

Manuale della Conservazione

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione	Firma
<i>Redazione</i>	16/02/2015	Claudio Della Ciana	<i>Responsabile della sicurezza dei sistemi per la conservazione</i>	
<i>Verifica</i>	16/02/2015	Michele Cirinei	<i>Responsabile dei sistemi informativi per la conservazione</i>	
<i>Approvazione</i>	16/02/2015	Luca Marconi	<i>Responsabile del servizio di conservazione</i>	

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
Prima emissione	16/02/2015		
Seconda emissione	29/01/2016	Aggiornamento manuale secondo direttive AgID	
Seconda emissione/rev. 1	12/02/2016	Aggiornamento manuale secondo direttive AgID	

Seconda emissione/rev. 2	15/01/2018	<ul style="list-style-type: none"> • Aggiornamento manuale secondo direttive AgID • Integrazione Standard di riferimento • Modifica nomina Responsabile dei servizi informativi (descrizione, matrice e organigramma) • Inserimento della definizione di "fruitore" in 5.2 Strutture organizzative • Inserimento monitoraggio interno dei log • Inserimento supporti fisici per il trasferimento • Inserimento Piano di cessazione o modifica del servizio • Integrazione Change Management 	
Seconda emissione/rev. 3	16.11.2018	<ul style="list-style-type: none"> • Modifica al ruolo di Responsabile dei Sistemi Informativi (capitolo 4 e 5.1) • Modifica alla procedura di change management ed integrazione con procedura ISO 27001. 	
Seconda emissione/rev. 4	28.01.2019	<ul style="list-style-type: none"> • Aggiornamento Normative di Riferimento 	
Seconda emissione/rev.5	15.07.2020	<ul style="list-style-type: none"> • Aggiornamento Organigramma con nuovo Responsabile della Protezione dei Dati 	
Seconda emissione/rev.6	08.10.2020	<ul style="list-style-type: none"> • Aggiornamento Organigramma con aggiunta della figura Amministratore di Sistema • Aggiornamento supporti fisici per il trasferimento 	
Seconda emissione/rev.7	12.10.2020	<ul style="list-style-type: none"> • Sistema per l'apposizione della marca temporale 	

INDICE DEL DOCUMENTO

Manuale della Conservazione	1
EMMISSIONE DEL DOCUMENTO	1
REGISTRO DELLE VERSIONI	1
INDICE DEL DOCUMENTO	3
1. SCOPO E AMBITO DEL DOCUMENTO	5
Il presente manuale di conservazione è un documento informatico	5
2. TERMINOLOGIA (GLOSSARIO E ACRONIMI)	6
3. NORMATIVA E STANDARD DI RIFERIMENTO	13
3.1. Normativa di riferimento	13
3.2. Standard di riferimento	14
4. RUOLI E RESPONSABILITÀ	14
5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE	16
5.1. Organigramma	19
5.2. Strutture organizzative	19
6. OGGETTI SOTTOPOSTI A CONSERVAZIONE	21
6.1. Oggetti conservati	21
6.2. Pacchetto di versamento	26
6.3. Pacchetto di archiviazione	27
6.4. Pacchetto di distribuzione.....	30
7. IL PROCESSO DI CONSERVAZIONE	31
7.1. Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico.....	31
Osservazione:.....	33
7.2. Verifiche effettuate sui pacchetti di versamento e sugli oggetti in esso contenuti.....	33
7.3. Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico	34
7.4. Rifiuto del pacchetto di versamento e modalità di comunicazione delle anomalie	35
7.5. Preparazione e gestione del pacchetto di archiviazione	35
7.6. Preparazione e gestione del pacchetto di distribuzione (DIP) ai fini dell'esibizione.....	36
7.7. Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti.....	38
7.8. Scarto dei pacchetti di archiviazione.....	38
7.9. Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori.....	39
8. IL SISTEMA DI CONSERVAZIONE.	41
8.1. Componenti logiche.....	43
Sistema di Versamento (SV).....	43

Sistema di gestione dati (SGD)	44
Sistema di memorizzazione (SM)	45
Sistema di accesso	45
Sistema di firma digitale	46
Sistema per l'apposizione della marca temporale	46
8.2. Componenti tecnologiche	47
8.3. Componenti fisiche.....	48
8.4. Procedure di gestione ed evoluzione.	50
Conduzione e manutenzione del sistema di conservazione.	50
Gestione e conservazione dei log (anche in accordo con l'ente Produttore).	50
Monitoraggio del sistema di conservazione.	50
Change management.....	52
Revisione Utente.....	52
Verifica periodica di conformità a normativa e standard di riferimento.	52
9. MONITORAGGIO E CONTROLLI.....	53
9.1. Procedure di monitoraggio	53
Stato dei processi.....	53
Stato dell'impianto - Cluster	54
Monitoraggio dei log.....	54
9.2. Verifica integrità degli archivi.....	54
9.3. Soluzioni adottate in caso di anomalie.....	55
Anomalia dovuta a bug del software	55
Anomalia dovute a malfunzionamento dell'impianto	55

1. SCOPO E AMBITO DEL DOCUMENTO

Il presente documento costituisce il manuale di conservazione di Plurima S.p.A. e ha lo scopo di descrivere il sistema di conservazione dei documenti informatici adottato dall'azienda.

Il software utilizzato per la gestione del processo di conservazione dei documenti informatici è Legal Archive® di Ifin Sistemi.

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.

- 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	Plurima Spa
Indirizzo	Via Marie Curie 15 - 06073 - Corciano - Perugia
Legale Rappresentante	Dott. Luca Marconi
Referente tecnico (nome e cognome) cui rivolgersi in caso di problemi tecnico-operativi	Claudio Della Ciana; Michele Cirinei
E-mail del referente tecnico	claudio.dellaciana@plurima.info - michele.cirinei@plurima.info
N° telefono/fax	075-6059669 / 075-605245
Sito web istituzionale	www.plurima.info
E-mail istituzionale	plurima@plurima.info – segreteria@plurima.info

Contesto di riferimento

Con il DPCM del 3 dicembre 2013 (G.U. n. 59 del 12 marzo 2014 – S.O. 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 i 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 E 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

autenticità	Caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico
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. [da 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. [da 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

<i>fascicolo informatico</i>	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.
<i>file di indice</i>	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. [da 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 timestamping.
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

<i>responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi</i>	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.
<i>responsabile della conservazione</i>	soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 delle regole tecniche del sistema di conservazione
<i>responsabile del trattamento dei dati</i>	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. [da 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
- **IR**: Informazioni sulla rappresentazione
- **IRse**: Informazioni sulla rappresentazione semantiche
- **IRsi**: Informazioni sulla rappresentazione sintattiche
- **ISO**: International Organization for Standardization
- **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
- **VdC**: Volume di conservazione.

[Torna al sommario](#)

3. **NORMATIVA E STANDARD DI RIFERIMENTO**

3.1. **Normativa di riferimento**

Il presente documento riporta la normativa nazionale italiana e gli standard di riferimento in vigore nei luoghi dove sono conservati i 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, n. 241 e s.m.i.**
"Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi";
- Decreto legislativo 20 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";
- Nuovo Regolamento europeo 2016/679
Nuovo Regolamento Europeo in Materia di protezione dei Dati Personali
- Decreto legislativo del 10.08.2018, n.101
Decreto attuativo delegato di adeguamento della Normativa nazionale alle disposizioni del **GDPR** (General Data Protection Regulation);
- Decreto Ministero Economia e Finanze 17.06.2014
"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 Ministero Economia e Finanze del 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 legislativo 22 gennaio 2004, n. 42, e successive modificazioni

-
- “Codice dei beni culturali e del paesaggio”;
D. Lgs. 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”;
DPCM 22 Febbraio 2013
 - “Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali”;
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;
 - DPCM 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.

[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.
- **ISO 15489-1:2016** Information Documentation – Records Management

[Torna al sommario](#)

4. RUOLI E RESPONSABILITÀ

Si elencano in questo capitolo le figure professionali che compongono il gruppo di lavoro del servizio di conservazione dei documenti del conservatore, al fine di garantire la corretta esecuzione del servizio. Le procedure organizzative si basano su standard mandatori ISO 27001 e ISO 9001.

Responsabile del servizio di conservazione

Il responsabile del servizio di conservazione è Luca Marconi, figura interna al soggetto conservatore. Non ci sono precedenti responsabili del servizio di conservazione.

Responsabile della funzione archivistica di conservazione.

Il responsabile della funzione archivistica di conservazione è Lucia Mattioli. La nomina è stata formalizzata in data 12/02/2015 e decorre dal giorno 12/02/2015. La nomina è stata firmata per accettazione dal responsabile designato.

Responsabile della sicurezza dei sistemi per la conservazione

Il responsabile della sicurezza dei sistemi per la conservazione è Claudio Della Ciana. La nomina è stata formalizzata in data 12/02/2015 e decorre dal giorno 12/02/2015. La nomina è stata firmata per accettazione dal responsabile designato.

Responsabile dei sistemi informativi per la conservazione

Il responsabile dei sistemi informativi per la conservazione è Fabio Grossi Gondi. La nomina è stata formalizzata in data 16/11/2018 e decorre dal giorno 16/11/2018. La nomina è stata firmata per accettazione dal responsabile designato.

Precedentemente il responsabile dei sistemi informativi per la conservazione è stato Stefano Biondi, con nomina formalizzata il 06/06/2016 e relativa revoca in data 16/11/2018, data in cui è subentrato Stefano Biondi.

Precedentemente il responsabile dei sistemi informativi per la conservazione è stato Michele Cirinei, con nomina formalizzata il 12/02/2015 e relativa revoca in data 06/06/2016, data in cui è subentrato Stefano Biondi.

Responsabile dello sviluppo e della manutenzione del sistema di conservazione.

Il responsabile dello sviluppo e della manutenzione del sistema di conservazione è Michele Cirinei. La nomina è stata formalizzata in data 12/02/2015 e decorre dal giorno 12/02/2015. La nomina è stata firmata per accettazione dal responsabile designato.

Amministratore di Sistema

L'Amministratore di Sistema precedentemente è stato Claudio Della Ciana, con nomina formalizzata il 12/02/2015 e la relativa revoca in data 08/10/2020, data che è subentrato a lui, Paolo Giuliani per richiesta segregazione e separazione dei ruoli richiesta per adeguamento AgID.

Responsabile e incaricati al trattamento dei dati

Il conservatore Plurima S.p.A. quando eroga servizi di conservazione, così come stabilito all'art. 6 comma 8 del DPCM 3 dicembre 2013, assume il ruolo di responsabile del trattamento dei dati e tutti i collaboratori assumono il ruolo di incaricati al trattamento. Ogni collaboratore del conservatore, incaricato al trattamento è nominato per iscritto. Il responsabile per il trattamento dei dati è individuato in Giampaolo Rachini. La nomina è stata formalizzata in data 12/02/2015 e decorre dal giorno 12/02/2015.

La nomina è stata revocata in data 15/07/2020, data in cui è stata effettuata comunicazione al Garante in cui Giampaolo Rachini è stato sostituito da Niccolò Paperini per conto della società Quality Management S.r.l.s.

La nomina è stata firmata per accettazione dal responsabile designato

Cronologia dei responsabili del servizio di conservazione dei documenti informatici

Nome e Cognome	Funzione	Data nomina	Data Revoca
Luca Marconi	Responsabile del servizio di conservazione	12/02/2015	----
Lucia Mattioli	Responsabile della funzione archivistica di conservazione	12/02/2015	----
Claudio Della Ciana	Responsabile della sicurezza dei sistemi per la conservazione	12/02/2015	----
Michele Cirinei	Responsabile dei sistemi informativi per la conservazione	12/02/2015	06/06/2016

Stefano Biondi	Responsabile dei sistemi informativi	06/06/2016	16/11/2018
Fabio Grossi Gondi	Responsabile dei sistemi informativi	16/11/2018	----
Michele Cirinei	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	12/02/2015	----
Paolo Giuliani	Amministratore di sistema	08/10/2020	-----
Giampaolo Rachini	Responsabile del trattamento dei dati personali	12/02/2015	15/07/2020
Niccolò Paperini	Responsabile del trattamento dei dati personali	15/07/2020	-----

[Torna al sommario](#)

5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

La seguente tabella indica i ruoli e le diverse attività svolte dai soggetti incaricati nell'ambito del servizio di conservazione dei documenti informatici.

Responsabile del servizio di conservazione	Responsabile dello sviluppo	Responsabile della sicurezza	Amministratore di Sistema	Responsabile dei sistemi informativi	Responsabile del trattamento dei dati personali	Responsabile della funzione archivistica di conservazione
Definizione e attuazione delle politiche complessive e 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 e le modalità di erogazione dei servizi di conservazione						

Oggetti sottoposti a conservazione

		Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza	Sovrintende alle risorse del sistema informativo e alle risorse dell'infrastruttura di rete locale e geografica.			
						Definizione e gestione del processo di conservazione
						Definizione del set di metadati di conservazione dei documenti
				Gestione dell'esercizio delle componenti hardware e software del sistema di		
				Monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente		
						Monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione e
						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
		Segnalazione delle eventuali difformità al responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive	Predisporre o verifica i sistemi informatici affinché questi supportino le misure di sicurezza stabilite dalla Plurima S.p.A.			
	Monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione					

Oggetti sottoposti a conservazione

	Pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione					
	Coordinamento dello sviluppo e manutenzione delle componenti software del sistema di conservazione					
				Segnalazione delle eventuali difformità degli SLA al responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie		
				Pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di		
				Controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al responsabile del		
					Garanzia del rispetto delle vigenti disposizioni in materia di trattamento	
	Interfaccia con l'ente produttore relativamente alle modalità di trasferimento dei documenti e dei fascicoli informatici in merito ai formati elettronici da usare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche					
					Garanzia che il trattamento dei dati affidati dai clienti avverrà nel rispetto delle istruzioni impartite dal	
	Gestione dello sviluppo di siti web e portali connessi al servizio di conservazione					

[Torna al sommario](#)

5.1. Organigramma

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

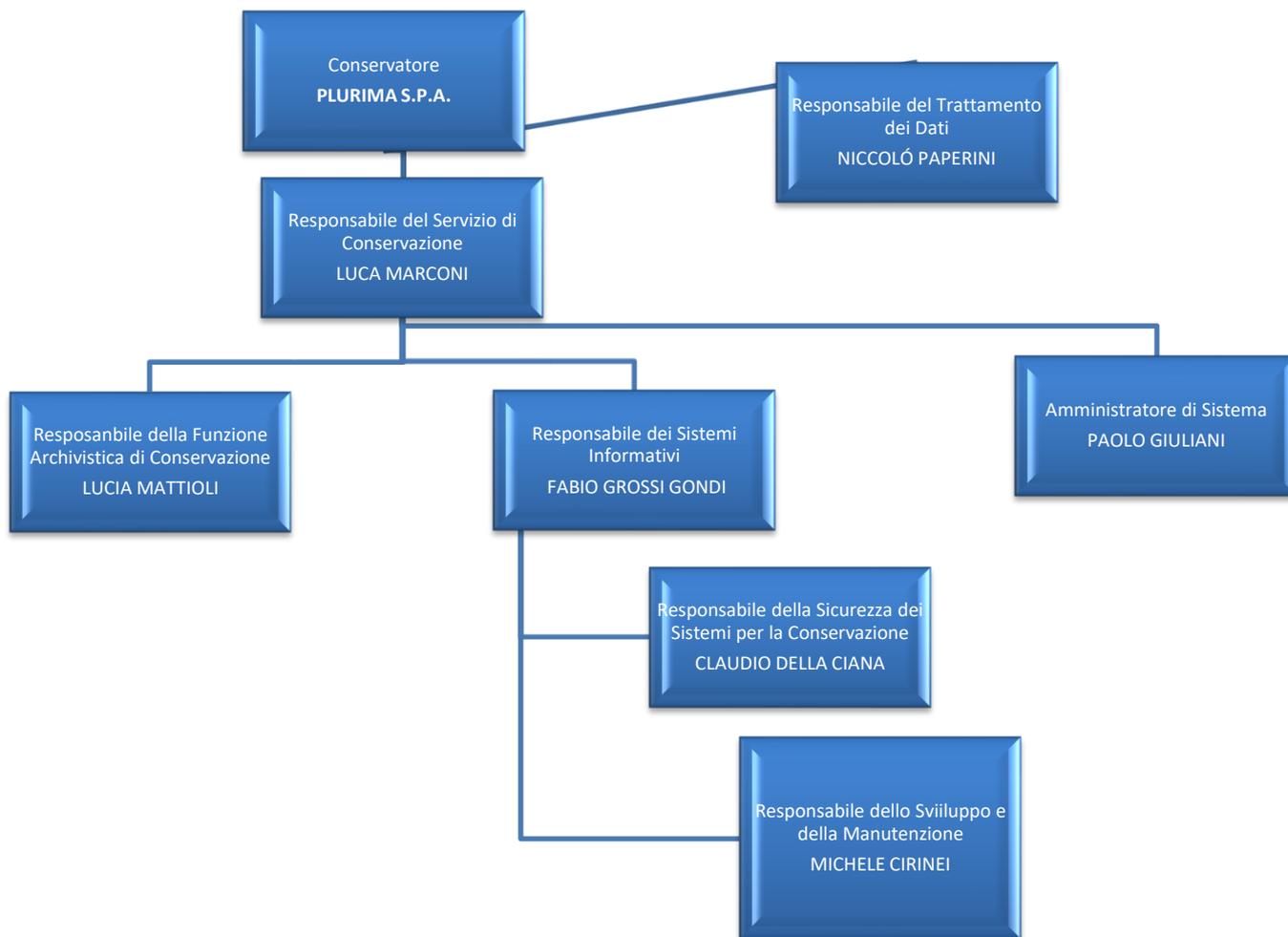


Figura 1: organigramma Plurima S.p.A.

[Torna al sommario](#)

5.2. Strutture organizzative

Il modello organizzativo adottato dal soggetto conservatore è strutturato in base a quanto stabilito dalle vigenti regole tecniche, DPCM 3 dicembre 2013 alla lettera b) comma 2 dell'articolo 5. Il sistema di conservazione opera secondo modelli organizzativi esplicitamente definiti che garantiscano la sua distinzione logica dal sistema di gestione documentale, se esistente. 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 accetti la responsabilità di conservare l'informazione e di renderla disponibile per una comunità di riferimento.

Seguendo quanto indicato dalle Regole tecniche vigenti e, sulla base dello stesso modello OAIS, si possono identificare i seguenti ruoli fondamentali: *Produttore* (o ente produttore o soggetto produttore), *Utente*,

*Responsabile della conservazione.***Produttore**

È il soggetto che affida la conservazione dei propri documenti informatici e le aggregazioni di documenti informatici al soggetto conservatore. Le informazioni di dettaglio sono esplicitate nel contratto di affidamento del servizio di conservazione. Secondo lo standard OAIS, il produttore è il ruolo svolto dalle persone o dai sistemi *client* che forniscono le informazioni da conservare. Possono svolgere il ruolo di produttore anche persone o sistemi interni all'OAIS, oppure altri OAIS.

I rapporti tra Plurima S.p.A. e il produttore sono concordati mediante un accordo formale (**specifiche tecniche** allegate al **contratto di affidamento**) che stabilisca le **tipologie documentarie**, i **metadati** oggetto di conservazione, i **formati** e le **modalità operative di versamento**.

Il responsabile di riferimento del produttore, per le amministrazioni pubbliche, è di norma individuato nel responsabile della gestione documentale. Il produttore è responsabile del contenuto del pacchetto di versamento (d'ora in poi SIP) ed è tenuto a trasmetterlo al soggetto conservatore, secondo quanto indicato nelle specifiche tecniche allegate al contratto di affidamento.

Il produttore ha accesso al sistema di conservazione direttamente dalla propria sede, tramite accesso da remoto. Il produttore, secondo quanto previsto nel contratto di affidamento del servizio di conservazione, si impegna a depositare i documenti informatici e le loro aggregazioni nei modi e nelle forme definite nelle *s p e c i f i c h e* tecniche, garantendone l'autenticità e l'integrità nelle fasi di produzione e di archiviazione. 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. Il produttore mantiene la titolarità e la proprietà dei documenti depositati.

Utente

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 direttamente acquisibile dai soggetti autorizzati. In termini OAIS la comunità degli utenti può essere definita come comunità di riferimento.

Nelle specifiche tecniche, documento allegato al contratto di affidamento del servizio di conservazione, vengono indicati quei soggetti abilitati dal soggetto produttore che possono accedere ai documenti versati dal produttore al conservatore. 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 da 31 a 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.

Fruitore

E' la persona, ente o sistema che usufruisce dei servizi offerti da un sistema per la conservazione di documenti informatici. Si intende tutti coloro a cui è permesso, tramite un accesso e relative credenziali, di usufruire di questo servizio nei termini stabiliti dalla legge e dal contratto in essere con l'ente produttore e, quindi, l'utilizzo dei dati conservati presso l'ente conservatore.

Responsabile del servizio della conservazione

È il soggetto conservatore o come soggetto che svolge le attività di conservazione, tramite il servizio di conservazione, così come stabilito nel contratto di affidamento del servizio. Le responsabilità del responsabile del servizio di conservazione sono definite all'art. 7 del DPCM 3 dicembre 2013. Nel contratto di affidamento del servizio di conservazione, sottoscritto tra il soggetto produttore e il soggetto conservatore vengono definite le attività e le responsabilità affidate al conservatore e quelle che rimangono a carico del produttore.

Organismo di tutela e vigilanza (in riferimento alle amministrazioni pubbliche)

Il Ministero per i beni e le attività culturali e del turismo (MiBACT) esercita funzioni di tutela e vigilanza dei

sistemi di conservazione degli archivi di enti pubblici o di enti privati dichiarati di interesse storico particolarmente importante e autorizza le operazioni di scarto e trasferimento della documentazione conservata ai sensi del D.lgs 42/2004.

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 mobili" compresi gli Archivi storici e di deposito è soggetto ad autorizzazione della Soprintendenza archivistica (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 privati per i quali sia intervenuta la dichiarazione ai sensi dell'articolo 13", sia che comporti o non comporti uno spostamento, rientra tra gli interventi soggetti ad autorizzazione della Soprintendenza archivistica (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), ai sensi del D.lgs 22 gen. 2004, n. 42, art.21, c. 1, lettera e)
- 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 a conservazione è parte integrante delle specifiche tecniche (allegato al contratto di affidamento del servizio di conservazione e al Piano della Sicurezza).

[Torna al sommario](#)

6.1. Oggetti conservati

Il sistema di conservazione di Plurima S.p.A. 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 trattati nel sistema nella forma di unità documentarie e fascicolo, specificamente descritte nel documento, oggetti sottoposti a conservazione e 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 anche per singola struttura (generalmente corrispondenti alle aree organizzative omogenee), consentendo di definire configurazioni e parametri ad hoc per ogni soggetto produttore, in base agli accordi stipulati all'atto della sottoscrizione del contratto di affidamento del servizio di conservazione.

Per mantenere anche nel sistema le informazioni relative alla struttura dell'archivio e dei relativi vincoli archivistici, le unità documentarie possono essere versate corredate di un set di metadati di profilo archivistico che include gli elementi identificativi e descrittivi del fascicolo, con riferimento alla voce di classificazione e l'eventuale articolazione in sotto fascicoli. Inoltre è gestita la presenza di classificazioni, fascicoli e sotto fascicoli secondari e collegamenti tra le diverse unità archivistiche e documentarie presenti nel sistema.

Le serie ed i fascicoli possono essere versati nel sistema quando sono completi e dichiarati chiusi, descritte 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 dal soggetto produttore.

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 (suddivise in titoli, classi e sottoclassi) 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, 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 è concordato un elenco di formati ammessi, che individua i formati che il sistema può accettare da ogni produttore e per ogni tipologia documentaria gestita. L'elenco dei formati ammessi è riportato (e gestito) nelle funzionalità "Amministrazione strutture versanti" del sistema ed è aggiornato continuamente in base alle esigenze del produttore. Le modalità con cui si procede a tale aggiornamento sono concordate con ciascun 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, vengano associate un insieme di informazioni (metadati) che ne permetta in futuro una facile reperibilità e 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.

È necessario, inoltre, ricordare che un sistema di conservazione che rispetti la normativa italiana, deve garantire il requisito di leggibilità degli oggetti dati conservati imposto dal comma 1 dell'art. 3 delle nuove regole tecniche e dal comma 1 dell'art. 44 del Codice dell'amministrazione digitale.

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 futura consultazione di tale oggetto.

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.

Classifichiamo quindi le informazioni sulla rappresentazione in:

- Strumenti per la leggibilità: tipicamente legati al formato dell’oggetto conservato (viewer);
- Informazioni sulla rappresentazione sintattica: tipicamente legate al formato dell’oggetto conservato (per esempio il documento di specifiche tecniche del formato del file);
- Informazioni sulla rappresentazione semantica: tipicamente legate alla descrizione archivistica dell’oggetto conservato (per esempio come leggere il contenuto di una fattura).

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 per tanto necessaria la capacità del software di generare, per ogni soggetto produttore, un insieme di descrizioni archivistiche “speciali” che diano modo al responsabile della conservazione di conservare le tre tipologie di informazioni sulla rappresentazione.

Nel sistema di conservazione distinguiamo tre descrizioni archivistiche speciali:

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

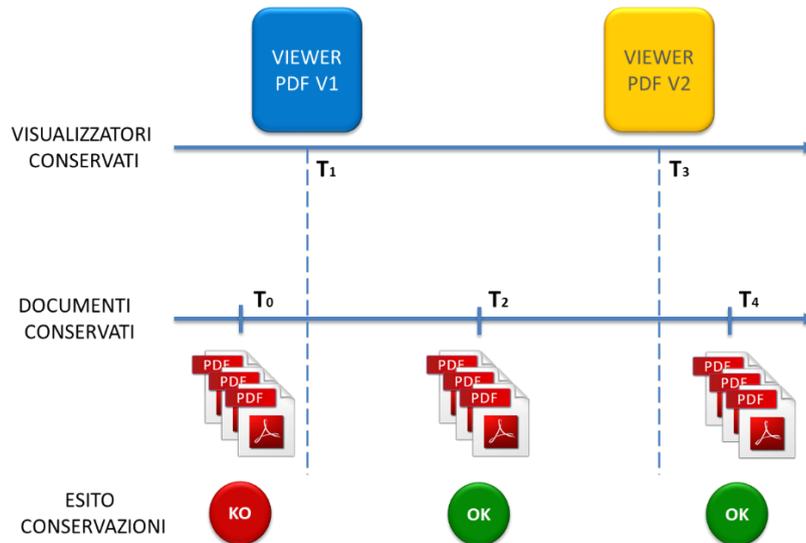


Figura 2: gestione dell'aggiornamento del viewer

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 il 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 soggetto 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.

Con Legal Archive® un soggetto produttore può scegliere, nella fase di negoziazione iniziale, alla stipula del contratto di affidamento del servizio, di 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 conservatore. Come anticipato, il sistema di conservazione dispone di tre modi per sottoporre un pacchetto di versamento:

- automatico - via web service
- semiautomatico - via file system
- manuale - via interfaccia web mediante upload manuale dei documenti.

Il sistema di versamento mette a disposizione del soggetto 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 soggetto 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 li stessi.

Una volta che i Pacchetti di versamento sono stati acquisiti, questi vengono trasformati in pacchetti di archiviazione (AIP).

Nel sistema di conservazione, 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.

- Dato generico.
- Dato personale.
- Dato sensibile.
- Dato giudiziario.

Così come definito dall'art 22 del Decreto Legislativo 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 individuato all'interno del soggetto produttore per concordare il set di metadati specifico per il fascicolo.

A parte i metadati obbligatori previsti dall'allegato 5 del DPCM del 3 dicembre 2013, il conservatore nell'allegato A "Oggetti sottoposti a conservazione".

[Torna al sommario](#)

6.3. Pacchetto di archiviazione

L'AIP è l'elemento fondamentale del sistema di conservazione, è il pacchetto informativo che racchiude in sé tutti gli elementi sufficienti e necessari per una conservazione a lungo termine.

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, ad una stessa pratica o ad uno stesso fascicolo tutti i documenti relativi ad 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.

La forza innovativa del sistema di conservazione risiede, oltre che negli elementi informativi che sono stati descritti sopra e che permettono una perfetta *compliance* al modello OAIS, anche nel livello descrittivo adottato.

Si assume che il livello di descrizione minimo che garantisca una gestione efficace di tutti i dati e metadati necessari per la conservazione e che permette quella necessaria contestualizzazione archivistica del documento, è rappresentato dall'unità archivistica. Essa rappresenta un livello di aggregazione minimo nel quale racchiudere le informazioni comuni a più documenti e contenuti digitali per relazionare i documenti afferenti al medesimo oggetto, pratica, procedimento o processo.

Tale livello diventa un file contenente i metadati identificativi e descrittivi, secondo il modello sopra proposto. Ovviamente 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.

Ciascun livello archivistico, così come previsto dalle modalità descrittiva multi livellare degli standard internazionali riconosciuti dalla comunità scientifica archivistica (v. ISAD/EAD), diverrà esso stesso oggetto di descrizione.

Si assume però che il livello di descrizione sufficiente e necessario per una corretta conservazione della risorsa digitale sia rappresentato proprio dall'unità archivistica (che può assumere di volta in volta la forma di aggregato logico legato a concetti di fascicolo, pratica o quant'altro). Tale livello, pertanto, diventa elemento conservato e incorporato (*embedded*) a tutti gli effetti all'AIP che contiene l'oggetto digitale che rappresenta il documento informatico da conservarsi a norma.

L'insieme, costituito dal *data object*, dai suoi metadati e dalle relazioni fra i documenti e fra questi e la struttura di archivio, costituisce il nucleo minimo e sufficiente della conservazione a lungo termine.

In concreto, una volta che i SIP sono stati accettati nel sistema, (e sono quindi stati oggetto di controlli sui metadati previsti dal contratto di servizio) essi sono pronti ad essere trasformati in AIP e quindi diventare l'oggetto della conservazione a lungo termine.

Il documento informatico, così trattato, sarà arricchito dei metadati previsti nel contratto di servizio, ma anche di tutti quei metadati tecnologici, relativi al documento stesso e al *viewer*, necessari per ostacolare l'obsolescenza tecnologica. Il pacchetto, così formato, sarà pronto per essere versato nei volumi di conservazione (VdC), previsti dalla normativa nazionale. Ogni VdC conterrà tutti gli AIP relativi ad un medesimo fascicolo digitale, le relazioni fra loro e l'AIP descrittivo del fascicolo stesso, nonché le relazioni fra il fascicolo e la struttura logica d'archivio. In tale maniera, si ritroveranno nello stesso VdC tutti gli elementi necessari e sufficienti per la corretta interpretazione del singolo AIP.

All'atto della conservazione verrà composto il pacchetto di archiviazione (AIP). Lo schema seguente mostra sinteticamente come sarà costruito l'AIP:

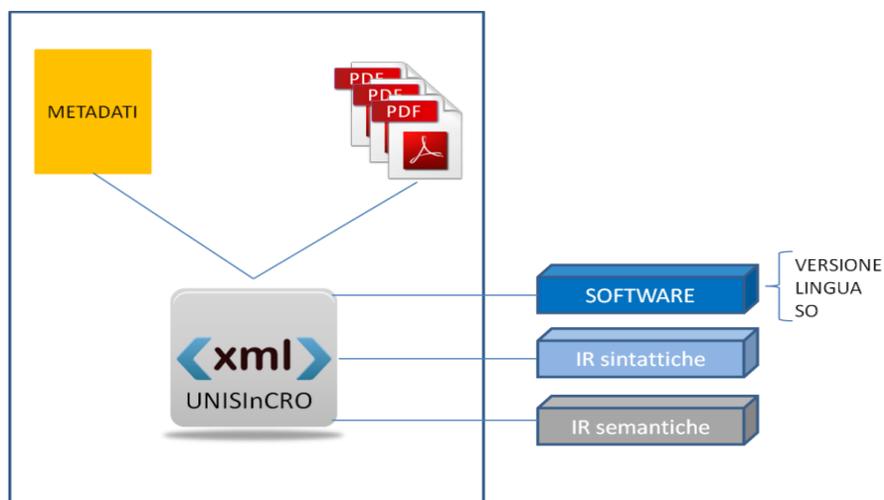


Figura 3: schema dell'AIP e dei collegamenti con le informazioni sulla rappresentazione

Ad ogni oggetto versato nel sistema di conservazione verrà associato:

- l'UID del software per la visualizzazione.
- l'UID del fascicolo delle informazioni sulla rappresentazione sintattica.
- l'UID del fascicolo delle informazioni sulla rappresentazione semantica.

In un sistema OAIS, si definisce pacchetto di archiviazione un pacchetto informativo composto dall'insieme delle informazioni che costituiscono l'obiettivo originario della conservazione e dalle relative informazioni sulla conservazione. 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 ed 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

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

Il sistema di conservazione erogato da Plurima S.p.A. è regolato dai seguenti documenti:

- Contratto di affidamento del servizio di conservazione;
- Specifiche tecniche (allegato al piano della sicurezza di Plurima Spa);
- 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.

[Torna al sommario](#)

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

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

Il modello di trasmissione del pacchetto informativo (SIP) dal soggetto produttore al soggetto conservatore viene concordato in fase contrattuale e descritto nelle specifiche tecniche.

In ogni caso il versamento potrà provenire:

- Web Services - caricamento automatico con interfacciamento di sistemi informatici.
- SFTP/VPN - caricamento via file system.
- Upload manuale del file - caricamento da interfaccia grafica.

La modalità di trasferimento via Web Service permette 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 di informazioni con i quali vengono passati come parametri i file e l'insieme dei metadati di ricerca a loro associati.

La modalità SFTP/VPN è costituita da un collegamento SFTP (Secure File Transfert Protocol) /VPN. Esso è un collegamento criptato punto-punto con la piattaforma del cliente e autorizzato dai firewall e dall'intero layer di sicurezza. Il Cliente ottiene le credenziali di autenticazione e può accedere dalla piattaforma tramite un set predefinito di IP statici. La modalità di versamento SFTP/VPN prevede che il soggetto produttore trasferisca il pacchetto di versamento in una posizione, all'interno del file system, accessibile al sistema di conservazione.

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

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 i metadati si susseguono in maniera ordinata: 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 è indispensabile conoscere la gerarchia tra i documenti del fascicolo.
- 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 m file (Unità Documentarie) tra loro indipendenti accompagnati dal relativo file dei metadati. Tutti gli m file appartengono alla stessa descrizione archivistica. Il file di indice avrà quindi m righe (1 riga di metadati 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 m file (Unità Documentarie) accompagnati dal relativo file dei metadati. Un numero x di questi m file sono allegati. I file principali, escludendo quindi gli allegati, appartengono tutti alla stessa descrizione archivistica. Il file di indice avrà quindi m righe (1 riga per ciascun file, comprendiamo sia i 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 di documenti di diversa tipologia ma afferenti allo stesso contesto di provenienza. I diversi oggetti vengono relazionati tra loro in funzione di alcuni metadati che fungono da nessi logici necessari, autonomi e determinati.

Il sistema di conservazione annota, in appositi log di sistema, il versamento dei pacchetti sui propri server tramite SFTP o VPN, registrando tutte le informazioni necessarie per l'identificazione di ogni singolo pacchetto di versamento.

Ogni volta che il processo effettua le operazioni di verifica sui pacchetti di versamento ricevuti, tutti gli eventi vengono appositamente tracciati all'interno di un log di sistema. Per maggiori dettagli si rimanda al manuale operativo.

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 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.
- In fine la conferma del versamento del pacchetto

Figura 4: 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).

[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 soggetto 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 composizione del pacchetto di versamento, sull'integrità dei file e sull'insieme dei metadati forniti.

Le validazioni sono concordate con il SP nel contratto di servizio di conservazione.

Le validazioni vengono 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 SP, 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 rispondenti alle caratteristiche configurate nella descrizione archivistica.

. Figura 5: finestra di configurazione metadati

La componente Engine (JLegalArchive-engine) è l'applicazione responsabile al trattamento dei pacchetti di versamento. Ogni pacchetto di versamento in ingresso subisce una serie di attività che vengono loggate in un file chiamato JLegalArchive-engine.log tale file viene generato ogni giorno e ha la seguente sintassi:

- data e ora al millisecondo;
- thread che esegue l'attività nel middleware;
- utente che esegue l'attività;
- ip address del server che esegue l'attività;
- process id;
- log level;
- classe attività;
- descrizione dell'accaduto.

[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 attestare l'avvenuta acquisizione e presa in carico del pacchetto di versamento (SIP), per ogni pacchetto accettato il sistema genera un rapporto di versamento che viene memorizzato nel database e associato logicamente al pacchetto di archiviazione cui si riferisce.

Il rapporto di versamento 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.

Il riferimento temporale può essere apposto, anche mediante marca temporale, secondo le specifiche tecniche concordate con il soggetto produttore.

Il rapporto di versamento è reso disponibile al soggetto produttore in varie modalità:

- è trasmesso in risposta al versamento del SIP;
- può essere richiesto utilizzando un apposito web service;

- può essere visualizzato e scaricato dall'interfaccia web del sistema di conservazione dagli utenti abilitati utilizzando le apposite funzionalità del sistema di conservazione.

[Torna al sommario](#)

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

Il SIP viene sottoposto ad una serie di controlli. Qualora il SIP non abbia superato i controlli, il sistema notifica l'avvenuto errore e dettaglia nei log la motivazione dell'errore.

Qualora il SIP non abbia superato tutti i controlli previsti, il sistema rifiuta l'intero il pacchetto di versamento e notifica all'utente l'avvenuto errore. La notifica avviene attraverso interfaccia grafica nell'area designata alle notifiche e attraverso un messaggio 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.

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

Lo stato del processo di conservazione del pacchetto di versamento che non ha superato la validazione viene impostato in "VALERR", via web service è possibile richiedere, a seguito de versamento, è possibile interrogare il sistema per ottenere lo stato del processo e ricevere la notifica dell'errore in modalità automatica.

Nel caso invece di versamento via file system, in caso di errore di validazione l'indice del pacchetto di versamento relativo al SIP rifiutato viene rinominato con l'aggiunta dell'estensione file "KO".

[Torna al sommario](#)

7.5. Preparazione e gestione del pacchetto di archiviazione

Legal Archive® garantisce la conformità a questo 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 salvato nella risorsa Archivio configurata a sistema.

E' possibile separare i versamenti in diversi pacchetti di archiviazione (AIP) dividendo i lotti 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 dei VIP, è richiesto il rispetto delle seguenti configurazioni:

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

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 che è 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 nel 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
- ID Descrizione Archivistica
- Anno
- ID volume di conservazione

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 (DIP) 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.

Nei contratti standard non è previsto da parte del soggetto conservatore né il rilascio di copie cartacee conformi agli originali digitali conservati.

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 e senza che su di esso debba gravare alcun particolare onere, il documento informatico conservato, qualora per un qualsiasi

motivo il soggetto produttore stesso abbia deciso di non acquistarlo 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 di 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 per l'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 via email ai diretti interessati.

L'accesso web consente al soggetto produttore di ricercare i documenti informatici versati, di effettuarne il download e di acquisire le prove delle attività di conservazione. Il produttore può richiedere i documenti e fascicoli informatici versati e conservati anche utilizzando gli appositi web services, chiamati secondo le modalità indicate nelle specifiche tecniche.

Il sistema di conservazione di Ifin Sistemi 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 all'indirizzo **<https://legalarchive.plurima.info>**

Il collegamento avviene tramite connessione sicura SSL con certificato rilasciato da Certification Authority che si attiene a standard internazionali.

L'accesso è consentito solo agli indirizzi ip autorizzati.

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 al 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.

Sarà cura del soggetto produttore fornire un'eventuale copia conforme, richiedendo la presenza di un pubblico ufficiale.

In merito alla produzione delle copie sarà cura del produttore fornire le copie e 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 la marca temporale apposte durante il processo di conservazione.

Tale procedura, non potendo essere effettuata stampando l'evidenza firmata della conservazione, deve necessariamente prevedere un supporto informatico.

[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 all'indirizzo **<https://legalarchive.plurima.info>**

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

Il collegamento avviene tramite connessione sicura SSL con certificato rilasciato da Certification Authority che si attiene a standard internazionali.

Una volta accreditato dal 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 può richiedere al responsabile del servizio di conservazione una copia, attraverso una funzione disponibile sul portale. Detta funzione consente di scaricare un file di tipo ISO o di tipo ZIP, attraverso il canale criptato SSL del portale.

Sarà così possibile per il soggetto produttore avere una copia del pacchetto di distribuzione (DIP) contenente i documenti conservati, il 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 produttore avrà cura di gestire tale scelta. Il 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 2, 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) ad 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 le massimario di selezione e scarto. Tale elenco di scarto, dopo una verifica da parte di Plurima S.p.A., viene comunicato al soggetto produttore che, utilizzando apposite funzionalità del sistema, può rifiutarlo (perché non intende procedere allo Scarto) o validarlo.

Nei casi previsti dalla legge, l'elenco di scarto così validato viene trasmesso dal soggetto produttore all'autorità di vigilanza che, in base alle norme vigenti, deve fornire il nulla-osta per lo scarto. Il soggetto produttore, una volta ricevuto il nulla-osta (che può essere concesso anche solo su una parte dell'elenco proposto), provvede ad adeguare, se necessario, l'elenco di scarto presente sul sistema alle decisioni dell'autorità. Una volta che l'elenco di scarto definitivo viene predisposto, il soggetto produttore lo valida e trasmette a Plurima S.p.A. la richiesta di procedere allo scarto. 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 scartati. Alla presenza di uno o più pacchetti, il processo avvisa il responsabile del servizio di conservazione, che avrà a disposizione una interfaccia che gli permetterà di decidere se scartare o meno i documenti. In caso affermativo, il processo di selezione e scarto provvederà ad 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 volume, una nota che indichi il fatto che il volume è stato sottoposto a 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 le regole che permettono successivamente di importare i pacchetti in un altro sistema OAIS *compliant*.

Allo stesso modo il sistema di conservazione è in grado di importare e archiviare pacchetti di distribuzione generati da altri sistemi OAIS *compliant*.

L'esportazione dei volumi di conservazione (pacchetti di archiviazione) può essere effettuata su supporto elettronico in formato ZIP oppure in formato ISO. Tali file, saranno messi a disposizione del cliente su server SFTP/VPN oppure memorizzati su supporto fisico e consegnati da personale autorizzato Plurima S.p.A.

Per rispondere ai requisiti richiesti dalla norma ISO27001, in quest'ultimo caso, i file memorizzati su supporto fisico trasportabile saranno criptati.

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

- Il 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 del dell'ex-cliente:
 - I file scaricati in formato ISO su server SFTP/VPN.
 - I file scaricati in formato ISO su supporto fisico anonimo, senza riferimenti al contenuto e consegnati da personale autorizzato di Ifin Sistemi.
- 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 verranno cancellati.

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

- I trasferimenti dei dati via web e via SFTP/VPN si appoggiano su protocolli sicuri cifrati (https ,SFTP, VPN).
- 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 esplicito 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 soggetto produttore nel sistema di conservazione.
- Il pacchetto di archiviazione (AIP): uno o più SIP sono 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. Il modello dati utilizzato dal sistema di conservazione prevede una strettissima aderenza a tale modello concettuale rivisitandolo ed ampliandolo con elementi di contestualizzazione provenienti dalla tradizione archivistica italiana.

Inoltre 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 a 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 di Plurima Spa è conforme allo standard OAIS.

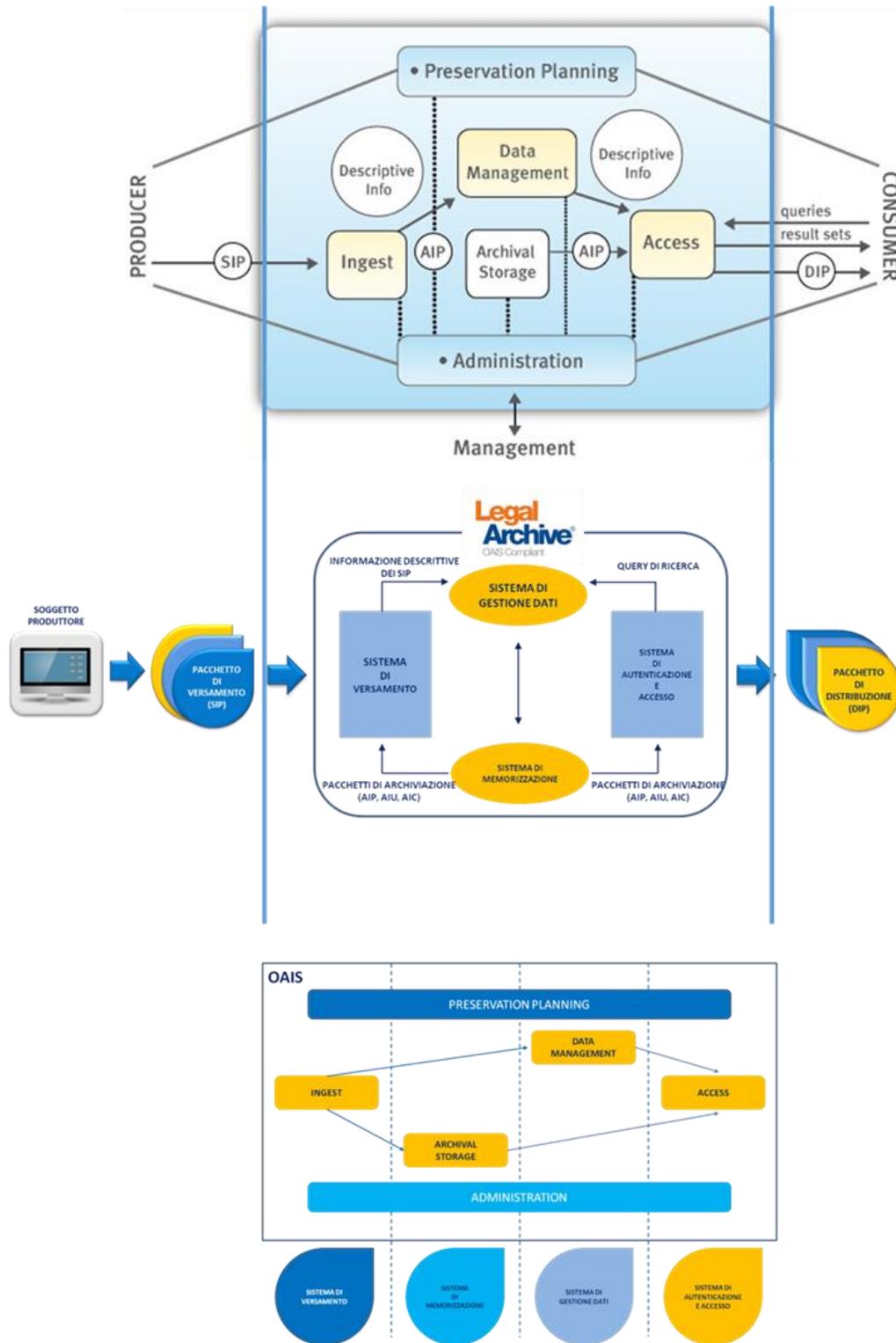


Figura 6 - Il modello OAIS

[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).

Sistema di Versamento (SV)

Il sistema di versamento, è la porta di ingresso dell'intero sistema ed ha il compito di ricevere i pacchetti di versamento da parte dei soggetti produttori, di verificarne l'aderenza al contratto di servizio di conservazione e ai requisiti di conservazione, di preparare i pacchetti di archiviazione ed 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, ad 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 soggetto 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 ed 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 ed 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 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) che può essere positivo o negativo. I documenti informatici, per i quali l’esito della convalida è risultato positivo, possono quindi essere inseriti in un volume di conservazione.

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 eseguiti sul pacchetto di versamento ed il loro rifiuto sono descritti al capitolo 7.3 7.4

Tipo Anomalia	Descrizione	Modalità di gestione
Mancata risposta al versamento	E’ 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 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	E’ 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	E’ il caso in cui 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 conservatore invia via e-mail una segnalazione dell’anomalia ai referenti del soggetto produttore, con i quali viene concordata la soluzione del problema.

Sistema di gestione dati (SGD)

Completata l’architettura, il sistema di gestione dati che 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 riteniamo questa componente essenziale per consentire ad un soggetto produttore di gestire al meglio il proprio deposito digitale.

Il soggetto produttore attraverso questo modulo, potrà vedere l'archivio come il complesso sistema di relazioni che in effetti è e, tramite le funzionalità che esso offre, potrà compiere tutte quelle operazioni tipicamente archivistiche, 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, Plurima S.p.A. 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 ad utenti dell'ente produttore.

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.

Sistema di accesso

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 accesso 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 volume di conservazione) 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.

Nel sistema di conservazione è possibile definire un numero illimitato di ruoli attraverso la definizione di profili d'uso che verrà illustrata più avanti.

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 ad 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 potrà 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.

Sistema di firma digitale

Il sottosistema per la firma digitale nel contesto della conservazione digitale si configura come elemento fondamentale per consentire di attuare la 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 volume, 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 ad 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 anche ad un pubblico ufficiale (o ruolo equivalente), deve essere apposta utilizzando un dispositivo di firma di un tipo approvato da AgID ed 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.
- 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 Actalis S.p.A.

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 ed 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.

I dispositivi HSM per la FEQ remota e la marcatura temporale sono siti al Datacenter Operativo primario sito in Arezzo, via P. Gobetti 96.

Actalis S.p.a per le procedure di disaster recovery si avvale del Datacenter sito in Ponte S. Pietro (BG), via S. Clemente 53 separato logicamente e separatamente da quello principale.

Actalis S.p.a garantisce ai dispositivi HSM ubicati presso il Datacenter operativo (riportate all'interno del "Manuale Operativo / Certification Practice Statement e Certificate Policy Versione 1.7"):

- controllo accessi fisici;
- continuità di alimentazione elettrica;
 - sistemi antincendio ed antiallagamento;
- ventilazione e condizionamento ottimali;
- connettività ad Internet ridondata e di capacità almeno doppia del minimo necessario

Gli elaboratori che offrono il servizio di VTEQ sono fisicamente protetti in modo da prevenire la possibilità di compromissioni fisiche grazie agli accorgimenti tecnici atti ad impedire accessi non autorizzati da persone e

danneggiamenti da eventi accidentale.

I server del sistema di validazione temporale elettronica qualificata sono ospitati in sale tecniche ad accesso controllato attraverso badge e/o fattore biometrico.

[Torna al sommario](#)

8.2. Componenti tecnologiche

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 (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.

Web Services: 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.

- **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.
- **Data Base**: la componente dedicata all'archiviazione delle informazioni associate al sistema e ai dati archiviati.
- **Repository**: la componente dedicata all'archiviazione degli oggetti digitali sottoposti a conservazione.

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 ad eventuali esigenze del produttore.

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

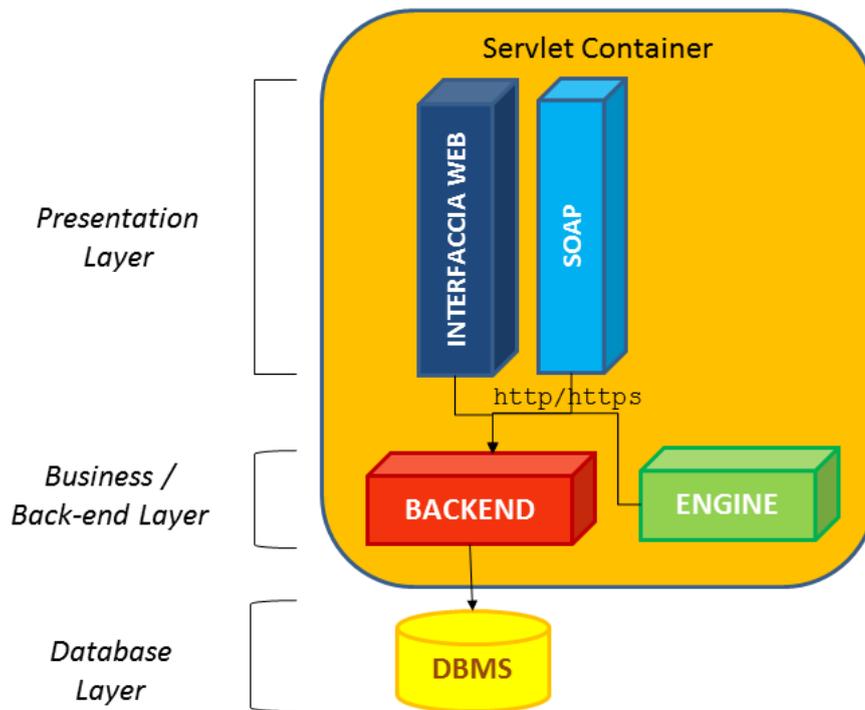


Figura 7: Componenti scalabili del sistema

[Torna al sommario](#)

8.3. Componenti fisiche

La struttura informatica di Plurima S.p.A. è articolata in tre siti:

La sede principale dove viene sviluppato il software, da dove viene erogata l'assistenza, da dove vengono erogati i servizi di conservazione dei documenti informatici.

La farm sistema di conservazione accreditato dove risiedono le infrastrutture di produzione del sistema di conservazione accreditato.

La farm dei servizi CA dove risiedono le infrastrutture di elaborazione di Firma Elettronica Qualificata Remota.

La farm di Disaster Recovery.

Sede principale Headquarter	Ifin Sistemi s.r.l. a socio unico. Via G. Medici 9/a 35138 Padova
Farm del sistema di conservazione accreditato	Plurima s.p.a. via Marie Curie n. 15 06073 Corciano (PG)

Sede primaria	
Farm dei servizi di CA	Actalis S.p.A. data center operativo primario ("IT1") via P. Gobetti 96 52100 Arezzo (AR)
Farm del DR Sede secondaria	Plurima s.p.a. via Pierobon n. 25 35010 Limena (PD)

Le figure sottostanti schematizzano l'infrastruttura virtuale ospitata nella server farm di produzione.

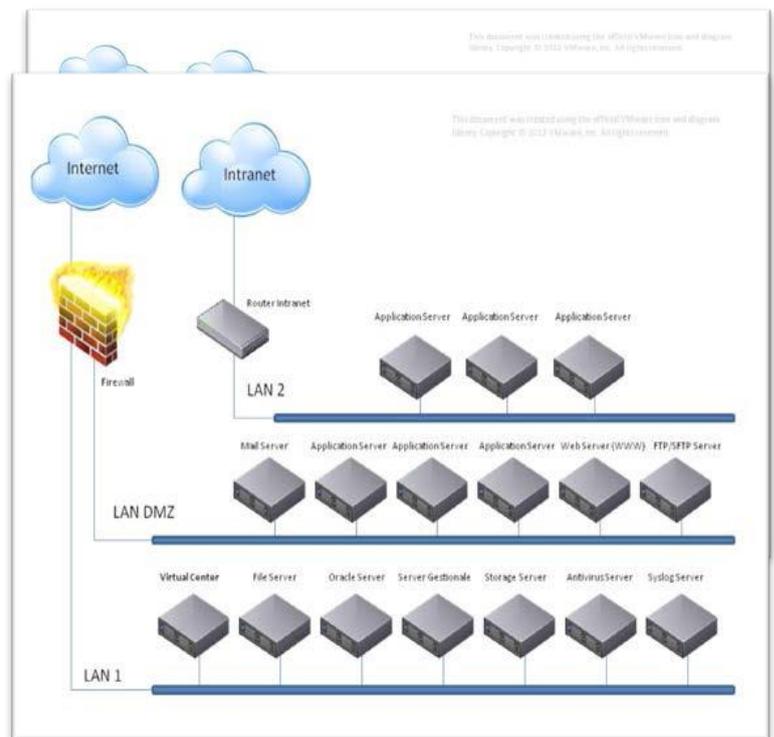
Il cuore del sistema è basato su di un cluster di server HP di ultima generazione, nei quali ogni nodo è dotato di doppio processore Intel per garantire la massima velocità e capacità di calcolo. Il cluster è basato su architettura VMWARE Vsphere. Si aggiungono:

Il Sistema di Conservazione, costituito da due server virtuali (database server e application server) ciascuno dotato di 16Gb di ram e 4 CPU core;

Il sistema di Disaster Recovery è allocato presso la sede di Limena (PD) a garanzia del mantenimento e dell'accesso ai dati gestiti e della Business Continuity. Il sistema, oltre al sottosistema storage già mirrorato al suo interno, prevede una finestra di allineamento giornaliera, assicurando la totale sicurezza e disponibilità dei dati, con uptime >99,95% e con garanzia di high availability, business continuity e disaster recovery su sito >200 Km. Il sistema di alimentazione della sala server è costituito da un apparato UPS On Line con batterie supplementari che garantiscono l'alimentazione di tutti i sistemi per almeno un'ora; la server farm è altresì dotata di gruppo elettrogeno diesel che permette di estendere ulteriormente l'autonomia, praticamente a tempo indeterminato.

Gruppo elettrogeno ed UPS sono sottoposti a controlli periodici per verificarne l'efficienza con rigorose procedure di controllo.

I collegamenti tra server e SAN sono in fibra ottica e ridondanti (doppio controller per ciascun server, doppio storage controller sulla SAN e collegamento multi-path tra server e SAN). Il sistema di monitoraggio del cluster (Virtual Center) provvede al monitoraggio automatico delle virtual machine e degli host VMWare.



La scalabilità del sistema di storage (SAN) è

garantita sia dall'espandibilità del sistema in uso sia dalla possibilità di aggiungere ulteriori sistemi di storage da collegare in fibra ottica al cluster VMWare. La scalabilità del cluster VMWare è garantita dalla possibilità di aggiungere ulteriori nodi al crescere della necessità di capacità di calcolo. La scelta dei sistemi operativi per l'acquisizione e la conservazione dei file si basa su soluzioni open source, ovvero sistemi operativi Red Hat Enterprise Linux e CentOS aggiornati all'ultima versione stabile. Per la conservazione logica dei dati la scelta si basa sulla piattaforma IFIN LegalArchive.

Per un maggiore dettaglio si rimanda al Piano per la Sicurezza e alla procedura **P. 4C "ISMS"**, che indica in dettaglio le diverse installazioni.



[Torna al sommario](#)

8.4. Procedure di gestione ed evoluzione.

Vengono descritte nel seguito tutte le procedure operative che permettono la corretta gestione e manutenzione del sistema di conservazione e l'evoluzione dello stesso.

Condizione e manutenzione del sistema di conservazione.

La conduzione e la manutenzione del sistema di conservazione è affidata al Responsabile dello sviluppo e della manutenzione del sistema di conservazione, in collaborazione con il responsabile della sicurezza dei sistemi per la conservazione.

E' stato definito ed attuato un processo di monitoraggio e di valutazione dell'uso delle risorse (**capacity management**), per analizzare e valutare le attuali prestazioni del sistema ed alla base delle proiezioni e definizione di future esigenze relative alle prestazioni od a nuove ed emergenti tecnologie tali da assicurare che le prestazioni del sistema di conservazione siano adeguate e conformi alle necessità, ai livelli di servizi concordati contrattualmente e nelle convenzioni e prevenivano l'obsolescenza tecnologica.

L'evoluzione del sistema di conservazione relativamente a modifiche organizzative di processi e tecnologici viene documentata nei verbali che compongono la ISO/IEC 27001:2013 relativa al sistema stesso.

Gestione e conservazione dei log (anche in accordo con l'ente Produttore).

Tutte le operazioni inerenti la conservazione, ivi inclusi gli accessi al sistema di conservazione, sono registrate in appositi file di log, i file di log sono sottoposti alle medesime procedure di backup e replica dei dati conservati (per il dettaglio degli eventi tracciati si faccia riferimento alla documentazione tecnica di Legal Archive® di proprietà di Ifin sistemi srl a socio unico).

Monitoraggio del sistema di conservazione.

Il sistema di conservazione è sottoposto a una serie di controlli automatici e manuali che ne garantiscono la disponibilità e la corretta funzionalità in particolare vengono monitorati i seguenti parametri di funzionalità attraverso il software PRTG network monitor:

- Raggiungibilità del servizio HTTP per la consultazione ed il versamento manuale;
- Raggiungibilità del servizio FTP/SFTP/VPN per il versamento in modalità batch;
- Uso medio della CPU;
- Stato della memoria;

- Stato dello storage;
- Stato di salute dell'hardware mediante accesso al software di autodiagnosi dei server (HP ILO);
- Sono stati implementati appositi alert automatici in caso di superamento di soglie critiche relative ai suddetti parametri.

Sempre in automatico vengono monitorati i sistemi di backup e disaster recovery remoto.

I processi di versamento vengono controllati manualmente con cadenza mensile e comunque su segnalazione di anomalie specifiche.

Monitoraggi interni su log

Periodicamente (ogni sei mesi) viene effettuato un controllo interno sul Sistema di Conservazione circa l'esatta creazione dei log al fine di rilevare eventi non conformi al funzionamento, questa revisione avviene tramite il modello **"Audit – Procedura generazione log"**. Il controllo viene effettuato in concomitanza dell'**"Indicatore ISMS Trimestrale"**.

Change management

Si faccia riferimento al sistema di change management di Legal Archive® di proprietà di Ifin Sistemi Srl.

Tramite l'ausilio del Sistema di Gestione per la Sicurezza delle Informazioni, Plurima S.p.a. gestisce gli eventi di change management attraverso la procedura **P. 4C "ISMS Gestione della Sicurezza delle Informazioni"** dove, al paragrafo 7.6 "Change Management", si descrivono le modalità di gestione del cambiamento.

Plurima Spa si assicura comunque di controllare eventuali evoluzioni e modifiche provenienti da Ifin Srl, si rimanda a **P. 4C** paragrafo **7.6 "Accettazione dei software e del trattamento delle informazioni"** e al Manuale delle procedure **P. 1B ISMS "Analisi dei rischi"**, mentre per il singolo contatto viene utilizzato il modello "Piano sviluppo e piano dei test" **M. 4C-1**.

Inoltre, le procedure **P. 6E "Procedura valutazione requisiti legislativi"** (con il registro **M. 6E-1 "Registro requisiti legali"**) e **P. 6B "NC AC AP"** assicurano il change management in caso di cambiamento della normativa e in caso di gestione di eventi o incidenti.

Monitoraggio sulla Capacità del Sistema di Conservazione

La percentuale di utilizzo dei sistemi di Plurima per la conservazione è periodicamente monitorata tramite l'**"Indicatore ISMS Trimestrale"** dove viene controllata la capacità del sistema e del suo funzionamento. L'azienda si riserva di poter sostenere un incremento del business di oltre il 50%, comunque non scendendo mai sotto il 20% di disponibilità. Il modello **M. 1B-4 "Asset Inventory"** permette il monitoraggio dettagliato per ogni componente a supporto dell'indicatore ISMS.

Revisione Utenze

I permessi di accesso alle funzionalità del sistema vengono controllati una volta al trimestre utilizzando "Indicatore ISMS Trimestrale".

Inoltre, la revisione avviene anche tramite l'analisi del comportamento dell'utente stesso nell'esplicazione delle proprie mansioni: oltre alla revisione periodica, sono individuati due possibili casi: nel primo, si revisiona in caso di danno avvenuto (la descrizione la possiamo trovare nella "Gestione della sicurezza delle Informazioni" P. 4C al capitolo 7.0 "Gestione degli eventi e degli incidenti per la sicurezza" mentre il modello utilizzato è M. 4A-11) e la variazione avviene tramite il modello M. 4A-36; nel secondo, invece, è sufficiente che non si verifichi la necessità di una variazione dei permessi di accesso.

Verifica periodica di conformità a normativa e standard di riferimento.

Il Responsabile del servizio di conservazione, il Responsabile della funzione archivistica di conservazione ed il Responsabile della privacy e sicurezza controllano costantemente l'evoluzione normativa e il quadro regolamentare per tenere il sistema e la corrispondente gestione al passo con le specifiche e i vincoli derivanti da leggi dello stato e regolamenti europei.

Supporti fisici per il trasferimento

Plurima Spa non utilizza supporti fisici per il trasferimento dei dati, quindi non è prevista l'applicazione del regolamento in questo ambito.

Il trasferimento è consentito esclusivamente tramite canale SFTP/SSH previo inserimento di credenziali forti al cliente per accesso al server, dopo la certezza del prelievo da parte del cliente, Plurima provvederà all'eliminazione di tali dati.

Piano di cessazione o modifica del servizio

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 le regole che permettono successivamente di importare i pacchetti in un altro sistema OAIS *compliant*.

Allo stesso modo il sistema di conservazione è in grado di importare e archiviare pacchetti di distribuzione generati da altri sistemi OAIS *compliant*.

L'esportazione dei volumi di conservazione (pacchetti di archiviazione) può essere effettuata su supporto elettronico in formato ZIP oppure in formato ISO. Tali file, saranno messi a disposizione del cliente su server SFTP/VPN oppure memorizzati su supporto fisico e consegnati da personale autorizzato Plurima S.p.A. Per rispondere ai requisiti richiesti dalla norma ISO27001, in quest'ultimo caso, i file memorizzati su supporto fisico trasportabile saranno criptati.

Al fine di assicurare la disponibilità dei dati e delle informazioni conservate in caso di dismissione o modifica attività si rimanda al **"Piano di cessazione/modifica attività"** .

[Torna al sommario](#)

9. MONITORAGGIO E CONTROLLI

Dal punto di vista tecnico il sistema 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 ed assicurare la riservatezza degli accessi.

Il monitoraggio e la valutazione dell'uso delle risorse (capacity management) considera tutte le diverse componenti del servizio, per assicurare una visione complessiva in ottica end to end.

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 i verifica interne e da parte di enti di certificazione esterni, atti a garantire che le procedure delineate al fine di garantire 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 di Plurima S.p.A.

[Torna al sommario](#)

9.1. Procedure di monitoraggio

Oltre al sistema di notifica 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 che riconosciute.

Stato dei processi

Il pannello "Stato dei processi" elenca i processi eseguiti ed 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.

Monitoraggio dei log

In aggiunta agli strumenti di monitoraggio immediato il software di conservazione traccia i log gli eventi di sistema e gli errori che vengono generati durante l'esecuzione dei processi.

Le diverse componenti logiche che soddisfano ai diversi aspetti funzionali, tracciano su log informazioni idonee all'analisi e al monitoraggio di sistema utilizzate per la gestione del sistema di conservazione.

- *Log di Back End*

Nel log relativo compilati dalla componente Back End vengono tracciate le informazioni associate alle diverse interrogazioni al sistema.

Per ciascuna di esse sono rese disponibili:

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

Di seguito sono indicate le richieste tracciate con le 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 volume di conservazione --> numero volume di conservazione.
- Dettaglio documento/fascicolo --> UID + lista metadati separati da pipe.
- Download --> UID + lista metadati separati da pipe.

- *Log di Engine*

La componente di Engine demandata all'elaborazione dei processi di conservazione traccia nel proprio log, per soggetto produttore, le informazioni associate alle elaborazioni.

Nelle righe di log sono resi disponibili:

- <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 come descritto nel piano per la sicurezza a cui si rimanda.

[Torna al sommario](#)

9.2. Verifica 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 schedulabile, 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

Il conservatore mette a disposizione del cliente un Servizio di Assistenza disponibile dal lunedì al venerdì dalle ore 9.00 alle ore 18.00 per garantire una tempestiva risposta sia alle problematiche tecniche sia a quelle applicative relative all'uso del sistema.

Un utente autorizzato dal soggetto produttore, potrà aprire una chiamata di assistenza (ticket) l'invio di una email comunicata alla sottoscrizione del contratto dove descrive il problema. L'Unità di Gestione, mette a disposizione un servizio in grado di assegnare ad ogni email un numero univoco per poter tracciare la chiamata.

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

Distinguiamo due tipi di anomalie:

- dovute a bug del software
- dovute a malfunzionamento dell'impianto

Anomalia dovuta a 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	Presenza 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 ed 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 dovute a 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 lotti ricevuti

Comunicazione eventuali anomalie nei lotti 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 lotti ricevuti
Invio ai clienti della segnalazione di errori che causano il blocco dell'elaborazione dei lotti da conservare.	Entro il giorno lavorativo successivo (festivi esclusi) dalla ricezione del pacchetto di versamento.	99,5% dei lotti ricevuti
Avvio rielaborazione dei lotti eventualmente impattati dall'anomalia.	Entro il giorno lavorativo successivo (festivi esclusi) dalla risoluzione anomalia (dalla data comunicazione al Cliente).	99,5% dei lotti 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 ferialo (Lun. - Ven.).	N.A.
Disponibilità dei servizi di caricamento (upload) <ul style="list-style-type: none"> • Upload Manuale • Modalità SFTP/VPN • 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

Qui di seguito sono riportate le condizioni in presenza delle quali, non sarà imputabile a Plurima il verificarsi di eventuali disservizi:

- cause di forza maggiore e cioè eventi che, oggettivamente, impediscano al personale di Plurima Spa intervenire per eseguire le attività poste dal contratto a carico della stessa Plurima S.p.A. (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 di 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 email 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 ad 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 di Plurima e comunque fuori dal suo controllo (in via meramente esemplificativa guasti o problemi).

[Torna al sommario](#)