Asmenet S.c.a.r.l.

MANUALE DI CONSERVAZIONE

EMISSIONE DEL DOCUMENTO CORRENTE

Azione	Data	Nominativo	Funzione
Redazione	07/10/2022	Cristina Falciano	Responsabile del servizio di conservazione
Verifica	26/04/2023	Cristina Falciano	Responsabile del servizio di conservazione
Approvazione	26/04/2023	Cristina Falciano	Responsabile del servizio di conservazione

REGISTRO DELLE VERSIONI

Numero versione	Data emissione	Modifiche apportate	Osservazioni
1.0	26/04/2023	Redazione del manuale di conservazione secondo quanto previsto dalle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici –AgID	**Nessuna osservazione**
2.0	08/05/2023	Integrazioni Asmenet	**Nessuna osservazione**

Sommario

1. SCOPO E AMBITO DEL DOCUMENTO

Il presente documento costituisce il manuale di conservazione[1] di Asmenet S.C.A.R.L. (da ora "Asmenet") e ha lo scopo di descrivere il sistema di conservazione[2] dei documenti informatici[3] adottato. Il manuale di conservazione illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture 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 particolare, secondo quanto previsto dal par. 4.6 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici (da ora Linee Guida – AgID), il presente manuale riporta nei successivi capitoli:

- i dati dei soggetti che nel tempo hanno assunto la responsabilità del sistema di conservazione, descrivendo in modo puntuale, in caso di delega, i soggetti, le funzioni e gli ambiti oggetto della delega stessa;
- la struttura organizzativa comprensiva delle funzioni, delle responsabilità e degli obblighi dei diversi soggetti che intervengono nel processo di conservazione;
- la descrizione delle tipologie degli oggetti digitali sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di documenti e delle eventuali eccezioni;
- la descrizione delle modalità di presa in carico di uno o più pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento;
- la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione;
- la modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione del pacchetto di distribuzione;
- la descrizione del sistema di conservazione, comprensivo di tutte le componenti tecnologiche, fisiche e logiche, opportunamente documentate e delle procedure di gestione e di evoluzione delle medesime;
- la descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie;
- la descrizione delle procedure per la produzione di duplicati o copie;
- i tempi entro i quali le diverse tipologie di oggetti digitali devono essere trasferite in conservazione ed eventualmente scartate;
- le modalità con cui viene richiesta la presenza di un pubblico ufficiale/notaio, indicando anche quali sono i casi per i quali è previsto il suo intervento.

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 software utilizzato per la gestione del processo di conservazione[4] dei documenti informatici è Legal Archive® di proprietà di Ifin Sistemi S.r.l.

---

1 Vedi paragrafo "Terminologia e acronimi"

2 Ibidem

3 Ibidem

4 Vedi paragrafo "Processo di conservazione"

Il presente manuale è così localizzato:

- Una copia del manuale della conservazione è archiviata presso il titolare dell'oggetto di conservazione[5];
- Una copia del manuale della conservazione è conservata presso il Conservatore[6].

1.1. Dati identificativi del Conservatore

Denominazione	ASMENET S.C.A.R.L.
Indirizzo	Via G. Porzio, 4-IS G1 80143 Napoli (NA)
Direttore	Arch. Tarallo Gennaro
E-mail di riferimento	supporto@asmenet.it
N° telefono	081 7877540
Sito web istituzionale	https://www.asmenet.it/
E-mail istituzionale	supporto.asmenet@asmepec.it

Contesto di riferimento

Il 1° gennaio 2022 sono entrate in vigore le Linee guida sulla formazione, gestione e conservazione dei documenti informatici (da ora Linee Guida) emanate da Agenzia per l'Italia Digitale (da ora AgID) ai sensi dell'art. 71 del D. lgs 7 marzo 2005 n. 82 recante il Codice dell'Amministrazione Digitale (da ora CAD). Asmenet si configura conservatore degli oggetti digitali iscritto al marketplace di AgID in ragione della natura giuridica dei titolari dell'oggetto di conservazione e secondo quanto previsto dal regolamento sui criteri per la fornitura del servizio di conservazione dei documenti informatici. Il servizio di conservazione degli oggetti digitali è formalizzato mediante accordo di affidamento tra ogni titolare dell'oggetto di conservazione e il conservatore in cui si definiscono le specifiche relative alla conservazione.

1.2. Modifiche al documento

Il presente documento e i dati contenuti sono puntualmente aggiornati. L'attività di aggiornamento può essere realizzata in merito a modifiche applicative, funzionali e procedurali che hanno impatti architetturali, infrastrutturali e organizzativi sulla gestione del servizio. Il numero delle versioni, le date e le modifiche apportate sono indicate nel "Registro delle versioni" a cui si rimanda. La responsabilità dell'aggiornamento è in capo al responsabile del servizio di conservazione di Asmenet, contattabile tramite i riferimenti riportati nel paragrafo "**4. RUOLI E** Responsabilità".

2. TERMINOLOGIA E ACRONIMI

2.1. Terminologia

Indichiamo di seguito il glossario dei termini utilizzati nel presente documento

5 Vedi paragrafo "Terminologia e acronimi"

6 Ibidem

Glossario dei termini	
TERMINE	**DEFINIZIONE**
Accesso	Operazione che consente di prendere visione dei documenti informatici
Affidabilità	Caratteristica che, con riferimento a un sistema di gestione documentale o conservazione, esprime il livello di fiducia che l'utente ripone nel sistema stesso, mentre con riferimento al documento informatico esprime la credibilità e l'accuratezza della rappresentazione di atti e fatti in esso contenuta
Aggregazione documentale informatica	Insieme di documenti informatici o insieme di fascicoli informatici riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente
Archivio	Complesso dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività
Archivio informatico	Archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche
Area Organizzativa Omogenea	Un insieme di funzioni e di uffici individuati dall'ente al fine di gestire i documenti in modo unitario e coordinato, secondo quanto disposto dall'art. 50 comma 4 del D.P.R. 28 dicembre 2000, n. 445. Essa rappresenta il canale ufficiale per l'invio di istanze e l'avvio di procedimenti amministrativi
Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico
Autenticità	Caratteristica in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto un oggetto è autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze
Certificazione	Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi
Classificazione	Attività di organizzazione di tutti i documenti secondo uno schema costituito da un insieme di voci articolate in modo gerarchico e che individuano, in astratto, le funzioni, competenze, attività e/o materie del soggetto produttore
Cloud della PA	Ambiente virtuale che consente alle Pubbliche Amministrazioni di erogare servizi digitali ai cittadini e alle imprese nel rispetto di requisiti minimi di sicurezza e affidabilità
Codec	Algoritmo di codifica e decodifica che consente di generare flussi binari, eventualmente imbustarli in un file o in un wrapper (codifica), così come di estrarli da esso (decodifica)
Conservatore	Soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici
Conservazione	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti
Convenzioni di denominazione del file	Insieme di regole sintattiche che definisce il nome dei file all'interno di un filesystem o pacchetto
Coordinatore della Gestione Documentale	Soggetto responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto

	dall'articolo 50 comma 4 del DPR 445/2000 nei casi di amministrazioni che abbiano istituito più AOO
Destinatario	Soggetto o sistema al quale il documento informatico è indirizzato
Digest	Vedi Impronta crittografica
Documento amministrativo informatico	Ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa
Documento elettronico	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva
Documento informatico	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Duplicato informatico	Vedi art. 1, comma 1, lett) i quinquies del CAD
eSeal	Vedi sigillo elettronico
Esibizione	operazione che consente di visualizzare un documento conservato
eSignature	Vedi firma elettronica
Estratto di documento informatico	Parte del documento tratto dal documento originale
Estratto per riassunto di documento informatico	Documento nel quale si attestano in maniera sintetica fatti, stati o qualità desunti da documenti informatici
Estrazione statica dei dati	Estrazione di informazioni utili da grandi quantità di dati (es. database, datawarehouse ecc.…), attraverso metodi automatici o semi-automatici
Evidenza informatica	Sequenza finita di bit che può essere elaborata da una procedura informatica
Fascicolo informatico	Aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento
File	Insieme di informazioni, dati o comandi logicamente correlati, raccolti sotto un unico nome e registrati, per mezzo di un programma di elaborazione o di scrittura, nella memoria di un computer
File container	Vedi Formato contenitore
File wrapper	Vedi Formato contenitore
File-manifesto	File che contiene metadati riferiti ad un file o ad un pacchetto di file
Filesystem	Sistema di gestione dei file, strutturato mediante una o più gerarchie ad albero, che determina le modalità di assegnazione dei nomi, memorizzazione e organizzazione all'interno di uno storage
Firma elettronica	Vedi articolo 3 del Regolamento eIDAS
Firma elettronica avanzata	Vedi articoli 3 e 26 del Regolamento eIDAS
Firma elettronica qualificata	Vedi articolo 3 del Regolamento eIDAS
Flusso (binario)	Sequenza di bit prodotta in un intervallo temporale finito e continuativo che ha un'origine precisa ma di cui potrebbe non essere predeterminato il suo istante di interruzione
Formato contenitore	Formato di file progettato per consentire l'inclusione ("imbustamento" o wrapping), in uno stesso file, di una o più evidenze informatiche soggette a differenti tipi di codifica e al quale possono essere associati specifici metadati
Formato del documento informatico	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file

Formato "deprecato"	Formato in passato considerato ufficiale il cui uso è attualmente sconsigliato a favore di una versione più recente
Funzioni aggiuntive del protocollo informatico	Nel sistema di protocollo informatico, componenti supplementari rispetto a quelle minime, necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni
Funzioni minime del protocollo informatico	Componenti del sistema di protocollo informatico che rispettano i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445
Funzione di hash crittografica	Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o digest (vedi) in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
Gestione Documentale	Processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta, uso, selezione e conservazione dei documenti
hash	Termine inglese usato, impropriamente, come sinonimo d'uso di "impronta crittografica" o "digest" (vedi)
Identificativo univoco	Sequenza di numeri o caratteri alfanumerici associata in modo univoco e persistente ad un'entità all'interno di uno specifico ambito di applicazione
Impronta crittografica	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di hash crittografica a un'evidenza informatica
Integrità	Caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità
Interoperabilità	Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi
Leggibilità	Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica
Manuale di conservazione	Documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture
Manuale di gestione	Documento informatico che descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi
Metadati	Dati associati a un o documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017
Naming convention	Vedi Convenzioni di denominazione
Oggetto di conservazione	Oggetto digitale versato in un sistema di conservazione
Oggetto digitale	Oggetto informativo digitale, che può assumere varie forme, tra le quali quelle di documento informatico, fascicolo informatico, aggregazione documentale informatica o archivio informatico
Pacchetto di archiviazione	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel manuale di conservazione

Pacchetto di distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione
Pacchetto di file (file package)	Insieme finito di più file (possibilmente organizzati in una struttura di sottoalbero all'interno di un filesystem) che costituiscono, collettivamente oltre che individualmente, un contenuto informativo unitario e auto-consistente
Pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione
Pacchetto informativo	Contenitore logico che racchiude uno o più oggetti di conservazione con i relativi metadati, oppure anche i soli metadati riferiti agli oggetti di conservazione
Path	Percorso (vedi)
Pathname	Concatenazione ordinata del percorso di un file e del suo nome
Percorso	Informazioni relative alla localizzazione virtuale del file all'interno del filesystem espressa come concatenazione ordinata del nome dei nodi del percorso
Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi
Piano della sicurezza del sistema di gestione Informatica dei documenti	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi
Piano di classificazione (Titolario)	Struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata
Piano di conservazione	Documento, allegato al manuale di gestione e integrato con il sistema di classificazione, in cui sono definiti i criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445
Piano di organizzazione delle aggregazioni documentali	Strumento integrato con il sistema di classificazione a partire dai livelli gerarchici inferiori di quest'ultimo e finalizzato a individuare le tipologie di aggregazioni documentali (tipologie di serie e tipologie di fascicoli) che devono essere prodotte e gestite in rapporto ai procedimenti e attività in cui si declinano le funzioni svolte dall'ente
Piano generale della sicurezza	Documento che pianifica le attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza
Presa in carico	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione e, in caso di affidamento del servizio all'esterno, dagli accordi stipulati tra il titolare dell'oggetto di conservazione e il responsabile del servizio di conservazione
Processo	Insieme di attività correlate o interagenti che trasformano elementi in ingresso in elementi in uscita
Produttore dei PdV	Persona fisica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con il responsabile della gestione documentale
qSeal	Sigillo elettronico qualificato, come da art. 35 del Regolamento eIDAS
qSignature	Firma elettronica qualificata, come da art. 25 del Regolamento eIDAS
Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore
Registro di protocollo	Registro informatico ove sono memorizzate le informazioni prescritte dalla normativa per tutti i documenti ricevuti e spediti da un ente e per tutti i documenti informatici dell'ente stesso

Registro particolare	Registro informatico individuato da una pubblica amministrazione per la memorizzazione delle informazioni relative a documenti soggetti a registrazione particolare
Regolamento eIDAS	electronic IDentification Authentication and Signature, Regolamento (UE) № 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE
Repertorio	Registro su cui vengono annotati con un numero progressivo i fascicoli secondo l'ordine cronologico in cui si costituiscono all'interno delle suddivisioni del piano di classificazione
Responsabile dei sistemi informativi per la conservazione	Soggetto che coordina i sistemi informativi all'interno del conservatore, in possesso dei requisiti professionali individuati da AgID
Responsabile del servizio di conservazione	Soggetto che coordina il processo di conservazione all'interno del conservatore, in possesso dei requisiti professionali individuati da AgID
Responsabile della conservazione	Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia
Responsabile della funzione archivistica di conservazione	Soggetto che coordina il processo di conservazione dal punto di vista archivistico all'interno del conservatore, in possesso dei requisiti professionali individuati da AgID
Responsabile della gestione documentale	Soggetto responsabile della gestione del sistema documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445
Responsabile della protezione dei dati	Persona con conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, in grado di assolvere i compiti di cui all'articolo 39 del Regolamento (UE) 2016/679
Responsabile della sicurezza dei sistemi di conservazione	Soggetto che assicura il rispetto dei requisiti di sicurezza all'interno del conservatore, in possesso dei requisiti professionali individuati da AgID
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Soggetto che assicura lo sviluppo e la manutenzione del sistema all'interno del conservatore, in possesso dei requisiti professionali individuati da AgID
Riferimento temporale	Insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC)
Riversamento	Procedura mediante la quale uno o più documenti informatici sono convertiti da un formato di file (ovvero di busta, ovvero di pacchetto di file) ad un altro, lasciandone invariato il contenuto per quanto possibilmente permesso dalle caratteristiche tecniche del formato (ovvero dei formati) dei file e delle codifiche di destinazione
Scarto	Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico-culturale
Serie	Raggruppamento di documenti con caratteristiche omogenee (vedi anche aggregazione documentale informatica)
Sidecar (file)	File-manifesto (vedi)
Sigillo elettronico	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi
Sistema di conservazione	Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, comma 1, del CAD
Sistema di gestione informatica dei documenti	Insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle organizzazioni per la gestione dei documenti.

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

2.2. Acronimi

Indichiamo, di seguito, gli acronimi dei termini utilizzati nel presente documento.

- **AgID**: Agenzia per l'Italia Digitale;
- **CA**: Certification Autorithy;
- **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;
- **DNS**: Domain Name System;
- **eIDAS**: Regolamento (UE) N. 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE;
- **FEA**: Si veda firma elettronica avanzata nel Glossario;
- **FEQ**: Si veda firma elettronica qualificata nel Glossario;
- **GDPR**: Regolamento (UE) N. 679/2016 del Parlamento Europeo e del Consiglio, del 27 aprile 2016 ("General Data Protection Regulation"), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- **HSM**: Hardware Security Module, è l'insieme di hardware e software che realizza dispositivi sicuri per la generazione delle firme in grado di gestire in modo sicuro una o più coppie di chiavi crittografiche;
- **IdC**: Indice di conservazione realizzato secondo le specifiche dello standard UNI SinCRO;
- **IR**: Informazioni sulla rappresentazione;
- **Irse**: Informazioni sulla rappresentazione semantiche;

- **Irsi**: Informazioni sulla rappresentazione sintattiche;
- **ISO**: International Organization for Standardization;
- **MIC**: Ministero della Cultura
- **OAIS**: Open archival information system;
- **PdA** : Pacchetto di archiviazione (Archival Information package – AIP);
- **PdD** : Pacchetto di distribuzione (Dissemination Information Package - DIP);
- **PdV** : Pacchetto di versamento (Submission Information Package - SIP).
- **PEC**: Posta Elettronica Certificata;
- **RdSC**: Responsabile del Servizio di Conservazione;
- **RdV**: Rapporto 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 degli oggetti di conservazione (titolare dell'oggetto di conservazione);
- **TSA**: Time Stamping Autorithy, è il soggetto che eroga la marca temporale;
- **UNI SinCRO**: UNI 11386:2020 - Supporto all'interoperabilità nella conservazione e nel recupero degli oggetti digitali.

3. NORMATIVA E STANDARD DI RIFERIMENTO

3.1. Normativa di riferimento

Il presente elenco riporta la normativa nazionale ed europea di riferimento relativa alla conservazione degli oggetti digitali:

- **Regolamento (UE) 910/2014 eIDAS**
  "in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno";
- **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;
- **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;
- **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";

- **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";
- **Linee Guida AgID**
"Linee Guida sulla formazione, gestione e conservazione dei documenti informatici (G.U. n.259 del 19 ottobre 2020)";
- **Regolamento AgID sui criteri per la fornitura dei servizi di conservazione dei documenti informatici.**

3.2. Standard di riferimento

Così come richiesto dalle Linee Guida – AgID, e secondo quanto previsto dall'Allegato 4, di seguito si riportano gli standard adottati 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 11386:2020 Standard SInCRO** - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- **ISO 15836:2019** Information and documentation - The Dublin Core metadata element set, Sistema di metadati del Dublin Core.

4. RUOLI E RESPONSABILITÀ

Il presente capitolo indica 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 di conservazione.

- ***Responsabile del servizio di conservazione**:* Cristina Falciano

La nomina è stata formalizzata in data 03/08/2020 e decorre dal giorno 03/08/2020. La nomina è stata firmata per accettazione dal responsabile designato.
Cronologia dei responsabili del servizio di conservazione.

Nome e Cognome	Funzione	Data nomina	Data Revoca

Cristina Falciano	Responsabile del servizio di conservazione	03/08/2020	//

- ***Responsabile della funzione archivistica di conservazione:*** Cristina Falciano

La nomina è stata formalizzata in data 03/08/2020 e decorre dal giorno 03/08/2020. La nomina è stata firmata per accettazione dal responsabile designato.
Cronologia dei responsabili della funzione archivistica di conservazione.

Nome e Cognome	Funzione	Data nomina	Data Revoca
Cristina Falciano	Responsabile della funzione archivistica di conservazione	03/08/2020	//

- ***Responsabile della sicurezza dei sistemi per la conservazione****:* Massimo Mazzella

La nomina è stata formalizzata in data 01/09/2021 e decorre dal giorno 01/09/2021. La nomina è stata firmata per accettazione dal responsabile designato.
Cronologia dei responsabili della sicurezza dei sistemi per la conservazione.

Nome e Cognome	Funzione	Data nomina	Data Revoca
Massimo Mazzella	Responsabile della sicurezza dei sistemi per la conservazione	01/09/2021	//

- ***Responsabile dei sistemi informativi per la conservazione:*** Massimo Mazzella

La nomina è stata formalizzata in data 01/09/2021 e decorre dal giorno 01/09/2021. La nomina è stata firmata per accettazione dal responsabile designato.
Cronologia dei responsabili dei sistemi informativi per la conservazione.

Nome e Cognome	Funzione	Data nomina	Data Revoca
Massimo Mazzella	Responsabile dei sistemi informativi per la conservazione	01/09/2021	//

- ***Responsabile dello sviluppo e della manutenzione del sistema di conservazione****:* Massimo Mazzella

La nomina è stata formalizzata in data 01/09/2021 e decorre dal giorno 01/09/2021. La nomina è stata firmata per accettazione dal responsabile designato.
Cronologia dei responsabili dello sviluppo e della manutenzione del sistema di conservazione.

Nome e Cognome	Funzione	Data nomina	Data Revoca
Massimo Mazzella	Responsabili dello sviluppo e della manutenzione del sistema di conservazione	01/09/2021	//

- **Responsabile del trattamento dei dati personali:** Ciro Pasquale Mancino

La nomina è stata formalizzata in data 05/04/2018 e decorre dal giorno 05/04/2018.

Nome e Cognome	Funzione	Data nomina	Data Revoca
Ciro Pasquale Mancino	Responsabile del trattamento dei dati personali	05/04/2018	//

Responsabile e incaricati al trattamento dei dati

Il conservatore Asmenet S.c.a.r.l., ogni qualvolta eroga servizi di conservazione, assume il ruolo di Responsabile del trattamento dei dati ai sensi dell'art. 28 del GDPR (così come stabilito inoltre dall'art. 3.9 delle Linee Guida AgID) e tutti i collaboratori autorizzati dal Responsabile del trattamento assumono il ruolo di incaricati del trattamento e vengono opportunamente istruiti in tal senso. I predetti ruoli sono nominati in conformità al Regolamento (UE) 2016/679 e alla normativa italiana (D.Lgs 196/2003 s.m.i.).

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	Cristina Falciano	• Definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato; • Gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente; • Genera e sottoscrive il Rapporto di versamento (RdV), secondo le modalità previste dal Manuale di conservazione; • Genera e sottoscrive il pacchetto di distribuzione (PdD) con firma digitale o firma elettronica qualificata, nei casi previsti dal Manuale di Conservazione; • Effettua il monitoraggio della corretta funzionalità del sistema di conservazione; • Effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi; • Al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati; • Provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto nel Manuale della Conservazione;	03/08/2020 - attualmente	

		• Predispone le misure necessarie per la sicurezza fisica e logica del sistema di conservazione secondo quanto previsto dalle Linee guida AgID; • Provvede per le amministrazioni statali centrali e periferiche a versare i documenti informatici, le aggregazioni informatiche e gli archivi informatici, nonché gli strumenti che ne garantiscono la consultazione, rispettivamente all'Archivio centrale dello Stato e agli archivi di Stato territorialmente competenti, secondo le tempistiche fissate dall'art. 41, comma 1, del Codice dei beni culturali; • Predispone il Manuale della conservazione e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti; • Assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza; • il Responsabile del servizio di conservazione ha altresì cura di predisporre "l'Allegato tecnico al servizio di conservazione" riportante le serie documentali, i relativi metadati utilizzati per la conservazione, i tempi di conservazione, la composizione dei pacchetti di versamento.		
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Massimo Mazzella	• 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.	01/09/2021	
Responsabile della sicurezza dei sistemi per la conservazione	Massimo Mazzella	• 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	01/09/2021	

Responsabile dei sistemi informativi	Massimo Mazzella	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.	01/09/2021	
Responsabile del trattamento dei dati personali	Ciro Pasquale Mancino	• 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.	05/04/2018	
Responsabile della funzione archivistica di conservazione	Cristina Falciano	● Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; • Definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici; • Monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione; • Collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza; • 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.	03/08/2020	

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

Cognome e Nome	Ruolo	Data nomina	Data revoca
Cristina Falciano	Responsabile del Servizio di conservazione	03/08/2020	
Massimo Mazzella	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	01/09/2021	
Massimo Mazzella	Responsabile della sicurezza dei sistemi per la conservazione	01/09/2021	

Massimo Mazzella	Responsabile dei sistemi informativi	01/09/2021	
Ciro Pasquale Mancino	Responsabile del trattamento dei dati personali	05/04/2018	
Cristina Falciano	Responsabile della funzione archivistica di conservazione	03/08/2020	

5.1. Organigramma

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

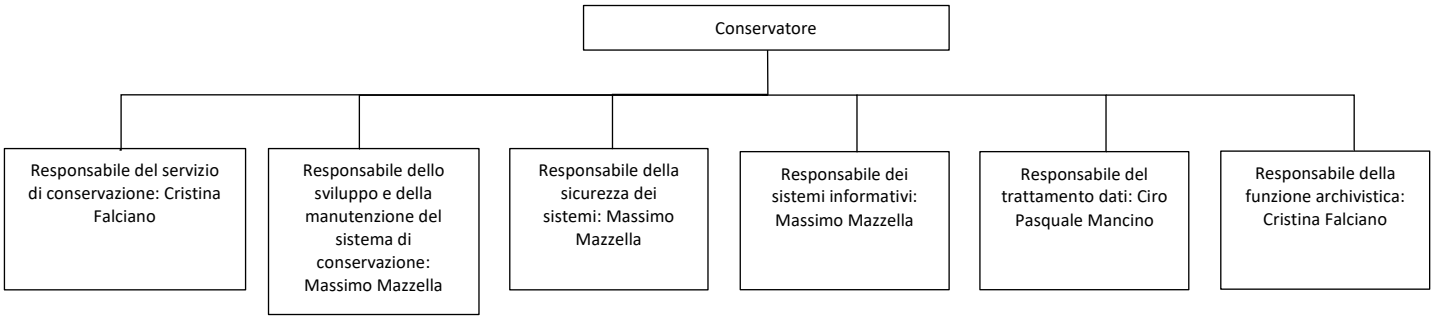


Figura 1. Organigramma servizio di conservazione di Asmenet S.c.a.r.l.

Le procedure organizzative si basano su standard mandatori ISO 27001 e ISO 9001.

5.2. Struttura organizzativa

Asmenet eroga servizi di conservazione digitale 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 Linee Guida all'art. 4.3. 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 secondo lo standard ISO 14721:2012 basato su una struttura organizzata di persone e sistemi, che accetti la responsabilità di conservare l'informazione e di renderla fruibile all'utente. Oltre a quanto sopra detto, il modello organizzativo del conservatore è stato realizzato tenendo conto anche dei requisiti di elevato livello in termini di qualità e sicurezza in aderenza allo standard ISO/IEC 27001. Seguendo quanto indicato dalle Linee Guida vigenti e, sulla base dello stesso modello di riferimento OAIS, il sistema identifica i seguenti ruoli:

a) Titolare dell'oggetto della conservazione;
b) Produttore dei PdV;
c) Responsabile della conservazione;
d) Utente abilitato;
e) Conservatore.

Titolare dell'oggetto della conservazione: è il soggetto produttore degli oggetti di conservazione. Può essere una persona fisica o giuridica, la pubblica amministrazione o l'ente titolare dei documenti informatici da conservare

Il titolare dell'oggetto di conservazione si impegna a depositare i documenti informatici e le loro aggregazioni nei modi e nelle forme concordate con Asmenet, garantendone l'autenticità e

l'integrità nelle fasi di produzione e di archiviazione corrente, effettuata nel rispetto delle norme sulla produzione 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. I rapporti tra Asmenet ed il titolare dell'oggetto di conservazione sono concordati mediante un accordo formale che definisce le specifiche relative alle tipologie documentali, i metadati, i formati, le modalità operative di versamento, le tempistiche di versamento e di conservazione.

Produttore dei PdV: è la persona fisica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni il Produttore dei PdV coincide con il Responsabile della gestione documentale o con il Coordinatore della gestione documentale. I dati identificativi del *produttore dei PdV* sono indicati nel contratto di affidamento del servizio di conservazione di ciascun titolare dell'oggetto di conservazione.

Responsabile della Conservazione: è il soggetto interno al titolare dell'oggetto di conservazione che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia e opera secondo quanto previsto dall'art. 44, comma 1-quater, del CAD. I dati identificativi dei Responsabili della conservazione sono indicati nell'accordo di affidamento del servizio di conservazione con ciascun Titolare dell'oggetto di conservazione e all'interno dei manuali di conservazione degli stessi.

Utente abilitato: è una persona, ente o sistema che interagisce con i servizi di un sistema per la conservazione di documenti informatici, come indicato nelle vigenti Linee Guida. L'utente abilitato 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. I nominativi degli utenti abilitati sono indicati nel contratto di affidamento del servizio di conservazione stipulato con ogni titolare dell'oggetto di conservazione. L'abilitazione e l'autenticazione degli utenti avviene in base alle procedure di gestione utenze ed in conformità alla legge italiana (D.Lgs 196/2003 s.m.i.) e dell'Unione Europea (Regolamento UE GDPR 2016/679).

Conservatore: è il soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici per conto del Titolare dell'oggetto di conservazione. 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. I dati identificativi del conservatore sono indicati nel paragrafo 1.1. del presente manuale.

Responsabile del servizio di conservazione: è il soggetto che coordina il processo di conservazione all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID.
Di seguito i dati identificativi del responsabile del servizio di conservazione.

N.	Cognome	Nome	Indirizzo	E-mail	Telefono
1	Falciano	Cristina	Centro Direzionale Isola G1 – 80143 Napoli	cfalciano@asmenet.it	0817877540

Le specifiche attività del responsabile del servizio sono riportate nelle specifiche tecniche e nel capitolo 5 del presente manuale.

Deleghe

Il Responsabile del servizio di conservazione può delegare, in tutto o in parte, lo svolgimento delle proprie attività ad una o più persone all'interno della propria struttura che, per competenza ed esperienza, garantiscano la corretta esecuzione delle operazioni ad esse delegate. Tutti gli atti di delega sono allegati al presente manuale della conservazione. Sono stati delegati alla conservazione dell'azienda le seguenti persone.

Nome	Luigi
Cognome	D'Agosto
e-mail	ldagosto@asmez.it
Data di firma della delega	10/01/2023
Compiti assegnati	Le mansioni di cui all'Ordine di servizio n.3 del 03/08/2020 di Cristina Falciano

6. OGGETTI DIGITALI SOTTOPOSTI A CONSERVAZIONE

Il sistema di conservazione assicura, dalla presa in carico fino all'eventuale scarto, la conservazione degli oggetti digitali e dei relativi metadati tramite l'adozione di regole, procedure e tecnologie, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità. Gli oggetti digitali versati al sistema di conservazione sono definiti con ciascun titolare dell'oggetto di conservazione nel contratto di affidamento del servizio di conservazione. Ciò consente di definire configurazioni e parametri adeguati ad ogni titolare dell'oggetto di conservazione definiti sulla base degli accordi stipulati all'atto della sottoscrizione del contratto di affidamento del servizio di conservazione.

6.1. Metadati

Il par. 2.1.1. "Formazione del documento informatico" delle Linee Guida prevede che "al momento della formazione del documento informatico immodificabile, devono essere generati e associati permanentemente ad esso i relativi metadati". I metadati associati agli oggetti digitali trasferiti nel sistema di conservazione di Asmenet sono quelli previsti dall'Allegato 5 delle citate Linee Guida nel formato CSV o XML. Lo schema di metadati associato a ciascun oggetti digitale è definito con ogni titolare dell'oggetto di conservazione. Tra i metadati obbligatori da associare figura il metadato "Modalità di formazione", che indica la modalità di generazione del documento informatico. In particolare, l'allegato 5 delle Linee Guida prevede che il metadato venga valorizzato con una delle seguenti modalità:

a) creazione tramite l'utilizzo di strumenti software che assicurino la produzione di documenti nei formati previsti nell'allegato 2 delle Linee Guida;

b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatico di un documento analogico;

c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;

d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

Per maggiore efficienza, il sistema di conservazione di Asmenet prevede che il metadato "Modalità di Formazione" sia valorizzato solo con le lettere sopraindicate corrispondenti ciascuna ad una specifica modalità di formazione.

6.2. Formati

Il sistema di conservazione utilizza i formati di conservazione elencati nell'allegato 2 delle Linee Guida. Inoltre, è in grado di gestire anche formati non compresi nel suddetto elenco, ma che il titolare dell'oggetto di conservazione 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 titolare dell'oggetto di conservazione è concordato l'elenco di formati ammessi che il sistema è in grado di accettare. L'elenco dei formati ammessi è riportato (e gestito) nelle funzionalità "Amministrazione strutture versanti" del sistema e viene aggiornato continuamente, anche in base alle esigenze del titolare dell'oggetto di conservazione. Il sistema di conservazione identifica i formati al momento del versamento 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 Linee guida AgID:

Formato	Proprietario	Estensione	Tipo	Standard
PDF - PDF/A	Adobe Systems http://www.adobe.com/	.pdf	application/pdf	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	ISO 12639 (TIFF/IT); ISO 12234 (TIFF/EP)
JPG e JPEG 2000	Joint Photographic Experts Group	.jpg, .jpeg, .jp2 (JPEG 2000)	image/jpeg	ISO/IEC 10918:1 (JPG); ISO/IEC 15444-1 (JPEG 2000)
Office Open XML (OOXML)	Microsoft	.docx, .xlsx, .pptx	MIME	ISO/IEC DIS 29500:2008
ODF Open Document Format	OASIS	.ods, .odp, .odg, .odb	application/vnd.oasis.opendocument.text	ISO/IEC 26300:2006; UNI CEI ISO/IEC 26300

XML Extensible Markup Language	W3C	.xml	application/xml text/xml	
PEC ed EMAIL	-	.eml	MIME	RFC 2822/MIME

6.3. Contenuto dei pacchetti informativi

Si riporta di seguito la rappresentazione del contenuto di un pacchetto informativo completo delle informazioni.

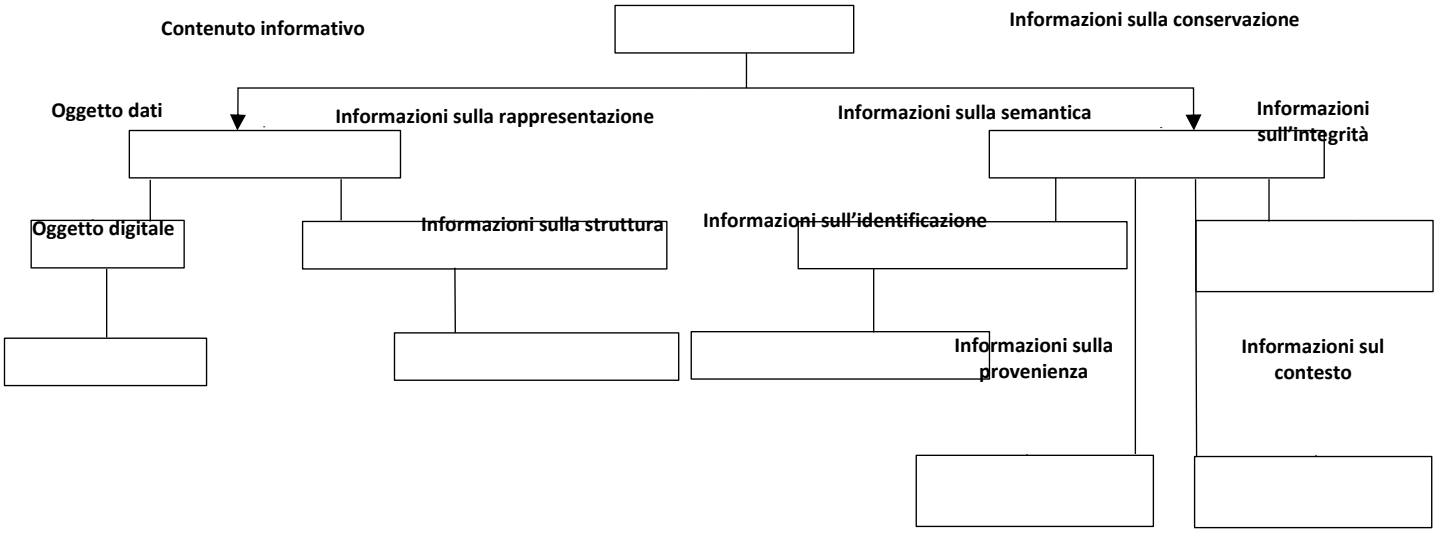


Figura 2. Struttura di un pacchetto informativo

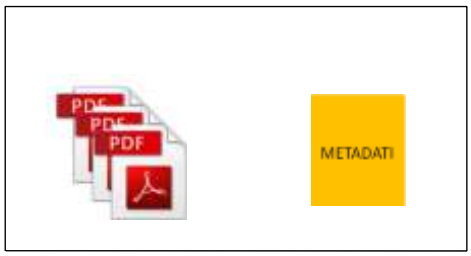
Il pacchetto informativo si distingue in:

- Pacchetto di Versamento – PdV;
- Pacchetto di Archiviazione – PdA;
- Pacchetto di Distribuzione – PdD.

Ciascuno dei pacchetti informativi è generato e gestito durante le diverse fasi del processo di conservazione. Pertanto, un pacchetto informativo è quindi determinato dalle componenti logiche fondamentali basate su un set di metadati per la rappresentazione delle informazioni e per la costruzione delle relazioni logiche del pacchetto informativo agli altri pacchetti informativi. Quest'ultimo elemento permette la definizione del vincolo archivistico tra i documenti relativi ad un medesimo affare.

6.4. Pacchetto di versamento (PdV)

Il Pacchetto di Versamento (da ora PdV) è il pacchetto informativo, contenente gli oggetti digitali e i relativi metadati, inviato dal produttore dei PdV al sistema di conservazione[7] secondo le modalità e le tempistiche di versamento concordate con il titolare dell'oggetto di conservazione nell'accordo di affidamento del servizio di conservazione. Il PdV è costituito dagli oggetti di conservazione e da un file denominato "File di indice" o "File dei metadati" in CSV o XML.



Il file di indice contiene i metadati per il recupero degli oggetti digitali conservati nel sistema di conservazione. Le informazioni sono configurate nel sistema di conservazione per ciascuna tipologia di oggetto digitale e, nella stessa configurazione, sono anche implementate le regole di validazione dei metadati. 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. La modalità di versamento dei pacchetti di versamento nel sistema di conservazione Legal Archive® può essere **automatica**, **semiautomatica** oppure **manuale**:

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

Figura 3. Struttura del Pacchetto di Versamento

6.4.1. Struttura del pacchetto di versamento

Il pacchetto di versamento può assumere una struttura differente in funzione della modalità concordata con il titolare dell'oggetto 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 costituto 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 informativo. L'indice dei metadati è solitamente un file in formato CSV, ma può essere anche un file di tipo XML da valutarsi di 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

[7] Allegato 1 "Glossario dei termini e degli acronimi"

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.

Il sistema di versamento permette al Produttore dei PdV di correggere la composizione dei pacchetti di versamento prima della sua acquisizione da parte del sistema di conservazione.
Inoltre, il sistema di conservazione è in grado di classificare i metadati versati in base al trattamento privacy a cui sono soggetti. In conformità al Regolamento (UE) 2016/679 (GDPR), la classificazione permette di gestire i seguenti casi:

1. Dati generici;
2. Dati personali;
3. Categorie particolari di dati personali (ex dati sensibili);
4. Dati personali relativi a condanne penali e reati (ex dati giudiziari).

L'identificazione dell'interessato da parte di un utente autorizzato viene tracciato in appositi log dal sistema di conservazione.
I PdV acquisiti nel sistema essi sono trasformati in pacchetto di archiviazione (PdA).

6.5. Pacchetto di archiviazione (PdA)

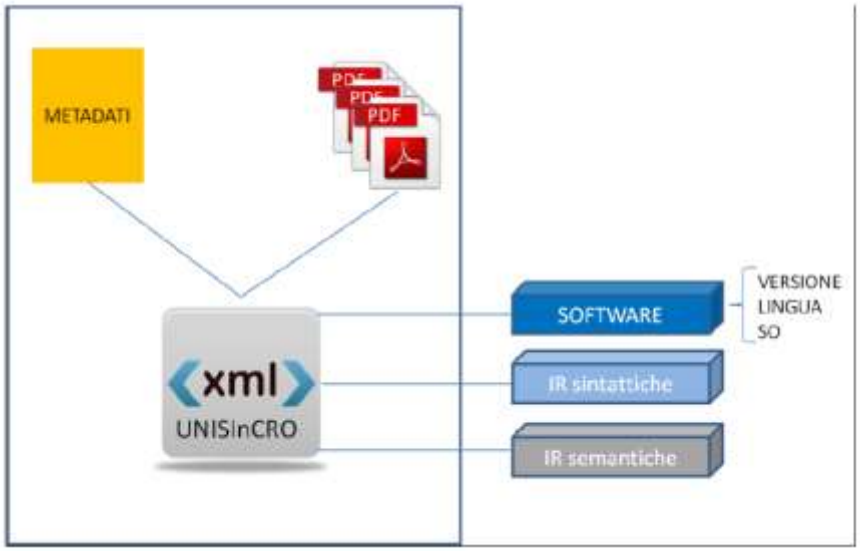
È un pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento. Il sistema di conservazione di Asmenet prevede che il pacchetto di archiviazione contenga, oltre all'oggetto digitale e ai relativi metadati, anche le seguenti informazioni codificate in XML:

- Lo schema di tag per la conservazione:
  a. metadati identificativi;
  b. metadati di provenienza;
  c. metadati di contesto;
  d. metadati descrittivi;
  e. metadati gestionali;
  f. metadati tecnologici.
- 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;
- 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.

Tali informazioni sono contenute nell'indice di conservazione strutturato secondo lo standard UNISinCRO:2020. Inoltre, esso conterrà due puntatori:

• 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).

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



Via G. Porzio, 4 - Is G1
80143 Napoli
Codice Fiscale e Partita IVA
05166621218

Telefono: 081 7877540
Fax: 081 19721004
E-mail: supporto@asmenet.it
Pec: supporto.asmenet@asmepec.it

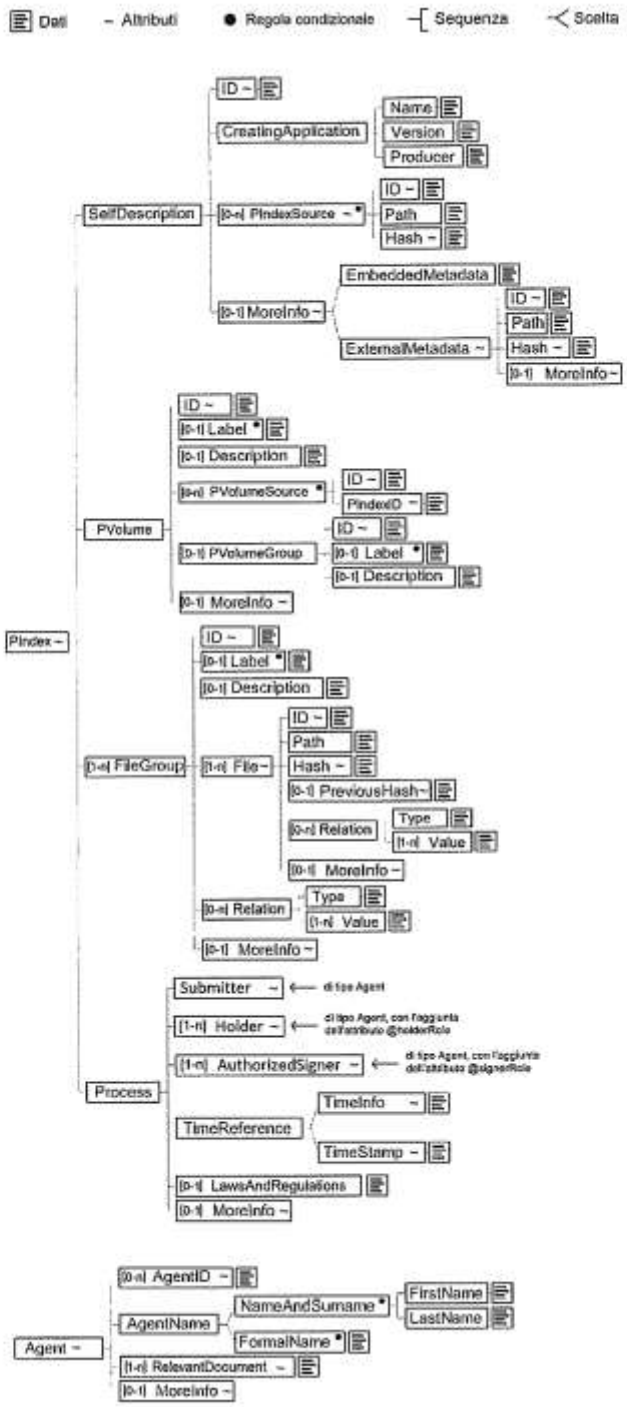


Figura 4 struttura dell'indice del pacchetto di archiviazione

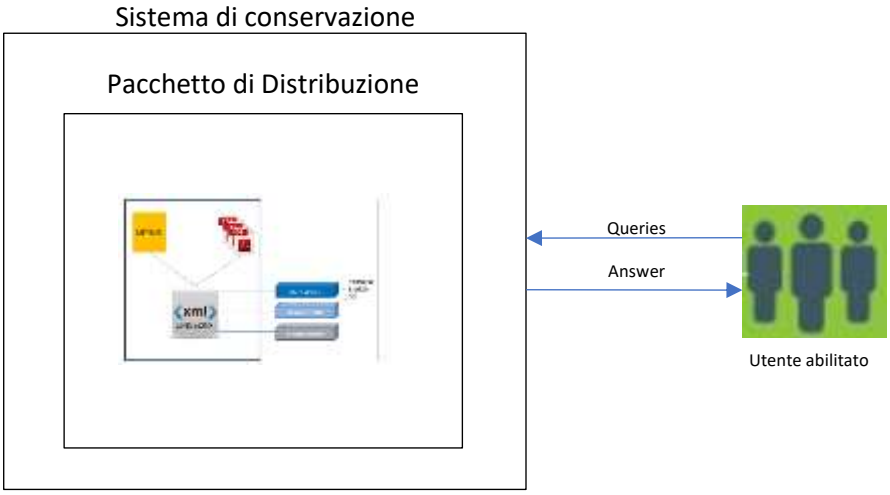
In particolare, l'elemento "ExtraInfo" presente può essere oggetto di ulteriori specificazioni. Si riporta di seguito la struttura dati del pacchetto di archiviazione completa delle strutture collegate ai diversi elementi "MoreInfo" previsti dallo standard SinCRO.

```
<?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:string" 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>
```

6.6. Pacchetto di distribuzione (PdD)

Il Pacchetto di Distribuzione (da ora PdD) è il pacchetto informativo inviato dal sistema di conservazione all'utente abilitato in risposta ad una sua richiesta di accesso a oggetti di conservazione. Un PdD può coincidere con uno o più PdA conservati nel sistema di conservazione in rapporto alla richiesta e ai diritti dell'utente abilitato. Il PdD generato dal sistema di conservazione contiene:

- Gli oggetti digitali richiesti nel formato previsto per la loro visualizzazione;
- Un'estrazione dei metadati associati ai documenti;
- L'indice di conservazione (IdC);
- I viewer necessari alla visualizzazione dei documenti informatici.



7. PROCESSO DI CONSERVAZIONE

Il processo di conservazione si attiva a seguito della sottoscrizione del contratto di affidamento del servizio di conservazione tra il titolare dell'oggetto di conservazione e il conservatore. Il servizio di conservazione erogato è regolato dai seguenti documenti:

- Determina di affidamento spesa per l'affidamento del servizio di conservazione;
- Atto di nomina responsabile del servizio di conservazione;
- Atto di nomina responsabile della funzione archivistica di conservazione;
- Manuale operativo del software di conservazione.

Si riportano le fasi del processo di conservazione di seguito descritte secondo quanto indicato dalla normativa in vigore:

a) l'acquisizione da parte del sistema di conservazione del PdV per la sua presa in carico; la verifica che il PdV e gli oggetti digitali contenuti siano coerenti con le modalità previste dal manuale di conservazione e con quanto indicato nell' allegato 2 "Formati di file e riversamento" relativo ai formati;
b) il rifiuto del PdV, nel caso in cui le verifiche di cui alla lettera b) abbiano evidenziato delle anomalie;
c) la generazione, anche in modo automatico, del rapporto di versamento relativo ad uno o più pacchetti di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo universale coordinato (UTC), e una o più impronte, calcolate sull'intero contenuto del pacchetto di versamento, secondo le modalità descritte nel manuale di conservazione;
d) la sottoscrizione del rapporto di versamento con la firma digitale o firma elettronica qualificata o avanzata apposta dal responsabile del servizio di conservazione;
e) la preparazione, la sottoscrizione con firma digitale o firma elettronica - qualificata o avanzata del responsabile della conservazione, nonché la gestione del pacchetto di archiviazione sulla base delle specifiche della struttura dati indicate dallo standard UNI 11386;
f) ai fini dell'esibizione richiesta dall'utente la preparazione e la sottoscrizione con firma digitale o firma elettronica qualificata o avanzata del responsabile del servizio di

conservazione di pacchetti di distribuzione che possono contenere parte, uno o più pacchetti di archiviazione;

g) ai soli fini della interoperabilità tra sistemi di conservazione, la produzione di pacchetti di distribuzione coincidenti con i pacchetti di archiviazione o comunque contenenti pacchetti di archiviazione generati sulla base delle specifiche della struttura dati indicate dallo standard UNI 11386 e secondo le modalità riportate nel manuale di conservazione;
h) la produzione di duplicati informatici o di copie informatiche effettuati su richiesta degli utenti in conformità a quanto previsto dalle presenti linee guida;
i) la produzione di copie informatiche tramite attività di riversamento al fine di adeguare il formato alle esigenze conservative di leggibilità nel tempo in base alle indicazioni previste dall'allegato 2 “Formati di file e riversamento”;
j) l’eventuale scarto del pacchetto di archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dalla norma o secondo quanto indicato dal piano di conservazione del titolare dell'oggetto di conservazione e le procedure descritte nel paragrafo 4.12 delle Linee Guida;
k) nel caso degli archivi pubblici o privati, che rivestono interesse storico particolarmente importante, l’eventuale scarto del pacchetto di archiviazione avviene previa autorizzazione del MIC rilasciata al Titolare dell’oggetto della conservazione secondo quanto previsto dalla normativa vigente in materia e al paragrafo 4.12 delle Linee Guida.

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

La prima fase del processo di conservazione prevede l’acquisizione del pacchetto di versamento nel sistema di conservazione. Il pacchetto di versamento può 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 attraverso l’interfacciamento diretto tra gli applicativi del titolare dell’oggetto di conservazione e il sistema di conservazione. Con la modalità Web Service l’applicativo chiamante del cliente 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 dei PdV 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.

Nel dettaglio, si descrivono di seguito le possibili modalità di costruzione dei pacchetti di versamento accettati ed elaborati dal sistema e il conseguente file di metadati.

- 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 è allegato. 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 il produttore dei PdV 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 5. 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 PdV non avviene mediante supporti fisici;
- In merito al versamento di tipologie documentarie informatiche fiscali, il conservatore si atterrà ai requisiti tecnologici richiesti dal legislatore (DMEF 17 giugno 2014).

Il modello di trasmissione è concordato tra il titolare dell'oggetto di conservazione e il conservatore nella determina di affidamento del servizio di conservazione.

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

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. 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.

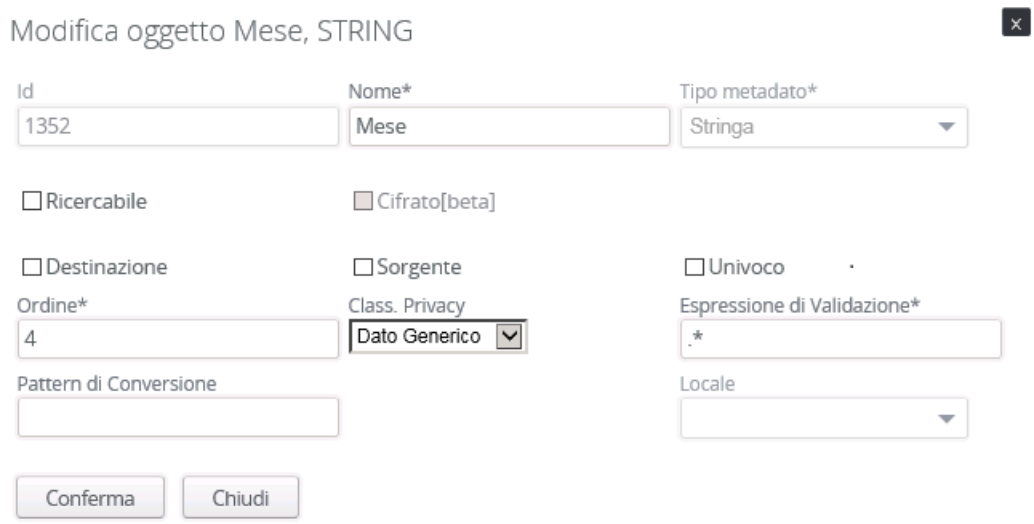


Figura 6: Finestra di configurazione metadati

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.

Il sistema di versamento mette a disposizione del titolare dell'oggetto di conservazione le funzionalità di validazione che consentono, se necessario, di correggere la composizione dei pacchetti di versamento prima della sua acquisizione da parte del conservatore.

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

Superate le verifiche, il sistema di conservazione genera, per ogni pacchetto accettato, il rapporto di versamento, memorizzato nel database. 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.

Il rapporto di versamento potrà essere firmato dal responsabile del servizio di conservazione ed eventualmente anche marcato temporalmente dal conservatore. È reso disponibile 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 una delle attività previste dal processo di conservazione. Come indicato nel paragrafo precedente, la componente Engine (JLegalArchive-engine) è l'applicazione responsabile del 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.

7.4 Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie

Qualora il PdV non abbia superato tutti i controlli previsti, il sistema notifica al produttore dei PdV 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 titolare dell'oggetto di conservazione. Inoltre, la notifica è 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 PdV viene rinominato con l'aggiunta dell'estensione file "KO".

7.5. Preparazione e gestione del pacchetto di archiviazione

Legal Archive® trasforma i pacchetti di versamento (PdV) in pacchetti di archiviazione (PdA) 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. Il pacchetto di archiviazione è salvato nella risorsa archivio configurata a sistema. E' possibile separare i versamenti in diversi pacchetti di archiviazione (PdA) 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 PdA, 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 ha 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 PdA fa riferimento alla norma UNI 11386:2020, 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 PdV 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 o con la firma digitale o con la marca temporale o entrambi sull'IdC e termina con la messa in evidenza di avvenuta conservazione (indice P7M) da parte del responsabile della conservazione. Il sistema di conservazione si occupa autonomamente di tutte le fasi di conservazione, tracciandone ogni passaggio e ogni esito nei file di log.

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

Gli utenti abilitati possono accedere al sistema di conservazione e interrogarlo per ottenere in risposta il pacchetto di distribuzione. Esistono diverse modalità di generazioni di PdD:

- PdD coincidente con l'PdA, che contiene;
  - Tutti gli elementi presenti nell'PdA;
  - I documenti del PdA 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.

- PdD dell'unità documentaria, che contiene:
  - Gli oggetti dati che la compongono;
  - PdD del documento, che contiene;
  - Gli oggetti dati del documento.

Il pacchetto di distribuzione è erogato dal sistema di conservazione in formato ZIP e in formato ISO a seconda della richiesta dell'utente abilitato. L'esibizione è un atto da svolgersi in ottemperanza a quanto previsto dalle Linee Guida. Essa consiste nel rendere leggibili, con mezzi idonei, tutte le scritture e i documenti conservati a norma. In particolare, il par. 4.9. delle Linee Guida, ribadisce che, ai fini dell'esibizione, il sistema di conservazione permette ai soggetti autorizzati l'accesso

diretto, anche da remoto, agli oggetti digitali conservati, attraverso la produzione di pacchetti di distribuzione (PdD) secondo le modalità descritte nel manuale di conservazione. L'utente abilitato può consultare i documenti informatici versati al sistema di conservazione tramite interfaccia web, autenticandosi tramite username e password preventivamente forniti dal conservatore.
L'accesso web consente all'utente abilitato di ricercare i documenti informatici versati, di effettuarne il download e di acquisire le prove delle attività di conservazione. L'accesso ai documenti e fascicoli informatici conservati può essere effettuato anche utilizzando gli appositi Web Service, richiamati secondo le modalità indicate nelle specifiche tecniche. Il sistema di conservazione di Asmenet S.c.a.r.l. 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 del modello di riferimento OAIS.
Il collegamento avviene tramite connessione sicura SSL con certificato rilasciato da Certification Authority accreditata presso AgID.
Una volta abilitato, 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 PdA;
- 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'PdA;
- Richiedere e scaricare i PdD da consegnare alle autorità competenti, in caso di necessità.

Nel PdD è compreso anche il necessario per la rappresentazione, i viewer nella versione coerente alla visualizzazione dei PdD e le informazioni in grado di supportare l'applicazione di visualizzazione.
È cura del titolare dell'oggetto di conservazione fornire un'eventuale copia conforme, richiedendo la presenza di un pubblico ufficiale.

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

Il sistema di conservazione consente di creare duplicati informatici di tutti i PdA versati nel sistema di conservazione dal titolare dell'oggetto di conservazione. In fase di attivazione del servizio, il titolare dell'oggetto di conservazione segnala al conservatore, su apposita documentazione allegata al contratto, i propri delegati alla visualizzazione e al download dei documenti informatici originali ai fini dell'esibizione. Il conservatore genera gli account e il sistema invia le credenziali all'utente per accedere al portale del sistema di conservazione. Detta piattaforma consente al titolare dell'oggetto di conservazione 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 PdD da consegnare alle autorità competenti, in caso di necessità;

- Produrre eventualmente una copia conforme richiedendo la presenza di un pubblico ufficiale.

Il titolare dell'oggetto di conservazione, o un suo delegato all'attività di consultazione e produzione di duplicati informatici, ricerca i documenti attraverso i campi che l'interfaccia grafica mette a disposizione. Si tratta degli stessi metadati con i quali sono stati accompagnati i file durante l'invio al sistema di conservazione. Una volta visualizzati i file conservati, il titolare dell'oggetto di conservazione può richiedere al responsabile del servizio di conservazione un duplicato, attraverso una funzione disponibile sul portale. Detta funzione consente di scaricare il PdD attraverso il canale criptato SSL del portale. Sarà così possibile per il titolare dell'oggetto di conservazione avere una copia del pacchetto di distribuzione (PdD) 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.

Durante l'erogazione del servizio di conservazione può essere necessario l'intervento di un Notaio o altro Pubblico Ufficiale per molteplici motivi, tra cui, ad esempio, attestare la conformità, da parte di un Pubblico Ufficiale/notaio, di una copia informatica di documento informatico conservato o una copia analogica di un documento informatico originale conservato nel sistema di conservazione.

Il Responsabile della conservazione interno al titolare dell'oggetto di conservazione assicura la presenza di un notaio o pubblico ufficiale nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività da realizzare. Più nel dettaglio, l'intervento del Notaio, o del Pubblico Ufficiale, potrebbe essere richiesto nelle ipotesi disciplinate puntualmente dal Codice dell'Amministrazione Digitale (artt. 22, 23 e 23-bis) e dal Decreto del MEF del 17 giugno 2014 (art. 4) e, in particolare, quando occorra procedere alla predisposizione di:

- Copie informatiche di documenti analogici;
- Copie analogiche di documenti informatici;
- Copie ed estratti informatici di documenti informatici;
- Copie per immagine di documenti analogici originali unici.

L'attestazione di conformità delle copie o dell'estratto informatico di un documento informatico potrà essere inserita nel documento informatico contenente la copia o l'estratto. Il documento informatico così formato sarà sottoscritto con firma digitale o altra firma elettronica qualificata del Notaio o Pubblico Ufficiale incaricato. L'attestazione di conformità delle copie o dell'estratto informatico di uno o più documenti informatici può essere altresì prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia o estratto informatico. Il documento informatico così prodotto è sottoscritto con firma digitale o altra firma elettronica qualificata del notaio o del pubblico ufficiale incaricato. Qualora fosse richiesta la

presenza di un Notaio o altro Pubblico Ufficiale per l'attestazione di conformità all'originale di copie informatiche o analogiche, Il titolare dell'oggetto di conservazione avrà cura di gestire tale scelta e descriverne il processo nel suo manuale.

7.8. Scarto dei pacchetti di archiviazione

Il paragrafo 4.11. delle Linee Guida – AgID stabilisce che deve essere effettuato lo scarto del PdA dal sistema di conservazione alla scadenza dei termini di conservazione previsti dalla norma dandone informativa al soggetto produttore.
Il sistema di gestione dati, grazie alla propria concezione, permette di gestire al meglio lo scarto del materiale documentario non destinato alla conservazione permanente, ma caratterizzato invece da tempi di conservazione limitati e diversificati. Negli archivi correnti, gestiti secondo criteri aggiornati è presente 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 dal soggetto produttore. Tale elenco di scarto, dopo una verifica da parte di Asmenet S.c.a.r.l., è trasmesso dal responsabile del servizio di conservazione al responsabile della conservazione, il quale verifica il rispetto dei termini temporali stabiliti dal piano di conservazione. Nei casi di archivi pubblici o privati di particolare interesse culturale, le procedure di scarto avvengono previa autorizzazione del Ministero della Cultura. Il titolare dell'oggetto di conservazione, una volta ricevuto l'autorizzazione dal Ministero, che può essere concessa anche solo su una parte dell'elenco proposto, provvede ad adeguare, se necessario, l'elenco di scarto. Una volta che l'elenco di scarto è definitivo, il responsabile della conservazione lo trasmette al responsabile del servizio di conservazione. Solo dopo aver ricevuto l'autorizzazione, il conservatore provvederà alla distruzione dei pacchetti di archiviazione, contenuti nell'elenco di scarto.
Nel caso in cui il soggetto produttore sia un soggetto privato, il responsabile del servizio di conservazione procederà alla cancellazione dei PdA solo a seguito di un'autorizzazione scritta formalmente comunicata dal soggetto produttore al conservatore.
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. In tal senso, l'operazione di scarto viene tracciata sul sistema mediante la produzione delle informazioni sullo scarto, inclusi gli estremi della richiesta di nulla osta allo scarto e il conseguente provvedimento autorizzatorio.

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

Per una corretta conservazione a norma, che risponda alle caratteristiche richieste dal modello di riferimento OAIS, il sistema di conservazione deve 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:

- Gli utenti con accesso alla piattaforma web possono collegarsi 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:
- Indicare le tipologie di file messi a disposizione e la tecnologia scelta (es. formato ISO su server SFTP, formato ZIP, ecc..)
- Il titolare dell'oggetto di conservazione è tenuto a verificare la coerenza dei propri dati.

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.

7.10 Cessazione delle attività di conservazione

Nel caso in cui Asmenet S.c.a.r.l. 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 ad AgID a mezzo PEC, almeno sessanta giorni prima della cessazione.
Allo stesso modo, Asmenet 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, Asmenet S.c.a.r.l. è liberata dall'obbligo di conservazione nonché dagli obblighi derivanti dalle Linee Guida AgiD. Al termine delle operazioni di restituzione i dati vengono rimossi dai sistemi di Asmenet S.c.a.r.l. in modalità sicura.

In Asmenet è presente un Piano di cessazione in linea con quanto indicato nell'allegato B del Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici. Nel Piano 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 viene applicato sia nel caso di cessazione volontaria che involontaria delle attività di conservazione erogate per conto delle Pubbliche Amministrazioni.

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 14721:2012 OAIS Open Archival Information System esplicato nella gestione di tre differenti tipologie di pacchetti informativi:

- Il pacchetto di versamento (PdV): 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 (PdA): uno o più PdV sono trasformati in pacchetto di archiviazione per la conservazione. Il PdA ha un insieme completo di informazioni sulla conservazione che si aggiungono al file di metadati;
- Il pacchetto di distribuzione (PdD): il documento digitale o l'insieme dei documenti digitali, corredati da tutti o da parte dei metadati previsti nell'PdA, 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.

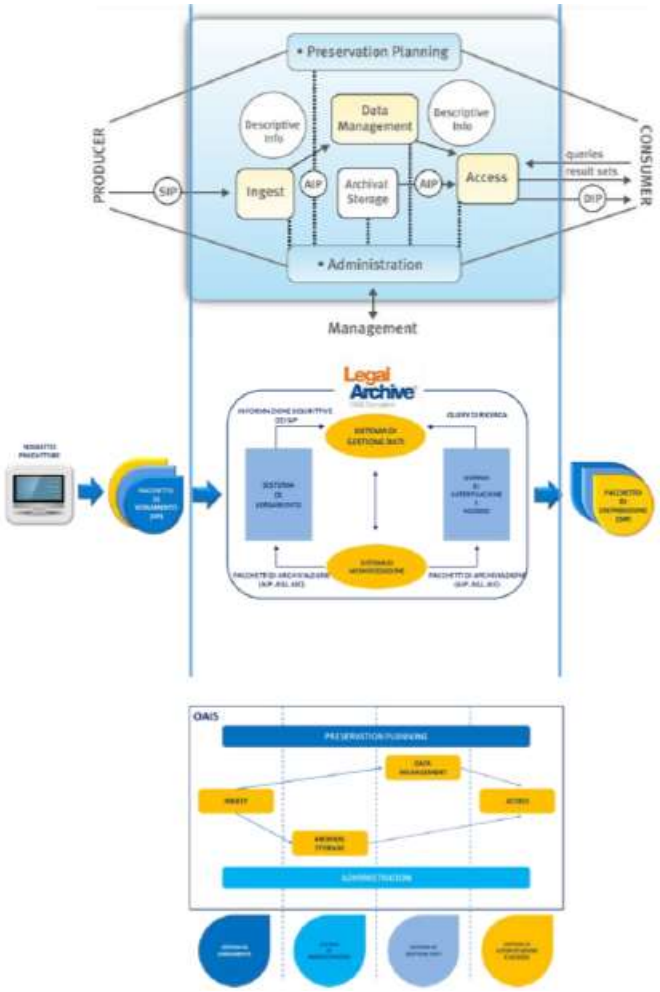


Figura 7: Il modello OAIS

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.

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 del Titolare dell'oggetto di conservazione, trasformare i pacchetti di versamento in pacchetti di archiviazione ed infine di inviare ai sistemi opportuni, le informazioni

e i dati per garantire la conservazione dei documenti informatici e la loro fruibilità alla comunità di riferimento.
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 PdV inviati dal produttore dei PdV. Innanzitutto, viene generata la "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 PdD 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 dei metadati: alcuni metadati potrebbero essere compilati in questa fase in maniera automatica (ad esempio potrebbero essere aggiunte le informazioni relative all'utente che ha effettuato il versamento e la data di versamento).

Il risultato della convalida è riepilogato da un esito in formato XML (rapporto di versamento). I documenti informatici, per i quali l'esito della convalida è risultato positivo, possono quindi essere inseriti in un pacchetto di archiviazione. L'esito restituito contiene, in un file in formato XML, la lista dei file, il relativo hash e l'identificativo univoco che è stato assegnato al file dal sistema di conservazione e che potrà essere utilizzato per accedere al file.

Tipo anomalia	Descrizione	Modalità di gestione
Mancata risposta al versamento	È il caso in cui l'oggetto digitale(documento) viene correttamente versato ma, per vari motivi, la risposta di avvenuta ricezione non perviene al produttore, che pertanto, erroneamente, lo reputa non versata.	Il produttore/conservatore deve trasmettere nuovamente e il sistema di conservazione restituisce una risposta di esito negativo con l'indicazione che l'unità documentaria risulta già versata. Tale risposta deve essere usata dal produttore come attestazione di avvenuto versamento e l'unità documentaria deve risultare come versata.
Errori temporanei	È il caso di errori dovuti a problemi temporanei che pregiudicano il versamento, ma si presume non si ripresentino a un successivo tentativo di versamento. Il caso più frequente è l'impossibilità temporanea di accedere alle CRL degli enti certificatori. In questi casi il sistema di conservazione dopo aver riprovato 10 volte genera un messaggio di errore perché non riesce a completare le verifiche previste sulla validità della firma e il versamento viene quindi rifiutato impostando il processo in stato ERRV.	Il produttore/conservatore deve provvedere a rinviare l'oggetto digitale(documento) 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 sistema di conservazione invia via e-mail una segnalazione dell'anomalia ai referenti indicati dal Titolare dell'oggetto di conservazione, 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 e alle descrizioni dei documenti. Inoltre, consente di avere una visione unitaria dell'archivio e consente di accedervi. Attraverso tale modulo il soggetto produttore potrà vedere il complesso sistema di relazioni tra gli oggetti digitali. 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 dell'archivio, il conservatore acquisisce gli strumenti archivistici del Titolare dell'oggetto di conservazione (piano di classificazione, piano di conservazione, ecc.). L'aggiornamento del piano di conservazione memorizzato nel sistema di conservazione è demandato Titolare dell'oggetto di conservazione.

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”.

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 della conservazione ed eventualmente anche ad un notaio (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 CA:
  - 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 Asmenet S.c.a.r.l. si avvale di: **Actalis Spa.**

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 Asmenet S.c.a.r.l. si avvale di: **Aruba Spa**.

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;
- Persistence layer.

L'estrema elasticità del software permette di sostituire, aggiornare 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 a cui l'applicazione attinge. Il Back End ha in carico la gestione e la distribuzione dei processi tra i vari nodi del cluster.
- **Engine**: è il motore di conservazione.
- **Front End** (Interfaccia Web): è un'applicazione realizzata attraverso l'uso di pagine web dinamiche per permettere l'interazione con il sistema.

Attraverso Front End gli utenti potranno accedere per configurare e monitorare il sistema. La tecnologia usata garantisce la compatibilità con una larga parte degli attuali browser senza la necessità di installare ulteriori plug-in sul client. Di seguito la lista dei browser dichiarati compatibili:

- Android 4 o superiore;
- Google Chrome 59 o superiore;
- Internet Explorer 11, Edge o superiore;
- iOS 9 o superiore;
- Mozilla Firefox 54 o superiore;
- Safari 9 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;
- **Data Base**: la componente dedicata all'archiviazione delle informazioni associate al sistema e ai dati archiviati;
- **Repository**: la componente dedicata all'archiviazione degli oggetti digitali sottoposti a conservazione.

In un'ottica di installazione su ambienti virtuali, il sistema consente una scalabilità al crescere degli utenti coinvolti e dei volumi di documenti da conservare, permettendo all'azienda di reagire tempestivamente ad eventuali esigenze del titolare dell'oggetto di conservazione. La figura seguente descrive schematicamente le dipendenze delle diverse componenti tecnologiche del software di conservazione sopra citate.

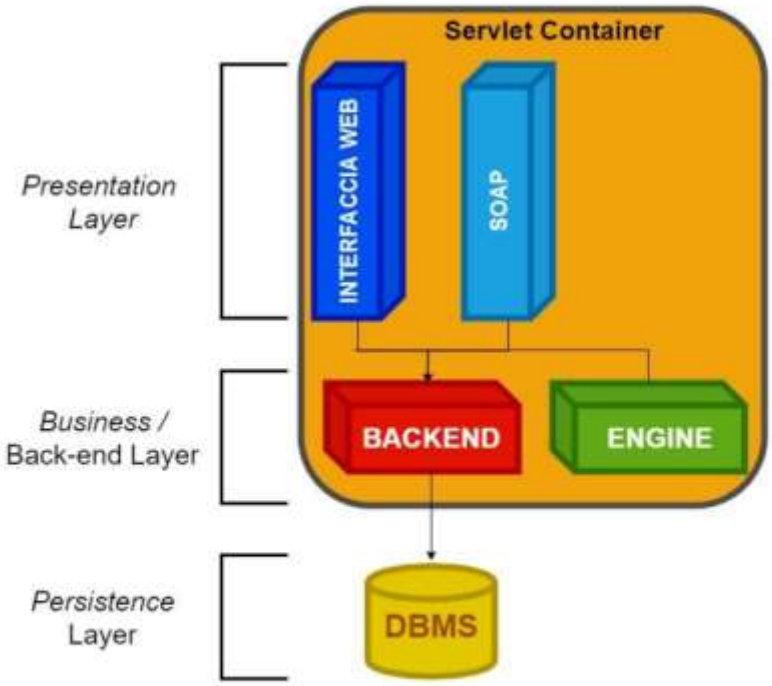


Figura 7: componenti scalabili del sistema

8.3. Componenti fisiche

L'impianto fisico del sistema di conservazione di Asmenet S.c.a.r.l. è situato in Europa, all'interno della struttura Google Cloud Platform, disponibile in diverse regioni, a partire da settembre 2018. Google Cloud Platform è disponibile in Europa e nel 2022 saranno inaugurate due nuove regioni in Italia. I dati saranno pertanto allocati in Europa, nel rispetto del GDPR 679/2016.

8.4 Procedure di gestione e di evoluzione

Gli interventi di manutenzione evolutiva sono assimilabili ad un insieme di piccoli progetti con durate 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.

Manutenzione correttiva del software

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

La presenza di un eventuale bug nel sistema di conservazione può essere segnalata dalla comunità di riferimento, dai tecnici di Asmenet S.c.a.r.l. oppure da Ifin Sistemi, tramite il proprio reparto tecnico.

La segnalazione di un bug rilevato dal personale di Asmenet S.c.a.r.l. può essere indirizzata ad Ifin Sistemi tramite l'apertura di un ticket di assistenza. Tale procedura viene espletata mediante l'apertura di un ticket presso il portale di assistenza IFIN Sistemi, disponibile all'URL *https://support.ifin.it*.
Il team di assistenza di IFIN Sistemi prende in carico la richiesta di correzione di malfunzionamento e ne verifica l'effettiva sussistenza. Se questa è verificata la segnalazione passa al gruppo di lavoro di Ifin Sistemi impegnato nella manutenzione del software.
Il team di manutenzione e sviluppo software di Ifin Sistemi analizza il bug, individua gli oggetti coinvolti dall'attività, eventuali effetti collaterali su altri oggetti software e 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 o gli eventuali fix rilasciati verranno resi disponibili al personale tecnico di Asmenet S.c.a.r.l. ed eventualmente installati dai tecnici Ifin sul sistema di conservazione seguendo le attività previste dai processi di change management.

8.5. 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.

8.6. Misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali

In conformità al Regolamento (UE) 2016/679 (GDPR), vengono adottate misure di sicurezza per il trattamento dei dati personali. Al riguardo, il Piano della Sicurezza di Asmenet S.c.a.r.l. (al quale si rimanda) prevede opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali ai sensi dell'art. 32 del Regolamento UE 679/2016 (GDPR), anche in funzione delle tipologie di dati trattati, quali quelli riferibili alle categorie particolari di cui agli artt. 9-10 del Regolamento stesso. Il Piano della Sicurezza prevede, altresì, l'applicazione di una procedura in caso di violazione dei dati personali ai sensi degli artt. 33-34 del GDPR. Sono previste, inoltre, l'adozione di eventuali altre misure necessarie a garantire i diritti degli interessati ai sensi dell'art. 12 del Regolamento (UE) 2016/679 (GDPR), nonché opportuni processi di gestione della continuità operativa (business continuity) secondo le buone pratiche previste dallo standard ISO/IEC 22313, in cui sono previste azioni orientate al ripristino dell'operatività del servizio e dei dati da esso gestiti al verificarsi di eventi catastrofici/imprevisti.
Per ulteriori dettagli, si rimanda al Piano della Sicurezza.

9. MONITORAGGIO E CONTROLLO

Descrizione generale della strategia della conservazione e dei conseguenti obiettivi di monitoraggio e controllo. In particolare, i log di Back End e i log di Engine sono scritti e gestiti direttamente dal software Legal Archive.

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. Per qualsiasi problema viene contattato l'HelpDesk di IFIN che provvede a visionare i Log. I campi contenuti nel Log sono stati definiti da IFIN in fase di progettazione del software.

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>;
- <tipo di operazione richiesta>;
- <dettaglio dell'operazione richiesta> (eventuale).

Di seguito sono indicate le richieste tracciate con le relative risposte:

- *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.

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 il Titolare dell'oggetto di conservazione. A ogni verifica effettuata viene generato un report in formato xml, che può essere consultato da parte del responsabile della conservazione per attestare la corretta esecuzione della verifica o per diagnosticare eventuali anomalie.

9.3. Soluzioni adottate in caso di anomalie

La gestione delle anomalie dovute a problemi legati ad infrastrutture o attività operative rientra nei processi gestionali di Asmenet S.c.a.r.l. In conformità al Regolamento (UE) 2016/679 (GDPR), vengono adottate misure di sicurezza per il trattamento dei dati personali. Al riguardo, il Piano della Sicurezza di Asmenet prevede opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali ai sensi dell'art. 32 del Regolamento UE 679/2016, anche in funzione delle tipologie di dati trattati, quali quelli riferibili alle categorie particolari di cui agli artt. 9-10 del Regolamento stesso. Il Piano della Sicurezza prevede, altresì, l'applicazione di una procedura in caso di violazione dei dati personali ai sensi degli artt. 33-34 del GDPR. Sono previste, inoltre, l'adozione di eventuali altre misure necessarie a garantire i diritti degli interessati ai sensi dell'art. 12 del Regolamento (UE) 2016/679 (GDPR), nonché opportuni processi di gestione della continuità operativa (business continuity), in cui sono previste azioni orientate al ripristino dell'operatività del servizio e dei dati da esso gestiti al verificarsi di eventi catastrofici/imprevisti.

9.4. Anomalia dovute a malfunzionamento dell'impianto

La gestione delle anomalie dovute a malfunzionamento dell'impianto rientra nei processi gestionali di Asmenet S.c.a.r.l.
Il Titolare del Trattamento Asmenet, coadiuvato dal suo Data Protection Officer, ha condotto in modo completo un'analisi con l'obiettivo di identificare i rischi per la sicurezza e la custodia dei dati personali trattati dalla società e per individuare le aree in cui vi è il pericolo di distruzione o perdita, anche accidentale dei dati.
Il Regolamento Europeo 2016-679 impone che i dati personali, a maggior ragione quelli qualificati come sensibili, debbano essere trattati in maniera da garantirne un'adeguata sicurezza e protezione, mediante l'adozione di misure tecniche ed organizzative, per ovviare a trattamenti non autorizzati, illeciti e dalla perdita, dalla distruzione o dal danno accidentali. In tal senso, la direzione ha scelto di trasferire l'infrastruttura attiva presso il Data Center TIM di Napoli su server Google Cloud Platform in data 21 gennaio 2022. Google applica e mantiene in vigore misure tecniche e

organizzative per proteggere i Dati di Asmenet da distruzione accidentale o illegale, perdita, alterazione, divulgazione o accesso non autorizzati. Le Misure di Sicurezza includono misure per la crittografia dei dati personali; per contribuire a garantire la costante riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di Google; per contribuire a ripristinare tempestivamente l'accesso ai dati personali in seguito ad un incidente; e per effettuare regolari test di efficacia. Nell'erogazione dei Servizi Google garantisce il mantenimento delle seguenti misure di sicurezza.

Sicurezza del data center e della rete

a) Data Center.

Infrastruttura. Google gestisce data center geograficamente distribuiti. Google conserva tutti i dati di produzione in data center sicuri in termini di misure di sicurezza fisiche.

Ridondanza. I sistemi infrastrutturali sono stati progettati per eliminare i singoli punti di guasto e ridurre al minimo l'impatto dei rischi ambientali previsti. I circuiti doppi, gli interruttori, le reti o altri dispositivi necessari contribuiscono a fornire questa ridondanza. I Servizi sono progettati in modo da consentire a Google di eseguire alcuni tipi di manutenzione preventiva e correttiva senza interruzioni. Tutte le apparecchiature e le strutture ambientali sono dotate di procedure di manutenzione preventiva documentate che descrivono in dettaglio il processo e la frequenza delle prestazioni in conformità alle specifiche del produttore o alle specifiche interne. La manutenzione preventiva e correttiva delle apparecchiature del data center è pianificata attraverso un processo di modifica standard secondo procedure documentate.

Alimentazione. I sistemi di alimentazione elettrica dei data center sono progettati per essere ridondanti e soggetti a manutenzione senza impatto per le operazioni continue, 24 ore al giorno, 7 giorni alla settimana. Nella maggior parte dei casi, una fonte di alimentazione primaria così come una fonte di alimentazione alternativa, ciascuna con uguale capacità, è fornita per i componenti critici dell'infrastruttura del data center. L'alimentazione di backup è fornita con varie modalità come le batterie dei gruppi di continuità (UPS), che forniscono una protezione di alimentazione costantemente affidabile durante i blackout, i blackout, le sovratensioni, le sottotensioni e le condizioni di frequenza fuori tolleranza. In caso di interruzione dell'alimentazione di rete, l'alimentazione di riserva è progettata per fornire energia transitoria al data center a piena capacità per un massimo di 10 minuti fino a quando i generatori diesel subentrano. I generatori diesel sono in grado di avviarsi automaticamente in pochi secondi per fornire energia elettrica di emergenza sufficiente a far funzionare il data center a piena capacità, tipicamente per un periodo di giorni.

Sistemi operativi dei server. I server di Google utilizzano un'implementazione basata su Linux personalizzata per l'ambiente applicativo. I dati sono memorizzati utilizzando algoritmi proprietari per aumentare la sicurezza e la ridondanza dei dati. Google impiega un processo di revisione del codice per aumentare la sicurezza del codice utilizzato per fornire i Servizi e migliorare i prodotti di sicurezza negli ambienti di produzione.

Business Continuity. Google ha progettato e pianifica e verifica regolarmente i suoi programmi di pianificazione di business continuity e di ripristino di emergenza.

b) Reti e trasmissione.

Trasmissione dati. I data center sono tipicamente collegati tramite collegamenti privati ad alta velocità per fornire un trasferimento dati sicuro e veloce tra i centri dati. Questo è progettato per evitare che i dati possano essere letti, copiati, alterati o rimossi senza autorizzazione durante il trasferimento o il trasporto elettronico o durante la registrazione su supporti di memorizzazione dei dati. Google trasferisce i dati tramite i protocolli standard di Internet.
Protezione da attacchi esterni. Google utilizza più strati di dispositivi di rete e di rilevamento delle intrusioni per proteggere la sua superficie di attacco esterno. Google analizza i potenziali vettori di attacco e incorpora tecnologie appropriate nei sistemi a tutela da attacchi esterni.
Rilevamento intrusioni. Il rilevamento delle intrusioni ha lo scopo di fornire informazioni sulle attività di attacco in corso e di fornire informazioni adeguate per rispondere agli incidenti. Il rilevamento delle intrusioni di Google comporta:

- rigorosi controlli sulle dimensioni e sulla composizione della superficie d'attacco di Google attraverso misure preventive;
- utilizzo di controlli di rilevamento intelligenti nei punti di ingresso dati; e
- utilizzo di tecnologie che pongono automaticamente rimedio ad alcune situazioni di pericolo.

Risposta agli incidenti. Google monitora una serie di canali di comunicazione per gli incidenti di sicurezza e il personale di sicurezza di Google reagisce prontamente agli incidenti noti.
Tecnologie di crittografia. Google mette a disposizione la crittografia HTTPS (chiamata anche connessione SSL o TLS). I server di Google supportano lo scambio di chiavi crittografiche effimere a curva ellittica Diffie-Hellman firmato con RSA ed ECDSA. Questi metodi di perfetta segretezza in avanti (PFS) aiutano a proteggere il traffico e a minimizzare l'impatto di una chiave compromessa, o di una svolta crittografica.

Controlli di accesso e del sito
(a) Controlli del Sito.
Operazione di Sicurezza del Data Center In Loco. I data center di Google mantengono un servizio di sicurezza in loco responsabile di tutte le funzioni di sicurezza dei data center fisici 24 ore al giorno, 7 giorni alla settimana. Il personale addetto alle operazioni di sicurezza in loco controlla le telecamere a circuito chiuso (CCTV) e tutti i sistemi di allarme. Il personale addetto alle operazioni di sicurezza in loco effettua regolarmente pattugliamenti interni ed esterni del centro dati.
Procedure di Accesso al Data Center. Google mantiene procedure di accesso formali per consentire l'accesso fisico ai data center. I data center sono ospitati in strutture che richiedono l'accesso con chiave elettronica, con allarmi collegati al servizio di sicurezza in loco. Tutti coloro che accedono al data center sono tenuti a identificarsi e a mostrare un documento di identità al servizio di sicurezza in loco. Solo i dipendenti autorizzati, gli appaltatori e i visitatori sono autorizzati ad entrare nei data center. Solo i dipendenti e gli appaltatori autorizzati sono autorizzati a richiedere l'accesso con chiave elettronica a queste strutture. Le richieste di accesso con chiave elettronica al data center devono essere effettuate tramite e-mail e richiedono l'approvazione del responsabile del richiedente e del direttore del data center. Tutti gli altri partecipanti che richiedono l'accesso temporaneo al data center devono: (i) ottenere l'approvazione in anticipo dai responsabili del data center per il data center specifico e le rispettive aree interne che desiderano visitare; (ii) registrarsi presso il servizio di sicurezza in loco; e (iii) registrarsi in un registro di accesso dei soggetti autorizzati al data center che identifichi l'individuo come approvato.

Dispositivi di Sicurezza del Data Center in loco. I data center di Google utilizzano una chiave elettronica e un sistema di controllo accessi biometrico collegato ad un sistema di allarme. Il sistema di controllo degli accessi monitora e registra la chiave elettronica di ogni individuo e quando accede alle porte perimetrali, all'area spedizione e ricevimento e ad altre aree critiche. Le attività non autorizzate e i tentativi di accesso non riusciti vengono registrati dal sistema di controllo d'accesso e investigati, a seconda dei casi. L'accesso autorizzato in tutte le aree aziendali e nei data center è limitato in base alle zone e alle responsabilità lavorative dell'individuo. Le porte antincendio dei data center sono allarmate. Le telecamere a circuito chiuso sono in funzione sia all'interno che all'esterno dei data center. Il posizionamento delle telecamere è stato progettato per coprire aree strategiche che comprendono, tra l'altro, il perimetro, le porte dell'edificio del data center e l'area spedizione/ricevimento. Il personale addetto al servizio di sicurezza in loco gestisce le apparecchiature di monitoraggio, registrazione e controllo delle telecamere a circuito chiuso. In tutti i data center le apparecchiature CCTV sono collegate da cavi cablati. Le telecamere registrano sul posto tramite videoregistratori digitali 24 ore al giorno, 7 giorni alla settimana. Le registrazioni di sorveglianza vengono conservate per un massimo di 30 giorni in base all'attività.

b) Controllo degli Accessi.

Personale di Sicurezza delle Infrastrutture. Google ha e mantiene una politica di sicurezza per il suo personale e ritiene necessaria una formazione sulla sicurezza come parte del pacchetto di formazione per il suo personale. Il personale addetto alla sicurezza delle infrastrutture di Google è responsabile del monitoraggio continuo dell'infrastruttura di sicurezza di Google, della revisione dei Servizi e della risposta agli incidenti di sicurezza.

Controllo degli Accessi e Gestione dei Privilegi. Per amministrare i Servizi gli amministratori del Partner devono autenticarsi tramite un sistema di autenticazione centrale o tramite sistema ad autenticazione singola.

Processi e Politiche Interne di Accesso ai Dati - Politica di Accesso. I processi e le politiche interne di accesso ai dati di Google sono definiti in modo da impedire a persone e/o sistemi non autorizzati di accedere ai sistemi utilizzati per il trattamento dei dati personali. Google progetta i propri sistemi in modo da (i) consentire solo alle persone autorizzate di accedere ai dati a cui sono autorizzate ad accedere; e (ii) garantire che i dati personali non possano essere letti, copiati, alterati o rimossi senza autorizzazione durante il trattamento, l'uso e dopo la registrazione. I sistemi sono progettati per rilevare qualsiasi accesso inappropriato. Google utilizza un sistema di gestione degli accessi centralizzato per controllare l'accesso del personale ai server di produzione e fornisce l'accesso solo a un numero limitato di persone autorizzate. I sistemi di autenticazione e autorizzazione di Google utilizzano certificati SSH e chiavi di sicurezza e sono progettati per fornire a Google meccanismi di accesso sicuri e flessibili. Questi meccanismi sono progettati per concedere solo diritti di accesso approvati agli host del sito, ai log, ai dati e alle informazioni di configurazione. Google richiede l'uso di ID utente univoci, password forti, autenticazione a due fattori e liste di accesso attentamente monitorate per ridurre al minimo il potenziale di utilizzo non autorizzato dell'account. La concessione o la modifica dei diritti di accesso si basa su: le responsabilità lavorative del personale autorizzato, i requisiti di lavoro necessari per svolgere le attività autorizzate e la necessità di conoscere le basi. La concessione o la modifica dei diritti di accesso deve anche essere conforme

alle politiche interne di accesso ai dati e alla formazione di Google. Le approvazioni sono gestite da strumenti di workflow che conservano registrazioni di audit di tutte le modifiche. L'accesso ai sistemi viene registrato per creare una traccia di audit per la responsabilità. Laddove le password vengono utilizzate per l'autenticazione (ad esempio, il login alle workstation), vengono implementate politiche di password che seguono almeno le pratiche standard del settore. Questi standard includono restrizioni sul riutilizzo delle password e una sufficiente robustezza delle password. Per l'accesso a informazioni estremamente sensibili (ad es. dati della carta di credito), Google utilizza token hardware.

Dati

a) Conservazione, Isolamento e Registrazione dei dati. Google memorizza i dati in un ambiente multi-tenant su server di proprietà di Google. Con riserva di eventuali istruzioni contrarie di TIM, in conformità alle istruzioni ricevute dal Titolare (ad esempio, sotto forma di decisione specifica sul luogo di conservazione dei dati), Google replica i Dati del Richiedente tra più data center geograficamente distribuiti. Google isola logicamente anche i Dati del Richiedente. TIM avrà il controllo su specifiche policy di condivisione dei dati che gestirà nel rispetto delle istruzioni ricevute dal Richiedente. Tali policy, in conformità con le funzionalità dei Servizi, consentiranno a TIM di determinare le impostazioni di condivisione dei prodotti applicabili al Richiedente per scopi specifici. TIM può scegliere di utilizzare le funzionalità di registrazione che Google mette a disposizione tramite i Servizi, se così istruito dal Richiedente.

b) Dischi Dismessi e Politica di Cancellazione dei Dischi. I dischi contenenti dati possono presentare problemi di prestazioni, errori o guasti hardware che li portano alla disattivazione ("Disco Dismesso"). Ogni Disco Dismesso è soggetto a una serie di processi di distruzione dei dati (la "Disk Erase Policy") prima di lasciare la sede di Google per il riutilizzo o la distruzione. I Dischi Dismessi vengono cancellati in un processo in più fasi e verificati da almeno due validatori indipendenti. I risultati della cancellazione vengono registrati dal numero di serie del disco dismesso per il tracciamento. Infine, il Disco Dismesso cancellato viene rilasciato nell'inventario per il riutilizzo e il riposizionamento. Se, a causa di un guasto dell'hardware, il Disco Dismesso non potesse essere cancellato, verrebbe conservato in modo sicuro fino a quando non può essere distrutto. Ogni struttura viene controllata regolarmente per monitorare la conformità con la Disk Erase Policy.

9.5. Malfunzionamento del sistema

La funzionalità di verifica di integrità degli archivi permette di verificare l'integrità dei documenti dal momento del versamento al sistema di conservazione. Tale funzionalità risulta utile nell'assolvimento dei requisiti di verifica periodica della leggibilità dei documenti, come richiesto dalla normativa. La verifica prevede un controllo periodico sui documenti archiviati e, al termine del processo di verifica, la generazione di un report che attesta la corretta esecuzione della verifica o per diagnosticare eventuali anomalie.