi associare un documento alle informazioni di rappresentazione);
- Document Type (per poter associare un documento di un fascicolo alla sua classe documentale).

Inoltre, per ogni metadato è possibile definire:

- Obbligatorietà;
- Univocità;
- Ricercabilità;

- Espressione regolare di validazione;
- Espressione di conversione (da stringa a intero oppure da stringa a data);
- Classificazione privacy: dato personale, sensibile, giudiziario, sanitario.

Inoltre, il sistema di conservazione, in quanto sistema di conservazione, è in grado di classificare i metadati versati in base alla gestione Privacy a cui sono soggetti. La classificazione permette di gestire i seguenti casi:

1. Dato generico
2. Dato personale
3. Dato sensibile
4. Dato giudiziario

Così come definito dall'art. 22 del D. Lgs. 196/2003 i dati sensibili e giudiziari (caso 3 e 4) vengono trattati con tecniche di cifratura dipendenti dal sistema di database utilizzato, e sono resi illeggibili anche a chi è autorizzato ad accedervi. L'identificazione dell'interessato da parte di un utente autorizzato, viene tracciato in appositi log dal sistema di conservazione.

Nel sistema di conservazione la definizione di un metadato di tipo generico o personale (caso 1 e 2) fornisce la possibilità di essere comunque gestito con tecniche di cifratura, se impostate nella configurazione della descrizione archivistica, e fornisce anche la possibilità di tracciare l'utente che ha visualizzato il dato personale e i documenti ad esso associato.

Si elenca di seguito una tabella riepilogativa:

Tipo Dato	Cifratura	Tracciabilità
Dato Generico	Opzionale	Opzionale
Dato Personale	Opzionale	Obbligatoria
Dato Sensibile	Obbligatoria	Obbligatoria
Dato Giudiziario	Obbligatoria	Obbligatoria

In merito alla conservazione dei fascicoli informatici il conservatore si interfacerà con il Responsabile della conservazione per concordare il set di metadati specifico per il fascicolo.

[Torna al sommario](#)

6.3. Pacchetto di archiviazione

Un pacchetto di archiviazione (AIP) è un oggetto informativo, contenitore a sua volta di altri oggetti informativi. All'interno del pacchetto di archiviazione, si trova l'oggetto informativo individuato per la conservazione, ovvero il contenuto informativo. Anche il pacchetto di archiviazione contiene un oggetto che prende il nome di informazioni sulla conservazione, (PDI).

Il principio su cui si basa l'architettura del modello dati del sistema di conservazione è quello di un'assoluta auto-consistenza del pacchetto informativo nel momento in cui è costituito l'AIP stesso, tale obiettivo viene raggiunto grazie all'aderenza al modello funzionale e al modello-dati previsto in OAIS.

La coerenza di un pacchetto informativo è data da due componenti logiche fondamentali:

- l'insieme delle informazioni statiche che prevedono un set complesso di metadati che descrivono in maniera "piatta" tutti gli elementi identificativi, descrittivi, gestionali, tecnologici, etc., relativi ad uno e uno solo pacchetto informativo;

- l'insieme delle relazioni di contesto che permettono la correlazione logica del pacchetto informativo agli altri pacchetti informativi e in generale ad un qualsiasi contesto di natura archivistico-gerarchica.

Quest'ultimo elemento è quello che ci permette di ricostruire il vincolo archivistico e quindi di ricondurre, ad esempio, a una stessa pratica o a uno stesso fascicolo, tutti i documenti relativi a un medesimo affare o procedimento amministrativo.

Concretamente si può prevedere che nel sistema si conserveranno, all'interno di un medesimo pacchetto informativo (e quindi incapsulate in una medesima busta), le seguenti componenti codificate in un XML:

- l'oggetto digitale possibilmente in un formato standard non proprietario;
- l'impronta del documento generata con funzione di hash;
- il riferimento temporale (rappresentato dalla marca temporale o altro riferimento temporale opponibile a terzi, come la segnatura di protocollo);
- il set di metadati per la conservazione:
 - metadati identificativi (per esempio possono essere utilizzati i metadati dello standard ISAD);
 - metadati descrittivi (per esempio possono essere utilizzati i metadati dello standard ISAD);
 - metadati gestionali (UNI SInCRO);
 - metadati tecnologici (per esempio possono essere utilizzati i metadati dello standard METS);
- il viewer necessario per la visualizzazione del documento stesso, o in alternativa, si inserisce il puntatore/riferimento al viewer comune a più pacchetti informativi per quel formato di file del documento;
- la documentazione tecnica necessaria alla comprensione del viewer stesso (anch'esso può essere un puntatore/riferimento che rimanda alla componente digitale descritta per più pacchetti informativi) oppure la documentazione per la comprensione del documento digitale e/o della classe documentale di riferimento.

Tale descrizione si concretizza in un file contenente i metadati secondo il modello sopra proposto che prende il nome di Indice del Pacchetto di Archiviazione (IPdA), indicato come Indice di Conservazione (IdC) nello standard UNISinCRO. L'indice di conservazione rispetta tale standard; esso non contiene un oggetto digitale, nella stretta accezione OAIS, ma diventa un container da conservare. Oltre ai metadati tipici (ad esempio, denominazione del fascicolo, estremi cronologici del fascicolo, riferimenti al procedimento amministrativo associato) esso conterrà due puntatori fondamentali:

- uno o più puntatori agli oggetti digitali contenuti nel fascicolo (un fascicolo può contenere uno o più data object);
- uno o più puntatori alla struttura archivistica di riferimento (quindi alla serie/sottoserie della rappresentazione attuale dell'archivio); in altre parole un fascicolo potrà riferirsi ad una o più serie archivistiche.

Una volta che i SIP sono stati acquisiti nel sistema (sono stati quindi oggetto di controlli sui metadati previsti dal contratto di servizio) essi sono pronti ad essere trasformati in AIP.

All'atto della conservazione verrà composto il pacchetto di archiviazione (AIP). Il Pacchetto di archiviazione è identificato dalle informazioni sull'impacchettamento.

Si riporta la rappresentazione grafica della struttura dell'Indice del Pacchetto di Archiviazione.

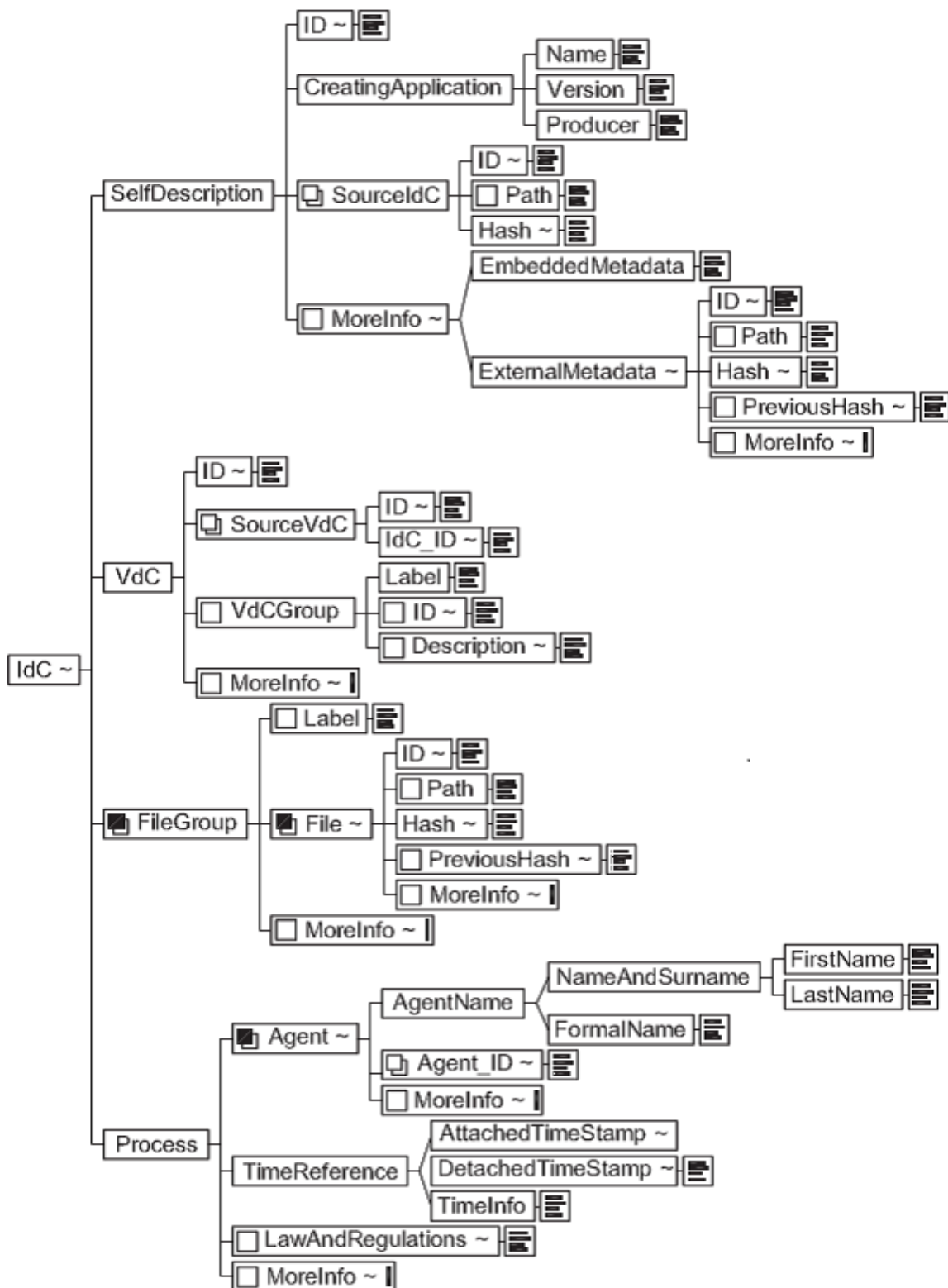


Figura 3: Struttura dell'Indice del Pacchetto di Archiviazione (IPdA)

L'elemento "MoreInfo" presente può essere oggetto di ulteriori specificazioni e deve essere inteso come una sorta di "plug-in" per strutture di metadati specialistiche.

Lo schema seguente mostra sinteticamente i legami tra l'Indice del Pacchetto di Archiviazione e gli oggetti digitali ad esso associati (documenti e more info) che costituiscono l'AIP:

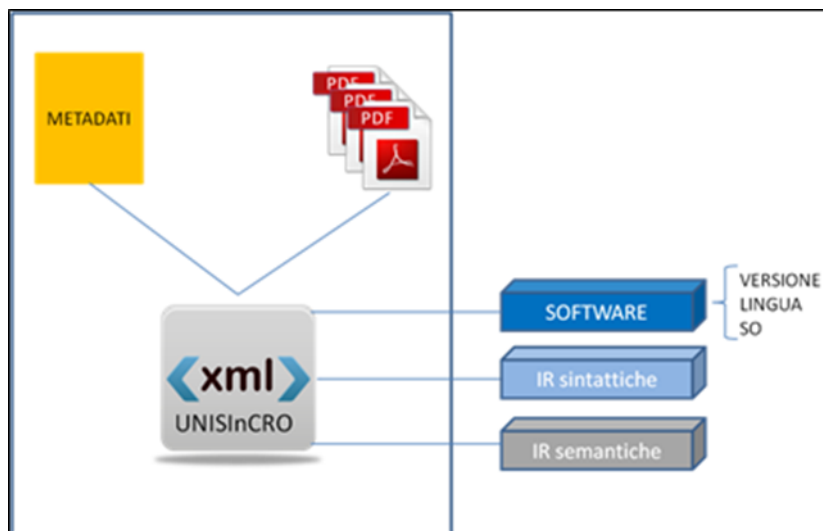


Figura 4: Schema dell'AIP e dei collegamenti con le informazioni sulla rappresentazione

In un contesto OAIS il pacchetto di archiviazione deve essere auto-consistente, ovvero, deve prevedere tutte le informazioni necessarie al recupero e alla ricostruzione dell'oggetto conservato e delle informazioni ad esso associate.

[Torna al sommario](#)

6.4. Pacchetto di distribuzione

Nel modello OAIS, il pacchetto di distribuzione (DIP) è strutturato nel modello dati come il pacchetto di archiviazione (AIP).

La differenza sta nella sua destinazione in quanto esso viene concepito per essere fruito e utilizzato dall'utente finale (esibizione). In questo caso, un DIP può anche non coincidere con un AIP originale conservato nel data center: anzi, molto spesso, ragioni di opportunità inducono a distribuire pacchetti informativi che sono un'estrazione del contenuto informativo di un AIP (negando ad esempio l'accesso ad una parte di esso). Può anche verificarsi il caso di DIP che sono il frutto di più AIP che vengono "spacchettati" e rimpacchettati per un più fruibile utilizzo da parte dell'utente.

Un utente autorizzato di un soggetto produttore è in grado di interrogare il sistema per ricevere in uscita uno specifico DIP. L'utente utilizzerà le funzionalità di richiesta di esibizione di un documento o di un insieme di documenti, per ottenerne una replica esatta secondo i fini previsti dalla norma.

Il sistema di conservazione gestisce un archivio dei software eseguibili, ciascuno dei quali utile a visualizzare un determinato formato file cui appartengono i documenti conservati. I software dell'archivio sono associati ad una descrizione archivistica in modo tale che, al momento della generazione dei pacchetti di distribuzione dei documenti informatici da esibire, vengano automaticamente inclusi anche e solo i software necessari alla

loro visualizzazione. In risposta alla richiesta iniziale di esibizione, da parte dell'utente, il sistema risponderà restituendo un DIP che nel caso più completo conterrà:

- I documenti richiesti nel formato previsto per la loro visualizzazione;
- Un'estrazione dei metadati associati ai documenti;
- L'indice di conservazione firmato e marcato;
- I viewer necessari alla visualizzazione dei documenti del pacchetto.

Inoltre, nei pacchetti di distribuzione, è possibile inserire tutta la catena di documentazione necessaria a rispondere alle esigenze dello standard OAIS.

[Torna al sommario](#)

7. Il processo di conservazione

Per processo di conservazione si intende l'insieme delle attività finalizzate alla conservazione dei documenti informatici; Legal Archive[®] è lo strumento utilizzato da Olsa Informatica per espletare il servizio di conservazione dei clienti che si affidano all'outsourcing.

Il processo di conservazione digitale a norma di Olsa Informatica prevede, come definito dall'articolo 9 del DPCM del 3 dicembre 2013, quanto segue:

- l'acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico;
- la verifica che il pacchetto di versamento e gli oggetti contenuti siano coerenti con le modalità previste dal manuale di conservazione;
- l'eventuale rifiuto del pacchetto di versamento, nel caso in cui i controlli di cui sopra abbiano evidenziato delle anomalie;
- la generazione in modo automatico del rapporto di versamento relativo ad un pacchetto di versamento, univocamente identificato dal sistema di conservazione, secondo le modalità descritte nel presente manuale di conservazione;
- la preparazione, la sottoscrizione con firma digitale del responsabile della conservazione o di un suo delegato e la gestione del pacchetto di archiviazione sulla base delle specifiche della struttura dati contenute nell'allegato 4 del DPCM del 3 dicembre 2013 e secondo le modalità riportate nel presente manuale della conservazione;
- la preparazione e la sottoscrizione con firma digitale e con l'apposizione della marca temporale sull'Indice del pacchetto di distribuzione ai fini di ottemperare alla richiesta di esibizione dell'utente.

Il sistema di conservazione, fornito da Olsa Informatica in qualità di soggetto conservatore, garantisce la reperibilità e la leggibilità dell'oggetto conservato, per il periodo prescritto dalla norma, indipendentemente dall'evoluzione tecnologica.

Il processo di conservazione è suddiviso in tre sotto-processi:

- Versamento
- Conservazione
- Distribuzione

Di seguito viene riportato un diagramma di flusso che esemplifica lo scenario relativo al processo di conservazione così come attuato da Olsa Informatica.

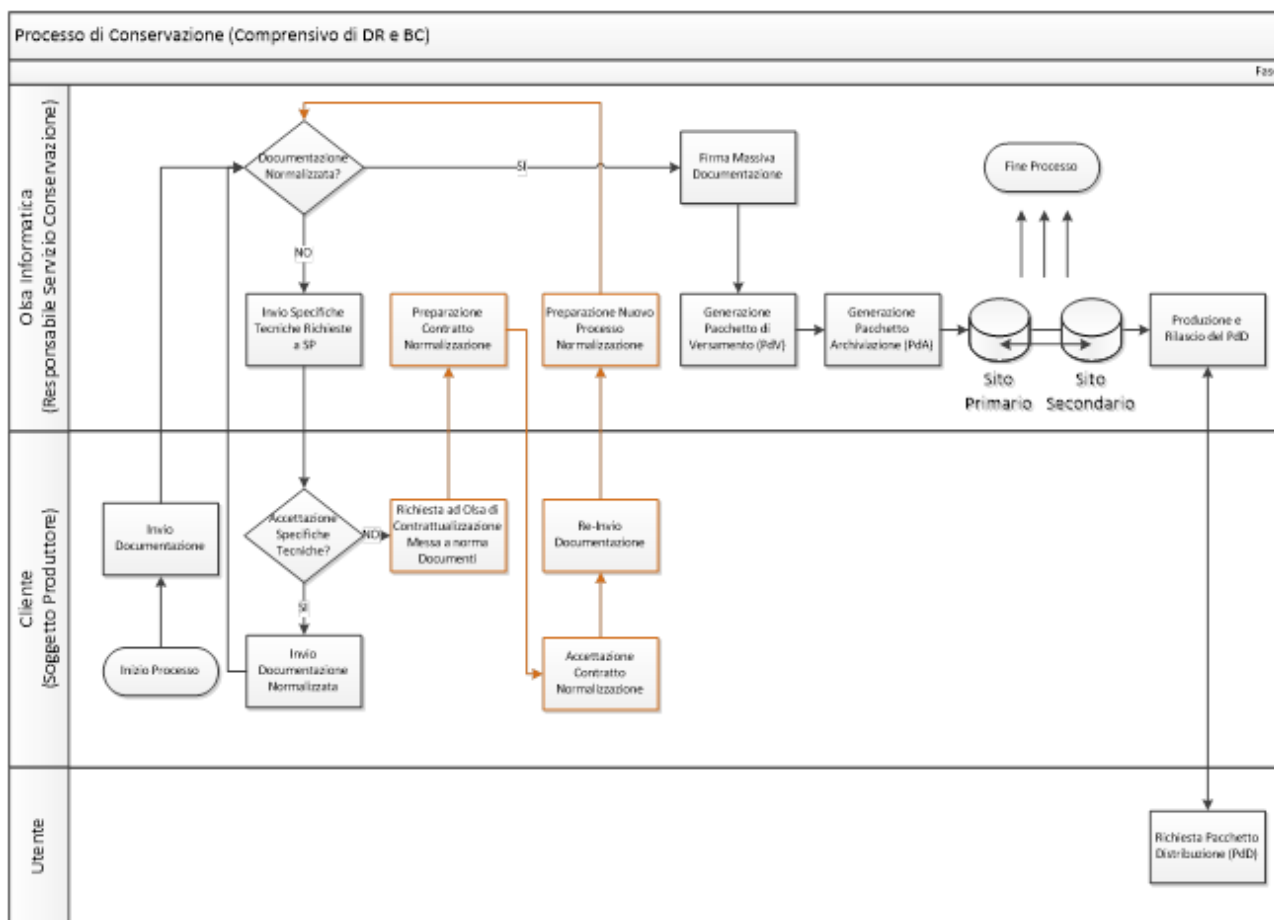


Figura 5: Diagramma di flusso del processo di conservazione

Il processo di conservazione si attiva a seguito della sottoscrizione del Contratto di affidamento del servizio di conservazione, le cui procedure vengono dettagliate nell'allegato specifiche tecniche.

Il servizio di conservazione erogato è regolato dai seguenti documenti:

- Contratto di affidamento del servizio di conservazione;
- Specifiche tecniche (allegato del contratto);
- Atto di nomina Responsabile del servizio di conservazione;
- Nomine dei responsabili delle aree coinvolte nel processo di conservazione;
- Oggetti da sottoporre a conservazione (parte integrante delle Specifiche tecniche, allegato del Contratto di affidamento del servizio di conservazione);
- Manuale operativo del software di conservazione.

Tutti i processi afferenti al versamento, all'accettazione, alla validazione degli oggetti digitali contenuti nel pacchetto informativo sono tracciati dai log come riportato nel paragrafo [8.5](#).

[Torna al sommario](#)

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

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

Le modalità di trasmissione del pacchetto informativo (SIP) vengono concordate in fase contrattuale e descritte nelle Specifiche tecniche. In ogni caso il pacchetto di versamento potrà essere trasferito al sistema di conservazione con una delle seguenti modalità:

- Web Service - caricamento automatico con interfacciamento di sistemi informatici;
- Upload manuale del file - caricamento da interfaccia grafica.
- SFTP e caricamento via file system;

Per i soli soggetti privati, sulla base di precisi accordi sottoscritti con il cliente in fase contrattuale, sarà possibile utilizzare anche altre modalità di trasferimento che prevedono la presa in carico da parte di Olsa Informatica i parte delle attività di predisposizione dei pacchetti di versamento, come illustrato in dettaglio nel paragrafo 7.1.2. In nessun caso tale modalità di gestione potrà essere utilizzata per il trasferimento di pacchetti informativi prodotti da amministrazioni pubbliche.

[Torna al sommario](#)

7.1.1. Acquisizione dei pacchetti di versamento dai soggetti produttori tramite Web Service e SFTP

La modalità di trasferimento via Web Service assicura i più alti livelli di automatizzazione dei processi di versamento, permettendo l'interfacciamento diretto tra gli applicativi del soggetto produttore e il sistema di conservazione.

Con la modalità Web Service l'applicativo chiamante del cliente, dopo l'autenticazione, istanzia un processo di conservazione nel sistema durante il quale invia a Legal Archive[®] pacchetti informativi con i quali vengono passati come parametri i file e l'insieme dei metadati di ricerca a loro associati.

La modalità SFTP è costituita da un collegamento SFTP (Secure File Transfert Protocol). Esso è un collegamento criptato punto-punto tra la piattaforma del cliente, autorizzato dai firewall, e dall'intero layer di sicurezza, e quella del conservatore.

Con il cliente, viene scambiato un documento di riferimento ISO 27001:2013, con il quale vengono resi noti una serie di parametri (indirizzi IP sorgenti, pacchetti di transito, orari di accesso, giorni di accesso, ecc.); il canale di invio di tali moduli non potrà essere che a mezzo PEC, ai fini della registrazione e accettazione del servizio in questione, attraverso le modalità ISO 9001:2008.

La modalità di versamento SFTP prevede che il trasferimento da parte del produttore del pacchetto di versamento nell'area concordata all'interno del file system dedicato; successivamente le procedure di workflow del conservatore faranno in modo che tali dati vengano processati dal sistema di conservazione, il tutto a garanzia ulteriore di policy 27001:2013.

In questa modalità di trasferimento il pacchetto è costituito nella sua forma standard dai file dei documenti da conservare accompagnati da indice dei metadati.

[Torna al sommario](#)

7.1.2. Acquisizione dei pacchetti di versamento per conto dei soggetti privati

In qualità di fornitore di servizi di gestione documentale Olsa può offrire, limitatamente ai soggetti privati, il servizio di preparazione e versamento dei pacchetti per conto del cliente assumendo, nell'ambito del processo di conservazione, il ruolo di produttore dei pacchetti di versamento.

Questo scenario, definito da appositi accordi contrattuali tra le parti, si configura come una modalità particolare del caricamento via file system dedicata ai soggetti produttori non facenti parte della Pubblica Amministrazione: Olsa riceve dal Soggetto Produttore dell'archivio il materiale documentario da versare e lo elabora tramite software dedicato, al fine di rendere il contenuto ed i metadati del pacchetto compatibili con il sistema di conservazione.

Il cliente che abbia optato per la fornitura di questo tipo di servizio fornisce ad Olsa, tramite canale SFTP o altra modalità sicura, i documenti da conservare ed i relativi metadati in un formato non immediatamente compatibile con il sistema di conservazione. Olsa provvede ad elaborare gli oggetti digitali ricevuti e ed i relativi metadati dando luogo ad un pacchetto di versamento compatibile con il sistema di conservazione.

L'elaborazione avviene con lo strumento software ad uso interno denominato **PDF Sign Tool**.

I file da conservare e i relativi metadati sono elaborati dal software tramite i seguenti passaggi:

- Selezione dell'intervallo di file da elaborare in base ai parametri impostati (intervallo cronologico; intervallo numerico; dimensioni del pacchetto ecc.);
- Firma massiva dei file selezionati;
- Copia dei file nell'area del file system configurata per l'estrazione dei file e il caricamento massivo tramite schedulazione processi in Legal Archive;
- Estrazione dei metadati e compilazione del file indice in formato compatibile con il caricamento.

I pacchetti così configurati sono estratti dal software in modo automatico tramite l'opportuna schedulazione dei processi.

[Torna al sommario](#)

7.1.3. Struttura del file di indice

In linea generale il file di indice può essere composto secondo le seguenti regole:

- Il file deve contenere i metadati di ricerca elencati per righe, una riga corrisponde ad un oggetto che sarà possibile ricercare a sistema;
- Ciascun metadato è separato dal successivo da un carattere separatore che può essere "|" o ",";
- In ciascuna riga lo stesso tipo dato sarà sempre nella medesima posizione;
- La prima colonna è sempre il percorso al file;
- Nel caso in cui sia riportato nome del file senza il percorso, Legal Archive[®] assume che il file referenziato si trovi sempre nella stessa cartella del file di indice;
- Il carattere "+" ad inizio riga indica al sistema di conservazione che il file referenziato è un allegato/annesso al documento referenziato nella riga superiore precedente contenente nome file e metadati;

- Nel caso di versamento di un fascicolo il file di indice deve riportare la struttura gerarchica espressione del vincolo archivistico;
- Nel caso di versamento di un fascicolo è indispensabile conoscere i metadati che legano i documenti tra di loro.

Inoltre esistono delle caratteristiche che permettono di definire all'interno del file di metadati:

- il percorso di output desiderato;
- metadati ripetibili indefinitamente.

Scendendo più nel dettaglio descriviamo di seguito come potrebbero essere costruiti i diversi pacchetti di versamento accettati ed elaborati dal sistema e il conseguente file di metadati.

Alcuni esempi dei diversi file di metadati descritti sono presenti nel manuale operativo del software.

- Tipo 1: il pacchetto di versamento è costituito da un insieme di n. file (Unità Documentarie) tra loro indipendenti accompagnati dal relativo file dei metadati. Tutti gli n. file appartengono alla stessa descrizione archivistica. Il file di indice avrà quindi n. righe (1 record per ciascun file), ciascuna riga contiene n. campi separati tra loro dal carattere “|” contenente il valore di ciascun metadato.
- Tipo 2: il pacchetto di versamento è costituito da un insieme di n. file (Unità Documentarie) accompagnati dal relativo file dei metadati. Un numero x di questi n. file sono allegati. I file principali, escludendo quindi gli allegati, appartengono tutti alla stessa descrizione archivistica. Il file di indice avrà quindi n. righe (1 record per ciascun file, riferito sia ai documenti principali che gli allegati), ciascuna riga relazionata ai file principali contiene n campi separati tra loro dal carattere “|” contenente il valore di ciascun metadato, mentre x righe relazionate agli allegati contengono solo path e nome file preceduto al segno “+”.
- Tipo 3: il pacchetto di versamento contiene fascicoli informatici afferenti allo stesso contesto di provenienza. I diversi oggetti digitali vengono relazionati tra loro in funzione di alcuni metadati che fungono da nessi logici necessari, autonomi e determinati.

[Torna al sommario](#)

7.1.4. Trasferimento dei pacchetti di versamento tramite upload manuale

La modalità di trasferimento via upload manuale prevede che l'utente abilitato carichi da interfaccia web il file del documento da conservare e imputi i metadati ad esso associati nei campi appositi e predefiniti.

La procedura di upload nel dettaglio prevede:

- La selezione della descrizione archivistica cui appartengono i documenti informatici che si stanno per versare;
- La selezione del file che dovrà essere caricato a sistema attraverso un browsing da file system;
- L'imputazione manuale dei diversi metadati associati al singolo file, direttamente nei campi della maschera di input (vedi immagine sottostante);
- La selezione di eventuali allegati al documento principale attraverso un browsing da file system;
- La conferma del versamento del pacchetto.



Figura 6: Finestra di upload da web

Tutti i documenti versati devono appartenere alla stessa descrizione archivistica.

L'utente che vuole eseguire l'upload dei file da interfaccia grafica deve avere i diritti per accedere al menu che abilita tale funzionalità.

Osservazione:

- La trasmissione dei SIP non avviene mediante supporti fisici;
- In merito al versamento di tipologie documentarie informatiche fiscali, il conservatore si atterrà ai requisiti tecnologici richiesti dal legislatore (DMEF 17 giugno 2014).

Il sistema prevede la presenza di log/registri dei pacchetti di versamento ricevuti (si rimanda al paragrafo [8.5](#)).

[Torna al sommario](#)

7.2. Verifiche effettuate sui pacchetti di versamento e sugli oggetti in esso contenuti

Il sistema di versamento mette a disposizione del produttore una serie di funzionalità di validazione che gli consentono, se necessario, di correggere la composizione dei pacchetti di versamento prima della sua acquisizione da parte del conservatore.

Il sistema di conservazione prevede la possibilità di eseguire verifiche sulla validità della firma, sulla composizione del pacchetto di versamento, sull'integrità dei file e sull'insieme dei metadati forniti.

Le validazioni vengono concordate nel contratto di servizio di conservazione e configurate per ciascuna descrizione archivistica.

Di seguito descriviamo i diversi tipi di validazione previsti:

- Validazioni del pacchetto di versamento: il sistema di conservazione verifica la congruità delle informazioni contenute nell'indice dei metadati con il numero di documenti presenti nel pacchetto di versamento: per superare la validazione il pacchetto di versamento deve contenere tutti i documenti elencati nell'indice di conservazione (*Controllo Obbligatorio*).
- Validazioni sul singolo documento: il sistema di conservazione permette di verificare che:
 - il mime type del documento in elaborazione appartenga ad alla lista dei mime type per i quali il sistema conserva i viewer;
 - il mime type di un file corrisponda a quanto dichiarato (*Controllo Obbligatorio*);
 - la firma di un file sia valida (impostabile solo nel caso p7m o pdf);
 - la marca temporale di un file sia valida (impostabile solo nel caso tsd o p7m);

- nel caso in cui il file dei metadati, prodotto e versato dal produttore, includa anche un campo contenente l'hash di ciascun file, il sottosistema di validazione ricalcola l'hash di ogni documento e lo confronta con quello dell'indice verificando l'integrità del file versato.
- Validazioni sui metadati: il sistema di conservazione definisce per ciascuna descrizione archivistica il set di metadati previsti e oggetto dell'accordo tra SP e conservatore.
Per ciascun metadato è possibile configurare:
 - nel campo "**Tipo metadato**": la tipologia di dato (stringa, numero, data...);
 - nel campo "**Espressione di Validazione**": l'espressione regolare con la quale il valore del metadato dovrà coincidere;
 - nel campo "**Pattern di Conversione**": il tipo di pattern accettato per il tipo di metadato.

In fase di acquisizione del pacchetto di versamento il sistema elabora i metadati e verifica che siano

Figura 7: Finestra di configurazione metadati

rispondenti alle caratteristiche configurate nella descrizione archivistica.

Il sistema prevede i seguenti controlli per il pacchetto di versamento:

- la verifica dell'identificazione certa del soggetto produttore;
- la verifica che il soggetto produttore non sia bloccato;
- la verifica del raggiungimento dei limiti di contratto;
- la verifica che sia stato definito almeno un certificato di firma;
- la verifica che sia stato definito un responsabile della conservazione per il soggetto produttore;
- la verifica che sia stato definito un account di marca temporale per la descrizione archivistica;
- la verifica che siano state definite informazioni di rappresentazioni valide;
- la normalizzazione del file di metadati del pacchetto di versamento;
- il caricamento nel database dei metadati del pacchetto di versamento;
- la validazione dei metadati secondo le specifiche concordate con il soggetto produttore.

La funzione del sistema dedicata all'esecuzione dei processi applicativi denominata fase di "engine" (paragrafo 8.5 a cui si rimanda) prevede inoltre la tracciatura, mediante log, delle seguenti informazioni:

- data e ora di esecuzione del processo;
- utente che ha richiesto il processo;

- tipo di processo richiesto;
- esito del processo.

[Torna al sommario](#)

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

Il sistema, superate le validazioni dei documenti del pacchetto di versamento, restituisce al produttore il rapporto di versamento.

Per ogni pacchetto accettato il sistema genera un rapporto di versamento che viene memorizzato nel database e associato logicamente al pacchetto di archiviazione a cui si riferisce.

Il rapporto di versamento è un file XML che contiene:

- l'identificativo univoco del rapporto, ovvero l'identificativo univoco del processo che l'ha generato;
- il riferimento temporale relativo alla sua creazione (specificato con riferimento al tempo UTC);
- gli identificativi univoci dei documenti versati;
- gli identificativi univoci dei file versati;
- le impronte degli oggetti-dati che ne fanno parte;
- la lista dei metadati versati suddivisi per documento.

A seconda di quanto concordato nelle specifiche tecniche, il rapporto di versamento può essere firmato dal soggetto conservatore ed eventualmente ad esso può essere apposto un riferimento temporale anche mediante marca temporale. Nel caso si tratti di documentazione che coinvolge la Pubblica Amministrazione, la piattaforma di conservazione prevede che il SIP debba obbligatoriamente essere firmato digitalmente e marcato temporalmente, cosa non prevista nel settore privato (business-to-business).

Il rapporto di versamento viene reso disponibile in varie forme, direttamente dipendenti dalla modalità scelta per il versamento dei documenti:

- versamento via Web Services: può essere richiesto utilizzando un'apposita chiamata web service;
- versamento via SFTP: è restituito nella stessa folder di input dove il produttore ha trasferito il pacchetto di versamento; come ulteriore feedback il file di indice viene rinominato con estensione "OK" in caso di processo di conservazione eseguito con successo o in "KO" in caso di processo di conservazione in errore;
- in tutti i casi: può essere visualizzato e scaricato dall'interfaccia web del sistema di conservazione dagli utenti abilitati utilizzando le apposite funzionalità del sistema stesso.

Il sistema garantisce il controllo dei processi relativi all'accettazione dei pacchetti di versamento e alla generazione del rapporto di versamento grazie alla creazione di log (si rimanda al paragrafo [8.5](#)) nei quali sono riportate le seguenti informazioni:

- data e ora di esecuzione del processo;
- utente che ha richiesto il processo;
- tipo di processo richiesto;
- esito del processo.

[Torna al sommario](#)

7.4. Rifiuto del pacchetto di versamento e modalità di comunicazione delle anomalie

Il pacchetto di versamento viene sottoposto ai controlli di validazione descritti nel precedente paragrafo, alcuni di questi vengono eseguiti obbligatoriamente altri invece sono oggetto dell'accordo tra soggetto produttore e conservatore.

Qualora il pacchetto di versamento non abbia superato tutti i controlli previsti, il sistema rifiuta l'intero pacchetto e notifica all'utente l'avvenuto errore. La notifica avviene attraverso interfaccia grafica nell'area designata alle notifiche e attraverso un messaggio e-mail che il sistema invia direttamente alle persone di riferimento, opportunamente configurate sulla piattaforma all'atto dell'attivazione dello specifico soggetto produttore. La mail viene sicuramente inviata al responsabile della conservazione o ad un suo delegato/i.

In aggiunta, oltre alla notifica mail e web, il sistema dettaglia nei log la causa dell'errore.

E' possibile avviare un'attività di validazione sia dei file che dei metadati rispetto alle regole e agli standard previsti dalle descrizioni archivistiche di appartenenza. I risultati possono essere allegati al documento oggetto della convalida per essere eventualmente portati in conservazione insieme al documento stesso. (vedi anche paragrafo 8.1.1).

Il processo di convalida include:

- la verifica dell'integrità del documento memorizzato sul supporto rispetto all'impronta associata allo stesso;
- la verifica che il formato del contenuto binario sia coerente con quanto dichiarato nei suoi metadati, altrimenti si potrebbe consentire l'invio di formati di file non adatti alla conservazione;
- la verifica delle eventuali firme digitali apposte su di esso, comprensiva di convalida del certificato rispetto a uno "store" locale e alle liste di revoca on-line;
- l'eventuale verifica della presenza in archivio di un documento identico (i.e.: stessa impronta e/o metadati);
- la compilazione dei metadati: alcuni di essi potrebbero essere compilati in questa fase in maniera automatica (ad esempio potrebbero essere aggiunte le informazioni relative all'utente che ha effettuato il versamento e la data di versamento).

La piattaforma utilizzata consente di definire l'invio di notifiche relative a eventi associati alla conservazione, specificando i seguenti campi:

- descrizione archivistica
- gruppo notificato
- tipo notifica:
 - notifica via email e/o
 - notifica via web (nella pagina di accesso)
- evento notifica:
 - in fase di esecuzione
 - eseguito senza errori
 - sospeso/da non terminare
 - eseguito con segnalazioni

- eseguito con errori
- in attesa/da terminare
- in attesa di conclusione conservazione
- errore di validazione
- annullato dall'utente
- cancellato

E' possibile aggiungere alla notifica e-mail:

- l'oggetto della e-mail
- testo della e-mail

L'oggetto e il testo della e-mail sono personalizzabili in termini di:

- testo libero
- [ID_Volumes]: identificativi dei pacchetti di archiviazione
- [SP_ALIAS]: alias del soggetto produttore
- [DATA], [MESSAGE] data e messaggio della notifica
- [PRO_ID], [PRO-DATE], [PRO_STATUS]: identificativi del processo

Nella tabella sottostante si riportano le anomalie che determinano il rifiuto del pacchetto di versamento e la relativa modalità di gestione.

Tipo Anomalia	Descrizione	Gestione
Mancata risposta al versamento	L'unità documentaria è correttamente versata ma, per svariati motivi, la risposta di avvenuta ricezione non è pervenuta al produttore che di conseguenza, erroneamente, la considera non versata.	Il produttore deve versare nuovamente: il sistema di conservazione restituirà una risposta di esito negativo con l'indicazione che l'unità documentaria risulta già versata. Tale risposta deve essere usata dal produttore come attestazione di avvenuto versamento e l'unità documentaria deve risultare come versata.
Errori temporanei	È il caso di errori dovuti a problemi temporanei che pregiudicano il versamento, ma si presume non si ripresentino a un successivo tentativo di versamento. Il caso più frequente è l'impossibilità temporanea di accedere alle CRL degli enti certificatori. In questi casi il sistema di conservazione dopo aver riprovato 10 volte, genera un messaggio di errore perché non riesce a completare le verifiche previste sulla validità della firma e il versamento viene quindi rifiutato impostando il processo in stato ERRV.	Il produttore deve provvedere a rinviare l'unità documentaria in un momento successivo. L'operazione potrebbe dover essere ripetuta più volte qualora il problema, seppur temporaneo, dovesse protrarsi nel tempo.

Versamenti non conformi alle regole concordate	È il caso in cui il versamento non viene accettato perché non conforme alle regole concordate (firma non valida, formato file non previsto, file corrotto, mancanza di metadati obbligatori ecc.).	Il soggetto conservatore invia via e-mail una segnalazione dell'anomalia ai referenti del soggetto produttore, con i quali viene concordata la soluzione del problema.
Errori interni o dovuti a casistiche non previste o non gestite	In alcuni casi è possibile che il sistema di conservazione risponda con un messaggio di errore generico che non indica le cause dell'anomalia riscontrata in quanto dovuta a un errore interno o perché legata a una casistica non prevista, non gestita o non gestibile dal sistema di conservazione.	I referenti del soggetto produttore segnalano il problema via e-mail al soggetto conservatore, che si attiverà per la sua risoluzione.

In caso di errore, nel log del processo di conservazione viene registrato un messaggio che identifica cosa manca o quale altro processo è propedeutico per l'avanzamento dello stesso.

Nelle righe del log sono resi disponibili:

- data e ora di esecuzione del processo;
- utente che ha richiesto il processo;
- tipo di processo richiesto;
- esito del processo.

Le anomalie sono affrontate con diverse metodologie, secondo la natura dell'anomalia stessa e la collocazione dell'evento che l'ha generata nel processo di conservazione: pertanto, oltre alle procedure atte a garantire l'Integrità degli archivi, esistono anche procedure atte a risolvere anomalie in altre componenti del sistema.

Le caratteristiche comuni e le specificità delle procedure di risoluzione delle anomalie dipendono da diversi fattori organizzativi e tecnologici:

- tutte le funzionalità del sistema che inseriscono o modificano dati nel Data Base e file nell'area SFTP o nel File System operano in modalità transazionale;
- il backup del Data Base assicura il ripristino all'ultima transazione completata correttamente;
- il File System e l'area SFTP sono sottoposte a backup giornaliero.

[Torna al sommario](#)

7.5. Preparazione e gestione del pacchetto di archiviazione

Legal Archive[®] garantisce la conformità al requisito OAIS, creando dei pacchetti di archiviazione contenenti tutti i file necessari alla loro ricostruzione e ricerca, e collegando i documenti alle informazioni sulla rappresentazione loro associate e ai viewer associati al relativo formato file.

Un pacchetto di archiviazione viene reso disponibile al SP, sulla base degli accordi stabiliti in fase contrattuale, mediante uno storage dedicato alla Conservazione a Norma; il soggetto conservatore è responsabile della sua funzionalità.

E' possibile separare i versamenti in diversi pacchetti di archiviazione (AIP) dividendo i pacchetti di archiviazione in base a diverse logiche:

- Per file di metadati;
- Per chiamata diretta (WS);
- In base ai Megabyte;
- In base al tempo.

Ad ogni buon conto, nella definizione degli AIP, è richiesto il rispetto delle seguenti configurazioni:

- Massimo 4 GB di documenti conservati per pacchetto di archiviazione;
- Massimo 80mila documenti/file (allegati inclusi) per pacchetto di archiviazione;
- Massimo 5 MB per ogni file inviato (fino a 350 MB per invii tramite SFTP);

Ogni file dovrà infatti avere almeno un record contenente i valori che lo contraddistinguono e attraverso i quali sarà possibile effettuare la sua ricerca, dopo la conservazione.

La struttura utilizzata nella costruzione degli AIP fa riferimento alla norma UNI 11386:2010, lo standard nazionale riguardante la struttura dell'insieme dei dati, a supporto del processo di conservazione.

In concreto, il pacchetto di archiviazione è un'entità logica contenuta in un'alberatura di file e cartelle e definita nel file indice UNI SInCRO generato nel corso del processo di conservazione e contenente tutte le informazioni inviate dal SIP o definite sul sistema di conservazione.

Gli oggetti conservati sono salvati nel file system, in una sottocartella della directory indicata come radice nel pannello di configurazione dell'Archivio.

Il pacchetto di archiviazione è salvato in una posizione relativa associata a:

- soggetto produttore
- anno
- ID pacchetto di archiviazione

I file facenti parte dei documenti oggetto di conservazione potranno trovarsi in una sottocartella del pacchetto di archiviazione.

Il pacchetto di archiviazione contiene:

- Indice_<N° del pacchetto>.XML: file XML con la descrizione del pacchetto di archiviazione.
- Tutti i file XML e XSD necessari per l'eventuale ricostruzione dell'archivio.

La conservazione si conclude con la firma digitale e la marca temporale dell'indice UNI SInCRO e termina con la messa a disposizione del cliente di questa evidenza di avvenuta conservazione (indice P7M) da parte del Responsabile del servizio di conservazione.

Il sistema di conservazione si occupa autonomamente di tutte le fasi di conservazione, tracciandone ogni passaggio e ogni esito nei file di log.

[Torna al sommario](#)

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

I pacchetti di archiviazione (AIP) sono nel sistema. In un momento successivo alla generazione degli AIP, utenti con profilo di esibizione o ricerca possono accedere al sistema di conservazione e interrogarlo per ottenere un pacchetto di distribuzione.

Ci possono essere varie generazioni di DIP:

- DIP coincidente con l’AIP che contiene:
 - tutti gli elementi presenti nell’AIP;
 - i documenti dell’AIP richiesto;
 - un'estrazione delle informazioni di conservazione dei documenti e dei fascicoli;
 - l’indice di conservazione firmato e marcato e le informazioni sulla conservazione associate ai fascicoli;
 - i viewer necessari alla visualizzazione dei documenti del pacchetto e le informazioni sulla rappresentazione;
 - le informazioni sull’impacchettamento e le informazioni descrittive associate al pacchetto informativo.

Inoltre, nei pacchetti di distribuzione, è possibile inserire tutta la catena di documentazione necessaria a rispondere alle esigenze dello standard OAIS.

- DIP dell’unità documentaria che contiene:
 - gli oggetti dati che la compongono;
- DIP del documento che contiene:
 - gli oggetti dati del documento.

In linea generale il pacchetto di distribuzione può essere erogato dal sistema di conservazione come unico file in formato ZIP e in formato ISO a seconda della richiesta dell’utente; il SP potrà autonomamente richiedere al sistema informatico la generazione di un DIP e trattarlo come ritiene opportuno.

Pertanto, in merito all’esercizio del diritto d’accesso ai documenti conservati dal soggetto conservatore, questo si limita a fornire al soggetto produttore, su precisa richiesta di quest’ultimo, il documento informatico conservato, qualora per un qualsiasi motivo il soggetto produttore stesso abbia deciso di non acquisirlo direttamente mediante le modalità delineate nel presente manuale. Permane in carico allo stesso soggetto produttore sia la responsabilità di valutare la fondatezza giuridica della domanda di accesso, sia l’onere di far pervenire il documento (o sua eventuale copia cartacea conforme) al soggetto richiedente la consultazione se diverso da sé.

L’esibizione è un atto da svolgersi in ottemperanza a quanto previsto dall’ultimo comma dell’art. 2220 del Codice Civile, ribadito nell’art. 10 del DPCM del 3 dicembre 2013. Essa consiste nel rendere leggibili, con mezzi idonei, tutte le scritture e i documenti conservati a norma. L’articolo 10 del DPCM del 3 dicembre 2013, ribadisce le norme vigenti e specifica che, ai fini dell’esibizione, il sistema di conservazione permette ai soggetti autorizzati l’accesso diretto, anche da remoto, al documento informatico conservato, attraverso la produzione di un pacchetto di distribuzione (DIP) selettiva secondo le modalità descritte nel manuale di conservazione.

Il soggetto produttore può consultare i documenti informatici versati al sistema di conservazione tramite interfaccia web, collegandosi all’indirizzo comunicato dal soggetto conservatore, autenticandosi tramite username e password preventivamente forniti dal soggetto conservatore. Gli utenti da abilitare all’accesso, tramite interfaccia web al sistema di conservazione, sono comunicati dai referenti del soggetto produttore al conservatore, che provvede a inviare le credenziali di accesso ai diretti interessati via e-mail (in genere la password viene inviata via e-mail con la condizione *Change a Password at Next Logon*) o tramite altro mezzo da concordare.

L’accesso web consente di ricercare i documenti informatici versati, di effettuarne il download e di acquisire le prove dell’attività di conservazione. Il SP può richiedere i documenti e i fascicoli informatici versati e

conservati anche utilizzando gli appositi Web Services, chiamati secondo le modalità indicate nelle Specifiche tecniche.

Il sistema di conservazione di Olsa Informatica permette di richiedere, di generare e di scaricare i pacchetti di distribuzione (DIP), completi di indice di conservazione e delle informazioni di rappresentazione collegate. Inoltre, nei DIP è contenuta tutta la catena di documentazione necessaria a rispondere alle esigenze dello standard OAIS.

In fase di attivazione del servizio, il soggetto produttore segnala al conservatore, su apposita documentazione allegata al contratto, i propri delegati alla visualizzazione e al download dei documenti informatici originali ai fini dell'esibizione.

Il conservatore genera gli account e il sistema invia le credenziali all'utente per accedere al portale del sistema di conservazione.

Il collegamento avviene tramite connessione sicura SSL con certificato rilasciato da Certification Authority competenti.

Una volta accreditato, l'utente ha accesso ai servizi opportunamente profilati per la sua utenza, tra cui:

- Visualizzare direttamente i documenti informatici originali conservati da remoto;
- Visualizzare le informazioni di conservazione associate all'AIP;
- Scaricare i documenti informatici conservati (duplicati) e i file di evidenza della conservazione (indice di conservazione UNI SInCRO);
- Scaricare le informazioni sulla rappresentazione associate all'AIP;
- Richiedere e scaricare i DIP da consegnare alle autorità competenti, in caso di necessità.

In merito alla produzione delle copie sarà cura del soggetto produttore richiedere, quando necessario, la presenza di un Pubblico Ufficiale.

Nel DIP è compreso anche il necessario per la rappresentazione, viewer nella versione coerente alla visualizzazione dei DIP, e le informazioni in grado di supportare l'applicazione di visualizzazione.

Va sottolineato che l'esibizione degli oggetti digitali conservati deve avvenire in modo che le autorità competenti possano verificare la coerenza della firma digitale e della marca temporale apposte durante il processo di conservazione.

Tale procedura, prevede l'utilizzo del supporto informatico, come evidenziato nel capitolo 8.

[Torna al sommario](#)

7.7. Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti.

In fase di attivazione del servizio, il soggetto produttore segnala al conservatore, su apposita documentazione allegata al contratto, i propri delegati alla visualizzazione e al download dei documenti informatici originali ai fini dell'esibizione. Il conservatore genera gli account e il sistema invia le credenziali all'utente per accedere al portale del sistema di conservazione.

Detta piattaforma, consente al soggetto produttore di effettuare sia la produzione di duplicati e copie informatiche sia l'esibizione a norma dei documenti conservati.

Il collegamento avviene tramite connessione sicura SSL con certificato rilasciato da Certification Authority competenti.

Attraverso il portale, l'utente ha accesso ai servizi opportunamente profilati alla sua utenza.

A quel punto i soggetti produttori sono in grado di:

- Visualizzare direttamente i documenti informatici originali conservati;
- Scaricare i documenti informatici conservati (duplicati) e i file di evidenza della conservazione (indice di conservazione UNI SInCRO);
- Richiedere e scaricare i DIP da consegnare alle autorità competenti, in caso di necessità;
- Produrre eventualmente una copia conforme richiedendo la presenza di un pubblico ufficiale.

Il soggetto produttore o un suo delegato all'attività di consultazione e produzione di duplicati informatici, ricerca i documenti attraverso i campi che l'interfaccia grafica mette a disposizione. Si tratta degli stessi metadati con i quali sono stati accompagnati i file durante l'invio al sistema di conservazione.

Una volta visualizzati i file conservati, il soggetto produttore o suo delegato può richiedere al Responsabile del servizio di conservazione una copia, attraverso una funzione disponibile sul portale; questa funzione consente di scaricare un file di tipo ISO o di tipo ZIP, attraverso il canale criptato SSL del portale.

Sarà così possibile avere una copia del pacchetto di distribuzione (DIP) contenente i documenti conservati, i viewer per la loro corretta visualizzazione, l'indice di conservazione firmato e marcato e un'estrazione dei metadati associati ai documenti.

Il sistema di conservazione è stato progettato, anche in termini organizzativi e di *preservation planning*, proprio con l'obiettivo di prevenire l'obsolescenza dei formati gestiti: a questo scopo sono disponibili un sistema di gestione e tracciabilità delle informazioni sulla rappresentazione associate ai documenti, un sistema di esibizione degli strumenti di restituzione della rappresentazione dei documenti conservati, e infine un sistema di reportistica associato alle informazioni sulla rappresentazione. Tutte queste componenti permettono al Responsabile del servizio di conservazione l'aggiornamento delle informazioni sulla rappresentazione, nel tempo, con la relativa cristallizzazione, storicizzazione e tracciabilità.

Qualora fosse richiesta la presenza di un pubblico ufficiale, per l'attestazione di conformità all'originale di copie di documenti informatici originali conservati dal sistema di conservazione, il soggetto conservatore rimanda la gestione di tale attività al soggetto produttore, le cui modalità di intervento sono esplicitate nel Contratto di affidamento. Il conservatore garantisce la messa a disposizione dell'originale informatico attraverso un DIP eventualmente firmato dal Responsabile del servizio di conservazione.

[Torna al sommario](#)

7.8. Scarto dei pacchetti di archiviazione

L'art. 9 comma 1, lett. k del DPCM 3 dicembre 2013 stabilisce che deve essere effettuato lo scarto dal sistema di conservazione, alla scadenza dei termini di conservazione previsti dalla norma, dandone informativa al soggetto produttore. Il sistema di gestione dati, grazie alla propria concezione, permette di gestire al meglio lo scarto del materiale documentario non destinato alla conservazione permanente, ma caratterizzato invece da tempi di conservazione limitati e diversificati.

Negli archivi correnti gestiti secondo criteri aggiornati è presente, nel piano di classificazione e conservazione, un metadato, definibile per ciascuna tipologia documentaria o fascicolo (descrizione archivistica), che stabilisce i tempi di conservazione.

Sarà dunque il sistema di gestione dati (SGD) a incaricarsi di avvisare il Responsabile del servizio di conservazione, attraverso una o più notifiche impostabili, circa la scadenza dei tempi di conservazione dei

documenti e a supportarlo nell'effettuazione materiale dello scarto, a mantenere al proprio interno, ove richiesto, i metadati della documentazione fisicamente scartata.

Il sistema di conservazione produrrà quotidianamente un elenco dei pacchetti di archiviazione che hanno superato il tempo di conservazione, così come definito nel piano di conservazione del soggetto produttore. Tale elenco di scarto, dopo una verifica da parte di Olsa Informatica, viene comunicato al soggetto produttore per validarlo.

Nei casi 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 (MiBACT). Il soggetto produttore, una volta ricevuto il nulla-osta dal MiBACT, provvede ad adeguare, se necessario, l'elenco di scarto. Una volta che l'elenco di scarto è definitivo, il soggetto produttore lo trasmette a Olsa Informatica. Solo dopo aver ricevuto l'autorizzazione, il conservatore provvederà alla cancellazione dei pacchetti di archiviazione, contenuti nell'elenco di scarto.

Il sistema di conservazione, è quindi dotato di un processo di scarto che si occupa di controllare quotidianamente se esistono pacchetti di archiviazione che devono essere scartati.

Alla presenza di uno o più pacchetti, il processo avvisa il Responsabile del servizio di conservazione, che avrà a disposizione un'interfaccia che gli permetterà di decidere se scartare o meno i pacchetti. In caso affermativo, il processo di selezione e scarto provvederà a eliminare fisicamente i file presenti nel file system e a cancellare tutti i riferimenti nel database, mantenendo però l'indice di conservazione (in quanto contiene la lista dei file scartati) e aggiungendo automaticamente ai metadati del pacchetto di archiviazione, una nota che indichi il fatto che il pacchetto di archiviazione è stato sottoposto al processo di scarto, includendo data e ora di esecuzione.

[Torna al sommario](#)

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

Per una corretta erogazione di un servizio di conservazione a norma, che risponda alle caratteristiche richieste dallo standard OAIS, una qualsiasi applicazione di conservazione deve essere in grado di esportare i documenti informatici conservati in un formato che garantisca l'integrità della conservazione stessa.

Il sistema di conservazione, essendo progettato secondo lo standard OAIS, è in grado di esportare i singoli pacchetti di archiviazione generati durante gli anni, seguendo regole che permettono successivamente di importare i pacchetti in un altro sistema OAIS *compliant*.

Di seguito sono descritte le azioni da eseguire qualora i contratti in essere non venissero rinnovati:

- Il soggetto produttore aveva già nominato gli utenti abilitati all'accesso della piattaforma web, all'atto della sottoscrizione del contratto;
- Tali utenti potranno collegarsi alla piattaforma web per generare e scaricare i DIP contenenti tutti i documenti conservati;
- Per volumi di grandi dimensioni, quando previsto da contratto, il conservatore metterà a disposizione dell'ex-cliente:
 - I file scaricati in formato ISO su server SFTP;
 - I file scaricati in formato ISO su supporto fisico anonimo, senza riferimenti al contenuto e consegnati da personale autorizzato di Olsa Informatica;

- L'ex cliente è tenuto a verificare la coerenza dei dati consegnati entro i tempi prestabiliti dal contratto;
- Infine, il conservatore disattiverà l'account relativo al portale web e i dati subiranno un processo di eliminazione logica da concordare.

Si ricorda che in caso di movimentazione di dati, da un soggetto conservatore a un altro o da un soggetto conservatore a un utente autorizzato, è sempre obbligatorio l'uso di canali sicuri e criptati pertanto:

- I trasferimenti dei dati via web e via SFTP si appoggiano su protocolli sicuri cifrati (https, SFTP);
- I supporti fisici saranno cifrati.

Si ricorda che, in accordo con il modello OAIS, tutti i conservatori aderenti sono tenuti all'interoperabilità dei sistemi, che si concretizza con l'adozione e la produzione di pacchetti di distribuzione in formato standard, importabili su qualunque sistema di conservazione a norma.

Legal Archive[®] è in grado di importare dati di altri *outsourcer* qualora dette informazioni, precedentemente soggette a conservazione a norma, rispettino alcune caratteristiche. La verifica di dette caratteristiche è preventiva rispetto all'accettazione dei dati conservati da migrare. I contratti avranno pertanto una componente di valutazione preventiva della fattispecie.

[Torna al sommario](#)

8. Il sistema di conservazione

Il modello dei dati che viene utilizzato come base per l'implementazione del sistema di conservazione Legal Archive[®] è lo standard ISO 14721: OAIS Open Archival Information System esplicitato nella gestione di tre differenti tipologie di pacchetti informativi:

- Il pacchetto di versamento (SIP): il documento digitale o l'insieme dei documenti digitali, corredati da tutti i metadati descrittivi, versati dal produttore nel sistema di conservazione.
- Il pacchetto di archiviazione (AIP): uno o più SIP trasformati in pacchetto di archiviazione per la conservazione. L'AIP ha un insieme completo di informazioni sulla conservazione che si aggiungono al file di metadati.
- Il pacchetto di distribuzione (DIP): il documento digitale o l'insieme dei documenti digitali, corredati da tutti o da parte dei metadati previsti nell'AIP, finalizzati alla presentazione e distribuzione dei documenti conservati.

In termini generali, il modello OAIS definisce le componenti logiche comuni a tutti e tre i pacchetti informativi sopra descritti.

L'obiettivo del sistema di conservazione è quello di garantire non solo la gestione e la conservazione dell'insieme informativo e descrittivo del singolo documento (o collezione di documenti, nell'accezione OAIS, in riferimento ad AIC, Archival Information Collection), ma anche di tutte le informazioni di contesto dei metadati e, soprattutto, delle relazioni fra i documenti che servono per la ricostruzione del vincolo archivistico e, quindi, del fascicolo digitale di riferimento.

Come illustrato nella seguente figura il sistema di conservazione è conforme allo standard OAIS.

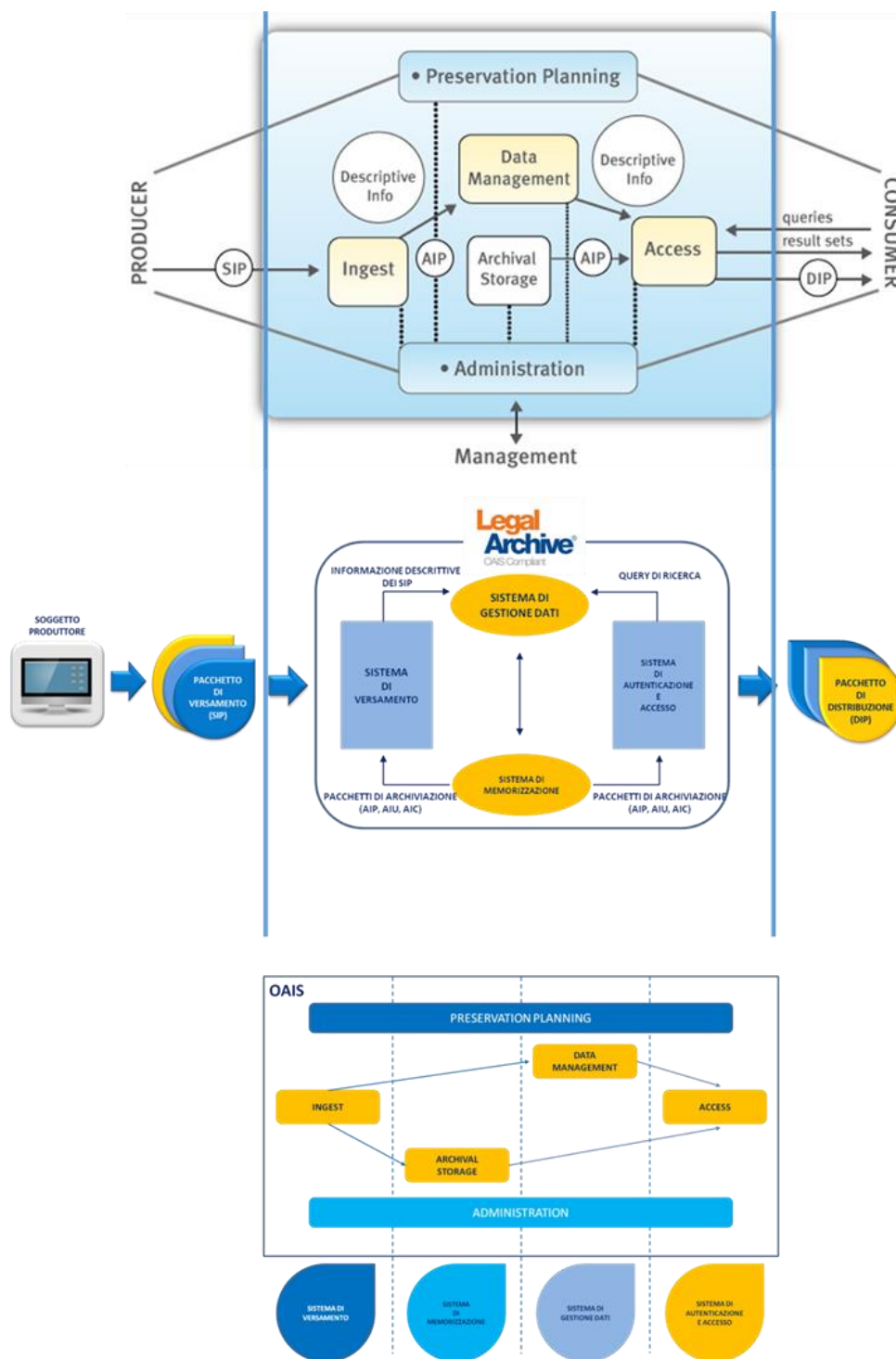


Figura 8: Il modello OAIS

[Torna al sommario](#)

8.1. Componenti logiche

Nel rispetto dello standard, il sistema è formato da 4 macro-componenti funzionali:

- Sistema di versamento (SV);

- Sistema di gestione dati (SGD);
- Sistema di memorizzazione (SM);
- Sistema di autenticazione e accesso (SAA).

[Torna al sommario](#)

8.1.1. Sistema di Versamento (SV)

Il sistema di versamento è la porta d'ingresso dell'intero sistema e ha il compito di ricevere i pacchetti di versamento, di verificarne l'aderenza al contratto di servizio di conservazione e ai requisiti di conservazione, di preparare i pacchetti di archiviazione e infine di inviare ai sistemi opportuni, le informazioni e i dati per garantire la conservazione a norma dei documenti informatici ricevuti.

Rispetto alla pluralità di situazioni documentarie possibili, il sistema si comporterà applicando le regole d'ingresso che saranno definite nell'accordo di servizio. Esattamente come avviene in un archivio di deposito tradizionale, le regole avranno lo scopo di stabilire:

- Le caratteristiche minime che la documentazione deve possedere per poter essere accettata in ingresso;
- I tempi di versamento della documentazione dotata di tali caratteristiche;
- Le modalità di versamento;
- I metadati di ciascun versamento che dovranno anch'essi essere conservati dal sistema.

In particolare, per quanto riguarda il primo punto, il sistema può gestire due ordini di caratteristiche:

- Caratteristiche tecnologiche, riferite ai singoli oggetti digitali;
- Caratteristiche archivistiche, ossia la presenza di alcuni metadati di contesto.

Le caratteristiche archivistiche possono riguardare, ad esempio, l'appartenenza di ciascun documento a un fascicolo o la possibilità di ricondurre un fascicolo all'attività di un determinato ufficio.

Le caratteristiche tecnologiche riguardano esclusivamente i documenti digitali e possono riferirsi al formato con cui sono stati prodotti, alla validità della firma e/o della marca temporale. Poiché i documenti informatici potrebbero giungere al sistema dopo un considerevole lasso di tempo dalla loro formazione, a causa dei tempi di chiusura delle relative pratiche, è quanto mai opportuno che il sistema si incarichi di verificare la sussistenza dei requisiti di base per la conservazione.

Una volta che la documentazione avrà superato i controlli di qualità previsti, il sistema di versamento dovrà applicare le regole previste dal *preservation planning* per costruire i pacchetti di archiviazione a partire dai SIP inviati dal produttore.

Innanzitutto viene generata la cosiddetta "descrizione del pacchetto" che consiste in una serie di informazioni descrittive (descrizioni associate) che consentirà l'accesso al documento informatico da parte dell'utente. Infatti sulla base di queste descrizioni è possibile effettuare delle ricerche, ed è a partire da queste descrizioni che verranno costruiti i *Dissemination Information Package* (DIP) differenti a seconda delle necessità dell'utente.

Sui documenti versati nel sistema di conservazione è possibile quindi avviare un'attività di validazione, sia dei file che dei metadati, rispetto alle regole e agli standard previsti dalle descrizioni archivistiche di appartenenza. I risultati della convalida possono essere allegati al documento oggetto della convalida per essere eventualmente portati in conservazione insieme al documento.

Il processo di convalida include:

- La verifica dell'integrità del documento memorizzato sul supporto rispetto all'impronta associata allo stesso;
- La verifica che il formato del contenuto binario sia coerente con quanto dichiarato nei suoi metadati, oppure, si potrebbe consentire l'invio di formati di file non adatti alla conservazione;
- La verifica delle eventuali firme digitali apposte su di esso, comprensiva di convalida del certificato rispetto ad uno *store* locale e alle liste di revoca on-line;
- L'eventuale verifica della presenza in archivio di un documento identico (i.e.: stessa impronta e/o metadati);
- La compilazione dei metadati: alcuni metadati potrebbero essere compilati in questa fase in maniera automatica (ad esempio potrebbero essere aggiunte le informazioni relative all'utente che ha effettuato il versamento e la data di versamento).

Il risultato della convalida è riepilogato da un esito in formato XML (rapporto di versamento). I documenti informatici, per i quali l'esito della convalida è risultato positivo, possono quindi essere inseriti in un pacchetto di archiviazione.

L'esito restituito contiene, in un file in formato XML, la lista dei file, il relativo hash e l'identificativo univoco che è stato assegnato al file dal sistema di conservazione e che potrà essere utilizzato per accedere al file.

Controlli al sistema di versamento:

Tipo anomalia	Descrizione	Modalità di gestione
Mancata risposta al Versamento	È il caso in cui l'unità documentaria viene correttamente versata ma, per vari motivi, la risposta di avvenuta ricezione non perviene al produttore, che pertanto, erroneamente, lo reputa non versata.	Il produttore deve trasmettere nuovamente e il sistema di conservazione restituisce una risposta di esito negativo con l'indicazione che l'unità documentaria risulta già versata. Tale risposta deve essere usata dal produttore come attestazione di avvenuto versamento e l'unità documentaria deve risultare come versata.
Errori temporanei	È il caso di errori dovuti a problemi temporanei che pregiudicano il versamento, ma si presume non si ripresentino a un successivo tentativo di versamento. Il caso più frequente è l'impossibilità temporanea di accedere alle CRL degli enti certificatori. In questi casi il sistema di conservazione dopo aver riprovato 10 volte, genera un messaggio di errore perché non riesce a completare le verifiche previste sulla validità della firma e il versamento viene quindi rifiutato impostando il processo in stato ERRV.	Il produttore deve provvedere a rinviare l'unità documentaria in un momento successivo. L'operazione potrebbe dover essere ripetuta più volte qualora il problema, seppur temporaneo, dovesse protrarsi nel tempo.
Versamenti non conformi alle regole concordate	È il caso in cui il versamento non viene accettato perché non conforme alle regole concordate (firma non valida, formato file non previsto, file corrotto, mancanza di Metadati obbligatori, ecc.).	Il soggetto conservatore invia via e-mail una segnalazione dell'anomalia ai referenti del soggetto produttore, con i quali viene concordata la soluzione del problema.

[Torna al sommario](#)

8.1.2. Sistema di gestione dati (SGD)

Il sistema di gestione dati ha il compito di gestire le informazioni legate al contesto archivistico e alle descrizioni dei documenti; questa macro-componente è in pratica il collante dell'intero sistema. Il sistema di gestione dati è il cuore archivistico del sistema ed è la componente che consente di avere una visione unitaria dell'archivio e quindi consente di accedervi. Il sistema di gestione dati ha una duplice valenza: da una parte offre servizi al sistema di accesso per consentire le ricerche e la navigazione e, dall'altra, consente all'ente produttore di gestire il proprio deposito digitale secondo canoni archivistici, offrendo funzionalità come la descrizione e il riordino, la selezione e lo scarto, la ricollocazione del materiale non digitale, ecc. Il sistema di gestione dati rappresenta il collante archivistico dell'intero sistema di conservazione e, per questo motivo, riteniamo questa componente essenziale per consentire a un soggetto produttore di gestire al meglio il proprio deposito digitale.

Il soggetto produttore potrà dunque vedere l'archivio come il complesso sistema di relazioni che è e, tramite le funzionalità che il sistema offre, potrà compiere tutte quelle operazioni necessarie per la gestione di un archivio (di deposito). Per esempio, il sistema di gestione dati, grazie alla propria particolare concezione, permette di gestire al meglio lo scarto del materiale documentario non destinato alla conservazione permanente, ma caratterizzato invece da tempi di conservazione limitati e diversificati.

Per la corretta formazione della struttura di archivio, il conservatore acquisisce gli strumenti archivistici del soggetto produttore (Piano di classificazione, Piano di conservazione, ecc.). L'aggiornamento del piano di conservazione memorizzato nel sistema di conservazione può essere demandato a utenti dell'ente produttore.

[Torna al sommario](#)

8.1.3. Sistema di memorizzazione (SM)

Il sistema di memorizzazione ha lo scopo di gestire in modo semplice e sicuro la conservazione a lungo termine dei documenti informatici, integrando una serie di servizi specifici di monitoraggio dello stato fisico e logico dell'archivio ed effettuando, per ogni documento conservato, una continua verifica di caratteristiche come la leggibilità, l'integrità, il valore legale, l'obsolescenza del formato e la possibilità di applicare la procedura di scarto d'archivio.

Nell'ambito del sistema complessivo, quindi, il sistema di memorizzazione ha il compito di garantire il mantenimento della validità nel tempo dei singoli "documenti digitali", preoccupandosi di aspetti quali l'affidabilità, l'autenticità e l'accessibilità.

Il sistema di memorizzazione, in primo luogo acquisisce quanto inviato dal sistema di versamento durante la fase di versamento e, verificandone preventivamente l'affidabilità, provvederà a gestirne lo *storage*. Sui documenti conservati verranno applicate opportune politiche di gestione atte a garantire, non solo la catena ininterrotta della custodia dei documenti, ma anche la piena tracciabilità delle azioni conservative finalizzate a garantire nel tempo la salvaguardia della fonte.

[Torna al sommario](#)

8.1.4. Sistema di autenticazione e accesso (SAA)

Il modulo per la gestione degli accessi orchestra il flusso di informazioni e servizi necessari per fornire le funzionalità di accesso al cosiddetto *consumer* ovvero all'utente che ha la necessità di accedere ad un determinato documento.

A seguito di una ricerca impostata dall'utente, il modulo di gestione degli accessi richiede i risultati della ricerca al sistema di gestione dati che, organizzando le informazioni descrittive degli AIP, è in grado di rispondere alla richiesta; l'utente, una volta individuato il documento desiderato (o i documenti, o addirittura un intero fascicolo o pacchetto di archiviazione), potrà inoltrare una richiesta di accesso ai dati; questa genererà la richiesta al modulo di generazione DIP il quale, interagendo sia con il sistema di gestione dati che con il sistema di memorizzazione, recupererà le informazioni necessarie (AIP e informazioni descrittive) per produrre il *Dissemination Information Package* (DIP) corrispondente alla richiesta.

Inoltre, il sistema di conservazione, consente anche ricerche trasversali tra tipologie documentarie differenti. Le funzionalità di ricerca saranno implementate dal sistema di gestione dati, mentre il sistema di accesso fornirà le interfacce per l'interrogazione e per la ricezione e visualizzazione dei risultati.

Le modalità di accesso, in generale, permettono quindi di poter ricercare il documento singolo o le aggregazioni di documenti, mediante tutti i criteri derivabili dai metadati ad esso direttamente associati, per poi risalire al suo contesto archivistico.

L'accesso alle funzionalità offerte dal software di conservazione è regolato anche da un sottosistema di autorizzazione che permette di suddividere l'utenza applicativa in gruppi ai quali è possibile assegnare permessi di esecuzione di specifiche operazioni. I singoli permessi (*capabilities*), assegnabili a un gruppo tramite la definizione di "profilo d'uso", attualmente sono poco più di 400. Grazie ai "profili d'uso", definibili autonomamente dall'amministratore dell'applicazione, ogni utente può accedere ad uno o più soggetti produttori e avere visibilità su uno o più descrizioni archivistiche, nonché è possibile assegnare visualizzazioni di singoli pulsanti e/o menù.

[Torna al sommario](#)

8.1.5. Sistema di firma digitale

Il sottosistema per la firma digitale nel contesto della conservazione digitale si configura come elemento fondamentale per l'attuazione della conservazione a norma dei documenti di un preciso flusso di lavoro.

Il processo essenziale per completare la procedura consiste nella firma dell'indice di conservazione (UNI 11386) del pacchetto di archiviazione, nonché nell'apposizione di una marca temporale su tale file.

Essendo presenti diversi dispositivi in grado di fornire queste funzionalità, l'architettura del sistema di conservazione prevede di demandare a un apposito sottosistema il compito di interfacciarsi con essi. Ciò consente al sistema di memorizzazione del software di utilizzare qualunque dispositivo di firma digitale, dato che le eventuali differenze nell'implementazione vengono mascherate dal sottosistema stesso.

Resta l'obbligo che la firma digitale, in questo contesto relativa al Responsabile del servizio di conservazione ed, eventualmente, al Pubblico Ufficiale (o ruolo equivalente), debba essere apposta utilizzando un dispositivo di firma di un tipo approvato da AgID e un certificato rilasciato da una *Certification Authority* (CA) appartenente all'elenco dei certificatori accreditati presso AgID.

Il sistema di conservazione è compatibile con i seguenti dispositivi di firma digitale:

- SmartCard.
- Token USB.
- HSM (Hardware Security Module) o servizi di Certification Authority:
 - Aruba Sign Box.
 - Aruba Remote Sign System.
 - Actalis BBF.

- Intesi Group PKBOX.
- Intesa-IBM.

Il sistema di conservazione è in grado di applicare la firma digitale utilizzando certificati rilasciati da tutte le *Certification Authority* accreditate presso AgID. Per i servizi di firma digitale il soggetto conservatore si avvale di: Aruba Posta Elettronica Certificata S.p.A. a Socio Unico.

[Torna al sommario](#)

8.1.6. Sistema per l'apposizione della marca temporale

La marca temporale consiste in un'ulteriore firma digitale apposta da un soggetto esterno, *Time Stamping Authority* (TSA), il quale registra e memorizza, presso la propria struttura organizzativa, l'impronta del file e la relativa data di firma. In questo caso il soggetto esterno non è, dunque, una persona fisica ma un ente certificatore. In linea di massima le TSA coincidono con le *Certification Authority* e questo servizio è offerto on-line utilizzando protocolli di comunicazione standard.

Il sistema è in grado di richiedere, in modo automatico e on-line, la marca temporale alle TSA utilizzate nel sistema. Per i servizi di marca temporale il soggetto conservatore si avvale di: Actalis S.p.A. Società per Azioni a Socio Unico.

[Torna al sommario](#)

8.2. Componenti Tecnologiche

8.2.1. Componente Legal Archive[®]

L'architettura del sistema di conservazione è basata su una soluzione multi-tier a 3 livelli:

- Presentation layer;
- Business logic (o application) layer;
- Database layer.

L'estrema elasticità del software permette di sostituire, upgradare a caldo oppure di aggiungere, a piacere, applicazioni in uno o più nuovi nodi di un eventuale cluster:

- **Back End** (Services): rappresenta il *core* della logica applicativa e l'interfaccia verso le basi dati (Microsoft SQL 2012 oppure Oracle 11g) a cui l'applicazione attinge. Il Back End ha in carico la gestione e la distribuzione dei processi tra i vari nodi del *cluster*. E' implementato tramite Spring ed espone le sue funzionalità remotamente via protocollo HTTP/HttpInvoker. Non si necessita di un container J2EE ma è sufficiente l'utilizzo di un *servlet container* quale Apache Tomcat per il *deploy* dello stesso;
- **Engine**: è il motore di conservazione;
- **Front End** (Interfaccia Web): è un'applicazione realizzata attraverso l'uso di pagine web dinamiche costruite secondo il design pattern MVVM e la tecnologia Vaadin.

Attraverso Front End gli utenti potranno accedere per configurare e monitorare il sistema.

La tecnologia Vaadin è basata su Google Web Toolkit che garantisce la compatibilità con un larga parte degli attuali browser senza la necessità di installare ulteriori plug-in sul client.

Di seguito la lista dei browser dichiarati compatibili:

- Android 2.3 o superiore

- Google Chrome 23 o superiore
- Internet Explorer 8 o superiore
- iOS 5 o superiore
- Mozilla Firefox 17 o superiore
- Opera 12 o superiore
- Safari 6 o superiore

L'applicazione è pensata per essere scalabile, aumentando il numero dei *web container*, attraverso una logica di *server clustering* gestita automaticamente dal sistema, che, a seconda del livello di carico di ciascun server, distribuirà al meglio le richieste dei client.

- **SOAP - Web Service:** sono un insieme di servizi web che permettono, ad applicazioni di terze parti, di versare documenti nel sistema di conservazione o di interrogare lo stesso sullo stato di un documento. In un'ottica di installazione su ambienti virtuali, il sistema consente una scalabilità al crescere degli utenti coinvolti e dei volumi di documenti da conservare, permettendo all'azienda di reagire tempestivamente a eventuali esigenze del soggetto produttore.

[Torna al sommario](#)

8.2.2. Scalabilità sugli utenti

Il Sistema di conservazione è stato progettato per supportare numeri elevati di utenti che vi accedono per consultare documenti in esso conservati. In ogni caso, trattandosi di un applicativo sviluppato a tre livelli e impiegando le più moderne tecnologie di implementazione software, è possibile far crescere la componente Interfaccia Web in funzione del numero di utenti. Anche la componente database è assolutamente scalabile in funzione del numero di utenti.

Riepilogando:

- La necessità di maggiore capacità elaborativa implica l'aggiunta di *application server e/o core* e RAM;
- La necessità di maggiore capacità elaborativa sui Database e Repository/Content Server implica l'aggiunta di ulteriori server ai rispettivi *cluster e/o core* e RAM;
- La necessità di archiviare una maggiore quantità di pacchetti di archiviazione implica l'aggiunta di nuovi dispositivi di *storage*;
- Alla saturazione di uno *storage* se ne aggiunge un altro;
- La necessità di maggiore banda fra il sito principale e il sito di *disaster recovery*: la presenza di accessi in fibra ottica sulle due sedi consente di ampliare agevolmente la banda disponibile per il collegamento.

[Torna al sommario](#)

8.2.3. Componente database

I dati del sistema di conservazione sono ospitati su un database relazionale costituito da un cluster geografico DBMS distribuito su più data center.

L'architettura è realizzata con standard di alta affidabilità e scalabilità che consentono di garantire il funzionamento del database anche a fronte della caduta di uno o più nodi.

Il cluster DBMS è realizzato secondo un'architettura database "always-on" che consente una recovery veloce anche in caso di malfunzionamento di un data center. Consente inoltre di avere nodi attivi e nodi passivi su tutte le sedi, offrendo elaborazioni applicative come se fossero eseguite su un unico cluster database.

I dati del Sistema di Conservazione presenti nel sito primario vengono completamente aggiornati sul sito secondario. Il database fornisce meccanismi di audit che garantiscono il tracciamento delle modifiche.

I dati del sistema di conservazione sono isolati dal resto dell'infrastruttura. La visibilità e l'accesso ai dati è limitato alle sole persone/componenti software autorizzate.

[Torna al sommario](#)

8.2.4. Componente storage

Le informazioni vengono archiviate su un repository dedicato e progettato per l'archiviazione a lungo termine. Esso assicura la non modificabilità delle informazioni del sistema di conservazione.

A garanzia della sicurezza dei dati conservati, i dispositivi sono collocati in entrambi i data center di Olsa Informatica.

La piattaforma utilizzata garantisce i tre parametri principali di sicurezza (disponibilità, integrità e riservatezza) nel rispetto delle normative vigenti per i sistemi di conservazione.

I dati del sistema di conservazione sono isolati dal resto dell'infrastruttura. La visibilità e l'accesso agli stessi è limitato alle sole persone/componenti software autorizzate.

La figura seguente descrive schematicamente le dipendenze delle diverse componenti tecnologiche del software di conservazione sopra citate.

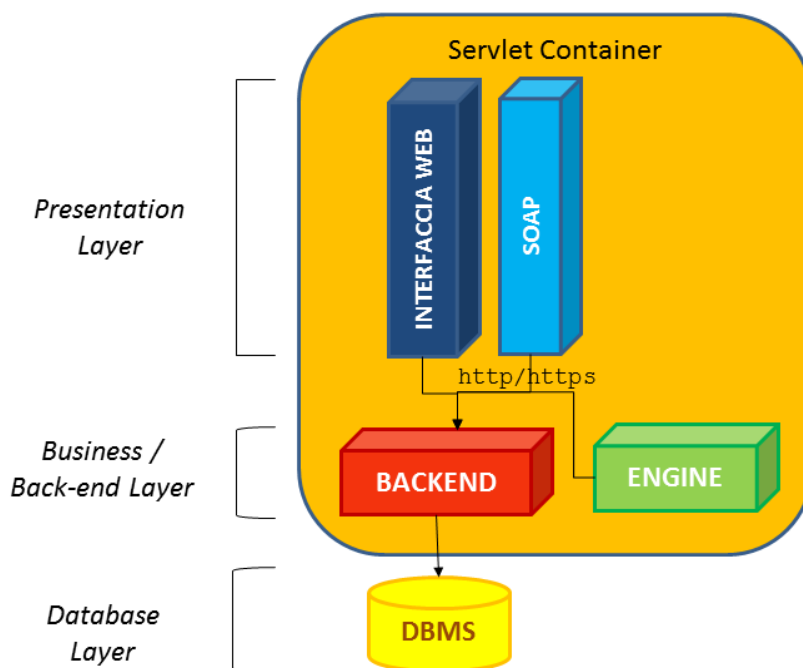


Figura 9: Componenti scalabili del sistema

[Torna al sommario](#)

8.3. Componenti fisiche

La struttura informatica è articolata in tre siti:

- Sito principale dove viene sviluppato il software e da dove vengono eseguite le attività di gestione e monitoraggio del sistema di conservazione;
- La farm di produzione dove vengono erogati i servizi di conservazione dei documenti informatici e ospitante i server virtuali nei quali sono installate le diverse componenti logiche del software di conservazione;
- La farm secondaria di *disaster recovery*.

La figura sottostante rappresenta l'infrastruttura virtuale ospitata nella server farm di produzione e nel sito di DR.

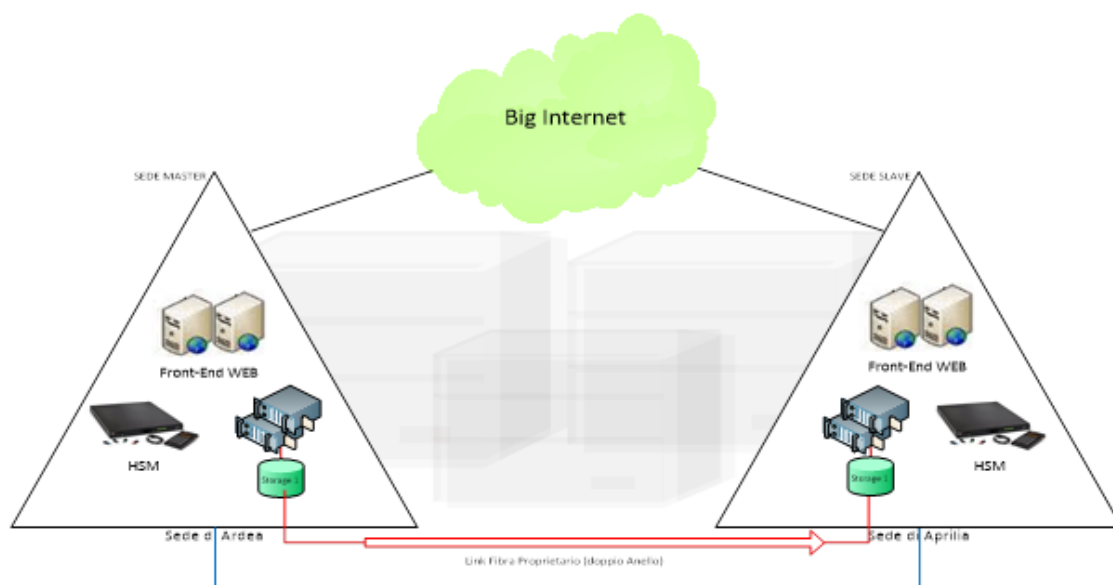


Figura 10: Schema dell'infrastruttura della farm di produzione e della farm di Disaster Recovery

Il sistema di conservazione è progettato e realizzato per fornire un'elevata continuità di servizio, garantire l'integrità degli oggetti digitali conservati, gestire grandi volumi di dati, mantenere performance stabili indipendentemente dai volumi di attività e assicurare la riservatezza degli accessi.

Le sedi di proprietà di Olsa informatica sono dislocate sul territorio nazionale e in particolare ad Aprilia (LT) e ad Ardea (RM).

Ogni sede è dotata di impianti di:

- anti intrusione e verifica accessi fisici
- alimentazione e di emergenza (Sistemi UPS)
- condizionamento
- antincendio
- ridondanza di rete

L'infrastruttura tecnologica di Olsa Informatica è composta da una sicurezza logica a più livelli a tutela dei dati gestiti.

Possiamo identificarla in:

- Firewall perimetrali
- Aree DMZ
- Aree VPN
- Suddivisione delle LAN in vLan con relative AC
- Policy di accesso restrittive file-system, applicativi e DB

I data center di Aprilia e Ardea di Olsa Informatica sono stati progettati secondo le linee guida della ISO 27001:2013.

Possiamo identificare parte della struttura in:

- quadri elettrici dedicati
- impianti di condizionamento dedicati
- impianti di spegnimento dedicati

Sui data center è stato attivato un piano di continuità operativa.

L'infrastruttura prevede delle VM in entrambi i data center dedicate al workflow della conservazione a norma; essa si suddivide in VM (server ospitanti la piattaforma Legal Archive) e apparati storage dedicati.

Lo storage dedicato al processo di conservazione garantisce integrità, riservatezza e disponibilità mediante l'attuazione di opportune policy attivate dal responsabile della sicurezza dei sistemi informativi.

La garanzia della conservazione del dato nel tempo è fornita dalle politiche di retention attuate; queste sono configurate per assicurare il "congelamento" del repository per il tempo concordato con il SP.

Nessun utente o applicazione avrà la possibilità di modificare e/o eliminare i dati e i rispettivi repository storage o di estendere la validità della stessa, sino allo scadere definito. E' previsto un uptime del 99,9% su base annuale.

Per un maggior dettaglio dei sistemi di sito primario e secondario si rimanda al Piano della Sicurezza di Olsa Informatica.

[Torna al sommario](#)

8.4. Procedure di gestione e di evoluzione

Il sistema di conservazione deve garantire che siano rispettati i requisiti per la conservazione dei documenti previsti dall'art. 44 del Codice dell'Amministrazione Digitale, nonché il rispetto delle misure di sicurezza previste dal D.Lgs. 30 giugno 2003, n. 196.

Le procedure di gestione del sistema di conservazione prevedono un costante monitoraggio del sistema stesso con il fine di poter intercettare in modo tempestivo eventuali necessità di ripristini, modifiche e/o evoluzioni del sistema stesso.

I requisiti di sicurezza (sicurezza fisica, logica e organizzativa) adottati nella conduzione e manutenzione del sistema di conservazione, nelle politiche di gestione dell'incident management e della continuità operativa del servizio di conservazione sono specificati e riportati nel Piano della Sicurezza.

Il change management, sia del software che dell'hardware, viene eseguito nel rispetto delle policy 27001:2013 in cui vengono descritti gli step da eseguire e che sono riportati di seguito:

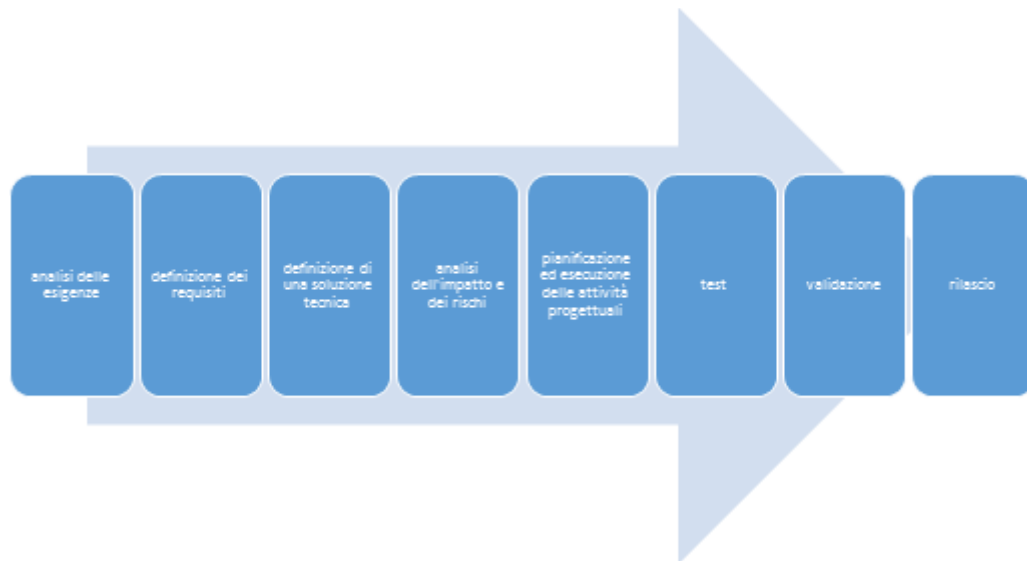


Figura 11: Flusso delle attività di change management

A seguito dell'analisi tecnica per MEV o MAC, le quali vengono prodotte nel rispetto dei procedimenti sopra descritti, vengono applicate delle procedure di change management al sistema di conservazione. Va sottolineato che lo stesso è realizzato mediante infrastrutture separate che rispettano policy di test e tuning per poi essere implementate nell'ambiente di produzione.

La manutenzione evolutiva del software viene eseguita in due scenari:

- adeguare il prodotto per scopi normativi;
- aggiungere funzionalità e migliorie al prodotto stesso.

Nel primo scenario la Business Unit di Olsa Informatica, dedicata alle normative per la conservazione, monitora, con cadenza almeno mensile, i siti istituzionali e verifica la presenza di eventuali nuovi requisiti normativi. Successivamente, se ritenuto opportuno, la questione verrà portata all'attenzione della Business Unit tecnica che procederà ad un'analisi di dettaglio, il cui risultato produrrà una pianificazione di tempi, costi e rischi.

Nel secondo scenario le modifiche sono solitamente suggerite dalla comunità di riferimento, la quale evidenzia migliorie che potrebbero essere apportate al prodotto o richiede nuove funzionalità adeguate alle proprie necessità procedurali.

Gli interventi di manutenzione evolutiva sono assimilabili a un insieme di piccoli progetti, con durate ipotizzabili, che oscillano secondo i requisiti individuati. Tali attività presentano le caratteristiche tipiche di ogni progetto e rispettano la sequenza prevista per la change management.

Il sistema di conservazione attualmente è conforme agli standard previsti ed elencati nel precedente paragrafo 3.2.

La manutenzione correttiva consiste nell'adeguamento del software in relazione a un bug o a un malfunzionamento riscontrato dalla comunità di riferimento.

In questo scenario, verrà aperto un verbale di non conformità (ISO 9001:2008), che verrà assegnato alla Business Unit Tecnica, la quale procederà con l'analisi di dettaglio, tempi, rischi, costi e implementazione della soluzione, rispettando gli ambienti di test e, successivamente, quelli di produzione.

Al termine di ciò, il software verrà rilasciato in esercizio rispettando i processi di change management.

Olsa Informatica mette a disposizione del cliente un Servizio di Assistenza disponibile dal lunedì al venerdì per un totale di 40 ore alla settimana per garantire una tempestiva risposta sia alle problematiche tecniche sia a quelle applicative relative all'uso del sistema. Ciascun utente potrà quindi aprire una chiamata di assistenza (ticket) via e-mail o via web dove l'utente potrà descrivere il problema. Il software di gestione dei ticket mette a disposizione un servizio in grado di assegnare ad ogni ticket un numero univoco per poter tracciare la chiamata (trouble ticketing e tracking ticketing).

Livelli di Servizio: I livelli di servizio vengono calcolati nella fascia oraria indicata successivamente per ciascuna tipologia di servizio. I livelli di servizio saranno applicati solo per quanto diretta responsabilità. L'operatività piena di tutte le funzionalità viene garantita nei giorni lavorativi (lun-ven) dalle 09:00 alle 18:00; resta comunque inteso che, trattandosi di servizi erogati sul web, la visibilità e le funzionalità sono garantite al meglio anche durante il week-end e le festività.

Tempo di presa in carico/risposta: è il tempo che intercorre tra la ricezione della chiamata e la presa in carico del problema. Entro il tempo massimo stabilito dallo SLA e concordato con il cliente, la segnalazione deve essere presa in carico con comunicazione delle evidenze sul problema e del relativo piano di lavoro che si intende intraprendere per la diagnosi e/o la risoluzione. Per piano di lavoro si intende l'iter procedurale (in termini di azioni e pianificazioni) che si intende intraprendere, sia per ottenere una corretta *problem determination* che per arrivare alla risoluzione del problema stesso. Il tempo di presa in carico non deve essere confuso con il tempo di risoluzione, in questo contesto viene classificata come azione anche l'attività di escalation e *problem determination* necessaria in caso non sia disponibile immediatamente una diagnosi esaustiva o una soluzione.

Disponibilità: indica le finestre temporali entro le quali vengono garantite le singole voci che compongono il servizio. Saranno esclusi dal calcolo della disponibilità del servizio, i periodi necessari per interventi tecnici sugli apparati e sulle linee costituenti la rete, come pure i tempi occorrenti per l'inserimento di nuove configurazioni e/o aggiornamenti sui nodi stessi.

Up-time: è il periodo di disponibilità (espresso in percentuale sul tempo) dei sistemi misurato nella fascia oraria di erogazione del servizio. Sono esclusi nella misurazione i fermi concordati (manutenzione programmata).

Criticità/Presa in carico: è il parametro che definisce i contenuti e le tempistiche per l'intervento all'evento segnalato ed è legato al livello di servizio.

Relativamente al monitoraggio del mantenimento dei livelli di servizio (SLA), in presenza di particolari condizioni non sarà imputabile al conservatore il verificarsi di eventuali disservizi:

- cause di forza maggiore e cioè eventi che, oggettivamente, impediscano al personale di intervenire per eseguire le attività poste dal contratto a carico dello stesso (in via meramente esemplificativa e non esaustiva: scioperi e manifestazioni con blocco delle vie di comunicazione, incidenti stradali, guerre e atti di terrorismo, catastrofi naturali quali alluvioni, tempeste, uragani etc.);
- interventi straordinari da effettuarsi con urgenza ad insindacabile giudizio del conservatore per evitare pericoli alla sicurezza e/o stabilità e/o riservatezza e/o integrità dei dati e/o informazioni del cliente. L'eventuale esecuzione di tali interventi sarà comunque comunicata al cliente a mezzo e-mail inviata all'indirizzo di posta elettronica indicato in fase d'ordine con preavviso anche inferiore alle 48 ore oppure contestualmente all'avvio delle operazioni in questione o comunque non appena

- possibile;
- indisponibilità o blocchi dell'Infrastruttura imputabili a:
 - errato utilizzo, errata configurazione o comandi di spegnimento, volontariamente o involontariamente eseguiti dal cliente;
 - anomalie e malfunzionamenti dei software applicativi/gestionali forniti da terze parti;
 - inadempimento o violazione del contratto imputabile al cliente;
 - anomalia o malfunzionamento del servizio, ovvero loro mancata o ritardata rimozione o eliminazione imputabili a inadempimento o violazione del contratto da parte del cliente ovvero ad un cattivo uso del servizio da parte sua;
 - cause che determinano l'inaccessibilità, totale o parziale, dell'infrastruttura dal cliente imputabili a guasti nella rete internet esterna al perimetro del conservatore e comunque fuori dal suo controllo (in via meramente esemplificativa guasti o problemi).

[Torna al sommario](#)

8.5. Log del sistema di conservazione

Le diverse componenti logiche che costituiscono la piattaforma del sistema di conservazione, tracciano su log informazioni di dettaglio che favoriscono le analisi e il monitoraggio del sistema stesso.

Log della componente di back-end

In esso vengono tracciate le informazioni relative alle diverse interrogazioni del sistema.

Per ciascuna di esse è disponibile:

- indirizzo da cui proviene la richiesta;
- data e ora della richiesta;
- utente;
- tipo di operazione richiesta;
- dettaglio dell'operazione richiesta (eventuale).

Si riportano le richieste tracciate e relative risposte:

- login --> userid;
- dettaglio soggetto produttore --> l'alias del soggetto produttore;
- dettaglio persona fisica --> codice fiscale della persona;
- dettaglio username --> username;
- dettaglio certificato --> codice fiscale;
- dettaglio pacchetto di archiviazione --> numero pacchetto di archiviazione;
- dettaglio documento/fascicolo --> UID + lista metadati separati da pipe;
- download --> UID + lista metadati separati da pipe.

[Torna al sommario](#)

Log della componente engine

La componente di Engine, che si occupa dell'elaborazione dei processi di conservazione, traccia nel proprio log le informazioni relative al singolo soggetto produttore.

Le informazioni fruibili sono:

- data e ora di esecuzione del processo;
- utente che ha richiesto il processo;
- tipo di processo richiesto;
- esito del processo.

Tutti i log vengono registrati e conservati nel sistema di conservazione di Olsa Informatica.

[Torna al sommario](#)

9. Monitoraggio e controlli

Dalla sede principale vengono svolte tutte le attività operative necessarie alla gestione, al mantenimento e al monitoraggio del sistema di conservazione.

Nello specifico caso del monitoraggio, il sistema è costantemente controllato dagli operatori che vi operano. L'adeguatezza delle risorse ai carichi di lavoro e ai volumi è costantemente verificata dagli operatori del sistema di conservazione.

Nelle varie macchine che costituiscono l'infrastruttura di produzione è installato un agente di controllo e monitoraggio che segnala anomalie e l'eventuale caduta di connessione alla macchina.

Periodicamente, come previsto dalle procedure interne, il sistema per la sicurezza delle informazioni e il sistema di gestione della qualità è sottoposto ad audit di verifica interna e da parte di enti di certificazione esterni atti a garantire che le procedure, delineate per assicurare la qualità del servizio e la sicurezza delle informazioni, siano rispettate.

Per maggiori dettagli sui monitoraggi interni ed esterni al sistema di conservazione, per i controlli sui dispositivi in uso e dismessi, per il controllo sulle forniture rimandiamo al Piano della Sicurezza.

[Torna al sommario](#)

9.1. Procedure di monitoraggio

Oltre al sistema di notifica e-mail e web, il software mette a disposizione dell'utente amministratore una serie di strumenti per monitorare lo stato del sistema di conservazione e poter gestire le anomalie e le eccezioni riconosciute.

Stato dei processi

Il pannello "Stato dei processi" elenca i processi eseguiti e in esecuzione, e il loro stato. Permette all'amministratore di prendere visione dei processi in errore e leggere un estratto sintetico del log chiarificativo della causa dell'errore.

Stato dell'impianto - Cluster

Il pannello "Gestione Cluster" permette all'utente amministratore di verificare in tempo reale la disponibilità dei server sui quali è installato il sistema di conservazione.

Monitoraggi esterni al sistema di conservazione

Dalla sede principale vengono svolte tutte le attività operative necessarie alla gestione, al mantenimento e al monitoraggio del sistema di conservazione. Nello specifico caso del monitoraggio, il sistema è costantemente controllato dagli operatori che vi operano.

Nei vari elementi che costituiscono l'infrastruttura di produzione è installato un agente di controllo e monitoraggio che segnala l'eventuale caduta di connessione, riportando tale informazione a una console centralizzata che viene costantemente monitorata; inoltre, Olsa Informatica ha implementato un sistema di messaggistica remota per allertare le persone preposte.

Periodicamente, come previsto dalle procedure interne, il sistema per la sicurezza delle informazioni e il sistema di gestione della qualità è sottoposto ad audit di verifica interno e da parte di enti di certificazione esterni. Per maggiori dettagli sui monitoraggi interni ed esterni al Sistema di conservazione, per i controlli sui dispositivi in uso e dismessi per il controllo sulle forniture rimandiamo al Piano della Sicurezza.

[Torna al sommario](#)

9.2. Verifica dell'integrità degli archivi

La funzionalità di verifica di integrità degli archivi permette di verificare l'integrità del documento dal momento della sua conservazione, confrontando l'impronta attuale con quella contenuta nell'indice di conservazione. Tale funzionalità viene applicata durante il processo di conservazione, subito dopo la fase di memorizzazione nel file system, e risulta poi utile, nell'assolvimento dei requisiti di verifica periodica della leggibilità dei documenti, come richiesto dalla normativa.

Questa funzionalità è presente nel sistema di conservazione, come processo schedabile e può essere quindi pianificata da parte del Responsabile del servizio di conservazione.

A ogni verifica effettuata viene generato un report in formato XML che può essere consultato da parte del Responsabile del servizio di conservazione per attestare la corretta esecuzione della verifica o per diagnosticare eventuali anomalie.

[Torna al sommario](#)

9.3. Soluzioni adottate in caso di anomalie

Le anomalie che possono riscontrarsi nell'operatività del servizio di conservazione vengono segnalate automaticamente, sia via e-mail che da interfaccia web, agli operatori e registrate nei log di sistema.

Le anomalie vengono affrontate con diverse metodologie, secondo la natura dell'anomalia stessa e la collocazione dell'evento che l'ha generata nel processo di conservazione; quindi oltre alle procedure atte a garantire l'integrità degli archivi, esistono anche procedure atte a risolvere anomalie in altre componenti del sistema.

Le caratteristiche comuni e le specificità delle procedure di risoluzione delle anomalie dipendono da diversi fattori organizzativi e tecnologici:

- tutte le funzionalità del sistema che inseriscono o modificano dati nel Data Base e file nell'area FTP o nel File System operano in modalità transazionale;
- il backup del Data Base assicura il *restore* all'ultima transazione completata correttamente (le politiche di backup sono descritte nel Piano della Sicurezza di Olsa Informatica).

Distinguiamo due principali tipi di anomalie:

- anomalie dovute a bug del software;
- anomalie dovute a malfunzionamento dell'impianto.

Anomalia dovuta al bug del software

Una volta segnalata l'anomalia e riconosciuta come bug del software questa viene risolta con una priorità direttamente proporzionale alla criticità della stessa, come indicato dalla seguente tabella:

Criticità	Descrizione	Presa in carico
Altissima	Grave indisponibilità del servizio, con un serio impatto sulle attività del cliente. Verranno classificati in questa categoria tutti gli eventi che pregiudicheranno totalmente l'intero servizio. Il servizio non è utilizzabile e il problema si ripercuote sulla totalità degli utenti finali.	2 ore lavorative

Alta	Parziale interruzione del servizio, non aggirabile. Si è verificato un problema serio che influisce su un numero limitato di utenti oppure si è verificato un problema che pregiudica solamente alcune funzionalità ma è riscontrato dalla totalità degli utenti finali.	4 ore lavorative
Media	Servizio degradato, il disservizio può essere temporaneamente aggirato. Il problema riscontrato non pregiudica le funzionalità del sistema (al massimo pregiudica delle funzionalità accessorie) pur presentando comunque qualche disagio per gli utenti finali.	8 ore lavorative
Bassa	Problemi che non hanno immediato impatto sul servizio, oppure per semplice richiesta di informazioni. Sono necessarie alcune attività pianificabili nel tempo (azioni pianificabili o azioni rimandabili in orari non critici per il servizio).	16 ore lavorative

Anomalia dovuta al malfunzionamento dell'impianto

Attività	Livelli di servizio	% di applicazione
Lavorazione dei pacchetti di versamento ricevuti.	Entro il giorno lavorativo successivo (festivi esclusi) dalla ricezione del pacchetto di versamento.	99,5% dei pacchetti di archiviazione ricevuti
Comunicazione eventuali anomalie nei pacchetti di archiviazione di documenti ricevuti (per errori strettamente riguardanti il contenuto dei file ricevuti).	Entro il giorno lavorativo successivo (festivi esclusi) dalla ricezione del pacchetto di versamento.	99,5% dei pacchetti di archiviazione ricevuti
Invio ai clienti della segnalazione di errori che causano il blocco dell'elaborazione dei pacchetti di archiviazione da conservare.	Entro il giorno lavorativo successivo (festivi esclusi) dalla ricezione del pacchetto di versamento.	99,5% dei pacchetti di archiviazione ricevuti
Avvio rielaborazione dei pacchetti di archiviazione eventualmente impattati dall'anomalia.	Entro il giorno lavorativo successivo (festivi esclusi) dalla risoluzione anomalia (dalla data comunicazione al Cliente).	99,5% dei pacchetti di archiviazione ricevuti
Risoluzione malfunzionamenti del servizio di CS.	Preso in carico: entro 16 ore lavorative nei seguenti orari: dalle ore 9.00 alle ore 13.00 e dalle ore 14.00 alle ore 18 di ciascun giorno feriale (Lun. - Ven.).	N.A.
Disponibilità dei servizi di caricamento <ul style="list-style-type: none"> • Upload Manuale • Modalità SFTP • Modalità Web Services N.B.: La disponibilità delle modalità Custom viene espressamente concordata con il soggetto produttore.	Entro il giorno lavorativo successivo (festivi esclusi) dalla segnalazione.	99,9% su base trimestrale
Disponibilità del servizio di consultazione ed esibizione dei documenti conservati (interfaccia Web).	Entro il giorno lavorativo successivo (festivi esclusi) dalla ricezione del pacchetto di versamento.	99% su base trimestrale

[Torna al sommario](#)

10. Trattamento dei dati personali

La direzione di Olsa Informatica S.p.A., al fine di garantire la tutela e la protezione delle informazioni acquisite e gestite nell'ambito delle proprie attività, e di assicurare che i dati personali siano trattati in conformità a quanto previsto dal **Regolamento Europeo UE 2016/679** e dal **Decreto Legislativo 30/06/2003 n 196**, modificato dal D.lgs n. 101 del 10 agosto 2018, ha definito e approvato il Regolamento Interno denominato *Regolamento generale sulla protezione dei dati e delle informazioni*.

Il regolamento rappresenta la privacy policy che tutto il personale coinvolto nella gestione delle informazioni e nel trattamento dei dati personali è tenuto a conoscere ed osservare.

Il regolamento individua gli adempimenti da compiere ai fini della compliance al **Regolamento Europeo UE 2016/679** e al **Decreto Legislativo 30/06/2003, n 196**, modificato dal D.lgs n. 101 del 10 agosto 2018, in particolare:

- Identifica ruoli e responsabilità connessi alla gestione del trattamento dei dati personali, incluso il ruolo assegnato al Data Protection Officer;
- Definisce le modalità di comunicazione con le autorità;
- Definisce le modalità di gestione dei dati personali con particolare riferimento ai principi di *Data protection by default* e *Data protection by design*;
- Definisce gli adempimenti da mettere in atto in caso di data breach;
- Definisce la procedura di valutazione di impatto;
- Descrive le misure tecniche e organizzative implementate ai fini della sicurezza dei dati personali.

I trattamenti effettuati da Olsa Informatica, sono monitorati in appositi registri predisposti secondo le indicazioni previste nell'art. 30 del Regolamento UE 2016/679, il registro contiene per ogni trattamento almeno le seguenti informazioni:

- a) dati del titolare del trattamento e del responsabile
- b) finalità del trattamento
- c) descrizione delle categorie di interessati
- d) descrizione delle categorie di dati trattati
- e) indicazione delle categorie di destinatari ai quali dati saranno comunicati
- f) descrizione di eventuali trasferimenti di dati all'estero
- g) termini previsti per la cancellazione dei dati
- h) descrizione delle misure di sicurezza tecniche e organizzative
- i) indicazione dei soggetti incaricati al trattamento

Olsa informatica conferisce apposito incarico a tutti i collaboratori impegnati in attività che prevedano trattamenti dei dati, tutti i soggetti ai quali è conferito tale incarico con apposito atto di nomina sono informati, dal proprio referente attraverso apposite istruzioni operative e sessioni formative, in merito ai trattamenti per i quali sono stati autorizzati.

Con riferimento ai trattamenti di dati personali condotti nello svolgimento delle attività connesse ai processi di conservazione è possibile individuare due aree di gestione dei dati personali nell'ambito delle quali Olsa riveste un diverso nella catena di responsabilità:

- dati personali raccolti e gestiti nei documenti oggetto dell'attività di conservazione, per il trattamento dei quali Olsa riveste il ruolo di responsabile ex art. 28 Regolamento UE 2016/679 per conto del soggetto produttore al quale spetta la titolarità;
- dati personali raccolti nelle attività di censimento e autorizzazione degli utenti del servizio di conservazione, nel trattamento dei quali Olsa riveste il ruolo di titolare.

Nell'ambito dei trattamenti di dati contenuti nei documenti oggetto di conservazione i contratti di servizio prevedono il riconoscimento della titolarità del trattamento al soggetto produttore il quale conferisce a Olsa tramite apposita nomina in allegato al contratto il ruolo di Responsabile ex art. 28. Con tale atto di nomina il titolare del dato definisce le disposizioni alle quali il titolare dovrà uniformarsi nello svolgimento dei trattamenti connessi alle attività di conservazione.

Con riferimento alle attività di trattamento effettuate per le attività di gestione e monitoraggio degli accessi al sistema di conservazione, Olsa in qualità di titolare, raccoglie e gestisce i dati personali strettamente necessari alla configurazione della piattaforma. Gli utenti compilano un modulo con il quale conferiscono i dati necessari all'attivazione dell'utenza e sottoscrivono il consenso al trattamento. L'informativa è resa disponibile al momento della sottoscrizione e come link al momento di accedere alla piattaforma.

Per approfondimenti in merito alla privacy policy adottata si rimanda al documento del sistema gestione POSI 24 REGOLAMENTO PROTEZIONE DATI E INFORMAZIONI.

[Torna al sommario](#)