

Ifin Sistemi srl a socio unico

Manuale di Conservazione

EMISSIONE DEL DOCUMENTO CORRENTE

Azione	Data	Nominativo	Funzione
Redazione	13/07/2021 modifica	Giovanni Maria Martingano	Responsabile Servizio di conservazione
Verifica	13/07/2021 modifica	Giovanni Maria Martingano	Responsabile Servizio di conservazione
Approvazione	13/07/2021 modifica	Giovanni Maria Martingano	Responsabile Servizio di conservazione

REGISTRO DELLE VERSIONI

N° Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
Versione 01 Revisione 02	30/09/2015	Aggiornamento secondo ultimo indice proposto da AgID	
Versione 02 Revisione 02	09/02/2016	Aggiornamento secondo indice e formati proposti da AgID	
Versione 03 Revisione 02	23/06/2016	Aggiornamento del Capitolo 6 Rettifica terminologia	
Versione 04 Revisione 03	11/01/2018	Aggiornamento delle definizioni (Cap. 2). Aggiornamento dei ruoli (Cap. 4). Struttura organizzativa (Cap. 5). Organigramma (Par. 5.1). Sistema per l'apposizione della marca temporale (Par. 8.1). Aggiornamento ruolo Responsabile della sicurezza per il sistema di conservazione. Modifica nominativi tabella "Emissione del documento corrente".	
Versione 05 Revisione 01	18/06/2018	Aggiornamento dei ruoli (CAP.4)	

		<p>Struttura organizzativa (Cap.5)</p> <p>Organigramma (Par. 5.1)</p> <p>Aggiornamento ruolo Responsabile della sicurezza per il sistema di conservazione.</p> <p>Aggiunta del paragrafo 7.10 Cessazione delle attività di conservazione</p> <p>Aggiornato paragrafo 8.3 Componenti fisiche sistema di conservazione accreditato.</p>	
Versione 05 Revisione 02	27/11/2018	<p>Aggiornato paragrafi 3.1, 4.1, 5.2, 6.2 di adeguamento riferimenti normativi privacy.</p> <p>Rettificato paragrafo 8.3 componenti fisiche sistema di conservazione accreditato.</p>	
Versione 05 Revisione 03	17/01/2019	<p>Rettificato paragrafo 8.3 componenti fisiche sistema di conservazione accreditato.</p>	Inesattezze nel paragrafo
Versione 05 Revisione 04	30/09/2020	<p>Aggiornamento paragrafo 3.1.</p> <p>Aggiornamento dei Ruoli e responsabilità (Cap. 4).</p> <p>Aggiornamento della Struttura organizzativa per il servizio di conservazione (Cap. 5).</p> <p>Aggiornamento organigramma paragrafo 5.1.</p> <p>Rettificati i paragrafi 7.6 e 7.7 che contenevano commenti.</p> <p>Aggiornamento 7.10. Cessazione delle attività di conservazione paragrafo 7.10</p>	
Versione 05 Revisione 05	02/04/2021	<p>Aggiornamento dei Ruoli e responsabilità (Cap. 4).</p> <p>Aggiornamento della Struttura organizzativa per il servizio di conservazione (Cap. 5).</p> <p>Aggiornamento organigramma (par. 5.1).</p> <p>Modifica componenti fisiche (par. 8.3)</p>	È stato aggiunto il Servizio di storage S3 di Amazon Web Services, è stata modificata l'ubicazione della Farm di Disaster Recovery (in Italia), nonché sono stati aggiornati gli schemi dell'infrastruttura (par. 8.3).
Versione 06 Revisione 01	13/07/2021	<p>Aggiornamento dei Ruoli e responsabilità (Cap. 4).</p>	Modifica del nominativo del Responsabile del servizio di conservazione



		Aggiornamento della Struttura organizzativa per il servizio di conservazione (Cap. 5). Aggiornamento organigramma (par. 5.1).	
--	--	--	--

SOMMARIO

1. Scopo e ambito del documento	6
2. Terminologia (Glossario, Acronimi).....	7
3. Normativa e standard di riferimento	14
3.1. Normativa di riferimento	14
3.2. Standard di riferimento.....	15
4. Ruoli e responsabilità	16
4.1. Responsabile e incaricati al trattamento dei dati.....	16
5. Struttura organizzativa per il servizio di conservazione	17
5.1. Organigramma.....	18
5.2. Strutture organizzative.....	19
6. Oggetti digitali sottoposti a conservazione.....	21
6.1. Oggetti conservati.....	21
6.2. Pacchetto di versamento (SIP)	25
6.3. Pacchetto di Archiviazione (AIP)	27
6.4. Pacchetto di distribuzione (DIP).....	30
7. Processo di conservazione	32
7.1. Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico	32
7.2. Verifiche effettuate sui pacchetti di versamento e sugli oggetti in esso contenuti	34
7.3. Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico	35
7.4. Rifiuto del pacchetto di versamento	36
7.5. Preparazione e gestione del pacchetto di archiviazione (AIP).....	36
7.6. Preparazione e gestione del pacchetto di distribuzione (DIP) ai fini dell'esibizione.....	37
7.7. Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti	39
7.8. Scarto dei pacchetti di archiviazione	40
7.9. Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori	40
7.10. Cessazione delle attività di conservazione	41
8. Sistema di conservazione.....	42
8.1. Componenti logiche	44
8.2. Componenti Tecnologiche	47
8.3. Componenti fisiche	49
8.4. Procedure di gestione e di evoluzione.....	52

9. Monitoraggio e controlli	54
9.1. Procedure di monitoraggio	54
9.2. Verifica dell'integrità degli archivi	55
9.3. Soluzioni adottate in caso di anomalie	55

1. Scopo e ambito del documento

Il presente documento costituisce il manuale di conservazione di Ifin Sistemi srl a socio unico e ha lo scopo di descrivere il sistema di conservazione dei documenti informatici adottato dall'azienda. In particolare il presente manuale descrive il modello organizzativo della conservazione adottato, illustra nel dettaglio l'organizzazione della struttura che realizza il processo di conservazione, definendo i soggetti coinvolti e i ruoli svolti dagli stessi nel modello organizzativo di funzionamento dell'attività di conservazione e descrive inoltre il processo, le architetture e le infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione. Il software utilizzato per la gestione del processo di conservazione dei documenti informatici è Legal Archive®. Il sistema di conservazione ha come oggetto la realizzazione di un insieme di funzionalità atte a consentire la conservazione dei documenti informatici e a fornire un supporto alle figure coinvolte nel processo di conservazione.

Il presente manuale è così localizzato:

- una copia del manuale della conservazione è archiviata presso l'ente produttore;
- una copia del manuale della conservazione è conservata presso il conservatore.

Dati identificativi del conservatore:

Denominazione	Ifin Sistemi srl a socio unico
Indirizzo	Via Giacomo Medici 9/A Padova
Legale Rappresentante	Roberto Reccanello
Referente tecnico (nome e cognome) cui rivolgersi in caso di problemi tecnico-operativi	Andrea Rossi
E-mail del referente tecnico	andrea.rossi@ifin.it
N° telefono/fax	0495001500
Sito web istituzionale	www.ifin.it
E-mail istituzionale	ifin@ifin.it

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 digitali sottoposti a conservazione e ai rapporti con i soggetti produttori, il presente manuale dev'essere integrato con le specifiche tecniche, documento allegato al contratto di affidamento del servizio di conservazione, redatto con ogni soggetto produttore, in cui si definiscono le specifiche operative, le modalità di descrizione e versamento nel sistema di conservazione digitale delle tipologie documentarie e delle aggregazioni documentali informatiche, oggetto di conservazione.

Il presente manuale di conservazione è un documento informatico.

[Torna al sommario](#)

2. Terminologia (Glossario, Acronimi)

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

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

Glossario dei termini	
TERMINE	DEFINIZIONE
Accesso	operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici.
Accreditamento	riconoscimento da parte dell'Agenzia per l'Italia digitale del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione.
Affidabilità	caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico.
Aggregazione documentale informatica	aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente.
Allegato	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.
Annesso	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.
Application server	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 <i>enterprise</i> , con alto grado di complessità, spesso orientate per il web (applicazioni web).
Archivio	complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività.
Archivio informatico	archivio costituito da documenti informatici, fascicoli informatici nonché da aggregazioni documentali informatiche gestiti e conservati in ambiente informatico.
Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.
Autenticità	caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico.

Base di dati	collezione di dati registrati e correlati tra loro.
Certificatore accreditato	soggetto, pubblico o privato, 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.
Codice eseguibile	insieme di istruzioni o comandi software direttamente elaborabili da sistemi informatici.
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.
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	insieme delle informazioni che costituisce l'obiettivo originario della conservazione. E' composto dall'oggetto-dati e dalle informazioni di rappresentazione. [da OAIS]
Coordinatore della gestione documentale	responsabile della definizione di criteri uniformi di classificazione ed archiviazione, nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall' art. 50 c.4 DPR 445/00, nei casi di amministrazioni che abbiano istituito più aree organizzative omogenee.
Copia analogica di documento informatico	documento analogico avente contenuto identico a quello del documento informatico da cui è tratto.
Copia di sicurezza	copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell'art.12 del DPCM 3 dicembre 2013 riguardo il sistema di conservazione.
Destinatario	identifica il soggetto/sistema al quale il documento informatico è indirizzato.
Duplicazione dei documenti informatici	produzione di duplicati informatici.

Data center	struttura utilizzata per ospitare computer e componenti associati quali dispositivi di telecomunicazioni e di <i>storage</i> , in generale con adeguati livelli di prestazioni e di sicurezza.
Disaster recovery	insieme delle misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi di business per imprese, associazioni o enti, a fronte di gravi emergenze che ne intacchino la regolare attività.
Esibizione	operazione che consente di visualizzare un documento conservato e di ottenerne copia.
Evidenza informatica	una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.
Fascicolo informatico	aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del Codice.
File di indice	indice dell'AIP, file XML che contiene tutti gli elementi del pacchetto di archiviazione, derivati sia dalle informazioni contenute nel SIP (o nei SIP) trasmessi dal produttore, sia da quelle generate dal sistema di conservazione nel corso del processo di conservazione.
Formato	modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
Funzione di hash	una funzione matematica che genera, a partire da una evidenza informatica, un'impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
Generazione automatica di un documento informatico	formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni.
Identificativo univoco	sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione.
Immodificabilità	caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso.
Impronta	la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di un'opportuna funzione di hash.
Insieme minimo di metadati del documento informatico	complesso dei metadati, la cui struttura è descritta nell'allegato 5 del presente decreto, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta.
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 per 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 riguardo il sistema di conservazione.
Marca temporale	sequenza di caratteri che rappresentano una data e/o un orario per accertare l'effettivo avvenimento di un certo evento. La data è di solito presentata in un formato compatibile, in modo che sia facile da comparare con un'altra per stabilirne l'ordine temporale. La pratica dell'applicazione di tale marca temporale è detto <i>timestamping</i> .
Memorizzazione	processo di trasposizione su un qualsiasi supporto idoneo, attraverso un processo di elaborazione, di documenti analogici o informatici.
Metadati	insieme di dati associati a un documento informatico, 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 delle regole tecniche sul sistema di conservazione 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.
Producer	produttore: le persone o i sistemi client che forniscono le informazioni da conservare. (OAIS – ISO 14721)
Produttore	persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale.
Rapporto di versamento	documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.
Responsabile del servizio di conservazione	soggetto individuato dai profili professionali, indicato nell'allegato alla circolare n. 65 del 10 aprile 2014, AGID.
Responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi	dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione.
Responsabile della conservazione	soggetto responsabile dell'insieme delle attività elencate nell'art. 8, comma 1 delle regole tecniche del sistema di conservazione.
Responsabile del trattamento dei dati	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.
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	<p>unità archivistiche o unità documentarie ordinate secondo un sistema di classificazione o conservati insieme perché:</p> <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. <p>(fonte: ISAD)</p>
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.
Soggetto produttore	persona fisica o giuridica, la pubblica amministrazione o l'ente titolare dei documenti informatici da conservare.
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 di descrizione	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 un'unità elementare di una serie. Un documento o un insieme di documenti, a prescindere dai loro caratteri fisici, considerati come un tutto unico e, come tali, costituenti l'oggetto di una singola descrizione [da ISAD].
Unità documentaria	unità minima, concettualmente non divisibile, di cui è composto un archivio, per esempio, una lettera, un memorandum, un rapporto, una fotografia, una registrazione sonora. (ISAD (G))
Versamento	azione di trasferimento di SIP dal produttore al sistema di conservazione.
Versamento agli archivi di stato	operazione con cui il responsabile della conservazione di un organo giudiziario o amministrativo dello Stato effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali.
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);
- **DNS:** Domain Name System;
- **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 semantica;
- **Irsi:** Informazioni sulla rappresentazione sintattica;
- **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.

[Torna al sommario](#)

3. Normativa e standard di riferimento

3.1. Normativa di riferimento

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

- **Codice civile (Libro Quinto del Lavoro, Titolo II del lavoro nell'impresa, Capo III delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili, art. 2215 bis)** - Documentazione informatica;
- **Legge n. 241 del 7 agosto 1990, n. 241 e s.m.i.**
"Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi";
- **Decreto legislativo 30 giugno 2003, n. 196 e s.m.i.**
"Codice in materia di protezione dei dati personali";
- **Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016**
"relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)", applicabile in tutti gli Stati membri a partire dal 25 maggio 2018;
- **Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445**
"Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa";
- **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)";
- **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";
- **Regolamento (UE) 910/2014 eIDAS**
"in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno".

[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 metadati del Dublin Core.

[Torna al sommario](#)

4. Ruoli e responsabilità

Si elencano in questo capitolo i nominativi delle persone che ricoprono i ruoli elencati nella tabella del capitolo 5 del presente manuale 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 Giovanni Maria Martingano.

Cronologia dei responsabili del servizio di conservazione:

Nome e Cognome	Funzione	Data nomina	Data Revoca
Roberto Reccanello	Responsabile del servizio di conservazione	//	10/11/2017
Antonio Taschin	Responsabile del servizio di conservazione	10/11/2017	13/07/2021
Giovanni Maria Martingano	Responsabile del servizio di conservazione	13/07/2021	//

Responsabile della funzione archivistica di conservazione:

Il responsabile della funzione archivistica di conservazione è Armando Bartucci. La nomina è stata formalizzata in data 01/04/2021 e decorre dal giorno 01/04/2021. 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 Stefano Solidoro. La nomina è stata formalizzata in data 30/09/2020 e decorre dal giorno 30/09/2020. 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 Andrea Rossi. La nomina è stata formalizzata in data 12/09/2014 e decorre dal giorno 12/09/2014. La nomina è stata firmata per accettazione dal responsabile designato.

Responsabile dello sviluppo e della manutenzione del sistema di conservazione:

Il responsabile dello sviluppo e della manutenzione del sistema di conservazione è Fabio Canevarolo. La nomina è stata formalizzata in data 30/09/2020 e decorre dal giorno 30/09/2020. La nomina è stata firmata per accettazione dal responsabile designato.

Responsabile del trattamento dei dati personali

Il responsabile per il trattamento dei dati personali per il sistema di conservazione è individuato in Stefania Rampazzo. La nomina è stata formalizzata in data 10/11/2017 e decorre dal giorno 10/11/2017.

4.1. Responsabile e incaricati al trattamento dei dati

Il conservatore I fin Sistemi 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 autorizzati dal Responsabile del trattamento assumono il ruolo di incaricati. Entrambi i ruoli sono nominati in conformità alla legge italiana (D.Lgs 196/2003 s.m.i.) e dell'Unione Europea (Regolamento UE 2016/679).

La nomina è stata firmata per accettazione dal responsabile designato.

[Torna al sommario](#)

5. Struttura organizzativa per il servizio di conservazione

Nella seguente tabella sono indicati i ruoli e le diverse attività svolte dai diversi soggetti incaricati nell'ambito del servizio di conservazione dei documenti informatici.

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo	Eventuali deleghe
Responsabile del servizio di conservazione	Giovanni Maria Martingano	<ul style="list-style-type: none"> 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. 	13/07/2021	
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Fabio Canevarolo	<ul style="list-style-type: none"> Monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione; Pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione; Coordinamento dello sviluppo e manutenzione delle componenti software del sistema di conservazione; 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; Gestione dello sviluppo di siti web e portali connessi al servizio di conservazione. 	30/09/2020	
Responsabile della sicurezza dei sistemi per la conservazione	Stefano Solidoro	<ul style="list-style-type: none"> Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; Segnalazione delle eventuali difformità al responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive. 	30/09/2020	
Responsabile dei sistemi informativi	Andrea Rossi	<ul style="list-style-type: none"> Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione; Monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore; Segnalazione delle eventuali difformità degli SLA al responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive; Pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione; Controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al responsabile del servizio di conservazione. 	12/09/2014	
Responsabile del trattamento dei dati personali	Stefania Rampazzo	<ul style="list-style-type: none"> Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; Garanzia che il trattamento dei dati affidati dai clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e riservatezza. 	10/11/2017	
Responsabile della funzione archivistica di conservazione	Armando Bartucci	<ul style="list-style-type: none"> Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; Definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici; 	01/04/2021	

		<ul style="list-style-type: none"> • Monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione; • Collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza; • Monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione; • Redazione e supervisione del Manuale di conservazione con i responsabili del servizio. 		
--	--	---	--	--

Di seguito sono storicizzate le figure professionali che hanno ricoperto dei ruoli nell'organigramma sopra indicato.

Cognome e Nome	Ruolo	Data nomina	Data revoca
Viviani Sebastiano	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	12/09/2014	12/06/2015
Taschin Antonio	Responsabile del trattamento dei dati personali	12/09/2014	30/10/2017
Stefania Rampazzo	Responsabile della funzione archivistica di conservazione	12/09/2014	10/11/2017
Davide Sartor	Responsabile della sicurezza dei sistemi per la conservazione	12/09/2014	29/12/2017
Gianluca Mogliani	Responsabile della sicurezza dei sistemi per la conservazione	29/12/2017	30/05/2018
Ricca Raffaele	Responsabile della sicurezza dei sistemi per la conservazione	31/05/2018	30/09/2020
Taschin Antonio	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	12/06/2015	30/09/2020
Giacomelli Margherita	Responsabile della funzione archivistica di conservazione	10/11/2017	01/04/2021
Taschin Antonio	Responsabile del servizio di conservazione	10/11/2017	13/07/2021

[Torna al sommario](#)

5.1. Organigramma

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



Figura 1: organigramma I fin Sistemi

[Torna al sommario](#)

5.2. Strutture organizzative

Ifin Sistemi eroga servizi di conservazione utilizzando soluzioni tecnologiche che soddisfano i requisiti di alta affidabilità, richiesti dalla normativa. Il modello organizzativo adottato dal conservatore è idoneo a gestire il servizio di conservazione in base a quanto stabilito dalle vigenti regole tecniche, DPCM 3 dicembre 2013 all'art. 5 comma 2 lettera b). Il sistema di conservazione opera secondo modelli organizzativi esplicitamente definiti che garantiscono la sua distinzione logica dal sistema di gestione documentale, se esistente. Il modello organizzativo del conservatore è stato realizzato tenendo conto del modello di riferimento 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 di riferimento OAIS, il sistema identifica i seguenti ruoli fondamentali: produttore, utente e responsabile del servizio di conservazione.

Produttore: è la persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con il responsabile della gestione documentale.

Il produttore si impegna a depositare i documenti informatici e le loro aggregazioni documentali informatiche nei modi e nelle forme definite, garantendone l'autenticità e l'integrità nelle fasi di formazione e di archiviazione, effettuate nel rispetto delle norme sulla formazione e sui sistemi di gestione dei documenti informatici. In particolare, garantisce che il trasferimento dei documenti informatici venga realizzato utilizzando formati compatibili con la funzione di conservazione e rispondenti a quanto previsto dalla normativa vigente. Si impegna, inoltre, a depositare e mantenere aggiornati gli strumenti di ricerca e gestione archivistica elaborati a supporto della formazione dei documenti informatici e della tenuta degli archivi digitali. I rapporti con l'ente produttore sono concordati mediante un accordo formale (**specifiche tecniche** allegate al **contratto di affidamento**) che stabilisce le **tipologie documentarie**, i **metadati** oggetto di conservazione, i **formati** e le **modalità operative di versamento**.

Nelle pubbliche amministrazioni, il ruolo di responsabile della conservazione può essere svolto dal responsabile della gestione documentale ovvero dal coordinatore della gestione documentale, ove nominato. Il produttore è responsabile del contenuto del pacchetto di versamento (d'ora in poi SIP) ed è tenuto a trasmetterlo al 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 anche 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 specifiche 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. L'ente produttore mantiene la titolarità e la proprietà dei documenti depositati.

Utente: è una persona, ente o sistema che interagisce con i servizi di un sistema per la conservazione di documenti informatici, come indicato nelle vigenti regole tecniche (DPCM 3 dicembre 2013, allegato 1, Glossario).

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 del modello di riferimento 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 ed in conformità alla legge italiana (D.Lgs 196/2003 s.m.i.) e dell'Unione Europea (Regolamento UE 2016/679).

Responsabile del servizio di conservazione: è la persona fisica nell'organizzazione del conservatore 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 conservatore vengono definite le attività e le responsabilità affidate al conservatore e quelle che rimangono a carico del soggetto produttore. Il conservatore è responsabile soltanto dei pacchetti di versamento (SIP) accettati.

Organismo di tutela e vigilanza (in riferimento alle amministrazioni pubbliche): è il Ministero per i beni e le attività culturali e del turismo (MiBACT) che 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 Dlg. 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 (Dlgs. 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 (Dlgs. 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 Dlgs. 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 il cui ruolo le viene attribuito in base all'art. 14-bis, comma 2, lettera i), del CAD.

[Torna al sommario](#)

6. Oggetti digitali 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).

[Torna al sommario](#)

6.1. Oggetti conservati

Il sistema conserva documenti informatici, con i metadati ad essi associati. I documenti informatici e le loro aggregazioni, specificamente descritte nel documento, sono inviati in conservazione sotto forma di pacchetti di versamento (SIP), contenenti anche i relativi metadati.

Il sistema gestisce gli oggetti digitali 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 adeguati ad ogni soggetto produttore e definiti sulla base degli 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 sottofascicoli. Inoltre è gestita la presenza di classificazioni, fascicoli e sottofascicoli 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 e descritti da un set di metadati, che include obbligatoriamente anche il tempo di conservazione previsto, oltre alle informazioni di identificazione, classificazione e descrizione. Nel caso delle serie, la chiusura può avvenire a cadenza annuale o comunque secondo una definizione temporale definita dal produttore. I documenti informatici si organizzano in fascicoli, così definiti secondo le voci del piano di classificazione. Il quadro di classificazione permette di aggregare la documentazione in serie ordinate.

Le tipologie documentarie trattate (suddivise in titoli, classi e sottoclassi) e i loro specifici metadati e articolazioni, sono indicate nell'allegato specifiche tecniche 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 il modello di riferimento OASIS.

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 altri elementi (un esempio: il messaggio di posta elettronica con i suoi allegati).

All'unità documentaria e agli elementi che la compongono sono associati i set di metadati, che li identificano e li descrivono secondo le logiche e le articolazioni esposte nelle specifiche tecniche descritte nel documento allegato al contratto di affidamento del servizio di conservazione.

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

Il sistema di conservazione utilizza come formati di conservazione quelli elencati nell'allegato 2 delle regole tecniche, 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 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 soggetto produttore e che identificano ognuna delle tipologie documentarie gestite. L'elenco dei formati ammessi è riportato (e gestito) nelle funzionalità "Amministrazione strutture

versanti” del sistema e viene aggiornato continuamente, in base alle esigenze del soggetto produttore. Le modalità con cui si procede a tale aggiornamento sono concordate con ciascun soggetto produttore e riportate nelle specifiche tecniche. Il sistema identifica i formati al momento della ricezione del SIP mediante l’analisi dei magic number o del contenuto del file, in modo tale da consentire l’individuazione dello specifico mime type. L’informazione sul formato è parte dei metadati dei componenti dell’unità documentaria e costituisce un elemento delle informazioni sulla rappresentazione.

Di seguito, viene fornito un riepilogo dei formati al momento ammessi per la conservazione, previsti dall’allegato 2 delle regole tecniche del DPCM 3 dicembre 2013.

Formato	Proprietario	Estensione	Tipo	Aperto	Standard
PDF PDF/A	- Adobe Systems http://www.adobe.com/	.pdf	application/pdf	Sì	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	Sì	ISO/IEC 10918:1 (JPG); ISO/IEC 15444-1 (JPEG 2000)
Office Open XML (OOXML)	Microsoft	.docx, .xlsx, .pptx	MIME	Sì	ISO/IEC DIS 29500:2008
ODF Open Document Format	OASIS	.ods, .odp, .odg, .odb	application/vnd.oasis.opendocument.text	Sì	ISO/IEC 26300:2006; UNI CEI ISO/IEC 26300
XML Extensible Markup Language	W3C	.xml	application/xml text/xml	Sì	
TXT	-	.txt	ASCII, UTF-8, UNICODE	Sì	ISO 646, RFC 3629, ISO/IEC 10646
PEC EMAIL	-	.eml	MIME	No	RFC 2822/MIME

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

Risulta necessario affrontare tre tematiche importanti:

- la prima riguarda cosa s’intende per informazioni sulla rappresentazione e come si intende associarle ad un oggetto digitale conservato;
- la seconda si riferisce al come rispettare il requisito di leggibilità;
- la terza si riferisce a cosa deve essere fornito assieme ad un oggetto digitale al momento della sua distribuzione e in che modalità.

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

Si classificano quindi le informazioni sulla rappresentazione in:

1. strumenti per la leggibilità: tipicamente legati al formato dell'oggetto conservato;
2. informazioni sulla rappresentazione sintattica: tipicamente legate al formato dell'oggetto conservato;
3. informazioni sulla rappresentazione semantica: tipicamente legate alla descrizione archivistica dell'oggetto conservato.

Sebbene le informazioni sulla rappresentazione sintattica (tipo 2) possano essere considerate le basi su cui poggiare le successive conservazioni di oggetti di uno specifico formato, poiché sono le informazioni necessarie a produrre/creare gli strumenti che ne permettono la leggibilità (tipo 1), fin dal principio resta fondamentale fornire 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 conservato almeno gli strumenti per la leggibilità (viewer) degli oggetti digitali dati da conservare.

Si ritiene pertanto necessaria la capacità del software di generare, per ogni soggetto produttore, un insieme di descrizioni archivistiche "speciali", che diano modo al responsabile del servizio di conservazione di conservare le tre tipologie di informazioni sulla rappresentazione.

Nel sistema di conservazione distinguiamo tre descrizioni archivistiche speciali:

1. viewer: di tipologia "unità documentaria" con file di indice di tipo multi-indice;
2. fascicolo: informazioni sulla rappresentazione di tipologia "fascicolo";
3. informazioni sulla rappresentazione di tipologia "unità documentaria" con file di indice di tipo indice singolo.

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

La prima è obbligatoria e, oltre ai classici metadati riportati dallo standard Dublin Core, permette di associare ad ogni documento informatico conservato (eseguibile dal 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) sia 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 informatico.

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 → Conservatore e Licenziatario.

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

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

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

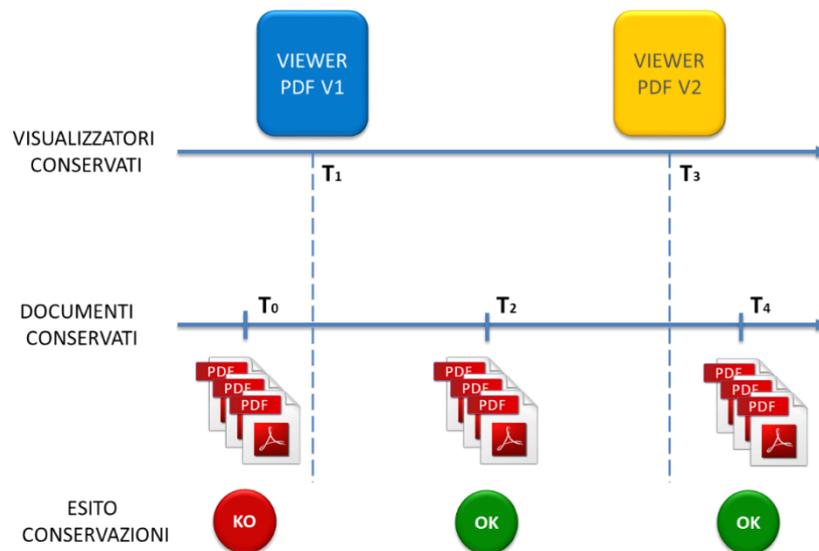


Figura 2: gestione dell'aggiornamento del viewer

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

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

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

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

[Torna al sommario](#)

6.2. Pacchetto di versamento (SIP)

Si tratta del pacchetto informativo inviato dal produttore al sistema di conservazione.

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

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

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

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

Il file di indice dovrà contenere i metadati per ricercare i documenti all'interno del sistema. Le informazioni sono concordate con il conservatore e configurate nel sistema di conservazione per ciascuna descrizione archivistica, nella stessa configurazione saranno anche implementate le regole di validazione dei metadati, concordate sempre con il conservatore.

Come anticipato nel paragrafo precedente, il file di indice potrà essere un file in formato CSV o un file XML con tracciato definito nell'allegato 5 delle nuove regole tecniche in materia di conservazione dei documenti informatici.

La struttura e la forma del file di indice dipendono sia dalla modalità di trasferimento scelta tra le tre disponibili, sia dalla natura dei file che costituiscono il pacchetto e dalle eventuali relazioni tra gli stessi.

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

Nel sistema di conservazione di IFin Sistemi i metadati possono essere di vari tipi.

Ci si è attenuti all'allegato 5 del DPCM 3 Dicembre 2013 recante le regole tecniche per il sistema di conservazione. In aggiunta ai metadati previsti 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 è in grado di classificare i metadati versati in base alla gestione privacy a cui sono soggetti. La classificazione permette di gestire i seguenti casi:

1. dato generico;
2. dato personale;
3. dato sensibile;
4. dato giudiziario.

A decorrere dal 25 maggio 2018 le espressioni «dati sensibili» e «dati giudiziari» utilizzate ai sensi dell'articolo 4, comma 1, lettere d) ed e), del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, ovunque ricorrano, si intendono riferite, rispettivamente, alle categorie particolari di dati di cui all'articolo 9 del Regolamento (UE) 2016/679 e ai dati di cui all'articolo 10 del medesimo regolamento.

In conformità al Regolamento (UE) 2016/679, si possono adottare misure di garanzia per il trattamento dei personali con particolare riferimento alle categorie particolari di dati di cui all'art. 9 del Regolamento suddetto. È consentito adottare misure di sicurezza ivi comprese tecniche di cifratura e di pseudonimizzazione, specifiche modalità di accesso selettivo ai dati, nonché eventuali altre misure necessarie a garantire i diritti degli interessati.

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 ne riporta l'elenco completo nell'allegato A "Oggetti sottoposti a conservazione".

Struttura del pacchetto di versamento

Il pacchetto di versamento ha una struttura differente in funzione della modalità adottata dal produttore per trasmetterlo al sistema di conservazione.

Di seguito descriviamo i tre casi possibili:

- **modalità automatica - via web services:** il trasferimento del pacchetto di versamento avviene in comunicazioni successive. In ciascuna comunicazione viene inviato il singolo documento assieme a tutti i metadati che lo accompagnano.
- **modalità semiautomatica - via file system:** il pacchetto di versamento è costituito dall'insieme degli oggetti dati accompagnati da un indice di metadati. L'indice di metadati contiene l'insieme dei metadati di tutti i documenti contenuti nel pacchetto.

L'indice dei metadati è solitamente un file in formato CSV, ma all'occorrenza può essere anche un file di tipo XML da valutarsi di volta in volta in sede in fase di contratto con il soggetto produttore.

- **modalità manuale - via upload da interfaccia web:** in questa modalità l'utente del soggetto produttore carica i file con un browsing del sistema operativo locale e imputa, nei campi messi a disposizione dall'interfaccia, i metadati associati a ciascun documento caricato. Il sistema di conservazione ricostruisce, con i dati imputati un file di indice di tipo CSV che associa al documento caricato. Questa struttura è pertanto riconducibile al caso precedente.

[Torna al sommario](#)

6.3. Pacchetto di Archiviazione (AIP)

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

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

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

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

1. l'oggetto digitale possibilmente in un formato standard non proprietario;
2. l'impronta del documento generata con funzione di hash;
3. il riferimento temporale (rappresentato dalla marca temporale o da altro riferimento temporale opponibile a terzi, come la segnatura di protocollo);
4. il set di metadati per la conservazione:
 - a. metadati identificativi (per esempio possono essere utilizzati i metadati degli standard ISAD (G) ISAAR (CPF));
 - b. metadati descrittivi (per esempio possono essere utilizzati i metadati dello standard ISAD);
 - c. metadati gestionali (UNI SinCRO);
 - d. metadati tecnologici (per esempio possono essere utilizzati i metadati dello standard METS);
5. il viewer necessario per la visualizzazione dell'oggetto digitale, o in alternativa, si inserisce il puntatore/riferimento al viewer comune a più pacchetti informativi per quel formato di file del documento;
6. 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 di riferimento.

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

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

Una volta che i SIP sono stati acquisiti nel sistema, (e sono quindi stati oggetto di controlli sui metadati previsti dal contratto di servizio) essi sono pronti ad essere trasformati in AIP. All'atto della conservazione verrà composto il pacchetto di archiviazione (AIP). Il pacchetto di archiviazione è identificato dalle informazioni sull'impacchettamento.

Si riporta la struttura dell'indice del pacchetto di archiviazione.

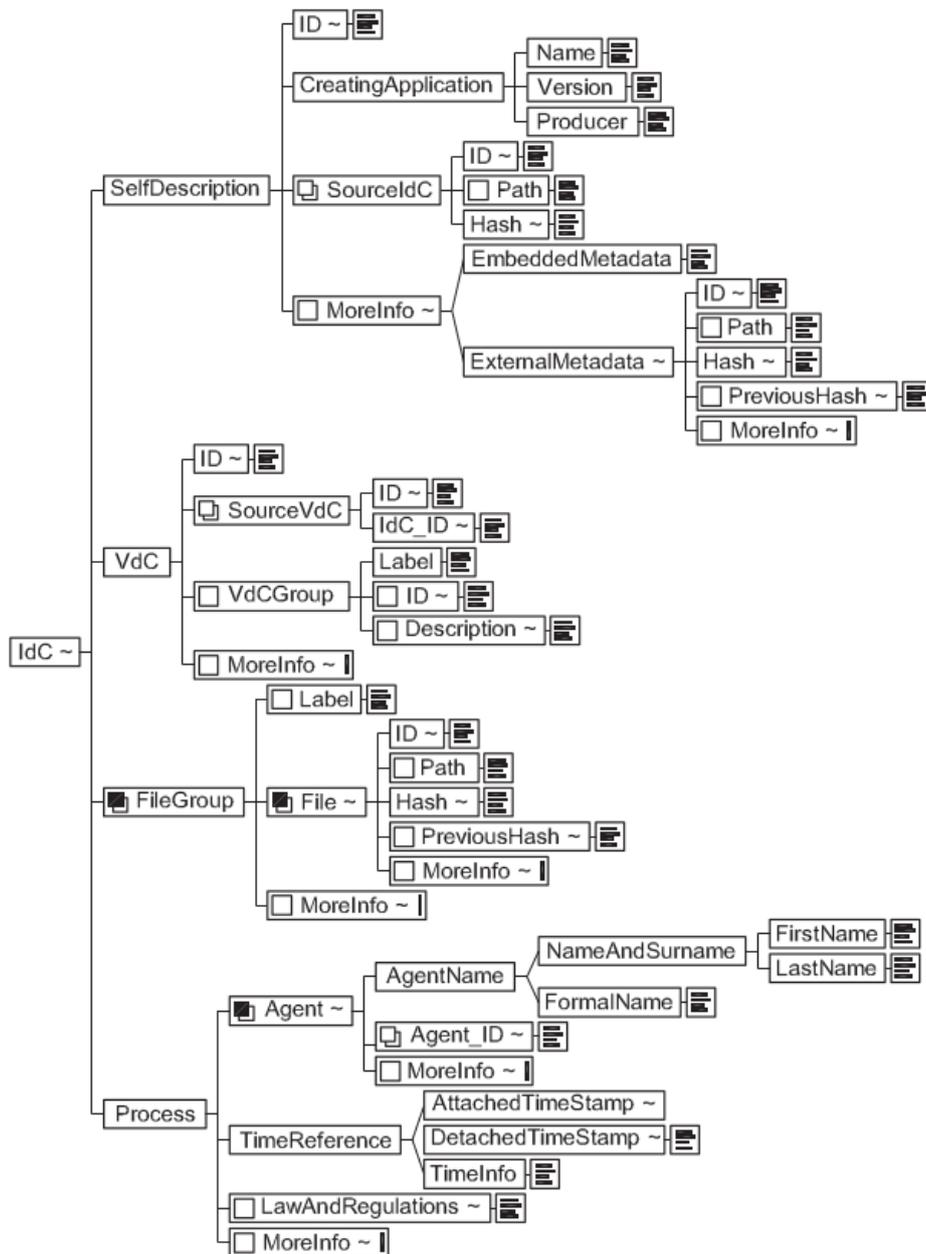


Figura 3: struttura dell'indice del pacchetto di archiviazione

Nella specificazione delle varie strutture dell'indice del pacchetto di archiviazione, l'elemento "ExtraInfo" presente può essere oggetto di ulteriori specificazioni e deve essere inteso come una sorta di "plug-in" per strutture di metadati specialistiche.

Si riporta di seguito la struttura dati del pacchetto di archiviazione completa delle strutture collegate ai diversi elementi "MoreInfo" previsti dallo standard SinCRO.

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema elementFormDefault="qualified" attributeFormDefault="qualified"
xmlns:dp="http://www.ifin.it/docpa" xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://www.ifin.it/docpa">
```

```

<xs:element name="MetadataComponent" type="dp:MetadataComponentType" />

<xs:complexType name="MetadataComponentType">
  <xs:sequence>
    <xs:element name="MetadataItem" type="dp:MetadataItemType" minOccurs="0"
maxOccurs="unbounded"/>
    <xs:element name="MetadataComponent" type="dp:MetadataComponentType" minOccurs="0"
maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:attribute name="type" type="xs:string" use="required" />
  <xs:attribute name="id" type="xs:unsignedByte" use="required" />
</xs:complexType>

<xs:complexType name="MetadataItemType">
  <xs:simpleContent>
    <xs:extension base="xs:string">
      <xs:attribute name="type" type="xs:string" use="required" />
      <xs:attribute name="id" type="xs:string" use="required" />
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

</xs:schema>

```

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

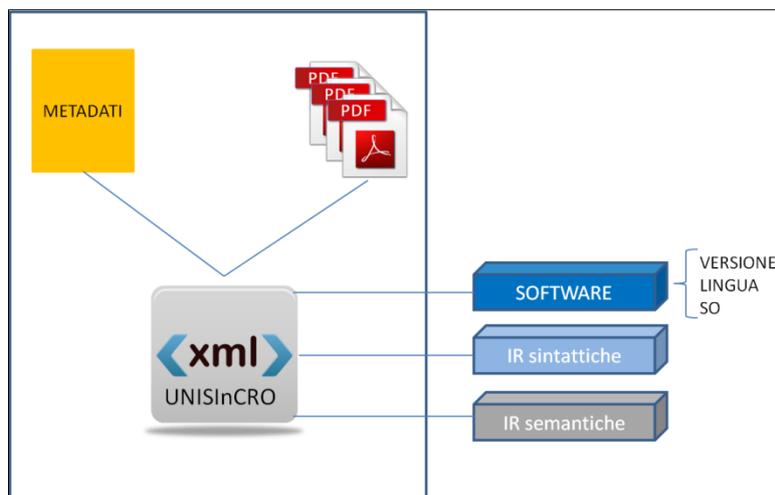


Figura 4: schema dell'AIP e dei collegamenti con le informazioni sulla rappresentazione

In un contesto OAIS il pacchetto di archiviazione dev'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 (DIP)

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 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 informatici.

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

[Torna al sommario](#)

7. Processo di conservazione

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

Il servizio di conservazione erogato è regolato dai seguenti documenti:

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

Tutti i processi afferenti al versamento, all'accettazione, alla validazione degli oggetti digitali contenuti nel pacchetto informativo sono tracciati dai log. Il sistema di conservazione, una volta censito il soggetto produttore, controlla la relativa identificazione del soggetto che ha formato il documento e il relativo ente produttore.

[Torna al sommario](#)

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

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

Il modello di trasmissione del pacchetto informativo (SIP) viene concordato in fase contrattuale e descritto nelle specifiche tecniche. In ogni caso il pacchetto di versamento potrà essere trasferito al sistema di conservazione con una delle seguenti modalità:

- Web service - caricamento automatico con interfacciamento di sistemi informatici;
- SFTP - 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, attiva un processo di conservazione nel sistema durante il quale invia a Legal Archive® pacchetti informativi, con i quali vengono passati come parametri i file e l'insieme dei metadati di ricerca a loro associati.

La modalità SFTP è costituita da un collegamento SFTP (Secure File Transfer Protocol). 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 alla piattaforma tramite un set predefinito di IP statici. La modalità di versamento SFTP prevede che il 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 dai file dei documenti da conservare accompagnati dall'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 del versamento di un fascicolo è indispensabile conoscere la gerarchia tra i documenti del fascicolo;
- Nel caso del 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 informatici, afferenti allo stesso contesto di provenienza. I diversi oggetti digitali vengono relazionati tra loro in funzione di alcuni metadati che fungono da nessi logici necessari, autonomi e determinati.

Il sistema di conservazione annota, in appositi log di sistema, il versamento dei pacchetti sui propri server SFTP, 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 informatici che verranno versati al sistema di conservazione;
- 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;
- Infine 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 dell'ente 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 affidamento del 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 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 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 è un file XML che contiene:

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

A seconda delle specifiche tecniche concordate con il soggetto produttore, il rapporto di versamento può essere firmato dal conservatore ed eventualmente ad esso può essere apposto un riferimento temporale, anche mediante marca temporale.

Il rapporto di versamento è reso disponibile all'ente produttore in varie forme, direttamente dipendenti alla modalità scelta per il versamento dei documenti:

- Versamento via Web Services: può essere richiesto utilizzando un'apposita chiamata web service;

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

La produzione del rapporto di versamento è uno delle attività previste dal processo di conservazione come indicato nel paragrafo precedente la componente Engine (JLegalArchive-engine) è l'applicazione responsabile al trattamento dei pacchetti di versamento. Tutte le elaborazioni cui è soggetto il pacchetto di versamento, per cui anche la generazione del rapporto di versamento, 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](#)

7.4. Rifiuto del pacchetto di versamento

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

Qualora il SIP non abbia superato tutti i controlli previsti, il sistema rifiuta l’intero 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 ente 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”; a seguito de versamento via Web Service 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 (AIP)

Legal Archive® trasforma i pacchetti di versamento (SIP) in pacchetti di archiviazione (AIP) contenenti tutti i file necessari alla loro ricostruzione e ricerca, 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 pacchetti di archiviazione in base a diverse logiche:

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

- In base al tempo.

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

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

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

La struttura utilizzata nella costruzione degli AIP fa riferimento alla norma UNI 11386:2010 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 dal SIP o definite sul sistema di conservazione.

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

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

- Soggetto Produttore;
- Anno;
- ID pacchetto di archiviazione.

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

Il pacchetto di archiviazione contiene:

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

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

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

[Torna al sommario](#)

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

I pacchetti di archiviazione (AIP) sono nel sistema. In un momento successivo alla generazione degli AIP, gli 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 del modello di riferimento 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 conservatore né il rilascio di copie cartacee conformi agli originali digitali conservati né il rilascio di copie informatiche di documenti informatici.

Pertanto, in merito all'esercizio del diritto d'accesso ai documenti conservati dal conservatore, questo si limita a fornire all'ente 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 l'ente produttore stesso abbia deciso di non acquisirlo direttamente mediante le modalità delineate nel presente manuale. Permane in carico allo stesso ente 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.

L'ente produttore può consultare i documenti informatici versati al sistema di conservazione tramite interfaccia web, collegandosi all'indirizzo comunicato dal conservatore, autenticandosi tramite username e password preventivamente forniti dal conservatore. Gli utenti da abilitare per l'accesso tramite interfaccia web al sistema di conservazione sono comunicati dai referenti dell'ente produttore al conservatore, che provvede a inviare le credenziali di accesso via email ai diretti interessati.

L'accesso web consente all'ente produttore di ricercare i documenti informatici versati, di effettuarne il download e di acquisire le prove delle attività di conservazione. L'ente produttore può richiedere i documenti e i fascicoli informatici versati e conservati anche utilizzando gli appositi Web Service, 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 modello di riferimento OAIS.

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

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

Il collegamento avviene tramite connessione sicura SSL con certificato rilasciato da Certification Authority accreditata presso AgID.

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 dell'ente produttore fornire un'eventuale copia conforme, richiedendo la presenza di un pubblico ufficiale.

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

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

Tale procedura, 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, l'ente produttore segnala al conservatore, su apposita documentazione allegata al contratto, i propri delegati alla visualizzazione e al download dei documenti informatici originali ai fini dell'esibizione.

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

Detta piattaforma consente all'ente produttore di effettuare sia la produzione di duplicati e copie informatiche sia di richiedere l'esibizione dei pacchetti di archiviazione conservati nel sistema di conservazione.

Il collegamento avviene tramite connessione sicura SSL con certificato rilasciato da Certification Authority accreditata presso AgID.

Una volta accreditato al 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.

L'ente 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, l'ente 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 l'ente 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 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, l'ente produttore avrà cura di gestire tale scelta. Il conservatore rimanda la gestione di tale attività all'ente 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 dell'AIP dal sistema di conservazione alla scadenza dei termini di conservazione previsti dalla norma, dandone informativa all'ente 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 un metadato, definibile per ciascuna tipologia documentaria o fascicolo, che stabilisce i tempi di conservazione. Sarà dunque il sistema di gestione dati (SGD) ad avvisare il responsabile del servizio di conservazione, attraverso una o più notifiche impostabili, riguardo la scadenza dei tempi di conservazione dei documenti, a supportarlo materialmente nella procedura di scarto e a mantenere al proprio interno, ove richiesto, i metadati della documentazione logicamente scartata.

Il sistema di conservazione produrrà quotidianamente un elenco dei pacchetti di archiviazione che hanno superato il tempo di conservazione, così come definito nel piano di conservazione dell'ente produttore. Tale elenco di scarto, dopo una verifica da parte di IFin Sistemi, viene comunicato all'ente produttore. Nei casi di archivi pubblici o privati di particolare interesse culturale, le procedure di scarto avvengono previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo. L'ente produttore, una volta ricevuto il nulla-osta dal Ministero, provvede ad adeguare, se necessario, l'elenco di scarto. Una volta che l'elenco di scarto è definitivo, l'ente produttore lo trasmette a IFin Sistemi. 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 una procedura di scarto che si occupa di controllare quotidianamente se esistono pacchetti di archiviazione che devono essere scartati. Alla presenza di uno o più pacchetti, il processo avvisa il responsabile del servizio di conservazione, che avrà a disposizione una interfaccia che gli permetterà di decidere se scartare o meno i pacchetti di archiviazione. In caso affermativo, la procedura di selezione 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 pacchetto di archiviazione, una nota che indichi il fatto che il pacchetto di archiviazione è stato sottoposto alla procedura 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 dal modello di riferimento OAIS, una qualsiasi applicazione di conservazione dev'essere in grado di esportare i documenti informatici conservati in un formato che garantisce l'integrità della conservazione stessa.

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

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

- L'ente produttore aveva già nominato gli utenti abilitati all'accesso della piattaforma web, all'atto della sottoscrizione del contratto;
- Tali utenti potranno collegarsi alla piattaforma web per generare e scaricare i DIP contenenti tutti i documenti conservati;

-
- Per volumi di grandi dimensioni, quando previsto da contratto, il conservatore metterà a disposizione dell'ex-cliente:
 - I file scaricati in formato ISO su server SFTP;
 - I file scaricati in formato ISO su supporto fisico anonimo, senza riferimenti al contenuto e consegnati da personale autorizzato di 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 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 si appoggiano su protocolli sicuri cifrati (https, SFTP);
- I supporti fisici saranno cifrati.

Si ricorda che, in accordo con il modello di riferimento 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.

Legal Archive® è in grado di importare dati di altri *outsourcer* qualora dette informazioni, precedentemente soggette a conservazione digitale, 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](#)

7.10. Cessazione delle attività di conservazione

Nel caso in cui Ifin Sistemi decidesse di cessare le proprie attività di conservazione a norma, ai sensi dell'art. 37 del d.lgs. n. 82/2005 Codice dell'Amministrazione Digitale, la stessa è tenuta a comunicarlo al AgID a mezzo PEC, almeno sessanta giorni prima della cessazione.

Allo stesso modo, Ifin Sistemi, comunica a mezzo PEC (o altra modalità concordata) all'indirizzo istituzionale del cliente (Soggetto Produttore) ovvero a quello indicato nell'affidamento del servizio:

- Data di cessazione del servizio di conservazione, secondo il preavviso concordato nel contratto di affidamento del servizio di conservazione
- Procedura di recupero degli archivi
- Intervallo di tempo disponibile ai soggetti produttori per il recupero.

Consegnati i dati, Ifin Sistemi è liberata dall'obbligo di conservazione nonché dagli obblighi derivanti dall'art. 7 comma 1 del DPCM 03/12/2013.

Al termine delle operazioni di restituzione i dati vengono rimossi dai sistemi di Ifin Sistemi in modalità sicura.

In Ifin Sistemi è presente un Piano di cessazione nel quale sono fissati gli obiettivi, nonché le condizioni tecniche ed organizzative atte a regolamentare l'esecuzione del processo di cessazione del servizio di conservazione a norma del patrimonio documentale (archivio di conservazione) e di gestione del subentro di altro Conservatore, previa autorizzazione del Soggetto Produttore.

Tale piano contiene gli orientamenti emanati ai sensi del Regolamento UE n. 910/2014 – eIDAS e lo schema documentale risulta conforme a quanto indicato nell'allegato A delle Linee Guida AgID per la stesura del piano di cessazione del servizio di conservazione dei documenti digitali.

[Torna al sommario](#)

8. 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 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 di riferimento 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 all' 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 informatico di riferimento.

Come illustrato nella seguente figura il sistema di conservazione è conforme al modello di riferimento OAIS.

Il sistema di conservazione è composto da un ambiente di produzione e un ambiente di collaudo, tutte le componenti (database, storage, application server) dei due ambienti sono distinti e separati e installati su reti network differenti.

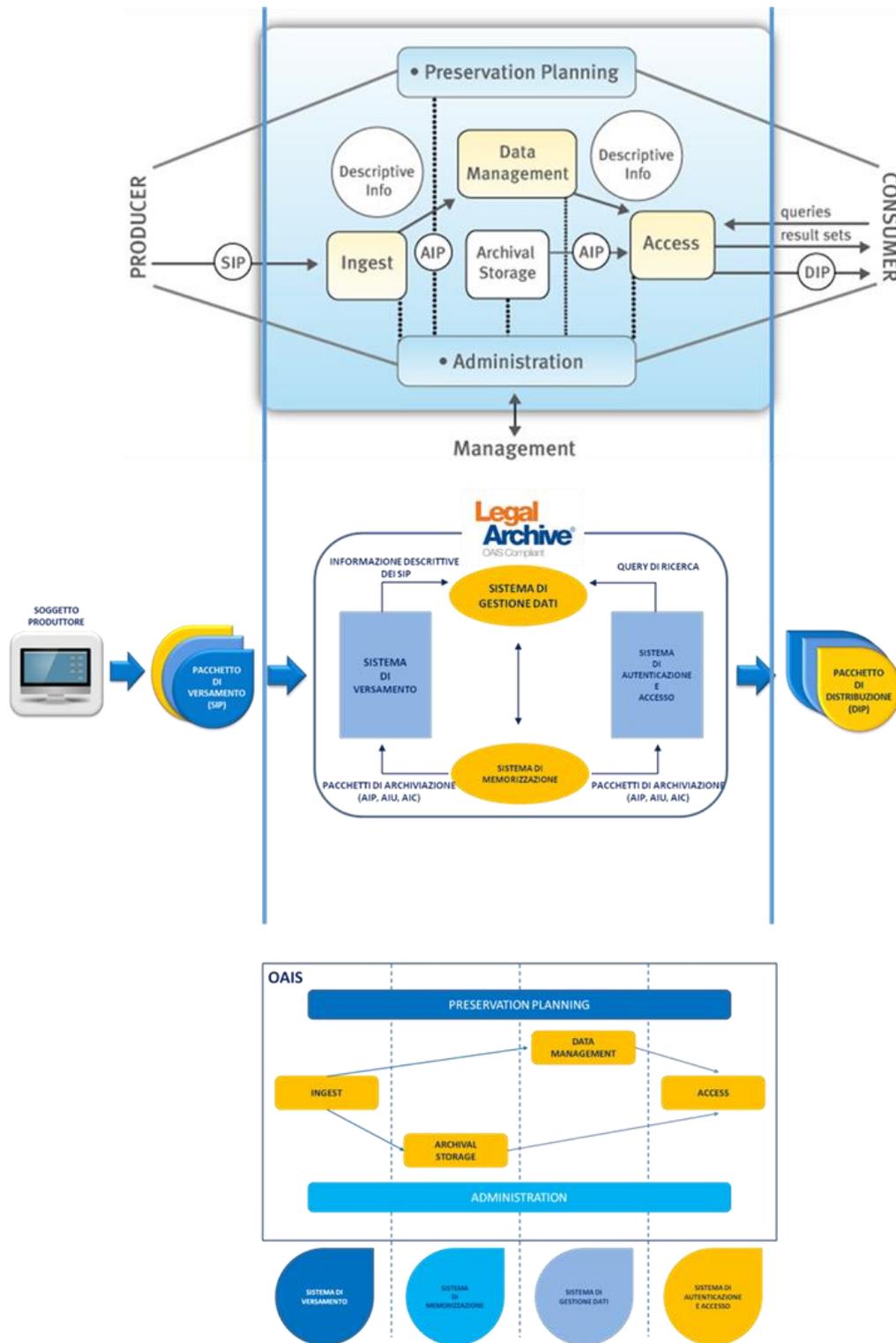


Figura 6: il modello OAIS

[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 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. Le procedure 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 produttore.

Innanzitutto viene generata la cosiddetta "descrizione del pacchetto informativo" 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). I documenti informatici, per i quali l'esito della convalida è risultato positivo, possono quindi essere inseriti in un pacchetto di archiviazione.

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

Controlli al sistema di versamento

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

Attraverso questo modulo l'ente produttore potrà vedere l'archivio come il complesso sistema di relazioni che è in effetti 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, il conservatore acquisisce gli strumenti archivistici dell'ente produttore (piano di classificazione, piano di conservazione, ecc.). L'aggiornamento del piano di conservazione memorizzato nel sistema di conservazione è demandato all'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 nel tempo della validità dei singoli "documenti informatici", 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, verificando 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 governa 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 "Accesso" richiede i risultati della ricerca al sistema di gestione dati che è in grado di rispondere alla richiesta, organizzando le informazioni descrittive degli AIP. Una volta individuato il documento desiderato (o i documenti, o addirittura un intero fascicolo o pacchetto di archiviazione), l'utente 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 sia 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, definendo i profili d'uso come verrà illustrato più avanti.

Le funzionalità di ricerca saranno implementate dal sistema di gestione dati, mentre il sistema di accesso fornirà le interfacce per l'interrogazione, la ricezione e la visualizzazione dei risultati.

In generale, le modalità di accesso permettono 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

Nel contesto della conservazione digitale, il sottosistema per la firma digitale si configura come elemento fondamentale per consentire di attuare la conservazione a norma dei documenti di un preciso flusso di lavoro. Per completare la procedura, il processo essenziale consiste nella firma dell'indice di conservazione (UNI 11386) del pacchetto di archiviazione, nonché nell'apposizione di una marca temporale su tale file.

Essendo presenti diversi dispositivi in grado di fornire queste funzionalità, l'architettura del sistema di conservazione prevede di demandare ad un apposito sottosistema il compito di interfacciarsi con essi.

Questo 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), dev'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:

- Smart Card.
- Token USB.
- HSM (Hardware Security Module) o servizi di Certification Authority:
 - Aruba Sign Box;
 - Aruba Remote Sign System;
 - Actalis BBF;
 - Intesi Group PKBOX;
 - Intesa-IBM.

Il sistema di conservazione è in grado di applicare la firma digitale utilizzando certificati rilasciati da tutte le *Certification Authority* accreditate presso AgID.

Per i servizi di firma digitale il soggetto conservatore si avvale di: Aruba Pec SpA a Socio Unico.

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)] che, presso la propria struttura organizzativa, registra e memorizza l'impronta del file e la relativa data di firma. Dunque, in questo caso il soggetto esterno non è 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 conservatore si avvale di Certification Authority iscritte alla Trust List Europea.

[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 (Microsoft SQL 2012 oppure Oracle 11g) a cui l'applicazione attinge. Il Back End ha in carico la gestione e la distribuzione dei processi tra i vari nodi del *cluster*, è 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 dell'ente produttore.

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

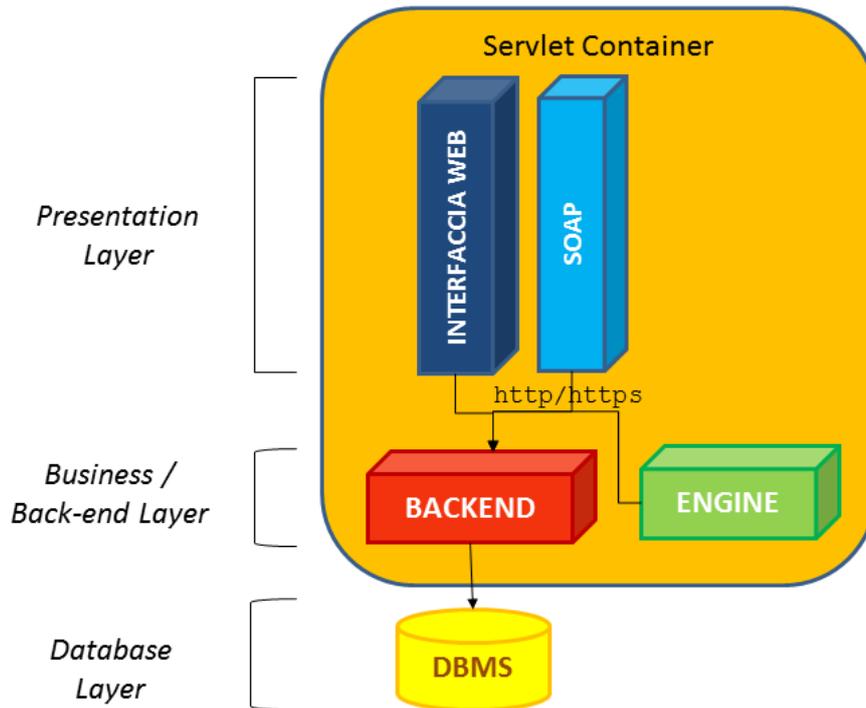


Figura 7: componenti scalabili del sistema

[Torna al sommario](#)

8.3. Componenti fisiche

Ifin Sistemi ha sviluppato la soluzione Legal Archive® che utilizza nel proprio sistema per erogare il servizio di conservazione dei documenti informatici.

La struttura informatica è suddivisa in quattro siti:

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

Farm di Produzione

I server ospitati nella sede di produzione sono logicamente divisi su reti distinte e gestiti con opportune regole di routing e firewalling per incrementare i livelli di sicurezza.

Sono definite:

- Un'area DMZ che ospita le componenti esposte al pubblico (SFTP e Front End);
- Un'area LAN, inaccessibile da rete esterna, che ospita le componenti di Back End, Engine, Storage e DB.

Le componenti più critiche di Data Base e Storage sono sottoposte a Backup giornaliero.

L'intera architettura è realizzata con server virtuali in ambiente Private Cloud, che permette estrema flessibilità e scalabilità dell'ambiente.

La server Farm è situata ad Arezzo e il data center è conforme ai principali standard di sicurezza internazionale ed in particolare implementa un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) certificato ISO 27001.

La figura sottostante schematizza l'infrastruttura virtuale ospitata nella server farm di produzione.

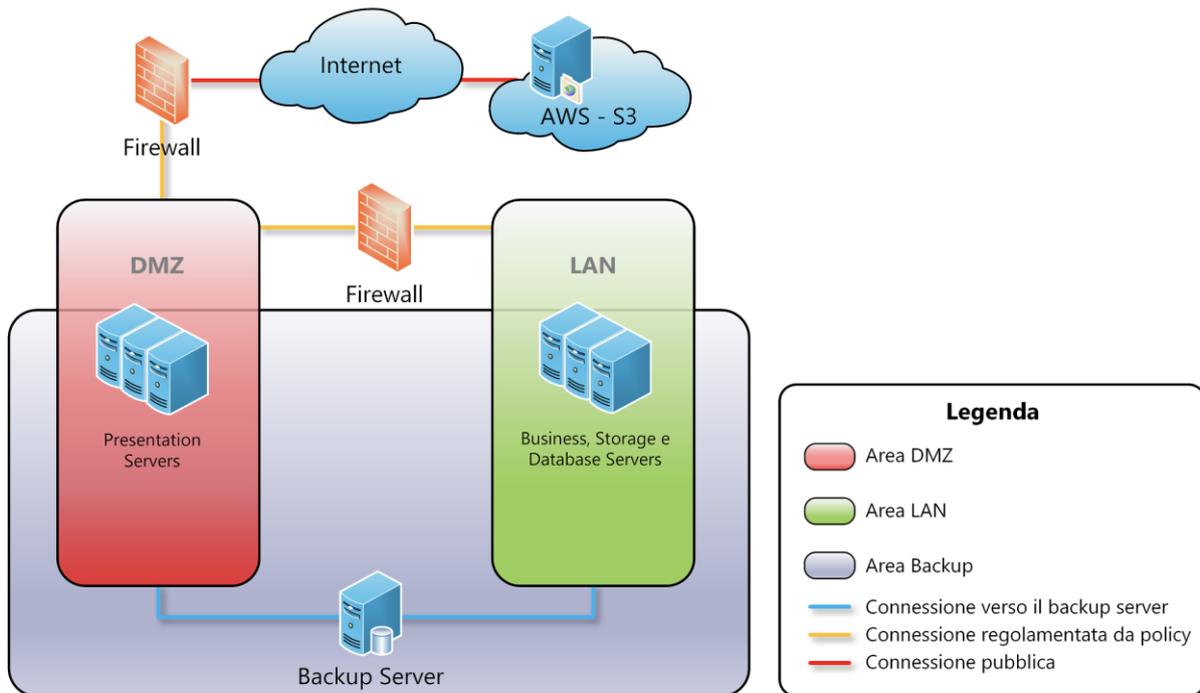


Figura 8: schema dell'infrastruttura della farm di produzione

La crescita dei documenti, vista la dimensione fisica degli oggetti, è sicuramente la parte più critica in termini di scalabilità. Per questo motivo il sistema di conservazione è stato sviluppato per essere indipendente dal sistema hardware che conserva i file. Oltre ad essere svincolato dal sistema hardware, il software è in grado di distribuire i documenti da conservare su più *storage* in funzione di regole che dipendono dalla tipologia di documenti o dalla disponibilità di risorse. Per questo motivo, al crescere dei volumi, è possibile affiancare, agli esistenti, altri storage con caratteristiche tecnologiche anche differenti rispetto ai precedenti.

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

Riepiloghiamo di seguito gli interventi necessari per far fronte a esigenze di carico crescente:

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

La soluzione tecnologica del *private cloud*, alla base dell'infrastruttura del sistema di conservazione, permette di scalare con facilità le risorse necessarie per l'adattamento al carico e ai volumi.

Farm di Disaster Recovery

Come per la farm principale, i server ospitati sono divisi su reti distinte, gestiti con opportune regole di routing, per incrementare i livelli di sicurezza.

Sono presenti:

- Un'area DMZ che ospita le componenti esposte (SFTP e Front End);
- Un'area LAN, inaccessibile da rete esterna, che ospita le componenti di Back End, Engine, Storage e DB.

La server Farm è situata a Ponte San Pietro (BG) e il data center è conforme ai principali standard di sicurezza internazionale ed in particolare implementa un sistema di gestione della sicurezza delle informazioni certificato ISO 27001.

Il Disaster Recovery viene garantito da un applicativo di sincronizzazione incrementale.

La figura sottostante schematizza l'infrastruttura virtuale nella server farm secondaria di *disaster recovery*.

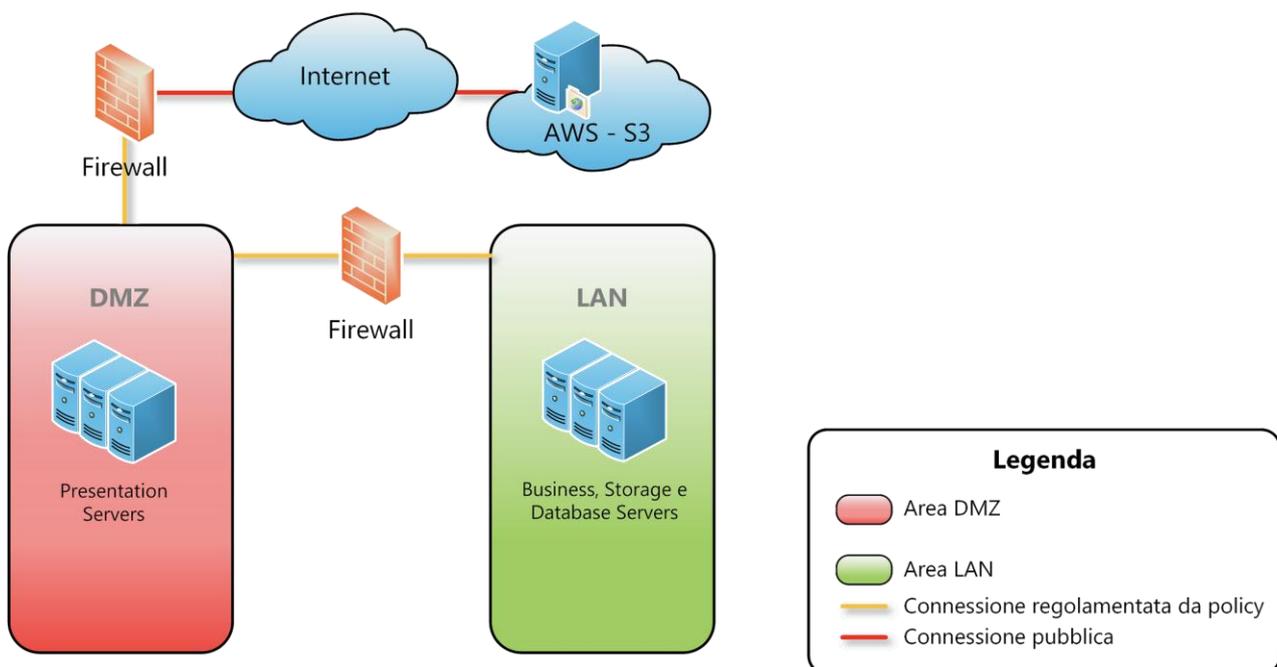


Figura 9: schema dell'infrastruttura della farm di DR

Sistema Storage

Il sistema di conservazione di IFIN Sistemi supporta la memorizzazione dei file sia su storage magnetici ad alte performance che su sistema Object Storage S3 di Amazon Web Services. Tali storage, garantiscono adeguati requisiti di affidabilità e di ridondanza interna del dato e rispondono all'esigenza di memorizzazione a lungo termine dei file che devono essere conservati con garanzia nel tempo di integrità e disponibilità del contenuto.

Per garantire la riservatezza vengono applicate appropriate politiche sulle autorizzazioni che prevedano la cifratura dei documenti che contengono dati sensibili ed eventualmente anche degli altri.

I sistemi di storage sono stati valutati da IFIN Sistemi sotto molteplici profili e, in virtù delle loro caratteristiche fisiche e architetture, sono ritenuti idonei ad essere utilizzati nel sistema di conservazione.

Nell'ambito del sistema di conservazione, lo storage magnetico ad alte performance rappresenta sia il supporto primario di conservazione posto fisicamente presso il DC di Aruba s.p.a. (DC01) - via Gobetti n.96 52100 Arezzo (AR), sia il supporto secondario posto nel sito di disaster recovery di Aruba s.p.a. (IT3) - via San Clemente n.53 24036 Ponte San Pietro (BG).

I due sistemi sono interconnessi mediante collegamenti ad alta velocità dedicati, completamente ridondati e protetti da misure di sicurezza. I collegamenti consentono la replicazione dei dati conservati eliminando il rischio di distruzione di tutte le copie delle informazioni in caso di danno irreparabile a livello di sito.

Questo secondo sistema funge anche da copia di sicurezza.

L'allineamento tra il sito primario e il sito secondario avviene coerentemente con le politiche generali di Disaster Recovery definite in IFIN che garantiscono RTO e RPO inferiori alle 48 ore.

Per il sistema di Object Storage S3, IFIN Sistemi si avvale dei servizi cloud computing Amazon Web Services (AWS) che garantisce la ridondanza e il rispetto delle misure di sicurezza.

Per un maggior dettaglio dei sistemi di sito primario si rimanda alla copia del piano per la sicurezza.

[Torna al sommario](#)

8.4. Procedure di gestione e di evoluzione

Ifin Sistemi in qualità di proprietario del software di conservazione Legal Archive® prevede la manutenzione evolutiva e correttiva del software stesso.

Il change management, sia del software che dell'hardware, viene eseguito secondo la seguente scaletta di attività.

Il change management, eseguito e completato con esito positivo, viene registrato negli appositi moduli previsti dalle procedure aziendali.

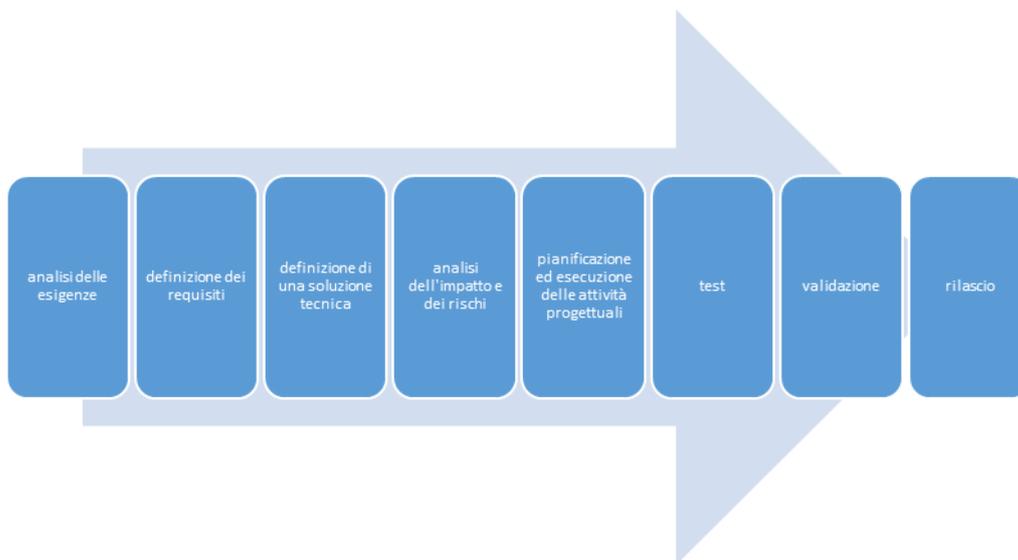


Figura 10: Flusso delle attività di Change Management

Manutenzione evolutiva ed adeguativa del software

La manutenzione evolutiva del software viene eseguita in due casi:

- Adeguare il prodotto a nuovi requisiti normativi;
- Aggiungere funzionalità e migliorie al prodotto.

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

Nel secondo caso la divisione Consulting di Ifin Sistemi monitora, con cadenza almeno mensile, i siti istituzionali e verifica la presenza di eventuali nuovi requisiti normativi nel caso questi vengono segnalati al reparto sviluppo. Di concerto le due aree verificano se il software è già rispondente, in caso contrario si procede con lo sviluppo del requisito richiesto.

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

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

Manutenzione correttiva del software

La manutenzione correttiva consiste nell'adeguamento del software in relazione ad un difetto o malfunzionamento.

L'eventuale bug al sistema può essere segnalato dalla comunità di riferimento o dallo stesso servizio outsourcing di Ifin Sistemi.

Il team di manutenzione prende in carico la richiesta di correzione di malfunzionamento giunta dal reparto outsourcing.

Il gruppo di lavoro impegnato nella risoluzione del bug analizza il bug, individua gli oggetti coinvolti dall'attività, eventuali effetti collaterali su altri oggetti software, attua la manutenzione richiesta, nel rispetto delle modalità definite (fasi e prodotti per le singole fasi), dichiarando, al termine dei lavori di sviluppo e test, la disponibilità al rilascio in esercizio, il software rilasciato verrà installato dagli operatori del reparto outsourcing seguendo le attività previste dai processi di change management.

Manutenzione dell'infrastruttura

Gli operatori della divisione outsourcing di Ifin Sistemi presiedono costantemente l'impianto e monitorano le sue diverse componenti come descritto nel capitolo successivo.

[Torna al sommario](#)

9. Monitoraggio e controlli

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

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

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

Periodicamente, come previsto dalle procedure interne, il sistema per la sicurezza delle informazioni e il sistema di gestione della qualità sono sottoposti ad audit di verifica sia interne sia 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 Ifin Sistemi.

[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 chiarificatore 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 i diversi aspetti funzionali tracciano sui log le 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 pacchetto di archiviazione --> numero pacchetto di archiviazione;
 - 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.

Segnalazioni di anomalie provenienti dal sistema di monitoraggio verranno gestite come descritto al paragrafo 9.3

[Torna al sommario](#)

9.2. Verifica dell'integrità degli archivi

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

Questa funzionalità è presente nel sistema di conservazione come processo schedulabile e viene pianificata da parte del responsabile del servizio di conservazione, secondo le regole definite dalla normativa vigente e secondo gli accordi con l'ente produttore.

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 dall'ente produttore potrà aprire una chiamata di assistenza (ticket) con 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 sia 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 pacchetto di versamento
Comunicazione eventuali anomalie nei pacchetti informativi 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 pacchetto di versamento
Invio ai clienti della segnalazione di errori che causano il blocco dell'elaborazione dei pacchetti di archiviazione da conservare.	Entro il giorno lavorativo successivo (festivi esclusi) dalla ricezione del pacchetto di versamento.	99,5% dei pacchetto di versamento
Avvio rielaborazione dei pacchetti di versamento eventualmente impattati dall'anomalia.	Entro il giorno lavorativo successivo (festivi esclusi) dalla risoluzione anomalia (dalla data comunicazione al cliente).	99,5% dei pacchetto di versamento
Risoluzione malfunzionamenti del servizio	Presenza in carico: entro 16 ore lavorative nei seguenti orari: dalle ore 9.00 alle ore 13.00 e dalle ore 14.00 alle ore 18 di ciascun giorno feriale (Lun. - Ven.).	N.A.
Disponibilità dei servizi di caricamento (upload) <ul style="list-style-type: none"> • Upload Manuale; • Modalità SFTP; • Modalità web service. N.B.: La disponibilità delle modalità custom viene espressamente concordata con il 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 saranno imputabili al conservatore il verificarsi di eventuali disservizi:

- Cause di forza maggiore e cioè eventi che, oggettivamente, ad I fin Sistemi di intervenire per eseguire le attività contrattualmente a carico di I fin Sistemi stessa (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 etc.);
- Interventi straordinari da effettuarsi con urgenza ad insindacabile giudizio di I fin Sistemi per evitare pericoli alla sicurezza, stabilità, riservatezza, integrità di dati e informazioni del cliente. L'eventuale esecuzione di tali interventi sarà comunque comunicata al cliente a mezzo e-mail inviata all'indirizzo di posta elettronica indicato in fase di attivazione 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 I fin Sistemi e comunque fuori dal suo controllo (in via meramente esemplificativa guasti o problemi).

[Torna al sommario](#)