MINISTERO DELL'ISTRUZIONE – *UFFICIO SCOLASTICO REGIONALE PER LA CALABRIA*
ISTITUTO COMPRENSIVO STATALE A INDIRIZZO MUSICALE – **CARIATI**
Scuola dell'Infanzia – Primaria – Secondaria di I grado

SEDE LEGALE E AMMINISTRATIVA IN VIA DANTE ALIGHIERI – 87062 CARIATI (CS) _ TEL./FAX 0983-91309
COD. MECC.: CSIC892009 – COD. FIS.: 97022300780 – COD. UNIVOCO: UFQA77
PEO: CSIC892009@ISTRUZIONE.IT PEC: CSIC892009@PEC.ISTRUZIONE.IT *WEBSITE*: WWW.ICCARIATI.EDU.IT

MANUALE DI CONSERVAZIONE
DEI DOCUMENTI INFORMATICI DELL'ISTITUZIONE SCOLASTICA

Adottato ai sensi del Codice dell'amministrazione digitale e delle Linee guida AgID sulla formazione, gestione e conservazione dei documenti informatici

Versione	1.0
Data di adozione	
Responsabile della Conservazione	Sara Giulia Aiello
Vicario del Responsabile della Conservazione	*DSGA Pro-tempore*
Conservatore accreditato	NAMIRIAL
Allegato	Manuale tecnico del Conservatore

Sommario

CAPITOLO 1 – FINALITÀ, NATURA E CAMPO DI APPLICAZIONE 4
1.1 Finalità del Manuale 4
1.2 Natura del Manuale 4
1.3 Campo di applicazione 5
1.4 Rapporto con il Manuale di gestione documentale 5
CAPITOLO 2 – RIFERIMENTI NORMATIVI 6
2.1 Quadro normativo generale 6
2.2 Principi applicabili 7
2.3 Rilevanza archivistica della conservazione 7
CAPITOLO 3 – DEFINIZIONI E ACRONIMI 8
3.1 Definizioni 8
3.2 Acronimi 9
CAPITOLO 4 – MODELLO ORGANIZZATIVO 10
4.1 Struttura organizzativa dell'Istituzione scolastica 10
4.2 Assetto generale e modello di conservazione adottato 10
4.3 Integrazione con il sistema di gestione documentale 10
CAPITOLO 5 – RUOLI E RESPONSABILITÀ 11
5.1 Il Responsabile della conservazione 11
5.2 Il Dirigente Scolastico 11
5.3 Il DSGA 12
5.4 Il personale di segreteria 12
5.5 Il conservatore accreditato 12
5.6 Il DPO 12
CAPITOLO 6 – TIPOLOGIA DEI DOCUMENTI SOGGETTI A CONSERVAZIONE 14
6.1 Criteri generali 14
6.2 Classificazione delle tipologie documentali 14
6.3 Formati ammessi 16
6.4 Metadati 16
6.5 Controlli di qualità 16
CAPITOLO 7 – IL PROCESSO DI CONSERVAZIONE 17
7.1 Descrizione del processo 17
7.2 Fasi del processo 17
7.2.1 Formazione del documento informatico 17
7.2.2 Registrazione e segnatura di protocollo 17
7.2.3 Classificazione e fascicolazione 17
7.2.4 Firma digitale e marcatura temporale 17
7.2.5 Versamento al sistema di conservazione 17
7.2.6 Presa in carico e archiviazione 18

7.2.7 Rifiuto o anomalia del versamento 18
7.2.8 Esibizione e recupero dei documenti 18
CAPITOLO 8 – MODALITÀ DI VERSAMENTO 19
8.1 Modalità operative 19
8.2 Predisposizione del pacchetto di versamento 19
8.3 Ricevuta di versamento e gestione degli errori 19
CAPITOLO 9 – MODALITÀ DI ESIBIZIONE E ACCESSO 20
9.1 Principi generali sull'accesso 20
9.2 Soggetti legittimati all'accesso 20
9.3 Esibizione dei documenti conservati 20
9.4 Esibizione per finalità legali e probatorie 20
9.5 Copie ed estratti 20
CAPITOLO 10 - MONITORAGGIO, VERIFICHE E AGGIORNAMENTO 21
10.1 Monitoraggio interno 21
10.2 Verifiche con il Conservatore 21
10.3 Aggiornamento del Manuale 21
CAPITOLO 11 – MISURE DI SICUREZZA 22
11.1 Principi generali 22
11.2 Misure a carico dell'Istituzione scolastica 22
11.3 Misure a carico del conservatore accreditato 22
11.4 Protezione dei dati personali 22
CAPITOLO 12 – VERIFICHE E AUDIT 23
12.1 Verifiche periodiche del sistema di conservazione 23
12.2 Audit del conservatore accreditato 23
CAPITOLO 13 – AGGIORNAMENTO E REVISIONE DEL MANUALE 24
13.1 Ciclo di vita del Manuale 24
13.2 Casi che determinano la revisione 24
13.3 Procedura di aggiornamento 24
CAPITOLO 14 - DISPOSIZIONI FINALI 24
14.1 Adozione 24
14.2 Obbligo di osservanza 24
14.3 Entrata in vigore 25
ALLEGATI 25

CAPITOLO 1 – FINALITÀ, NATURA E CAMPO DI APPLICAZIONE

1.1 Finalità del Manuale

Il presente **Manuale di conservazione** costituisce il documento operativo di riferimento per la gestione del processo di conservazione permanente dei documenti informatici prodotti e ricevuti dall'Istituzione scolastica nell'esercizio delle proprie funzioni istituzionali, amministrative, didattiche, contabili e organizzative. Esso è redatto in conformità alle disposizioni normative vigenti in materia di formazione, gestione e conservazione dei documenti informatici nelle pubbliche amministrazioni.

Il Manuale persegue le seguenti finalità principali: garantire la corretta esecuzione del processo di conservazione nel rispetto dei requisiti di autenticità, integrità,, affidabilità, leggibilità e reperibilità dei documenti nel tempo; descrivere l'organizzazione interna preposta alla conservazione, i ruoli e le responsabilità dei soggetti coinvolti; illustrare le tipologie documentali oggetto di conservazione; disciplinare le modalità di versamento, di accesso e di esibizione dei documenti conservati; definire le misure di sicurezza adottate a protezione del sistema di conservazione.

Il Manuale costituisce, dunque, il documento interno di riferimento attraverso il quale la scuola descrive come assicura nel tempo la conservazione dei documenti informatici, garantendone autenticità, integrità, affidabilità, leggibilità, reperibilità e utilizzabilità. La conservazione non rappresenta una fase meramente tecnica, ma una funzione essenziale dell'azione amministrativa, poiché consente alla scuola di mantenere nel tempo la validità giuridica, amministrativa, probatoria e archivistica dei propri documenti. Ha natura vincolante per tutto il personale dell'Istituzione scolastica che, a qualsiasi titolo, intervenga nel processo di produzione, gestione e conservazione dei documenti informatici, nonché per i soggetti terzi eventualmente coinvolti.

Il processo di conservazione è realizzato attraverso il Sistema di conservazione messo a disposizione dal Conservatore individuato dall'Istituzione scolastica. Il Conservatore opera secondo il proprio Manuale tecnico di conservazione, che viene allegato al presente Manuale e ne costituisce parte integrante per gli aspetti tecnici, infrastrutturali, applicativi e di sicurezza relativi al servizio erogato.

1.2 Natura del Manuale

Il Manuale definisce le scelte organizzative della scuola e chiarisce il rapporto tra la gestione documentale interna e il servizio di conservazione affidato all'esterno. La scuola conserva la titolarità dei propri documenti, delle proprie funzioni amministrative e delle decisioni relative alla corretta formazione, classificazione, fascicolazione, selezione e trasmissione in conservazione dei documenti informatici.

Il Conservatore assicura la gestione tecnica del sistema di conservazione, secondo quanto previsto dal contratto, dal proprio Manuale tecnico, dalle Linee guida AgID e dalla normativa applicabile.

1.3 Campo di applicazione

Il presente Manuale si applica a tutti i documenti informatici prodotti e ricevuti dall'Istituzione scolastica, nonché ai documenti analogici oggetto di dematerializzazione, che siano soggetti a obblighi di conservazione ai sensi della normativa vigente.

L'ambito applicativo comprende: i documenti del registro di protocollo informatico; i fascicoli del personale e degli alunni; i documenti di natura contabile e amministrativo-gestionale; gli atti deliberativi degli organi collegiali; la documentazione didattica e valutativa; ogni altro documento informatico che, per legge o per disposizione interna, debba essere conservato in modo permanente o per un arco temporale definito. Sono compresi i documenti informatici acquisiti da soggetti esterni, qualora entrino stabilmente nel sistema documentale della scuola e debbano essere conservati nell'ambito dei procedimenti amministrativi di competenza.

Il Manuale si applica altresì ai metadati associati ai documenti e alle aggregazioni documentali (fascicoli, serie), che costituiscono parte integrante del sistema di conservazione.

1.4 Rapporto con il Manuale di gestione documentale

Il presente Manuale si coordina con il Manuale di gestione documentale dell'Istituzione scolastica. Il Manuale di gestione documentale disciplina la formazione, ricezione, protocollazione, classificazione, fascicolazione, gestione e archiviazione corrente dei documenti. Il Manuale di conservazione disciplina invece la fase successiva e complementare, relativa al trasferimento dei documenti nel sistema di conservazione e alla loro conservazione nel tempo.

I due documenti devono essere letti congiuntamente, perché la corretta conservazione dipende dalla corretta formazione e gestione del documento fin dalla sua origine. Un documento formato in modo non corretto, privo dei metadati necessari, non classificato o non fascicolato correttamente, può generare criticità nella fase di conservazione, nella successiva ricerca e nell'eventuale esibizione.

CAPITOLO 2 – RIFERIMENTI NORMATIVI

2.1 Quadro normativo generale

Il processo di conservazione dei documenti informatici è disciplinato da un articolato sistema di fonti normative, di rango primario e secondario, di natura sia legislativa che tecnica. L'Istituzione scolastica è tenuta al rispetto di tale quadro normativo nella sua interezza, anche in relazione agli aggiornamenti che intervengano successivamente all'adozione del presente Manuale.

Le principali disposizioni di riferimento sono le seguenti.

Fonte normativa	Contenuto rilevante
D.Lgs. 82/2005 (Codice del consumo digitale – CAF)	Base normativa per la formazione, gestione e conservazione dei documenti informatici nelle PA
D.Lgs. 82/2005 – CAD (art. 44)	Requisiti del sistema di conservazione e conservatore accreditato
D.P.C.M. 3 dicembre 2013	Regole tecniche per il protocollo informatico
D.P.C.M. 13 novembre 2014	Regole tecniche per la formazione, gestione, conservazione e trasmissione dei documenti informatici
Linee guida AgID (D.Lgs. 82/2005, art. 71) – 2020 e ss.mm.ii.	Documento di riferimento tecnico-operativo per la gestione documentale e la conservazione
D.Lgs. 42/2004 (Codice dei beni culturali)	Disciplina dei beni archivistici e obblighi di conservazione
D.P.R. 445/2000	Testo unico sulla documentazione amministrativa
D.Lgs. 196/2003 e Reg. UE 2016/679 (GDPR)	Protezione dei dati personali nel trattamento e nella conservazione
Circolare AGID n. 65/2014	Modalità per l'accreditamento dei conservatori
Normativa scolastica specifica (D.I. 129/2018, D.Lgs. 297/1994, ecc.)	Obblighi di tenuta dei registri e della documentazione scolastica

2.2 Principi applicabili

Il processo di conservazione si ispira ai principi di legalità, buon andamento, imparzialità, trasparenza, responsabilizzazione, sicurezza, proporzionalità, continuità operativa e tutela dell'archivio pubblico.

La scuola organizza il processo di conservazione in modo da assicurare che i documenti mantengano nel tempo la loro validità giuridica e amministrativa. A tal fine, il processo deve garantire la corretta identificazione dei documenti, la completezza dei metadati, la tracciabilità delle operazioni, la protezione contro modifiche non autorizzate, la possibilità di ricerca e recupero, l'esibizione nei casi previsti e la conservazione per il periodo stabilito dalla normativa e dal piano di conservazione.

2.3 Rilevanza archivistica della conservazione

I documenti prodotti e acquisiti dalla scuola costituiscono archivio pubblico. La conservazione digitale deve quindi rispettare non solo le esigenze tecniche di mantenimento dei file, ma anche la corretta tenuta dell'archivio scolastico.

La scuola deve evitare una gestione frammentata, disordinata o meramente informatica dei documenti. Il documento conservato deve rimanere collegato al procedimento, al fascicolo, alla classificazione, al contesto amministrativo e ai metadati che ne consentono la comprensione nel tempo. La conservazione digitale non coincide con il semplice salvataggio di file in cartelle, server, cloud, registro elettronico, segreteria digitale o posta elettronica, ma un documento si considera correttamente conservato solo quando viene inserito in un processo strutturato di conservazione conforme alle regole vigenti.

CAPITOLO 3 – DEFINIZIONI E ACRONIMI

3.1 Definizioni

Ai fini del presente Manuale si adottano le definizioni contenute nelle Linee guida AgID sulla gestione documentale e nella normativa vigente. Le principali definizioni operative sono le seguenti.

a. Documento informatico

Per documento informatico si intende la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. Nella scuola il documento informatico può assumere molte forme: atto amministrativo firmato digitalmente, comunicazione protocollata, verbale, determina, contratto, registro, certificato, istanza, relazione, provvedimento, fattura elettronica, fascicolo, documento didattico-amministrativo o altro file prodotto o acquisito nell'ambito dell'attività istituzionale.

b. Conservazione

La conservazione è l'insieme delle attività finalizzate a proteggere e mantenere nel tempo i documenti informatici, assicurandone autenticità, integrità, affidabilità, leggibilità e reperibilità..

La conservazione non modifica il contenuto amministrativo del documento, ma ne garantisce il mantenimento nel tempo attraverso regole, controlli, metadati, pacchetti informativi, misure di sicurezza e responsabilità definite.

c. Sistema di conservazione

Il Sistema di conservazione è l'insieme di risorse, procedure, strumenti, infrastrutture, software, regole e responsabilità attraverso cui il Conservatore gestisce il processo tecnico di conservazione dei documenti versati dalla scuola.

Il Sistema di conservazione utilizzato dalla scuola è quello messo a disposizione dal Conservatore individuato secondo le procedure amministrative applicabili.

d. Pacchetto di versamento

Il pacchetto di versamento è l'insieme dei documenti, dei metadati e delle informazioni trasmesse dalla scuola al Sistema di conservazione. Esso rappresenta la modalità con cui i documenti entrano nel processo di conservazione.

e. Pacchetto di archiviazione

Il pacchetto di archiviazione è il pacchetto generato dal Sistema di conservazione dopo l'accettazione del versamento. Esso contiene i documenti e le informazioni necessarie a garantirne la conservazione nel tempo.

f. Pacchetto di distribuzione

Il pacchetto di distribuzione è il pacchetto prodotto dal Sistema di conservazione per consentire l'esibizione, la consultazione o l'estrazione dei documenti conservati, nei casi consentiti e secondo le autorizzazioni previste.

g. Produttore

Il produttore è il soggetto che produce, acquisisce e gestisce i documenti da conservare. Nel presente Manuale il produttore coincide con l'Istituzione scolastica.

h. Conservatore

Il Conservatore è il soggetto esterno che eroga il servizio di conservazione digitale per conto della scuola, secondo il contratto, il proprio Manuale tecnico e la normativa applicabile.

i. Responsabile della conservazione

Il Responsabile della conservazione è la persona fisica interna all'Istituzione scolastica che governa il processo di conservazione dal punto di vista del soggetto produttore. Nelle istituzioni scolastiche tale ruolo è normalmente attribuito al Dirigente scolastico o ad altro soggetto interno formalmente individuato, purché dotato di adeguate competenze e poteri organizzativi.

3.2 Acronimi

Acronimo	Significato
AgID	Agenzia per l'Italia Digitale
CAD	Codice dell'Amministrazione Digitale (D.Lgs. 82/2005)
DS	Dirigente Scolastico
DSGA	Direttore dei Servizi Generali e Amministrativi
PdV	Pacchetto di versamento
PdA	Pacchetto di archiviazione
PdD	Pacchetto di distribuzione
RdC	Responsabile della conservazione
GDPR	General Data Protection Regulation (Reg. UE 2016/679)
SdC	Sistema di conservazione del conservatore accreditato
RsC	Responsabile del Sistema di Conservazione

CAPITOLO 4 – MODELLO ORGANIZZATIVO

4.1 Struttura organizzativa dell'Istituzione scolastica

L'Istituzione scolastica è un ente di diritto pubblico dotato di personalità giuridica e autonomia amministrativa, didattica, organizzativa e di ricerca, ai sensi del D.P.R. 275/1999. In quanto pubblica amministrazione, è tenuta ad adottare sistemi di gestione documentale e di conservazione conformi alla normativa vigente.

La responsabilità amministrativa e legale dell'Istituzione scolastica fa capo al Dirigente Scolastico, che, ai sensi dell'art. 25 del D.Lgs. 165/2001, ha la rappresentanza legale dell'istituto e risponde della gestione dell'intera attività amministrativa. La gestione operativa dei servizi amministrativi è affidata al Direttore dei Servizi Generali e Amministrativi (DSGA), che coordina il personale di segreteria.

4.2 Assetto generale e modello di conservazione adottato

L'Istituzione scolastica ha adottato il modello di **conservazione esterna**, affidando l'esecuzione del processo di conservazione a un conservatore accreditato AgID, ai sensi dell'art. 44-bis del CAD. Tale scelta risponde all'esigenza di garantire la conformità normativa del processo, la continuità del servizio e l'adozione di standard tecnici aggiornati, senza gravare sull'organizzazione interna di competenze specialistiche di natura informatica e archivistica.

La scuola cura la formazione dei documenti, la gestione documentale, la protocollazione, la classificazione, la fascicolazione, la selezione dei documenti da conservare, la correttezza dei metadati, l'autorizzazione degli utenti interni, la verifica del processo e la gestione delle richieste di esibizione.
Il Conservatore cura la presa in carico dei pacchetti di versamento, i controlli tecnici, la generazione dei rapporti di versamento, la produzione dei pacchetti di archiviazione, la conservazione nel tempo, la gestione tecnica della sicurezza, la continuità del servizio e la produzione dei pacchetti di distribuzione.

Il rapporto tra l'Istituzione scolastica e il conservatore è regolato da apposita convenzione o contratto, nel quale sono definiti i servizi erogati, i livelli di servizio (SLA), le responsabilità reciproche e le condizioni di accesso ai documenti conservati.

Il manuale tecnico del conservatore, che descrive nel dettaglio l'architettura del sistema di conservazione, le infrastrutture tecnologiche, i formati supportati, le procedure di migrazione e le politiche di disaster recovery, è allegato al presente Manuale e ne costituisce parte integrante.

4.3 Integrazione con il sistema di gestione documentale

Il sistema di conservazione è integrato con il sistema di gestione documentale in uso presso l'Istituzione scolastica. I documenti informatici, una volta registrati nel protocollo informatico o formati attraverso le applicazioni gestionali in uso (piattaforme per la gestione del registro elettronico, del personale, della contabilità, ecc.), vengono inviati in conservazione secondo le modalità e le tempistiche descritte nel Capitolo 8 del presente Manuale.

CAPITOLO 5 – RUOLI E RESPONSABILITÀ

5.1 Il Responsabile della conservazione

Il Responsabile della conservazione (RdC) è la figura interna all'Istituzione scolastica cui è demandata la definizione e l'attuazione delle politiche complessive del sistema di conservazione, nonché la verifica periodica della sua corretta funzionalità, ai sensi delle Linee guida AgID e dell'art. 7 del D.P.C.M. 3 dicembre 2013.

Il RdC è nominato dal Dirigente Scolastico con apposito atto formale. Nell'ambito delle istituzioni scolastiche, tale ruolo è generalmente attribuito al Dirigente Scolastico (DS), in ragione delle sue responsabilità nel garantire che la scuola disponga di un sistema di conservazione conforme e coerente con la gestione documentale, nel definire e attuare le politiche di gestione e conservazione dei documenti informatici, redigere il Manuale di Conservazione dell'Istituto e garantire la loro integrità, autenticità, leggibilità e reperibilità nel tempo, ferma restando la possibilità di designare altro soggetto in possesso di adeguata professionalità.

Il Responsabile della conservazione svolge le seguenti funzioni principali:

- definisce le politiche di conservazione e le caratteristiche e i requisiti del sistema di conservazione in conformità alla normativa vigente;
- gestisce il processo di conservazione e ne verifica periodicamente la corretta esecuzione;
- assicura la presenza di misure di sicurezza idonee a proteggere il sistema di conservazione;
- provvede alla redazione e all'aggiornamento del presente Manuale;
- supervisiona il corretto versamento dei documenti al sistema di conservazione;
- coordina con il conservatore accreditato per la risoluzione di eventuali criticità;
- verifica il rispetto dei livelli di servizio contrattualmente previsti con il conservatore;
- nomina il proprio vicario.

Il Responsabile della conservazione può delegare specifiche attività operative a personale interno o a soggetti esterni, nei limiti consentiti dalla normativa, ma mantiene la responsabilità di governo del processo per conto dell'Istituzione scolastica. Le deleghe devono essere formalizzate, chiare e coerenti con l'organizzazione interna.

La delega non comporta il trasferimento della titolarità dell'archivio né della responsabilità amministrativa della scuola sulla corretta tenuta dei documenti.

5.2 Il Dirigente Scolastico

Il Dirigente Scolastico (DS) esercita la supervisione sull'intero processo di conservazione, in quanto titolare della responsabilità giuridica dell'istituto. Il DS nomina il Responsabile della conservazione e il vicario, adotta il presente Manuale con proprio provvedimento e provvede al suo aggiornamento. Autorizza altresì le operazioni di scarto documentale, previa acquisizione del parere della competente Soprintendenza archivistica..

5.3 Il DSGA

Il DSGA *pro-tempore* è generalmente nominato vicario del RdC, coordina gli uffici amministrativi, assicura l'applicazione operativa delle procedure e garantisce che il personale segua le istruzioni interne e che i flussi documentali siano corretti.

5.4 Il personale di segreteria

Il personale di segreteria è coinvolto operativamente nel processo di conservazione nelle fasi di produzione, registrazione, classificazione e versamento dei documenti. Ciascun operatore di segreteria è tenuto a operare nel rispetto delle istruzioni operative impartite dal Responsabile della conservazione e dal DSGA, e a segnalare tempestivamente eventuali anomalie riscontrate nel processo.

5.5 Il conservatore accreditato

Il conservatore accreditato è il soggetto terzo che gestisce il sistema di conservazione per conto dell'Istituzione scolastica. In tale veste è responsabile della corretta esecuzione del processo di conservazione dal punto di vista tecnico, garantisce l'integrità e l'immodificabilità dei documenti versati, assicura l'accessibilità nel tempo dei documenti conservati e provvede alla gestione dei pacchetti di versamento, archiviazione e distribuzione secondo le specifiche tecniche descritte nel proprio manuale tecnico allegato al presente documento. Il Manuale tecnico del Conservatore viene conservato agli atti e allegato al presente Manuale.

5.6 Il DPO

Il DPO dell'Istituto fornisce supporto all'Istituzione scolastica nella redazione e nell'aggiornamento del presente Manuale, per i profili che riguardano la protezione dei dati personali contenuti nei documenti destinati alla conservazione. Il DPO non sostituisce il Dirigente scolastico, il Responsabile della conservazione o il Conservatore nelle rispettive responsabilità, ma svolge una funzione di consulenza e supporto, secondo quanto previsto dagli articoli 37, 38 e 39 del Regolamento UE 2016/679.

Soggetto	Ruolo	Funzioni principali
Dirigente Scolastico (RdC)	Responsabile della conservazione	Supervisione, adozione del Manuale, nomine, autorizzazione scarti, gestione del processo, coordinamento, aggiornamento Manuale, verifiche
DSGA	Vicario del Responsabile della conservazione	Si sostituisce al RSC in caso di necessità e assicura l'applicazione operativa delle procedure
Personale di segreteria/Produttore dei PdV	Operatori del processo	Produzione, protocollazione, classificazione, versamento documenti

Soggetto	Ruolo	Funzioni principali
Conservatore accreditato (fornitore esterno)	Gestore tecnico del SdC	Ricezione, archiviazione, esibizione, sicurezza tecnica
Responsabile del servizio di conservazione (RsC)	Interno al Conservatore	Svolge le attività operative del processo di conservazione delegate dal RdC.
DPO	Responsabile Protezione Dati	Fornisce supporto per la redazione del Manuale per i profili che riguardano la protezione dei dati personali

CAPITOLO 6 – TIPOLOGIA DEI DOCUMENTI SOGGETTI A CONSERVAZIONE

6.1 Criteri generali

Non tutti i documenti prodotti o ricevuti dall'Istituzione scolastica sono soggetti a conservazione permanente. La selezione dei documenti da inviare in conservazione avviene in coerenza con il Manuale di gestione documentale, il titolario di classificazione, il piano di fascicolazione, il piano di conservazione e le regole interne adottate dalla scuola che individuano, per ogni tipologia documentale, i tempi di conservazione e il destino finale (conservazione permanente o scarto).

La selezione tiene conto delle disposizioni contenute nel Massimario di selezione e scarto per le istituzioni scolastiche emanato dal Ministero dell'Istruzione e approvato dalla Direzione Generale degli Archivi del Ministero della Cultura, nonché delle eventuali disposizioni specifiche emanate dall'Amministrazione centrale in relazione a tipologie documentali particolari.

La conservazione deve riguardare il documento nella sua forma completa, comprensiva dei metadati necessari, delle firme elettroniche o digitali presenti, delle segnature di protocollo, delle attestazioni, degli allegati e delle informazioni che ne consentono la corretta interpretazione.

6.2 Classificazione delle tipologie documentali

Le tipologie di documenti informatici soggetti a conservazione presso l'Istituzione scolastica sono suddivise nelle seguenti macro-categorie funzionali (elenco non esaustivo):

Categoria	Tipologia documentale	Termine minimo di conservazione	Destino finale
Documenti amministrativi e di governance	Delibere del Consiglio di Istituto e del Collegio dei Docenti	Illimitato	Conservazione permanente
Documenti amministrativi e di governance	Determinazioni dirigenziali	Illimitato	Conservazione permanente
Documenti amministrativi e di governance	Registri dei verbali degli organi collegiali	Illimitato	Conservazione permanente
Documenti amministrativi e di governance	Corrispondenza istituzionale (protocollo in entrata e uscita)	10 anni	Selezione / scarto parziale
Documenti del personale	Fascicoli personali del personale docente e ATA	Illimitato	Conservazione permanente
Documenti del personale	Contratti di lavoro e atti di nomina	50 anni	Conservazione permanente

Categoria	Tipologia documentale	Termine minimo di conservazione	Destino finale
Documenti del personale	Tabelle stipendi	50 anni	Scarto
Documenti del personale	Documentazione relativa alle assenze e permessi	10 anni	Scarto
Documenti degli alunni	Fascicoli personali degli alunni	Illimitato	Conservazione permanente
Documenti degli alunni	Pagelle e documenti di valutazione	Illimitato	Conservazione permanente
Documenti degli alunni	Diplomi e certificati di studio	Illimitato	Conservazione permanente
Documenti degli alunni	Registri di classe	Illimitato	Conservazione permanente
Documenti degli alunni	Registri personali dei docenti	10 anni	Scarto, conservazione permanente di un anno ogni 5
Documenti contabili	Bilanci e rendiconti finanziari	Illimitato	Conservazione permanente
Documenti contabili	Mandati di pagamento e reversali di incasso	10 anni	Conservazione permanente
Documenti contabili	Fatture elettroniche passive (sistema SDI)	10 anni	Conservazione permanente
Documenti contabili	Contratti e ordinativi di fornitura	50 anni	Conservazione permanente del registro
Documenti didattici e formativi	Piani dell'Offerta Formativa (PTOF)	Illimitato	Conservazione permanente
Documenti didattici e formativi	Piani Educativi Individualizzati (PEI) e Piani Didattici Personalizzati (PDP)	Illimitato	Conservazione permanente nel fascicolo dell’alunno

Categoria	Tipologia documentale	Termine minimo di conservazione	Destino finale
Documenti di sicurezza e salute	Documento di Valutazione dei Rischi (DVR)	Illimitato	Conservazione permanente

6.3 Formati ammessi

I documenti informatici sono versati in conservazione nei formati ritenuti idonei a garantire la leggibilità nel lungo periodo in conformità alle Linee guida AgID e agli allegati tecnici. Per i documenti amministrativi definitivi destinati alla conservazione, la scuola privilegia formati non modificabili o comunque idonei a garantire stabilità, leggibilità e integrità.

Il conservatore accreditato garantisce la gestione di eventuali procedure di migrazione del formato qualora, nel tempo, i formati originari diventassero obsoleti.

6.4 Metadati

I metadati sono informazioni associate al documento e servono a identificarlo, descriverlo, gestirlo, ricercarlo e conservarlo.
Tra i metadati rilevanti rientrano, in base alla tipologia documentale, identificativo, oggetto, data, autore, destinatario, numero di protocollo, classificazione, fascicolo, impronta, formato, stato, eventuale firma, ufficio produttore, livello di riservatezza, tempi di conservazione, collegamenti con altri documenti e procedimento amministrativo di riferimento.
La qualità dei metadati è essenziale: metadati incompleti,, errati o incoerenti compromettono la ricerca, la gestione archivistica e l'esibizione del documento.

6.5 Controlli di qualità

Prima del versamento in conservazione, il personale autorizzato verifica, secondo le procedure interne e le funzionalità disponibili nei sistemi gestionali, che i documenti siano completi, leggibili, correttamente associati al procedimento, classificati e fascicolati.
I controlli riguardano almeno:

- la presenza del documento e degli allegati;
- la leggibilità del file;
- la coerenza dell'oggetto;
- la corretta registrazione di protocollo, se prevista;
- la corretta classificazione;
- la presenza dei metadati essenziali;
- la presenza della firma, se richiesta;
- la corretta associazione al fascicolo;
- l'assenza di duplicazioni evidenti;
- la corretta gestione dei dati personali.

CAPITOLO 7 – IL PROCESSO DI CONSERVAZIONE

7.1 Descrizione del processo

Il processo di conservazione si articola in una sequenza di fasi distinte e tra loro consequenziali, che vanno dalla formazione del documento informatico fino alla sua conservazione nel sistema del conservatore accreditato. Ogni fase è presidiata da specifici controlli di qualità e sicurezza, descritti nel dettaglio nel manuale tecnico del conservatore allegato al presente Manuale.

Il modello di riferimento adottato è quello definito dallo standard ISO 14721 (OAIS), che distingue tre principali tipologie di pacchetti informativi: il Pacchetto di versamento (PdV), trasmesso dal produttore al sistema di conservazione; il Pacchetto di archiviazione (PdA), generato e conservato internamente al sistema; il Pacchetto di distribuzione (PdD), restituito al richiedente in fase di accesso.

7.2 Fasi del processo

7.2.1 Formazione del documento informatico

I documenti informatici sono formati dall'Istituzione scolastica attraverso le applicazioni in uso (sistema di protocollo informatico, applicativo gestionale per il personale, sistema contabile, registro elettronico). Ogni documento deve essere prodotto in un formato idoneo alla conservazione (preferibilmente PDF/A) e deve essere corredato dei metadati minimi obbligatori previsti dalle Linee guida AgID, tra cui: identificativo univoco, data e ora di formazione, oggetto, soggetto produttore, tipologia documentale, classificazione archivistica.

7.2.2 Registrazione e segnatura di protocollo

I documenti soggetti a obbligo di protocollazione sono registrati nel sistema di protocollo informatico dell'Istituzione scolastica. La registrazione attribuisce al documento un numero di protocollo univoco, una data certa e una segnatura di protocollo, che costituiscono elementi essenziali del fascicolo documentale e dei metadati di conservazione.

7.2.3 Classificazione e fascicolazione

I documenti sono classificati secondo il titolario di classificazione adottato dall'istituto e inseriti nei fascicoli di competenza. La corretta classificazione è presupposto indispensabile per la successiva operazione di versamento in conservazione, in quanto consente l'organizzazione logica dei documenti in serie archivistiche omogenee.

7.2.4 Firma digitale e marcatura temporale

I documenti informatici che richiedono sottoscrizione sono firmati digitalmente dal soggetto competente mediante certificato di firma digitale qualificata, ai sensi dell'art. 24 del CAD. Ove richiesto dalla normativa o dalle esigenze di certezza temporale, ai documenti è apposta una marca temporale che attesta la data e l'ora di formazione del documento con valore legale.

7.2.5 Versamento al sistema di conservazione

Il versamento dei documenti al sistema di conservazione del conservatore accreditato avviene attraverso la predisposizione del Pacchetto di versamento (PdV), contenente il documento e i relativi metadati. Le modalità tecniche di predisposizione e trasmissione del PdV sono descritte nel dettaglio nel manuale tecnico del conservatore.

7.2.6 Presa in carico e archiviazione

Il sistema di conservazione verifica la correttezza formale e la completezza del PdV ricevuto, genera il Pacchetto di archiviazione (PdA) e restituisce al produttore una ricevuta di presa in carico con indicazione dell'esito delle verifiche. Il PdA viene conservato nel sistema del conservatore insieme all'indice del pacchetto (IPdA), firmato digitalmente e marcato temporalmente dal responsabile del servizio di conservazione del conservatore. In caso di esito positivo, produce il rapporto di versamento, che attesta la presa in carico dei documenti da parte del sistema. Il rapporto di versamento rappresenta un elemento fondamentale di tracciabilità. La scuola deve poter accedere alle informazioni relative ai versamenti effettuati, agli esiti, agli eventuali rifiuti e alle anomalie rilevate.

7.2.7 Rifiuto o anomalia del versamento

Se il Sistema di conservazione rifiuta un pacchetto di versamento o segnala anomalie, il personale autorizzato verifica la causa del problema e provvede alla correzione, ove possibile.
Le anomalie possono riguardare, per esempio, formato non ammesso, file corrotto, metadati mancanti, incongruenze tra documento e informazioni associate, errore tecnico di trasmissione o problemi di firma. Le anomalie rilevanti devono essere segnalate al Responsabile della conservazione.

7.2.8 Esibizione e recupero dei documenti

La scuola può richiedere l'esibizione o il recupero dei documenti conservati per esigenze amministrative, ispettive, giudiziarie, di accesso documentale, accesso civico, controllo contabile, rendicontazione, tutela di diritti o altra finalità istituzionale legittima.
L'esibizione deve avvenire secondo le procedure previste dal Conservatore e nel rispetto delle autorizzazioni interne. Il personale non autorizzato non può richiedere o ottenere documenti conservati.
Quando il documento contiene dati personali, l'esibizione deve rispettare i principi di necessità, pertinenza e minimizzazione. Se occorre rilasciare copia a terzi, la scuola valuta l'eventuale oscuramento dei dati non pertinenti.

CAPITOLO 8 – MODALITÀ DI VERSAMENTO

8.1 Modalità operative

Il versamento dei documenti al sistema di conservazione avviene secondo le modalità tecniche specificate nel manuale tecnico del conservatore accreditato, al quale si fa espresso rinvio per i dettagli implementativi. In questa sede si descrivono le modalità operative a livello di processo, con riferimento alle responsabilità interne all'Istituzione scolastica.

Il versamento può avvenire in modalità automatica, attraverso l'integrazione applicativa tra i sistemi gestionali dell'istituto e il sistema di conservazione del conservatore, oppure in modalità manuale, attraverso l'upload diretto dei documenti nell'interfaccia web messa a disposizione dal conservatore. La modalità prevalente è quella automatica, che garantisce la sistematicità e la tempestività dei versamenti riducendo il rischio di omissioni.

8.2 Predisposizione del pacchetto di versamento

Prima di procedere al versamento, il responsabile operativo dell'Istituzione scolastica (personale di segreteria incaricato) verifica che i documenti da versare siano: in formato idoneo alla conservazione; corredati dei metadati minimi obbligatori; ove previsto, firmati digitalmente e marcati temporalmente; classificati e fascicolati correttamente nel sistema di gestione documentale.

Il Pacchetto di versamento è strutturato secondo le specifiche tecniche del conservatore, che recepiscono lo standard UNI 11386 (SInCRO). Ogni PdV è identificato da un codice univoco e contiene l'indice del pacchetto (IPdV), la descrizione dei componenti versati e i metadati di conservazione.

8.3 Ricevuta di versamento e gestione degli errori

A seguito di ogni versamento, il sistema di conservazione restituisce una ricevuta di presa in carico che attesta l'avvenuta ricezione e il superamento dei controlli di conformità. Tale ricevuta è conservata agli atti dell'Istituzione scolastica come prova dell'avvenuto versamento. In caso di esito negativo del versamento, il sistema di conservazione restituisce una notifica di errore con indicazione delle anomalie riscontrate.. Il personale incaricato è tenuto a correggere le anomalie segnalate e a procedere a un nuovo versamento entro i termini previsti.

CAPITOLO 9 – MODALITÀ DI ESIBIZIONE E ACCESSO

9.1 Principi generali sull'accesso

L'Istituzione scolastica garantisce l'accesso ai documenti conservati nel rispetto dei principi di trasparenza, riservatezza e protezione dei dati personali. L'accesso ai documenti è disciplinato dalla normativa vigente in materia di accesso agli atti (L. 241/1990 e D.Lgs. 33/2013) e di protezione dei dati personali (Reg. UE 2016/679 e D.Lgs. 196/2003), tenendo conto delle eventuali limitazioni connesse alla presenza di dati sensibili o riservati nei documenti conservati.

9.2 Soggetti legittimati all'accesso

Hanno diritto di accesso ai documenti conservati: il personale dell'Istituzione scolastica, nell'ambito dei propri compiti e responsabilità; i soggetti direttamente interessati (alunni, ex alunni, genitori, personale scolastico), in relazione ai propri documenti personali; le autorità giudiziarie, amministrative e di controllo (Ministero dell'Istruzione, Ufficio Scolastico Regionale, Corte dei Conti, ecc.) nell'esercizio dei propri poteri istituzionali; i terzi aventi titolo ai sensi della normativa sull'accesso agli atti amministrativi.

9.3 Esibizione dei documenti conservati

L'esibizione di un documento conservato avviene attraverso la richiesta al sistema di conservazione del Pacchetto di distribuzione (PdD), che contiene il documento in formato leggibile e i metadati che ne attestano l'autenticità e l'integrità. Il documento esibito ha piena validità giuridica e probatoria, essendo accompagnato dall'attestazione di conformità all'originale rilasciata dal sistema di conservazione.

Le richieste di accesso ai documenti conservati sono gestite dall'Istituzione scolastica attraverso il responsabile della conservazione, che coordina con il conservatore la predisposizione e la trasmissione dei PdD richiesti. I tempi di evasione delle richieste sono definiti nella convenzione stipulata con il conservatore e non possono in ogni caso superare i termini previsti dalla normativa sull'accesso agli atti (30 giorni dalla richiesta).

9.4 Esibizione per finalità legali e probatorie

I documenti estratti dal sistema di conservazione possono essere utilizzati come prova documentale in procedimenti giudiziari, amministrativi e contabili. A tal fine, il responsabile della conservazione può richiedere al conservatore il rilascio di una copia conforme del documento, accompagnata da apposita attestazione di conformità all'originale informatico conservato, ai sensi dell'art. 23-bis del CAD.

9.5 Copie ed estratti

Quando viene rilasciata copia o estratto di documenti conservati, la scuola verifica che la copia corrisponda alla richiesta e non contenga dati eccedenti.
In presenza di dati personali non necessari, la scuola procede all’oscuramento selettivo, salvo che la legge imponga la consegna integrale o che l’accesso integrale risulti giuridicamente necessario e motivato.

CAPITOLO 10 - MONITORAGGIO, VERIFICHE E AGGIORNAMENTO

10.1 Monitoraggio interno

Il Responsabile della conservazione, con il supporto del DSGA, verifica periodicamente il corretto funzionamento del processo di conservazione.
Il monitoraggio riguarda almeno:

- regolarità dei versamenti;
- presenza dei rapporti di versamento;
- anomalie o rifiuti;
- correttezza dei flussi documentali;
- adeguatezza delle abilitazioni;
- aggiornamento delle procedure;
- coerenza con il Manuale di gestione documentale;
- eventuali modifiche del servizio del Conservatore.

10.2 Verifiche con il Conservatore

La scuola può richiedere al Conservatore informazioni, report, evidenze o chiarimenti sul servizio erogato, nei limiti previsti dal contratto.
In particolare, la scuola verifica che il Conservatore mantenga aggiornato il proprio Manuale tecnico, comunichi eventuali modifiche rilevanti, gestisca correttamente gli incidenti e garantisca la disponibilità dei documenti conservati.

10.3 Aggiornamento del Manuale

Il presente Manuale viene aggiornato quando intervengono modifiche normative, organizzative, tecnologiche o contrattuali rilevanti.
L'aggiornamento è necessario, in particolare, nei seguenti casi:

- cambio del Conservatore;
- modifica significativa del Sistema di conservazione;
- modifica dei flussi di versamento;
- modifica dei ruoli interni;
- adozione di nuovi sistemi gestionali;
- introduzione di nuove tipologie documentali;
- modifica del Manuale di gestione documentale;
- rilievi emersi da controlli, audit o ispezioni;
- aggiornamenti normativi o AgID.

Ogni nuova versione deve riportare data, numero di versione, oggetto delle modifiche e atto di approvazione.

CAPITOLO 11 – MISURE DI SICUREZZA

11.1 Principi generali

La sicurezza del sistema di conservazione è garantita attraverso un insieme coordinato di misure tecniche, organizzative e procedurali, adottate sia dall'Istituzione scolastica che dal conservatore accreditato, ciascuno nell'ambito delle proprie responsabilità. Le misure di sicurezza sono dimensionate in relazione al livello di rischio valutato per le tipologie documentali trattate, con particolare attenzione ai documenti contenenti dati personali o sensibili.

11.2 Misure a carico dell'Istituzione scolastica

L'Istituzione scolastica adotta le seguenti misure di sicurezza nell'ambito del proprio perimetro di responsabilità.

Sul piano dell'accesso fisico e logico, le postazioni di lavoro del personale di segreteria sono protette da credenziali di accesso individuali; i profili di autorizzazione al sistema di gestione documentale e al portale del conservatore sono definiti in base al principio del minimo privilegio; le credenziali di accesso sono gestite con politiche di complessità e rinnovo periodico. L'accesso ai locali della segreteria è limitato al personale autorizzato.

Sul piano della formazione e della consapevolezza, il personale operante nel processo di conservazione è destinatario di indicazioni informative in materia di gestione documentale, sicurezza informatica e protezione dei dati personali.

Sul piano della continuità operativa, l'Istituzione scolastica mantiene una copia di backup locale dei documenti informatici più rilevanti, in attesa del loro versamento in conservazione, al fine di garantire la continuità operativa in caso di indisponibilità temporanea del sistema di conservazione.

11.3 Misure a carico del conservatore accreditato

Il conservatore accreditato è tenuto, ai sensi della normativa vigente e delle condizioni contrattuali, ad adottare tutte le misure di sicurezza idonee a garantire l'integrità, la disponibilità e la riservatezza dei documenti conservati. Le misure adottate dal conservatore sono descritte nel dettaglio nel manuale tecnico allegato e comprendono, tra l'altro, i seguenti ambiti: integrità dei dati, disponibilità e business continuity, riservatezza, sicurezza fisica, gestione delle vulnerabilità, gestione degli incidenti.

11.4 Protezione dei dati personali

I documenti conservati nel sistema di conservazione contengono frequentemente dati personali di alunni, famiglie e personale scolastico. Il trattamento di tali dati nell'ambito del processo di conservazione avviene nel rispetto del Regolamento UE 2016/679 (GDPR) e del D.Lgs. 196/2003. Il conservatore accreditato opera in qualità di responsabile del trattamento ai sensi dell'art. 28 GDPR, sulla base di apposito contratto o altro atto giuridico vincolante che definisce le finalità, le modalità del trattamento e le garanzie di sicurezza.

Il Responsabile della protezione dei dati (DPO) dell'Istituzione scolastica, è consultato in caso di necessità per gli aspetti attinenti alla conformità al GDPR. I trattamenti connessi alla conservazione sono iscritti nel Registro delle attività di trattamento dell'istituto.

CAPITOLO 12 – VERIFICHE E AUDIT

12.1 Verifiche periodiche del sistema di conservazione

Il Responsabile della conservazione effettua, con cadenza almeno annuale, una verifica del corretto funzionamento del sistema di conservazione, con riferimento sia alla componente organizzativa interna all'istituto sia alla componente tecnica gestita dal conservatore accreditato. La verifica ha per oggetto, in particolare: la completezza e la correttezza dei versamenti effettuati nel periodo; il rispetto delle tempistiche di versamento; la disponibilità e la leggibilità dei documenti conservati; la corrispondenza tra i documenti versati e quelli effettivamente conservati nel sistema; il rispetto dei livelli di servizio contrattualmente previsti con il conservatore.. In caso di criticità riscontrate, il RdC attiva le opportune azioni correttive in coordinamento con il conservatore.

12.2 Audit del conservatore accreditato

Il conservatore accreditato è soggetto a verifiche periodiche da parte di AgID, nell'ambito delle attività di vigilanza sull'accreditamento. Gli esiti di tali verifiche sono comunicati all'Istituzione scolastica e tenuti in considerazione dal RdC in sede di valutazione della qualità del servizio erogato.

L'Istituzione scolastica ha facoltà di richiedere al conservatore, nei limiti previsti dalla convenzione, l'effettuazione di audit specifici sul sistema di conservazione, finalizzati a verificare la conformità del servizio alle prescrizioni normative e contrattuali.

CAPITOLO 13 – AGGIORNAMENTO E REVISIONE DEL MANUALE

13.1 Ciclo di vita del Manuale

Il presente Manuale è adottato con decreto del Dirigente Scolastico e pubblicato sul sito istituzionale dell'Istituzione scolastica nella sezione Amministrazione trasparente>Disposizioni generali>Atti amministrativi generali. Il Manuale è soggetto a revisione periodica con cadenza almeno biennale, ovvero ogni qualvolta intervengano modifiche normative, organizzative o tecnologiche rilevanti che ne rendano necessario l'aggiornamento.

13.2 Casi che determinano la revisione

La revisione del Manuale è obbligatoria nei seguenti casi: modifica della normativa di riferimento in materia di formazione, gestione e conservazione dei documenti informatici; sostituzione o modifica significativa del sistema di gestione documentale in uso presso l'istituto; cambiamento del conservatore accreditato o modifica sostanziale del contratto di conservazione; variazione dei soggetti titolari dei ruoli descritti nel Manuale; emersione di criticità di processo che rendano necessaria la revisione delle procedure operative.

13.3 Procedura di aggiornamento

L'aggiornamento del Manuale è proposto dal Responsabile della conservazione e approvato dal Dirigente Scolastico con apposito decreto. Ogni versione aggiornata del Manuale è identificata da un numero di versione progressivo e dalla data di adozione, riportati in copertina, e le versioni precedenti sono conservate agli atti dell'istituto.. L'aggiornamento è comunicato al personale interessato.

CAPITOLO 14 - DISPOSIZIONI FINALI

14.1 Adozione

Il presente Manuale è adottato con provvedimento del Dirigente scolastico entro il 30 giugno 2026, secondo quanto previsto dagli obblighi applicabili alle pubbliche amministrazioni in materia di gestione e conservazione dei documenti informatici.

Il Manuale viene portato a conoscenza del personale amministrativo interessato e reso disponibile secondo le modalità stabilite dalla scuola.

14.2 Obbligo di osservanza

Il personale scolastico coinvolto nella formazione, gestione, protocollazione, classificazione, fascicolazione, versamento, consultazione ed esibizione dei documenti informatici è tenuto a rispettare il presente Manuale, il Manuale di gestione documentale, le istruzioni interne, le autorizzazioni ricevute e le misure di sicurezza adottate.

La violazione delle procedure può compromettere la validità amministrativa dei documenti, la sicurezza dei dati, la corretta tenuta dell’archivio e la responsabilità dell’Istituzione scolastica.

14.3 Entrata in vigore

Il presente Manuale entra in vigore dalla data di adozione e resta valido fino a successivo aggiornamento.

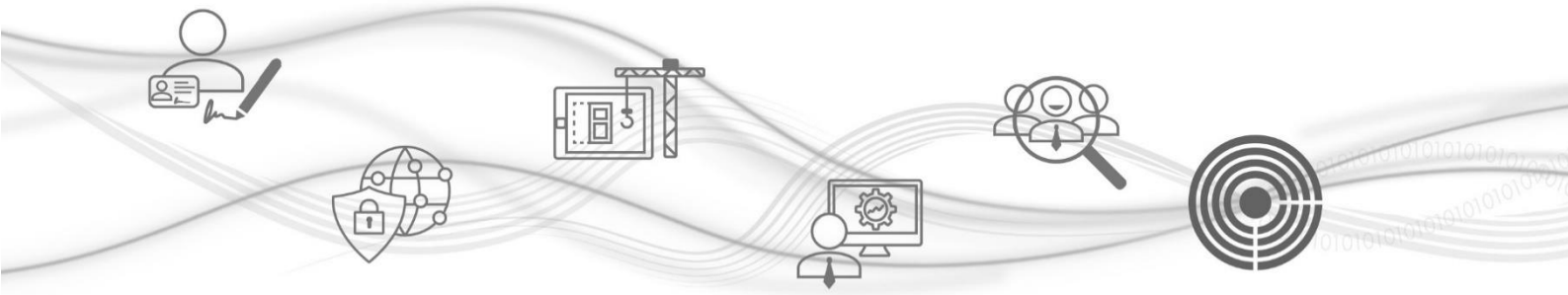
Il Dirigente scolastico assicura, tramite il Responsabile della conservazione, il monitoraggio dell'attuazione e l'aggiornamento periodico del documento.

ALLEGATI

Manuale tecnico di conservazione redatto dal Conservatore.

Manuale del Conservatore

Servizio di Conservazione
Long Term Archiving - LTA



Categoria	**LTA**	Codice Documento	**NAM-LTA-MO**	**Namirial S.p.A.**
Redatto da	**Enrico Giunta**	Nota di riservatezza	**Documento pubblico**	Il Legale Rappresentante
Verificato da	**Davide Coletto**	Versione	**11**	**Massimiliano Pellegrini**
Approvato da	**Massimiliano Pellegrini**	Data di emissione	**08/09/2023**	_____

Namirial S.p.A.
Via Caduti sul Lavoro n. 4, 60019 Senigallia (An) - Italia | Tel. +39 071 63494
www.namirial.com | amm.namirial@sicurezzapostale.it | P.IVA IT02046570426
C.F. e iscriz. al Reg. Impr. Ancona N. 02046570426 | REA N. AN - 157295
Codice destinatario T04ZHR3 | Capitale sociale € 8.238.145,00 i.v.

Signed by: PELLEGRINI MASSIMILIANO
Issued by: Namirial CA Firma Qualificata
Signing time: 11-09-2023 13:32:11
IP address: 5.90.120.2

Indice del documento

Indice del documento 2
Emissione del documento 4
Registro delle versioni 4
1 SCOPO E AMBITO DEL DOCUMENTO 8
2 TERMINOLOGIA 10
2.1 Glossario 10
2.2 Acronimi 17
3 NORMATIVA E STANDARD DI RIFERIMENTO 18
3.1 Normativa di riferimento 18
3.1.1 Unione Europea 18
3.1.2 Italia 18
3.1.3 Romania 19
3.1.4 Francia 19
3.2 Standard di riferimento 19
4 RUOLI E RESPONSABILITÀ 21
4.1 Deleghe 25
5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE 26
5.1 Organigramma 26
5.2 Strutture organizzative 26
6 OGGETTI SOTTOPOSTI A CONSERVAZIONE 30
6.1 Oggetti conservati 31
6.2 Formati 31
6.2.1 Valutazione ed indice di interoperabilità 33
6.3 Submission Information Package (SIP) 34
6.3.1 Pre-pacchetto 38
6.3.2 Revisione Information Package 38
6.4 Archival Information Package (AIP) 39
6.5 Dissemination Information Package 46
7 IL PROCESSO DI CONSERVAZIONE 50
7.1 Modalità di acquisizione dei Submission Information Package per la loro presa in carico 51
7.2 Verifiche effettuate sui Submission Information Package e sugli oggetti in essi contenuti 52

7.3 Accettazione dei Submission Information Package e generazione del Submission Report 54
7.4 Rifiuto dei Submission Information Package e modalità di comunicazione delle anomalie 57
7.5 Preparazione e gestione dell'Archival Information Package 58
7.6 Cifratura degli oggetti di conservazione 58
7.7 Gestione di documenti contenenti dati sensibili 59
7.8 Preparazione e gestione del Dissemination Information Package ai fini dell'esibizione 60
7.9 Accesso al Sistema 60
7.10 Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti 61
7.11 Scarto 62
7.12 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori 62
8 IL SISTEMA DI CONSERVAZIONE 63
8.1 Componenti Logiche 65
8.2 Componenti Tecnologiche 66
8.3 Componenti Fisiche 67
8.3.1 Italia 68
8.3.2 Francia 68
8.3.3 Romania 68
8.4 Componenti software 68
8.5 Procedure di gestione e di evoluzione 69
8.5.1 Conduzione e manutenzione del Sistema di conservazione 69
8.5.2 Gestione e mantenimento dei log 70
8.5.3 Monitoraggio del Sistema di conservazione 70
8.5.4 Change management 70
8.5.5 Verifica periodica di conformità a normativa e standard di riferimento 71
8.5.6 Gestione della sicurezza e valutazione del rischio 71
9 MONITORAGGIO E CONTROLLI 72
9.1 Procedure di monitoraggio 72
9.2 Verifica dell'integrità degli archivi 74
9.3 Soluzioni adottate in caso di anomalie 74
10 ANNEX 76

Emissione del documento

Azione	*Data*	*Nominativo*	*Funzione*
Redazione	06/09/2023	Enrico Giunta	Responsabile della funzione archivistica di conservazione (Archival Manager)
Verifica	07/09/2023	Davide Coletto	Responsabile del servizio di conservazione (Preservation Service Manager)
Approvazione	08/09/2023	Massimiliano Pellegrini	Legale rappresentante (CEO)

Registro delle versioni

N°Ver/Rev/Bozza	*Data emissione*	*Descrizione*	*Osservazioni*
1.0	28/11/2014	Prima emissione del documento secondo lo schema del manuale AgID per l'accreditamento	Prima versione secondo il modello dell'Agenzia per l'Italia Digitale (AgID)
2.0	22/01/2015	Nuova emissione per revisioni	Variazioni ai paragrafi 2.1, 6.1, 6.2, 6.3, 7.1, 7.2, 7.4 e 7.6
3.0	05/02/2015	Integrazione del manuale per l'accreditamento	Variazioni ai paragrafi 2.1, 6.2, 7, 7.3, 7.4 e 7.6
4.0	22/02/2016	Revisioni varie in tutti i capitoli del manuale	Variazioni in tutti i capitoli
5.0	26/09/2016	Revisione della topologia dei siti di erogazione del servizio, revisione dell'organigramma	Variazioni ai paragrafi 5.1, 8.3
6.0	26/10/2017	Revisioni varie in tutti i capitoli del manuale. In particolare: revisione della topologia dei siti di erogazione del servizio; ristrutturazione e riformulazione dei contenuti; aggiornamento delle specifiche tecniche rispetto all'ultima versione del documento SDK	Variazione in tutti i capitoli

6.1	11/10/2018	Aggiornamento glossario e normativa di riferimento; revisione dell'organigramma; aggiornamento tabella dei formati	Variazioni ai paragrafi 2.1, 3.1, 5.1, 6.1
7.0	19/09/2019	Aggiornamento definizioni, aggiornamento struttura IPdV, IPdA, IPdD; specificata modalità di versamento per la trasmissione sicura dei dati; aggiunta sito ausiliario in caso di indisponibilità della sede di Senigallia	Variazioni ai paragrafi 2.2, 6.2, 6.3, 6.4, 7.1, 8.3
8.0	04/06/2020	Aggiornamento Ruoli e Responsabilità	Variazioni ai paragrafi 4, 6.4, 7.9, 9.1
9	04/08/2021	Revisioni e adeguamenti in tutti i capitoli del Manuale. In particolare: -Aggiornamento della Terminologia per adeguamento alle LLGG AgID (par.2) -Aggiornamento della normativa per adeguamento alle LLGG AgID (par. 3) -Aggiornamento dei Ruoli (par. 4) -Aggiornamento dei draft di tabelle relative agli oggetti conservati (par. 6.1) -Aggiornamento dei Formati e inserimento della Valutazione di Interoperabilità per adeguamento alle LLGG (par. 6.2) -Adeguamento degli Indici relativi al processo di conservazione (PdV, PdA, DIP) (par. 6.3, 6.4., 6.5)	Variazioni ai paragrafi: 2 3 4 6.1 6.2 6.3 6.4 6.5 7.6 8.3 9.1

		-Inserimento del paragrafo relativo alla cifratura degli oggetti informatici (par. 7.6) -Aggiornamento Componenti fisiche (par. 8.3) -Correzione refusi Procedure di monitoraggio (par. 9.1)	
10	09/05/2022	Revisioni e adeguamenti della struttura del documento. Aggiornamento dei seguenti capitoli: -Aggiornamento glossario (2.1) -Aggiornamento normativa e standard (31, 3.2) -Aggiornamento dei ruoli (4) -Aggiornamento della struttura organizzativa (5.1, 5.2) -Aggiornamento dei formati supportati con rimando all'allegato 2 delle LLGG AgID (6.2) -Aggiornamento delle procedure di monitoraggio/piattaforma di ticketing (9.1) -Aggiornamento numerazione immagini	Variazioni ai paragrafi: 2.1 3.1 3.2 4 5.1 5.2 6.2 9.1
10.1	27/06/2022	Aggiornamento dei seguenti capitoli: -Aggiornamento acronimi (2.2) -Inserimento del paragrafo relativo alla gestione di documenti contenenti dati sensibili (par. 7.7)	Variazioni ai paragrafi: 2.2 7.7
10.2	27/02/2023	Aggiornamento dei seguenti capitoli: -Aggiornamento componenti fisiche (8.3)	Variazioni ai paragrafi: 8.3

11	08/09/2023	Aggiornamento dell'intero documento: -Aggiornamento sigla documento Aggiornamento glossario(2.1) -Aggiornamento acronimi (2.2) - Aggiornamento norme e standard (3) -Aggiornamento ruoli (4) -Adeguamento della terminologia relativa ai pacchetti informativi (tutti i paragrafi) -Aggiunto paragrafo 6.3.1 "Pre-pacchetto" -Aggiunto paragrafo 6.3.2 "Revision Information Package" -Aggiornamento paragrafo 7.7 -Aggiunto paragrafo 7.9 "Accesso al Sistema" -Aggiornamento delle componenti (8) -Aggiunto paragrafo 10 "Annex" -Aggiornamento delle immagini	Variazioni ai paragrafi: 2.1 2.2 3 4 6.3.1 6.3.2 7.7 7.9 8 10

1 SCOPO E AMBITO DEL DOCUMENTO

Il presente documento rappresenta il Manuale del Conservatore relativo al servizio di conservazione a norma dei documenti informatici (Long Term Archiving – LTA), erogato e gestito da Namirial S.p.A., ed è adottato secondo le normative in materia di formazione, gestione e conservazione dei documenti informatici.

Il presente Manuale ha lo scopo di illustrare 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, secondo quanto disposto dalle Linee Guida.

Il Manuale, inoltre, descrive tutte le procedure e le prassi seguite dal Responsabile del servizio di conservazione e dal Conservatore in materia di gestione della sicurezza del servizio, dei documenti e delle informazioni trattate nel Sistema di conservazione.

Il presente documento è stato redatto secondo i seguenti principi:

- **Principio di Conformità**: il manuale mira a descrivere un sistema e un processo di conservazione secondo le disposizioni normative vigenti nel tempo;
- **Principio di Trasparenza**: il manuale mira a fornire una chiara spiegazione del Sistema di conservazione documentale e dei processi effettivamente erogati;
- **Ottica di Processo**: il documento mira a descrivere le fasi del processo di conservazione secondo le regole tecniche e i modelli di riferimento, fra cui l'OAIS (Open Archival Information System) standard ISO 14721;
- **Principio di Rilevanza**: nel manuale sono contenute solamente le informazioni rilevanti, con un livello di dettaglio mirante ad agevolare le ispezioni, verifiche e controlli, senza dettagli tecnici e procedurali specifici e/o superflui;
- **Principio di Accuratezza**: le informazioni sono state revisionate da più persone, poste ai diversi livelli della catena decisionale;
- **Principio di Concretezza**: il manuale è il documento che descrive il Sistema di conservazione relativamente a tutti gli aspetti connessi alla conservazione e alla fruizione del patrimonio informativo digitale, in conformità ai modelli di riferimento;
- **Principio di Personalizzazione**: la descrizione di eventuali specifiche forniture del servizio di conservazione per una determinata comunità di riferimento che accede al Sistema di conservazione è eseguita sulla base di un'analisi e uno studio preliminare delle esigenze del Titolare dei documenti e degli utenti del sistema, in conformità al modello di riferimento OAIS (Open Archival Information System) standard ISO 14721, ed è riportata come *addendum* contrattuale.

Il presente Manuale del Conservatore è collegato ai documenti riportati nella successiva tabella, che entrano più nel dettaglio in diversi aspetti del Sistema di conservazione.

Documenti collegati	*Descrizione*
Scheda Servizio	È il disciplinare tecnico - allegato al Contratto - contenente determinate "Specificità del contratto", in particolare i requisiti essenziali del Servizio, le relative specifiche tecnico-funzionali e procedurali, oltre alle tempistiche del processo di conservazione. Tale documento costituisce parte integrante e sostanziale del *Manuale della conservazione* redatto dal Cliente e completa il Manuale del Conservatore in quegli aspetti relativi al servizio come la descrizione delle tipologie documentali attivate dal Cliente e i relativi metadati, le regole di versamento, gli utenti abilitati, etc.
Richiesta di attivazione	Ove prevista, è il documento proposto al Cliente da Namirial, dal Distributore o dal Committente, che, unitamente alla Scheda Servizio, contiene talune specificità del contratto.

Il presente documento è identificato attraverso il livello di revisione e la data di emissione. Il Conservatore esegue periodicamente un controllo di conformità del processo di erogazione del servizio di conservazione e, ove necessario, aggiorna il documento in oggetto anche in considerazione dell'evoluzione della normativa e degli standard tecnologici.

Il Manuale è messo a disposizione tramite pubblicazione nel sito web del Conservatore ed è un documento informatico prodotto nel formato PDF/A, firmato digitalmente e conservato secondo le disposizioni della normativa vigente, al fine di assicurarne l'origine, la data certa e l'integrità del contenuto dalla sua emissione e per tutto il periodo di conservazione.

Torna al Sommario

2 TERMINOLOGIA

2.1 Glossario

N.	Termini	Descrizione
1.	Accesso	Operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici
2.	AgID	L'Agenzia per l'Italia Digitale è l'agenzia tecnica della Presidenza del Consiglio dei Ministri che ha il compito di garantire la realizzazione degli obiettivi dell'Agenda digitale italiana e contribuire alla diffusione dell'utilizzo delle tecnologie dell'informazione e della comunicazione, favorendo l'innovazione e la crescita economica
3.	Affidabilità	Caratteristica che esprime il livello di fiducia che l'utente ripone nel documento
4.	Aggregazione documentale informatica	Aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni del Titolare dell'oggetto di conservazione
5.	Archival Information Package (AIP)	Pacchetto informativo composto dalla trasformazione di uno o più Submission Information Package (SIP) in conformità allo standard OAIS
6.	Archiviazione	Processo di trattamento e gestione dei documenti di uso corrente e/o nel medio lungo periodo che permette una loro classificazione (indicizzazione) ai fini della ricerca e consultazione
7.	Archivio	Complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un Titolare dell'oggetto di conservazione durante lo svolgimento della propria attività
8.	Archivio informatico	Archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico
9.	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
10.	Autenticazione del documento informatico	La validazione del documento informatico attraverso l'associazione di dati informatici relativi all'autore o alle circostanze, anche temporali, della redazione
11.	Autenticità	Caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico

12.	Base di dati	Collezione di dati correlati e registrati tra loro
13.	Certificato qualificato	È un documento elettronico che attesta, con una firma digitale, l'associazione tra una chiave pubblica e l'identità di un soggetto (persona fisica)
14.	Certification authority (CA)	È l'ente, pubblico o privato, abilitato a rilasciare certificati digitali tramite procedura di certificazione che segue standard internazionali e conforme alla normativa italiana ed europea in materia
15.	Chiave privata	L'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico
16.	Chiave pubblica	L'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche
17.	Ciclo di gestione	Arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo
18.	Comunità di riferimento	Un gruppo ben individuato di potenziali Utenti che dovrebbero essere in grado di comprendere l'informazione conservata, secondo lo standard OAIS. Una comunità di riferimento può essere composta anche da più comunità di Utenti
19.	Conservatore qualificato	Soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
20.	Conservazione	Servizio di conservazione dei Documenti informatici, costituito dall'insieme delle attività finalizzate a definire e attuare le politiche complessive del Sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato. La Conservazione è finalizzata a preservare nel lungo termine i documenti espressamente indicati dal Cliente a livello contrattuale allo scopo di assicurare ai documenti stessi integrità, autenticità e leggibilità, mantenendone la validità legale per tutto il periodo di conservazione, stabilito contrattualmente
21.	Copia analogica del documento informatico	Documento analogico avente contenuto identico a quello del documento informatico da cui è tratto
22.	Copia di sicurezza	Copia di backup degli archivi del Sistema di conservazione
23.	Copia informatica di documento analogico	Il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto

24.	Copia informatica di documento informatico	Il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari
25.	Copia per immagine su supporto informatico di documento analogico	Il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto
26.	Destinatario	Identifica il soggetto/sistema al quale il documento informatico è indirizzato
27.	Discard Information Package	Pacchetto di Scarto, pacchetto informativo contenente i documenti da scartare dal Sistema di conservazione una volta raggiunto il termine temporale di conservazione
28.	Dispositivo sicuro per la creazione della firma	I dispositivi sicuri per la generazione della firma qualificata che devono essere dotati di certificazione di sicurezza secondo l'art. 35 del CAD
29.	Dissemination Information Package (DIP)	Pacchetto informativo inviato dal Sistema di conservazione all'Utente in risposta ad una sua richiesta in conformità allo standard OAIS
30.	Documento analogico	La rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti
31.	Documento informatico	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
32.	Duplicato informatico	Documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario
33.	Esibizione	Operazione che consente di visualizzare un documento conservato e di ottenerne copia
34.	Evidenza informatica	Una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica
35.	Fascicolo informatico	Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'art. 41 del CAD
36.	Firma elettronica	L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica
37.	Firma elettronica avanzata	Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da

		consentire di rilevare se i dati stessi siano stati successivamente modificati
38.	Firma elettronica qualificata	Un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma
39.	Firma digitale	Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici
40.	Formato	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
41.	Formazione	Il processo atto ad assicurare l'autenticità dell'origine e l'integrità del contenuto dei documenti informatici, con le modalità indicate nelle Regole tecniche
42.	FTP Server	Programma che permette di accettare connessioni in entrata e di comunicare in maniera sicura con un Client attraverso il protocollo FTP
43.	Funzioni archivistiche	Funzioni per la conservazione delle informazioni (acquisizione, archiviazione, gestione dei dati, accesso, distribuzione)
44.	Funzione di hash	Una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
45.	Identificativo univoco	Sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione
46.	Identificazione informatica	La validazione dell'insieme di dati attribuiti in modo esclusivo e univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso
47.	IDM	Strumento per rilasciare le informazioni di identificazione di tutti i soggetti che cercano di interagire con un Sistema; ciò si ottiene tramite un modulo di autenticazione che verifica un token di sicurezza come alternativa all'autenticazione esplicita di un utente all'interno di un ambito di sicurezza
48.	Immodificabilità	Caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso

49.	Impronta	La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash
50.	Index of the Archival Information Package	Indice dell'Archival Information Package, struttura dell'insieme dei dati a supporto del processo di conservazione, riferita allo standard SInCRO (UNI 11386)
51.	Index of the Submission Information Package	Indice del Submission Information Package, struttura dell'insieme dei dati a supporto del processo di versamento del Submission Information Package e definita nello specifico dal Conservatore
52.	Index of the Dissemination Information Package	Indice del Dissemination Information Package, struttura dell'insieme dei dati a supporto del processo di distribuzione del Dissemination Information Package e definita nello specifico dal Conservatore
53.	Index of the Discard Information Package	Indice del Discard Information Package, struttura dell'insieme dei dati a supporto del processo di scarto del Discard Information Package e definita nello specifico dal Conservatore
54.	Information Package	Pacchetto Informativo, contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare in conformità allo standard OAIS che prevede pacchetti informativi di diversa natura che interagiscono con il Sistema di conservazione (SIP, AIP, DIP, etc).
55.	Linee Guida sulla formazione, gestione e conservazione dei documenti informatici (Linee Guida)	Regole tecniche emanate da AgID in materia di formazione, protocollazione, gestione e conservazione del documento informatico
56.	Log di sistema	Registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati
57.	Manuale del Conservatore	È il documento analitico, relativo al Sistema di conservazione, redatto dal Conservatore e pubblicato nella sua versione più aggiornata sul proprio sito, nel quale sono dettagliate le specifiche procedure relative al Servizio, oltre alle politiche generali del Sistema di conservazione dei Documenti informatici.
58.	Manuale della conservazione	È il documento informatico, redatto dal Titolare dell'oggetto di conservazione, nel quale sono dettagliate le specifiche procedure relative al Servizio. Lo stesso può indicare anche le attività del processo di conservazione affidate al Conservatore, in conformità con il contenuto del Manuale del Conservatore, e rinviare, per le parti di competenza, allo stesso.

59.	Memorizzazione	Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici
60.	Metadati	Insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel Sistema di conservazione
61.	Originali non unici	I documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi
62.	Pacchetto di Archiviazione (PdA)	Denominazione del AIP secondo il quadro normativo italiano in materia di formazione, gestione, conservazione dei documenti informatici
63.	Pacchetto di Versamento (PdV)	Denominazione del SIP secondo il quadro normativo italiano in materia di formazione, gestione, conservazione dei documenti informatici
64.	Pacchetto di Distribuzione (PdD)	Denominazione del DIP secondo il quadro normativo italiano in materia di formazione, gestione, conservazione dei documenti informatici
65.	Piano per la sicurezza	È il documento aziendale che analizza il contesto in cui l'azienda opera riportando i fattori interni ed esterni che lo influenzano ed evidenzia le principali criticità legate alla gestione della sicurezza delle informazioni gestite
66.	Presa in carico	Accettazione da parte del Sistema di conservazione di un SIP in quanto conforme alle modalità previste dal Manuale del Conservatore
67.	Processo di conservazione	Insieme delle attività finalizzate alla conservazione dei documenti informatici
68.	Produttore	È il responsabile della generazione del SIP e della relativa trasmissione al Conservatore
69.	Qualificazione	Riconoscimento, da parte degli enti preposti, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza, ad un soggetto pubblico o privato che svolge attività di conservazione
70.	Rapporto di Versamento (RdV)	Denominazione del Submission Report secondo il quadro normativo italiano in materia di formazione, gestione, conservazione dei documenti informatici
71.	Responsabile della conservazione	Soggetto, individuato dal Titolare dell'oggetto di conservazione responsabile dell'erogazione del Servizio che gestisce e attua le politiche complessive del Sistema di conservazione dei Documenti informatici, garantendo il rispetto dei requisiti previsti dalle norme in vigore nel tempo per i sistemi di conservazione

72.	Responsabile del servizio di conservazione (Preservation Service Manager)	Soggetto persona fisica nominato Responsabile del servizio di conservazione di Namirial, secondo quanto previsto dalla normativa vigente
73.	Responsabile della funzione archivistica di conservazione (Archival Manager)	Soggetto persona fisica nominato Responsabile della funzione archivistica di conservazione di Namirial, secondo quanto previsto dalla normativa vigente
74.	Riferimento temporale	Informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento
75.	Revision Package	Pacchetto di Revisione, pacchetto informativo inviato dal Produttore al Sistema di conservazione secondo un formato predefinito al fine di apportare una revisione ai dati precedentemente conservati dal Sistema
76.	Scarto	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale
77.	Service Level Agreement (SLA)	È l'accordo tra Titolare dell'oggetto di conservazione, Produttore, Responsabile della conservazione e Conservatore sui livelli servizio da garantire
78.	Sessione di distribuzione	Sessione per la consegna (distribuzione) di uno o più Pacchetti di Distribuzione dal Conservatore al Titolare
79.	Sessione di ricerca	Una sessione avviata da un Utente di un Sistema di conservazione, durante la quale l'Utente usa gli Strumenti di Ricerca del sistema per individuare e consultare gli oggetti digitali in esso presenti
80.	Sessione di versamento	Sessione per la consegna (versamento) di uno o più SIP dal Produttore al Conservatore, sulla base di un modello-dati per i formati e i contenuti definito e concordato tra le parti
81.	Sistema di conservazione/Long Term Archiving System (LTA)	Sistema di conservazione dei documenti informatici
82.	Submission Information Package (SIP)	Pacchetto informativo inviato dal Produttore al Sistema di conservazione secondo un formato predefinito e in conformità allo standard OAIS
83.	Submission Report	Documento informatico che attesta l'avvenuta presa in carico da parte del Sistema di conservazione dei SIP inviati dal Produttore
84.	Titolare dell'oggetto di conservazione (o "Soggetto produttore")	Soggetto che ha originariamente formato per uso proprio o commissionato ad altro soggetto o acquisito il Documento informatico nell'espletamento della propria attività o che ne ha la disponibilità.

85.	Titolare di firma	La persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica
86.	Utente	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse
87.	Validazione temporale	Il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data e un orario opponibili ai terzi

Torna al Sommario

2.2 Acronimi

N.	*Acronimi*	*Descrizione*
1.	AgID	Agenzia per l'Italia Digitale
2.	LTA	Long Term Archiving
3.	OAIS	Open Archival Information System, ISO 14721
4.	AIP	Archival Information Package
5.	DIP	Dissemination Information Package
6.	SiNCRO	Support for Interoperability in Preservation and Recovery of Digital Objects - Supporto all'interoperabilità nella conservazione e recupero degli oggetti digitali (UNI 11386)
7.	SIP	Submission Information Package
8.	SR	Submission Report

Torna al Sommario

3 NORMATIVA E STANDARD DI RIFERIMENTO

3.1 Normativa di riferimento

Nel presente paragrafo è riportata la principale normativa di riferimento per l'attività di conservazione a livello nazionale ed internazionale a cui l'attività di conservazione del Conservatore Namirial si riferisce.

3.1.1 Unione Europea

- **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016** on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - **GDPR**);
- **Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014** on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (**eIDAS**)

3.1.2 Italia

- **Codice Civile** [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- **Legge 7 agosto 1990, n. 241 e s.m.i.** – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- **Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i.** – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- **Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i.** – Codice in materia di protezione dei dati personali;
- **Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i.** – Codice dei Beni Culturali e del Paesaggio;
- **Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i.** – Codice dell'amministrazione digitale (CAD);
- **Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013** - Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005, nelle disposizioni attualmente vigenti indicate nelle Linee Guida emanate da AgID;
- **Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013** – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;

- **AgID, Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, maggio 2021**;
- **AgID, Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici**, **giugno 2021**

3.1.3 Romania

- **Lege nr. 135 din 15 mai 2007** privind arhivarea documentelor în formă electronică;
- **Ordin nr. 489 din 15 iunie 2009** privind normele metodologice de autorizare a centrelor de date;
- **Ordin nr. 493 din 15 iunie 2009** privind normele tehnice şi metodologice pentru aplicarea Legii nr. 135/2007 privind arhivarea documentelor în formă electronică;
- **Ordin nr. 585 din 9 mai 2011** pentru completarea Ordinului ministrului comunicațiilor și societății informaționale nr. 489/2009 privind normele metodologice de autorizare a centrelor de date;
- **Ordin nr. 1167 din 25 noiembrie 2011** pentru modificarea Anexei nr. 3 la Ordinul ministrului comunicaţiilor şi societăţii informaţionale nr. 489/2009 privind normele metodologice de autorizare a centrelor de date

3.1.4 Francia

- **Ordonnance n° 2004-178 du 20 février 2004** relative à la partie législative du code du patrimoine per la sua parte legislativa, con Décret n° 2011-573 du 24 mai 2011 relatif à la partie réglementaire du code du patrimoine (Décrets en Conseil d'Etat et en conseil des ministres) Décret n° 2011-574 du 24 mai 2011 relatif à la partie réglementaire du code du patrimoine (livres Ier à VI);
- **Arrêté du 4 décembre 2009** précisant les normes relatives aux prestations en archivage et gestion externalisée;
- **Décret n° 2020-733 du 15 juin 2020** relatif à la déconcentration des décisions administratives individuelles dans le domaine de la culture

3.2 Standard di riferimento

Si riportano di seguito gli standard di riferimento a cui l'attività di conservazione del Conservatore Namirial si riferisce.

- **ISO 9001** Quality management systems – Requirements;
- **ISO/IEC 27001** Information technology - Security techniques - Information security management systems – Requirements;
- **ISO/IEC 27017** Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services;

- **ISO/IEC 27018** Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors;
- **ISO/IEC 22313** Security and resilience - Business continuity management systems - Guidance on the use of ISO 22301;
- **ISO 14721 Space data and information transfer systems** - **Open archival information system** (**OAIS**) Reference model;
- **ISO 14641** Electronic document management - Design and operation of an information system for the preservation of electronic documents - Specifications;
- **NF 461** Système d'archivage électronique;
- **ETSI EN 319 401** Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- **ETSI TS 119 511** Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques;
- **UNI 11386 Standard SInCRO** Support for Interoperability in Preservation and Recovery of Digital Objects - Supporto all'interoperabilità nella conservazione e recupero degli oggetti digitali;
- **ISO 16363** Space data and information transfer systems - Audit and certification of trustworthy digital repositories.

Torna al Sommario

4 RUOLI E RESPONSABILITÀ

Il Sistema di conservazione descritto nel presente manuale definisce e adotta uno specifico modello organizzativo, che coinvolge soggetti, strutture e/o funzioni deputate al versamento, all'implementazione, all'erogazione del processo, alla gestione e al controllo del Sistema di conservazione di documenti informatici. Il modello organizzativo di riferimento è definito formalmente nei ruoli e nelle responsabilità dei vari attori coinvolti nel processo di conservazione dei documenti informatici, come riportato nella tabella successiva, in conformità ai ruoli e alle attività ad essi associati indicati dalla normativa e dagli standard di riferimento, fra cui l'OAIS.

Si precisa che le attività affidate al Responsabile del servizio di conservazione, sono indicate nel Contratto che il Cliente sottoscrive all'attivazione del servizio.

Ruoli	*Nominativo*	*Attività di competenza*	*Periodo nel ruolo*	*Eventuali deleghe*
Responsabile del servizio di conservazione (Preservation Service Manager)	**Davide Coletto**	– definizione e attuazione delle politiche complessive del Sistema di conservazione, nonché del governo della gestione del Sistema di conservazione; – definizione delle caratteristiche e dei requisiti del Sistema di conservazione in conformità alla normativa vigente; – corretta erogazione del servizio di conservazione al Soggetto produttore; – gestione delle convenzioni, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.	Dal 22 gennaio 2015	
	Luca Romagnoli	come sopra	Dal 24 novembre 2014 al 22 gennaio 2015	
Responsabile della sicurezza dei sistemi per	**Mario Veltini**	– rispetto e monitoraggio dei requisiti di sicurezza del Sistema di conservazione stabiliti dagli standard, dalle normative e dalle	Dal 5 luglio 2021	

la conservazione (Security Officer)		politiche e procedure interne di sicurezza; – segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.		
	Davide Coletto (interim)	come sopra	Dal 20 luglio 2018 al 5 luglio 2021	
	Andrea Lazzari	come sopra	Dal 24 novembre 2014 al 20 luglio 2018	
Responsabile della funzione archivistica di conservazione (Archival Manager)	**Enrico Giunta**	– definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte del 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 il 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.	Dal 26 maggio 2021	già *Delegato alla funzione archivistica di conservazione* dal 20 aprile 2020 al 25 maggio 2021

	Valeria Mocci	come sopra	Dal 24 ottobre 2016 al 14 aprile 2021	
	Matteo Sisti	come sopra	Dal 24 novembre 2014 al 24 ottobre 2016	
Responsabile del trattamento dei dati personali (DPO)	**Luca Santalucia**	– garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; – garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.	Dal 3 luglio 2023	
	Vanessa Cocca	come sopra	Dal 5 ottobre 2021 al 2 luglio 2023	
	Serena Donegani	come sopra	Dal 20 luglio 2018 al 4 ottobre 2021	
	Luca Romagnoli	come sopra	Dal 24 novembre 2014 al 20 luglio 2018	
Responsabile dei sistemi informativi per la conservazione (Information System Manager)	**Mario Veltini**	– gestione dell'esercizio delle componenti hardware e software del Sistema di conservazione; – monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con il Soggetto produttore; – segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive;	Dal 5 luglio 2021	

		– 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.		
	Genesio Di Sabatino	come sopra	Dal 24 ottobre 2016 al 5 luglio 2021	
	Giuseppe Benedetti	come sopra	Dal 24 novembre 2014 al 24 ottobre 2016	
Responsabile dello sviluppo e della manutenzione del sistema di conservazione (Development and Maintenance Manager)	**Fabio Didonè**	– coordinamento dello sviluppo e manutenzione delle componenti hardware e software del Sistema di conservazione; – pianificazione e monitoraggio dei progetti di sviluppo del Sistema di conservazione; – monitoraggio degli SLA relativi alla manutenzione del Sistema di conservazione; – interfaccia con il Produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche; – gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.	Dal 5 luglio 2021	

	Davide Coletto (interim)	come sopra	Dal 24 ottobre 2016 al 5 luglio 2021	
	Gianluca Cigliano	come sopra	Dal 24 novembre 2014 al 24 ottobre 2016	
Responsabile degli audit e delle verifiche (System and regulatory Auditor)	Federica Marti	– revisione periodica e completa dell'aderenza del servizio a tutte le leggi, i regolamenti e gli standard applicabili	Dal 31 luglio 2023	
	Margherita Menghini	come sopra	Dal 10 giugno 2022 al 31 luglio 2023	

4.1 Deleghe

In Romania, Adrian Dinculescu, assegnatario di tutti gli incarichi previsti per il Servizio di conservazione (eccetto DPO e System and regulatory Auditor), delega le proprie funzioni ai soggetti indicati nella tabella precedente.

Torna al Sommario

5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Organigramma

Di seguito l'organigramma adottato dall'organizzazione Namirial per la gestione del Servizio di conservazione di documenti informatici:

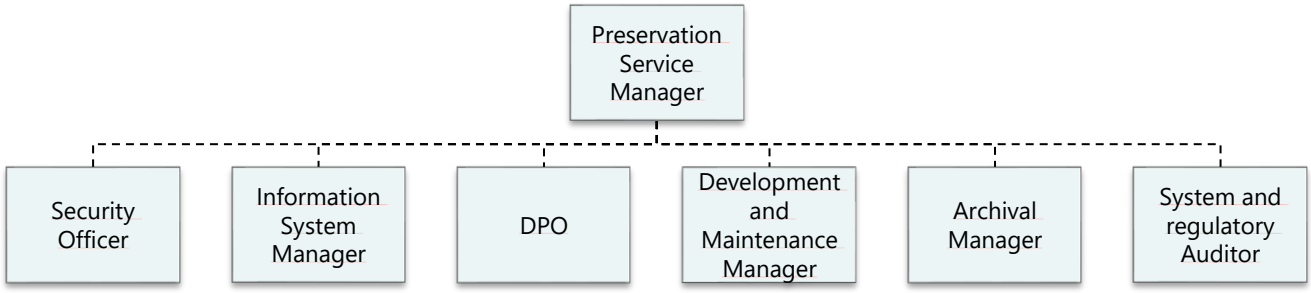


Figura 1 Organigramma del servizio e Sistema di conservazione

5.2 Strutture organizzative

Namirial considera il miglioramento continuo delle performance dei propri processi e servizi, nonché del Sistema della Sicurezza delle informazioni, uno degli strumenti strategici attraverso il quale conseguire gli obiettivi del proprio business, costituito dalla fornitura di risorse e professionalità e quindi di una struttura organizzativa a supporto per la progettazione, sviluppo, gestione, erogazione e commercializzazione dei propri servizi.

In particolare, per il servizio di conservazione di documenti informatici, Namirial ha certificato il proprio sistema di gestione della sicurezza delle informazioni nel dominio logico, fisico e organizzativo nel quale viene realizzato il processo di conservazione (certificazioni ISO/IEC 27001, 27017 e 27018) nel perimetro "Progettazione ed erogazione di servizi gestiti in modalità Saas, Paas e on premise in ambito Enterprise Content Management e paperless business (Business Process Management, acquisizione e trasmissione dei documenti, fatturazione elettronica, formazione documenti, gestione archiviazione e conservazione a Norma di documenti informatici)".

Le attività aziendali e i ruoli di coordinamento relativamente al Servizio di Conservazione tengono inoltre conto del modello concettuale relativo allo standard ISO 14721 OAIS (Open Archival Information System), in cui sono chiaramente distinti gli ambiti del Produttore (Producer/Cliente), del Management (Conservatore o Provider del Servizio) e della Comunità designata (Utenti abilitati alla fruizione dei documenti conservati, al fine di poter effettuare richieste di dissemination/distribuzione).

Il Servizio di Conservazione di Namirial presenta un ciclo di vita caratterizzato da tre fasi principali: *Attivazione, Esercizio e Post-Produzione*.

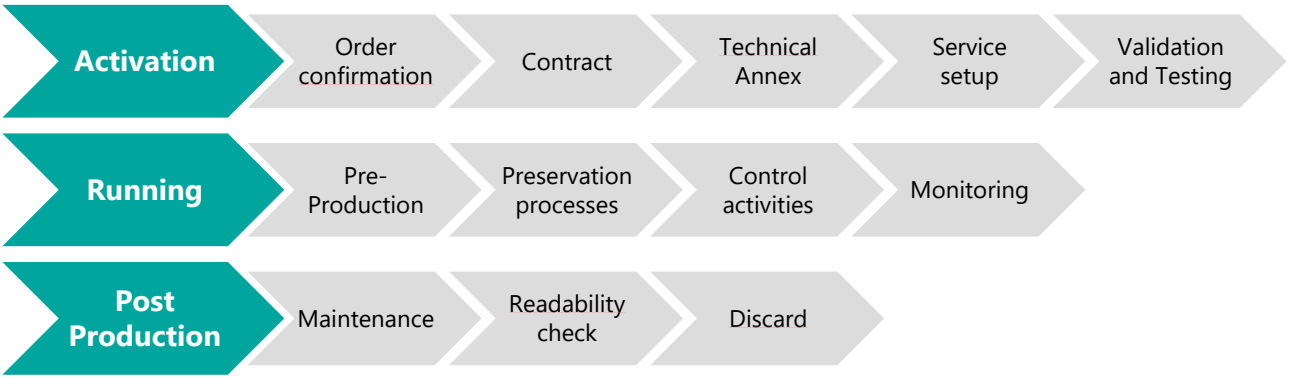


Figura 2 Ciclo di vita del Servizio di Conservazione

In ciascuna fase del servizio sono presenti sotto fasi.

Figura 3 Fase di attivazione

La fase di **Attivazione** del servizio avviene in caso di formale accettazione dell'offerta commerciale e delle condizioni contrattuali da parte del Cliente/Titolare dell'oggetto di conservazione, inclusi gli atti di nomina sottoscritti tra le parti per svolgere il ruolo di Conservatore, Responsabile del servizio di Conservazione e Responsabile del trattamento dei dati.

L'**Area Commerciale**, una volta ricevuta l'offerta commerciale, provvede a comunicare l'attivazione all'ufficio amministrativo, il quale provvede alla gestione di inserimento nei sistemi informativi dell'anagrafica del cliente e la compilazione della **conferma d'ordine** da mandare al cliente.

Successivamente all'invio della conferma d'ordine al cliente, vengono attivati tramite il sistema informativo interno le attività per l'Area di Supporto che prende in carico l'attività, contatta il cliente ed avvia la predisposizione del "Contratto" e del documento "Specificità del Contratto". Quest'ultimo documento è fondamentale per l'erogazione del servizio ad un determinato Cliente/Titolare ed è parte integrante del contratto di servizio.

Successivamente alla fase di avvio formale dell'acquisizione dell'ordine, l'area supporto prende contatto con il cliente per definire eventuali pre-processi o integrazioni necessarie per il versamento dei SIP fornendo supporto al cliente.

La predisposizione della corretta definizione iniziale dei requisiti e quindi la conformità alla normativa vigente in materia di sistemi di conservazione, con anche l'individuazione degli adempimenti correlati, è assicurata in fase di analisi dalla predisposizione del documento "Specificità del contratto - Scheda servizio", con il controllo e la supervisione da parte del **Responsabile della funzione archivistica di conservazione**, del **Responsabile del trattamento dei dati personali** (in caso di necessità) e del **Responsabile del servizio di conservazione**, che ha in carico l'approvazione finale.

Successivamente, il processo prevede che ad ogni variazione del Servizio (Change Process), il documento Specificità del contratto debba essere aggiornato e nuovamente condiviso tra le parti.

Predisposto e condiviso il documento "Specificità del contratto", validato dal **Responsabile del servizio di conservazione** e dal **Cliente**, l'area di Supporto ingaggia l'**Area di Produzione** che avvia le attività di configurazione del servizio nella piattaforma.

Prima viene eseguito un collaudo interno (verifica interna dell'**Area di Produzione delle configurazioni eseguite** in coerenza con quanto concordato nel **Documento "Specificità del Contratto"**). È poi se richiesto, si esegue il collaudo con il cliente.

Le modalità dell'eventuale collaudo sono indicate nel documento "Specificità del contratto"; a seguito dell'eventuale collaudo e della sua validazione formale da parte del cliente si procede con la successiva fase di messa in produzione.

Figura 4 Fase di esercizio

L'area organizzativa di **Produzione** si occupa di gestire le componenti hardware e software del servizio e di presidiare, controllare e monitorare il corretto funzionamento dei sistemi per la sua erogazione tramite l'ausilio del sistema di monitoraggio **Nagios e un sistema SIEM QRadar** sotto la supervisione del SOC.

Inoltre, l'**Area di Produzione** presidia e gestisce gli asset di infrastruttura e la corretta esecuzione del processo, dalla fase di presa in carico, al controllo di coerenza, dalla generazione del Submission Report (Rapporto di versamento), alla preparazione e gestione dei pacchetti di archiviazione, fino alla preparazione e gestione del DIP ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta dell'utente.

In particolare, il **Responsabile dei sistemi informativi** per la conservazione ha l'ownership delle attività di controllo degli asset e di monitorare il corretto svolgimento del servizio. In caso di riscontro di incident viene attivato il processo di gestione e risoluzione dell'incident attraverso la creazione di un ticket automatico al fine di tracciare l'accaduto e risolvere l'anomalia. Eventuali incident di rilievo e difformità sono segnalate al **Responsabile del servizio di conservazione** attraverso la procedura prevista dallo standard ISO/IEC 27001.

Completato con esito positivo il processo produttivo della conservazione dei documenti, il servizio per un determinato Cliente deve essere mantenuto nel tempo anche nella fase di post-produzione, per tutta la durata contrattuale concordata, garantendo ai documenti ed ai pacchetti informativi integrità, autenticità dell'origine, leggibilità, disponibilità e reperibilità, sicurezza e riservatezza.

Figura 5 Fase di Post-Produzione

Il mantenimento dei documenti e dei pacchetti generati nel processo di conservazione è garantito dalle attività dell'Area di Produzione (owner Responsabile dei sistemi informativi per la conservazione) e dall'Area di Ricerca e Sviluppo (owner Responsabile dello sviluppo e della manutenzione del sistema di conservazione) che garantiscono sia dal punto di vista infrastrutturale che applicativo il presidio e il controllo degli asset del servizio e quindi il corretto mantenimento dei documenti e dei pacchetti per tutto il periodo di conservazione concordato con il produttore dei documenti.

Durante la fase di post-produzione la struttura organizzativa del Conservatore, in particolare con le attività dell'Area di Assistenza e di Produzione, supporta gli adempimenti previsti dalla normativa.

Infine, scaduto il periodo di conservazione, concordato contrattualmente tra produttore, Responsabile della conservazione dei documenti e Responsabile del servizio di conservazione, viene avviata la procedura di Scarto concordata, la notifica dello scarto e la chiusura del servizio. Owner di queste attività sono l'**Area di Supporto** e **Produzione**.

In tutte le suddette fasi del servizio di conservazione ed in generale in tutte le attività indicate in carico al Conservatore è necessario garantire la Gestione dei sistemi informativi e della sicurezza a supporto del servizio. Tale obiettivo viene perseguito dall'organizzazione Namirial attraverso la definizione dei compiti, dei ruoli e delle responsabilità descritte nel presente manuale, attraverso verifiche e **audit periodici** e tramite l'ausilio di strumenti per il controllo e il monitoraggio. Le procedure definite all'interno del sistema di gestione della sicurezza (conforme allo standard ISO 27001) e della qualità aziendale (conforme allo standard ISO 9001) sono gli strumenti primari anche ai fini dell'analisi del rischio, della pianificazione e dell'adozione di misure per la prevenzione, la manutenzione e il miglioramento continuo del servizio.

Attori primari dell'attuazione della Gestione dei sistemi informativi e della sicurezza sono i responsabili definiti nell'organigramma per la conservazione, che di concerto devono garantire l'obiettivo aziendale e gestire la conformità alla normativa e il miglioramento continuo della qualità del servizio.

Torna al Sommario

6 OGGETTI SOTTOPOSTI A CONSERVAZIONE

Il funzionamento del Sistema di conservazione è conforme alla normativa in materia di formazione, gestione e conservazione dei documenti informatici e allo standard ISO 14721 OAIS (Open Archival Information System), modello di riferimento per la realizzazione e gestione di sistemi informativi per l'archiviazione e la conservazione degli oggetti digitali.

Alla base del funzionamento del modello OAIS, ripreso dalle regole tecniche vigenti, vi è il concetto di informazione da conservare (nella forma del cosiddetto "Information Package", pacchetto informativo).

Il versamento dei pacchetti (contenenti documenti e/o dati) al Sistema da parte di un Produttore, nonché ogni distribuzione di documenti dal Sistema ad un Utente autorizzato, avvengono infatti nella forma di una o più trasmissioni distinte (sessioni) ossia tramite lo scambio (versamento o distribuzione) di pacchetti informativi.

Il Conservatore Namirial, in conformità allo standard OAIS, ha implementato nel Sistema di conservazione, per ciascuna delle fasi fondamentali del processo descritte in precedenza, i pacchetti informativi intesi come contenitori astratti contenenti due tipologie di informazioni:

- Contenuto informativo;
- Informazioni sulla Conservazione (Preservation Description Information - PDI).

Contenuto informativo

Rappresenta l'insieme delle informazioni che costituisce l'oggetto della conservazione; è un *Oggetto informativo* composto dal suo *Oggetto dati* e dalle sue *Informazioni di rappresentazione*:

- Oggetto dati: è l'oggetto digitale, composto da un insieme di sequenze di bit;
- Informazioni sulla rappresentazione: sono le informazioni che rappresentano un Oggetto dati, ossia lo associano a concetti più significativi (es: formato). Include le *Information properties*, le informazioni significative che devono essere mantenute nel tempo (es.: elementi di formattazione, ecc.)

Informazioni sulla Conservazione (PDI Preservation Description Information):

Rappresentano le informazioni necessarie per un'adeguata conservazione del Contenuto informativo: sono fornite dai metadati e possono essere classificate in:

- Informazioni sulla provenienza: documentano la storia del Contenuto informativo: ad esempio forniscono informazioni sull'origine/sulla fonte del Contenuto informativo e su chi ne ha curato la custodia sin dalla sua origine;
- Informazioni sull'identificazione: identificano e, se necessario, descrivono uno o più meccanismi di attribuzione di identificatori al Contenuto informativo;
- Informazioni sull'integrità: garantiscono che il Contenuto informativo non sia stato alterato senza una documentazione dell'evento;
- Informazioni sul contesto: documentano le relazioni del Contenuto informativo con il suo ambiente, inclusi i motivi della creazione del Contenuto informativo, e il modo in cui è in relazione con altri Contenuti informativi;

- Informazioni sui diritti di accesso: possono identificare i limiti di accesso al contenuto informativo, inclusi i termini di licenza, le restrizioni legali e i sistemi di controllo.

Il Contenuto informativo e le Informazioni sulla conservazione sono incapsulati e identificabili mediante le Informazioni sull'Impacchettamento, ossia informazioni usate per collegare e identificare le componenti di un pacchetto informativo (Contenuto informativo e Informazioni sulla conservazione).

Il pacchetto informativo può essere ricercato all'interno del Sistema di conservazione tramite le informazioni descrittive, ossia l'insieme delle informazioni – composto essenzialmente dalla Descrizione del pacchetto – necessarie all'Utente per ricercare, richiedere e recuperare le informazioni conservate dal Sistema.

Affinché la conservazione dell'oggetto informativo avvenga correttamente, il Sistema è basato, quindi, su un modello che permette di identificare e comprendere l'oggetto dati e le relative informazioni sulla rappresentazione, che contengono informazioni sia di natura sintattica che semantica.

Torna al Sommario

6.1 Oggetti conservati

Nella Scheda Servizio, allegato contrattuale concordato tra il Conservatore e il Titolare dell'oggetto, redatta sulla base delle informazioni condivise in fase di analisi o predisposta a seconda del tipo di servizio da attivare, sono elencate e descritte le tipologie di documenti sottoposti a conservazione per un determinato Titolare e le relative politiche di conservazione, che specificano, per ciascuna tipologia individuata:

- la natura e l'oggetto della tipologia documentale;
- l'elenco e la descrizione dei metadati associati ai documenti;
- il periodo di conservazione;
- le tempistiche del processo di conservazione concordate con il Titolare dell'oggetto;
- altre politiche (regole) che caratterizzano il processo di conservazione.

Le tipologie di documenti che caratterizzano gli oggetti digitali da versare nel Sistema di conservazione sono definite attraverso le attività di analisi e di classificazione o sulla base del servizio da attivare.

6.2 Formati

Il Sistema di Conservazione accetta formati conformi all'elenco dei formati adatti alla conservazione indicati nell'**Allegato 2** delle **Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici**. File con formati non conformi verranno scartati in fase di presa in carico.
Per quanto riguarda la conservazione di file in formato TXT, non riportato tra i formati indicati da AgID, il Conservatore ha effettuato la valutazione di interoperabilità per il proprio sistema di conservazione secondo quanto indicato al par. 3.1 dell'Allegato 2 delle Linee Guida. La valutazione e il relativo di indice di interoperabilità sono riportati nel paragrafo successivo.

Si riporta di seguito un **elenco dei formati più comuni** utilizzati per la conservazione dei documenti informatici e **si rimanda all'Allegato 2 delle Linee Guida per l'elenco completo dei formati supportati**.

Formato del file	*Proprietario*	*Estensione*	*Tipo Mime*	*Visualizzatore*	*Produttore del visualizzatore*
PDF	Adobe Systems - www.adobe.com Ai fini della conservazione, nell'uso di tale formato occorre formare i documenti esclusivamemente con caratteri tipografici interoperabili, considerati "standard" da diversi organi di settore, come meglio specificato nel paragrafo 2.8 Caratteri tipografici dell'Allegato 2 delle Linee Guida AgID	.pdf	application/pdf	Adobe Reader	Adobe Systems www.adobe.com
PDF/A	Adobe Systems - www.adobe.com	.pdf	application/pdf	Adobe Reader http://www.pdfa.org/doku.php	Adobe Systems www.adobe.com
XML	W3C Ai fini della conservazione, nell'uso di tale formato è obbligatorio per il Titolare mantenere nel tempo anche il file XML Schema .xsd	.xml	application/xml text/xml	Mozilla -Chrome - Internet Explorer	Firefox - Google - Microsoft -
TXT	Ai fini della conservazione nell'uso di tale formato, è importante specificare la codifica del carattere (Character Encoding) adottata	.txt		Mozilla -Chrome - Internet Explorer	Firefox - Google - Microsoft -
TIFF	Aldus Corporation in seguito acquistata da Adobe	.tif, .tiff	image/tiff	Vari visualizzatori di immagini	
JPG	Joint Photographic Experts Group	.jpg, .jpeg	image/jpeg	Vari visualizzatori di immagini	Per maggiori informazioni sul formato www.jpeg.org
EML	Vari	.eml		Client di posta elettronica supportano la visualizzazione di file eml	Vari
OOXML	Microsoft Tale formato deve garantire alcune caratteristiche che lo rendono adatto alla conservazione nel lungo	.docx, .xlsx, .pptx			

	periodo, tra queste l'embedding dei font, la presenza di indicazioni di presentazione del documento, la possibilità di applicare al documento la firma digitale XML. È opportuno utilizzare il profilo *Strict* che consente di eliminare alcune estensioni "proprietarie" che possono ridurre l'interoperabilità del formato stesso				
ODF	Consorzio OASIS OpenOffice.org	.ods, .odp, .odg, .odt	application/vnd.oasis.opendocument.text		www.oasis-open.org

In tutti i casi il Produttore dei SIP si impegna a versare al Sistema di conservazione documenti **privi di codici eseguibili o macro-istruzioni** che ne possano alterare il contenuto.

Resta inteso che sui documenti oggetto del Servizio di Conservazione il Titolare può apporre una firma digitale nei formati standard di firma CAdES (.p7m), PAdES (.pdf) e XAdES (.xml) e/o una marca temporale.

6.2.1 Valutazione ed indice di interoperabilità

Il Sistema di Conservazione supporta il formato TXT, anche se non riportato tra i formati indicati nell'Allegato 2 delle Linee Guida emanate da AgID, in quanto formato ampiamente utilizzato in molteplici ambiti e riconosciuto dalla maggior parte dei programmi di elaborazione. Ai fini della conservazione, nell'uso di tale formato, **è necessario indicare** la specifica codifica del carattere (Character Encoding) adottata, su cui il Titolare è obbligato ad utilizzare font interoperabili standard.

Come indicato da AgID al par. 3.2 dell'Allegato 2 delle Linee Guida, si riporta di seguito **l'indice di interoperabilità relativo al formato TXT**:

Caratteristica	*Intervallo*	*Valutazione*	*Valore*
Standardizzazione	da 0 a 3	Il formato TXT è standard de facto e de jure. È basato su codifica ASCII; l'ASCII nella sua versione originaria a 7 bit (chiamata anche ASCII ristretto, o US-ASCII) è stato riconosciuto come standard dall'ISO con il codice ISO 646:1972. Esiste tuttavia una seconda più recente versione, la quale, essendo ad 8 bit, consente una gamma più ampia di caratteri (256 in totale) e quindi può meglio adattarsi alle esigenze di lingue in cui gli alfabeti sono particolarmente vasti: questa seconda versione è chiamata ASCII esteso e si è affermata dapprima come standard de facto (nel corso degli anni 80) e successivamente come standard ISO/IEC 8859. Esiste, poi, una terza versione enormemente più estesa (attualmente si parla di oltre un milione di caratteri possibili), chiamata UNICODE e sviluppata nel 1991, i cui primi 256 code points ricalcano esattamente quelli dell'ISO 8859-1.	3
Apertura	da 0 a 3	Il formato TXT è un formato aperto	3
Non proprietà	da 0 a 4	Il formato TXT non è proprietario	2
Estendibilità	da 0 a 2	Il formato TXT è un formato estensibile	2
Livello di metadati	da 0 a 3	Il formato TXT non consente di incorporare alcun metadato all'interno del file	0
Robustezza	da 0 a 2	Il formato TXT non è binario. Essendo testuale è tra i formati più robusti	2
Indipendenza da dispositivi	da 0 a 4	Il formato TXT è leggibile su qualsiasi ambiente operativo o device.	4

Compatibilità in avanti e all'indietro	non specificato	Il formato TXT appartiene alla categoria file di testo e sono presenti molteplici software di elaborazione testi, installabili su piattaforma di sistema Android, Linux, Mac OS, Windows, Windows Phone, al fine di accedere e visualizzare i file nel formato TXT.	2
Testuale o binario	non specificato	Formato non formattato il cui contenuto è puramente testuale (ASCII)	2
		TOTALE	**20**

I valori e la scala utilizzati sono quelli consigliati nel par. 3.2 dell'Allegato 2 delle Linee Guida:

- formato più interoperabile: totale ≥ 20
- formato meno interoperabile: totale = 0
- soglia minima: totale = 12

Torna al Sommario

6.3 Submission Information Package (SIP)

Il Submission Information Package (SIP) è costituito da un archivio zip non compresso, composto da:

- i documenti oggetto della conservazione (*Content Information*), eventualmente firmati digitalmente (nello standard di firma CAdES ".p7m" o PAdES o XAdES) o eventualmente marcati temporalmente (nello standard di validazione temporale CAdES-T, o PAdES-T o XAdES-T);
- un file SIP Index (SIPindex) finalizzato alla descrizione delle *Preservation Description Information*, ossia alla descrizione delle informazioni relative all'oggetto della conservazione, all'identificazione del Titolare dell'oggetto e del Produttore del SIP, ai dati descrittivi e informativi sull'impacchettamento e su ciascun documento contenuto nel pacchetto.

Il file Indice del SIP è un file nel formato XML, che assicura:

- l'identificazione del soggetto che ha prodotto il SIP (Producer);
- l'identificazione dell'applicativo che lo ha prodotto;
- la definizione della tipologia documentale a cui appartengono i documenti inclusi nel pacchetto ed eventuali messaggi del Responsabile della conservazione;
- la definizione dei documenti inclusi nel pacchetto, con le relative informazioni quali: nome file, hash calcolato, indici (metadati) e relativi valori, messaggi del Responsabile della conservazione, ecc.

Il file Indice del SIP può essere eventualmente firmato digitalmente dal Produttore.

Di seguito la rappresentazione grafica del file XSD dell'Indice del SIP:

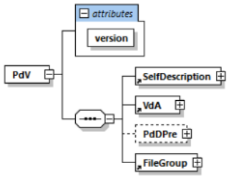
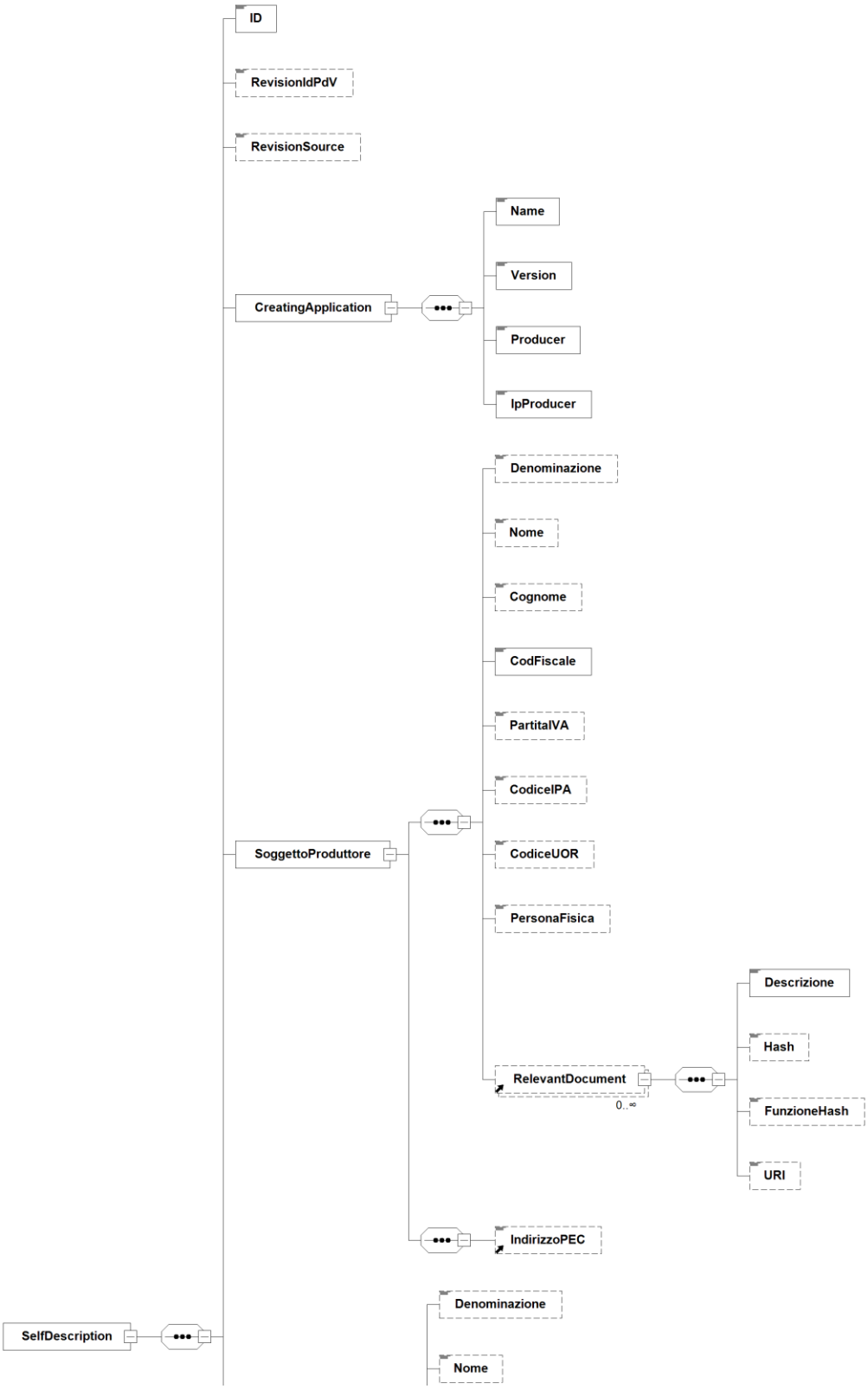


Figura 6 Struttura Indice SIP suddiviso nelle componenti principali


ID
RevisionIdPdV
RevisionSource
CreatingApplication
Name
Version
Producer
IpProducer
SoggettoProduttore
Denominazione
Nome
Cognome
CodFiscale
PartitaIVA
CodiceIPA
CodiceUOR
PersonaFisica
RelevantDocument
0..∞
Descrizione
Hash
FunzioneHash
URI
IndirizzoPEC
SelfDescription
Denominazione
Nome

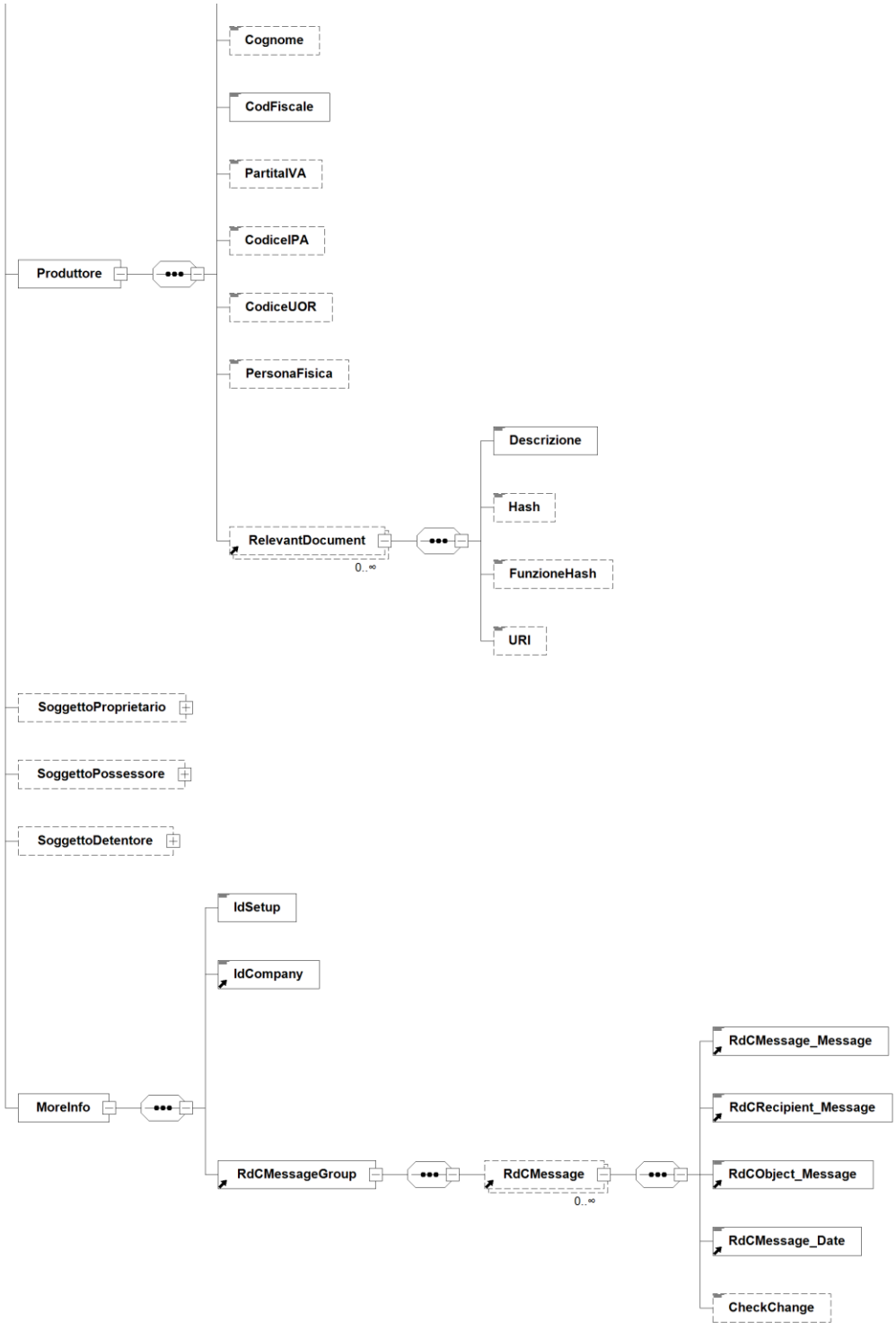


Figura 7 Struttura Indice SIP (Sezione SelfDescription)

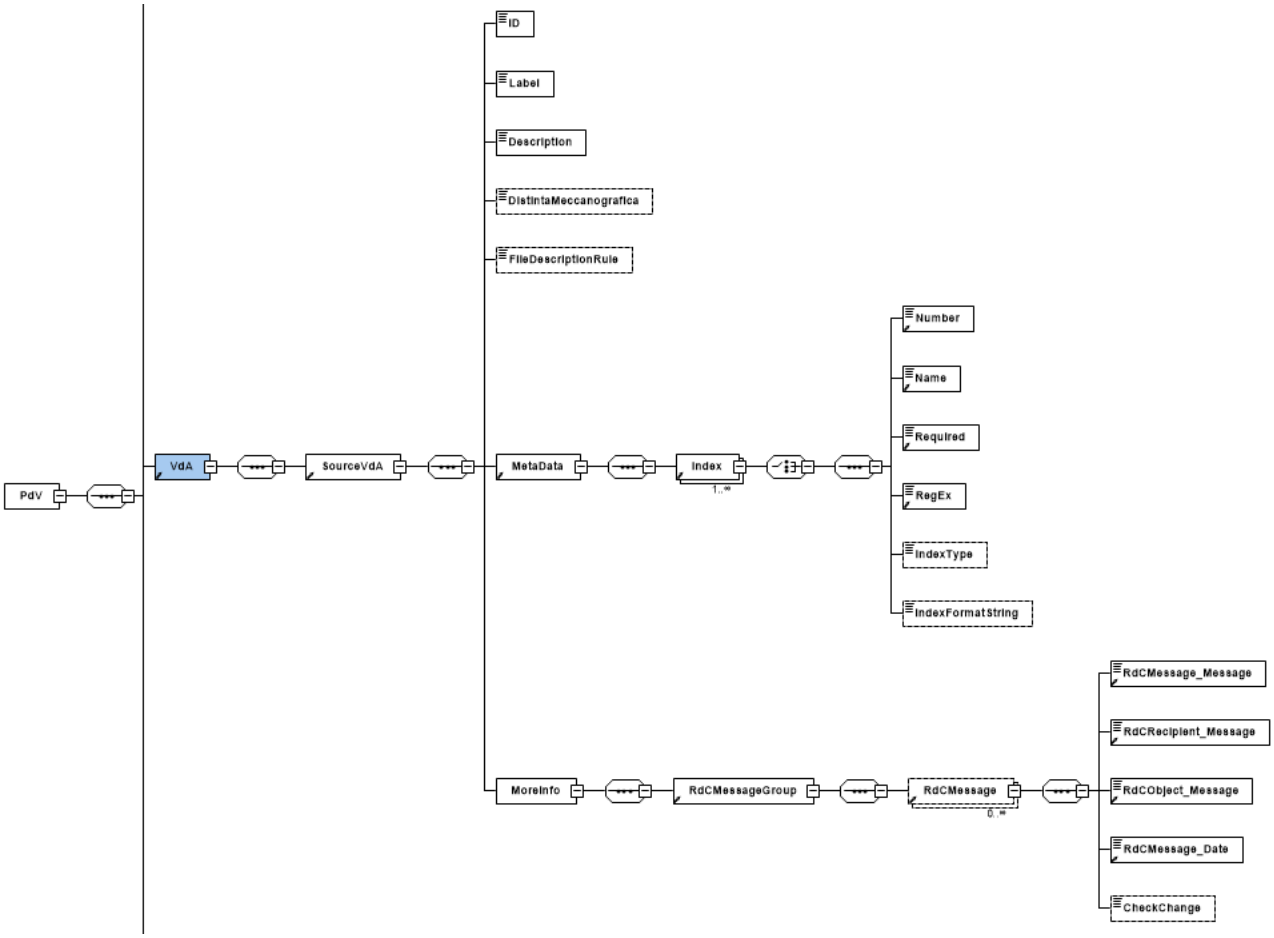


Figura 8 Struttura Indice SIP (Sezione VdA)

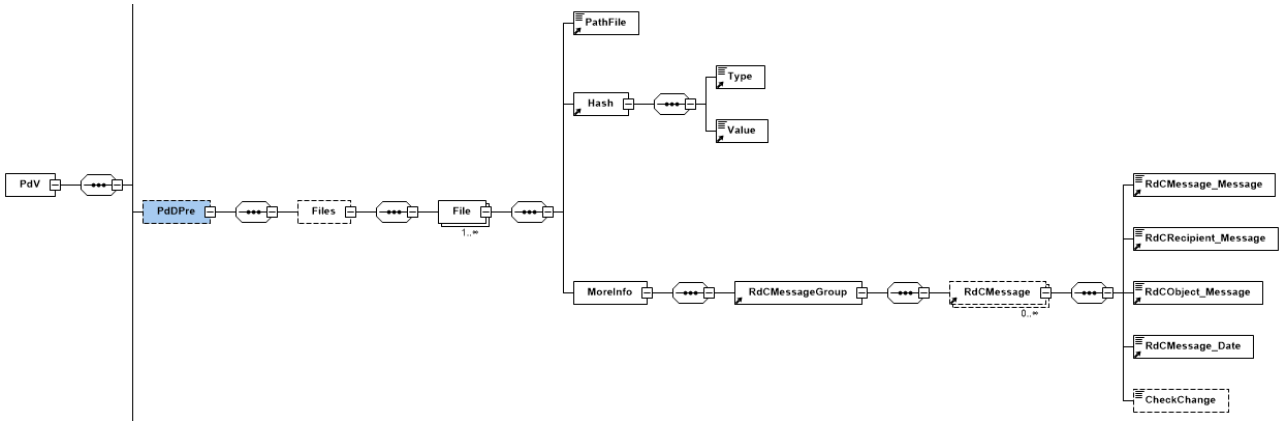


Figura 9 Struttura Indice SIP (Sezione DIPPre)

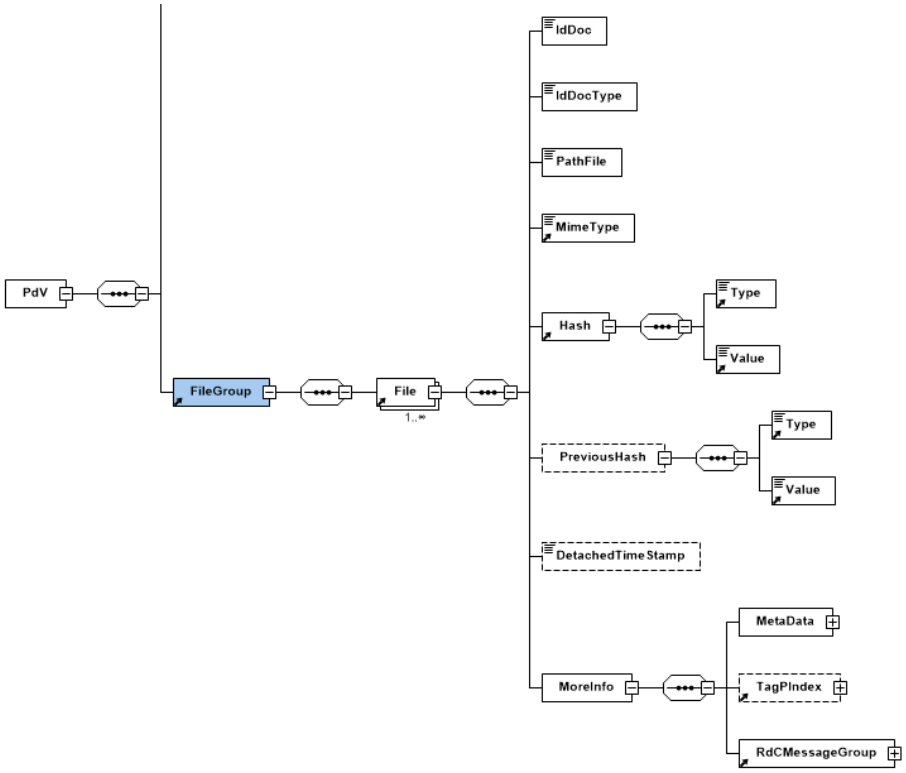


Figura 10 Struttura Indice SIP (Sezione FileGroup)

6.3.1 Pre-pacchetto

In caso di versamento di file non firmati o marcati temporalmente e di implementazione di funzionalità di apposizione automatica di certificati nella fase di versamento (modalità opzionale), il Produttore deve versare al Conservatore un pre-pacchetto (pSIP) contenente indice e documenti da conservare non firmati.

In caso di esito positivo dei controlli di coerenza, il Conservatore appone massivamente il certificato sui documenti del Titolare individuato dal Produttore, completando il processo di versamento con un SIP contenente i documenti firmati ed un nuovo Indice del SIP, nel quale è riportato l'hash del documento non firmato ed il nuovo hash del documento firmato.

Sia l'hash del documento non firmato (*Previoushash*), sia l'hash del documento firmato, sono riportati nell'Indice del AIP generato dal Conservatore Namirial al termine del processo di conservazione.

6.3.2 Revisione Information Package

Un pacchetto di revisione consente di apportare modifiche ad un SIP già versato, tramite la creazione di un nuovo SIP contenente il riferimento univoco (Id) del SIP originario da revisionare.

Per poter essere accettato dal sistema, un pacchetto di revisione deve contenere il tipo di modifica richiesta:

- Rettifica: Intervento volto a correggere o modificare un atto o una condizione precedente
- Integrazione: Intervento volto ad aggiungere un atto o una condizione precedente

- Annotazione: Registrazione sintetica per fini amministrativi, disciplinari, etc

Si ricorre all'utilizzo del pacchetto di revisione anche nei casi in cui sia necessario apporre un nuovo certificato relativamente alle evidenze di conservazione.

Torna al Sommario

6.4 Archival Information Package (AIP)

L'Archival Information Package (AIP) generato nel processo di conservazione del sistema è una specializzazione del pacchetto informativo ed è composto dalla trasformazione di uno o più Submission Information Package secondo le modalità riportate nel presente Manuale.

Un AIP contiene:

- gli oggetti informativi individuati per la conservazione (documenti e/o aggregazioni documentali sottoposti al processo di conservazione a lungo termine);
- un Indice dell'Archival Information Package (AIPindex) che rappresenta le Informazioni sulla Conservazione.

La struttura dati dell'Indice del AIP è conforme allo standard nazionale SInCRO (UNI 11386) riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione.

L'impronta informatica degli oggetti è calcolata tramite **algoritmo crittografico SHA-256** (Secure Hash Algorithm a 256 bit) al fine di generare Hash irreversibili e unici.

L'**Indice** del AIP è l'evidenza di conservazione prodotta in **formato XML** associata ad ogni AIP in cui è riportata nel dettaglio la struttura dati prevista. Su ciascun Indice dell'AIP viene apposta una **firma elettronica qualificata** del Responsabile del Servizio di Conservazione Namirial e una **marca temporale**, generati anch'essi con algoritmo SHA-256. La firma e la marca temporale sono emessi da Namirial in qualità, rispettivamente, di Certification Authority (CA) e di Time Stamping Authority.

Si riporta di seguito la struttura dati del AIP completa delle ulteriori strutture collegate ai diversi elementi "MoreInfo" previsti dallo standard SInCRO (PIndex).

- **SelfDescription (1)***: Descrizione generale del pacchetto.
  - **ID (1)**: Id univoco del AIP generato dal Sistema di conservazione (Id AIP generato dal database).
  - **CreatingApplication (1)**:
    - **Name (1)**: Sistema di conservazione.
    - **Version (1)**: Versione ricavata dal Web Service.
    - **Producer (1)**: Produttore del Sistema di conservazione
  - **PIndexSource (0-n)**
    - **ID (1):** Id dell'eventuale pacchetto archiviazione (AIP) precedente.
    - **Path (1):** Percorso relativo all'Indice AIP (SInCRO) dell'eventuale pacchetto precedente.

- **Hash (1):** Valore restituito dalla funzione applicandola al file Indice AIP dell'eventuale pacchetto precedente; contiene l'attributo "hashFunction" che identifica la funzione di hash utilizzata per il calcolo.

- **MoreInfo (1)**
  - **EmbeddedMetadata (1)**: Riferimenti del soggetto titolare dei documenti a cui si riferisce il processo di conservazione.
    - **MoreInfoSelfDescription (1)**
      - **IdSetup (1):** Id di attivazione per il soggetto titolare dei documenti all'interno del sistema.
      - **IdAzienda (1):** Id del soggetto titolare dei documenti all'interno del sistema.
      - **VersionIndexAIP (1):** Versione dell'indice AIP definita dal Conservatore.

➢ **PVolume (1):**
- **ID (1)**: Id univoco del AIP generato dal Sistema di conservazione (Id AIP generato dal database).
- **Label (0-1):** Nome dell'aggregazione.
- **Description (0-1):** Descrizione dell'aggregazione.
- **PVolumeSource (0-n):** Informazioni relative a un volume di conservazione da cui è originato quello in oggetto.
  - **ID (1):** Identificativo dell'aggregazione.
  - **PIndexID (1):** Identificativo dell'indice di conservazione associato al precedente volume di conservazione.
- **PVolumeGroup (0-1):** Informazioni relative a un'aggregazione cui il volume di conservazione appartiene.
  - **ID (1):** Identificativo dell'aggregazione.
  - **Label (0-1):** Nome dell'aggregazione.
  - **Description (0-1):** Descrizione dell'aggregazione.
- **MoreInfo (1)**
  - **EmbeddedMetadata (1)**: Elenco dei SIP inclusi all'interno del AIP
    - **MoreInfoPVolume (1)**
      - **SIPGruppo (1)**
        - **SIP (0-n)**
          - **IdSIP (1)**: Id del SIP restituito dal Sistema di conservazione al termine della presa in carico.
          - **RevisionIdSIP (0-1)**: Id del SIP revisionato (può essere il SIP di origine oppure l'ultima versione pubblicata per il SIP di origine). Il nodo è presente solo se il SIP rappresenta una revisione.
          - **RevisionIdSIPOrigin (0-1):** Id del SIP di origine (SIP iniziale da cui hanno origine tutte le revisioni). Il nodo è presente solo se il SIP rappresenta una revisione.
          - **RevisionNumber (0-1):** Numero della revisione necessario per ordinare la sequenza delle revisioni relative al SIP di origine. Il nodo è presente solo se il SIP rappresenta una revisione.

- **RevisionSource (0-1):** Definisce la provenienza del pacchetto di revisione. Valori ammessi: RequestProducer o Internal. Il nodo è presente solo se il SIP rappresenta una revisione.
- **FunzioneHash (1)**: Funzione di hash utilizzata per calcolare l'hash dell'SIP_INDEX.
- **Hash (1)**: Valore restituito dalla funzione di hash applicata al file SIP_INDEX.
- **IdSubmissionReport (1)**: Id del SR restituito dal Sistema di conservazione al momento della generazione.
- **FunzioneHashSubmissionReport (1):** Funzione di hash utilizzata per calcolare l'hash del SubmissionReport.
- **HashSubmissionReport (1):** Valore restituito dalla funzione di hash applicata al SubmissionReport.
- **DataSubmissionReport (1):** Data di generazione del SubmissionReport.
- **PMMessageGroup (1)**: Eventuali comunicazioni tra il produttore e il Responsabile della conservazione o il suo Delegato relative al SIP.
    - **PMMessage (0-n)**
        - **PMMessage_Message:** Testo del messaggio.
        - **PMRecipient_Message:** Testo del messaggio per chi riceve il Submission Information Package.
        - **PMObject_Message:** Eventuale file allegato riferito alla comunicazione.
        - **PMMessage_Date:** Data di inserimento del messaggio.
        - **CheckChange:** Metadato aggiuntivo che consente di specificare la verifica della modifica del documento. Valori ammessi: Rettifica; Integrazione; Annotazione.

- **DIPPre (0-1)**
    - **Files (1)**
        - **File (0-n)**
            - **PathFile (1):** Uri del file relativo ad un allegato DIPPre (riversamento da conservatore precedente). Necessario per meglio identificare l'allegato e poter capire in quale SIP si trova il file.
            - **Hash (1)**
                - **Type (1):** Funzione di hash applicata all'allegato DIPPre.

- **Value (1):** Valore restituito dalla funzione di hash applicata all'allegato DIPPre.

- **PMMessageGroup (1)**
  - **PMMessage (0-n):**
    - **PMMessage_Message:** Testo del messaggio.
    - **PMRecipient_Message:** Testo del messaggio per chi riceve il Submission Information Package.
    - **PMObject_Message:** Eventuale file allegato riferito alla comunicazione.
    - **PMMessage_Date:** Data di inserimento del messaggio.
    - **CheckChange:** Metadato aggiuntivo che consente di specificare la verifica della modifica del documento. Valori ammessi: Rettifica; Integrazione; Annotazione.

- **FileGroup (1-n)**:
  - **ID (1)**: Id della tipologia documentale alla quale si riferiscono i documenti.
  - **Label (0-1):** Nome della tipologia documentale alla quale si riferiscono i documenti.
  - **Description (0-1):** Descrizione della tipologia documentale alla quale si riferiscono i documenti.
  - **File (1-n)**: Definizione del file comprensiva di codifica, estensione e formato (MimeType)
    - **ID (1)**: Id del documento assegnato dal Sistema di conservazione (univoco all'interno del Sistema di Conservazione).
    - **Path (1)**: Indirizzo logico del file rappresentato da un URI (individua il file all'interno dello storage).
    - **Hash (1)**: Funzione di hash utilizzata e valore restituito dalla funzione applicandola al file oggetto della Conservazione.
    - **PreviousHash (1)**: Funzione di hash utilizzata e valore restituito dalla funzione applicandola al file oggetto della Conservazione (riferita ad un indice di Conservazione precedente).
    - **MoreInfo**:
      - **EmbeddedMetadata:**
        - **MoreInfoFile:** Informazioni relative al documento nel Sistema di conservazione utilizzate per identificare e descrivere il documento all'interno dell'archivio.
          - **File (1)**
            - **IdDoc**: Identificativo univoco del file assegnato dal Produttore (univoco all'interno della tipologia documentale definita per l'azienda).
            - **IdSIP**: Id del SIP associato al documento.
            - **Indici (1)**

        - **Indice (1-n)**
            - **Nome**: Nome del campo indice (metadato).
            - **Valore**: Valore del campo indice (metadato).
    - **AnnoRiferimentoDoc**: Anno di riferimento del documento (ad es. anno del periodo di imposta)
    - **Oggetto**: Metadato funzionale a riassumere brevemente il contenuto del documento o comunque a chiarirne la natura. Viene calcolato in automatico dal sistema, in funzione alle regole definite in fase di versamento.
    - **CheckChange:** Metadato aggiuntivo che consente di specificare la verifica della modifica del documento. Valori ammessi: Rettifica; Integrazione; Annotazione
    - **PMMessageGroup (1)**: Eventuali comunicazioni tra il produttore e il Responsabile della conservazione o il suo Delegato relative al file.
        - **PMMessage (0-n)**
            - **PMMessage_Message:** Testo del messaggio.
            - **PMRecipient_Message:** Testo del messaggio per chi riceve il Submission Information Package.
            - **PMObject_Message:** Eventuale file allegato riferito alla comunicazione.
            - **PMMessage_Date:** Data di inserimento del messaggio
    - **DetachedTimeStamp:** Riferimenti ad una eventuale marca temporale detached associata al documento.
    - **AdditionalMetaData:** Metadati aggiuntivi richiesti dalle linee guida AgID.
- **MoreInfo**
    - **EmbeddedMetadata**
        - **MoreInfoFileGroup (1):** Definizione della Tipologia documentale a cui appartiene il documento.
            - **Tipologia (1)**
                - **IdTipologia (1)**: Id della Tipologia documentale a cui appartiene il documento.
                - **Indici (1)**
                    - **Indice (1-n)**
                        - **Numero**: Numero indice. Posizione del campo indice (metadato) all'interno della definizione della Tipologia.
                        - **Nome**: Nome del campo indice (metadato)
                        - **Richiesto**: Indica se il valore dell'indice (metadato) è obbligatorio (possibili valori: True, False).

- **RegEx**: Eventuale espressione di validazione per il valore dell'indice (metadato).
- **IndexType**: Tipo di dato del metadato (possibili valori: stringa, intero, data)
- **IndexFormatString**: Formato del tipo di dato.

➢ **Process (1)**

- **Submitter (1):** Informazioni relative al soggetto che effettua il trasferimento fisico degli oggetti digitali nel sistema di conservazione.
  - **AgentID:** Identificativo del soggetto sulla base di uno dei tipi di identificazione predefiniti dalla norma ETSI.
  - **AgentName:** Denominazione del soggetto (NameAndSurname oppure FormalName).
    - **NameAndSurname**
      - **FirstName:** Nome del soggetto.
      - **LastName:** Cognome del soggetto.
    - **FormalName:** Denominazione o ragione sociale del soggetto.
  - **RelevantDocument (1-n):** Riferimento ad un documento del soggetto che interviene nel processo di conservazione, rilevante per la comprensione del processo stesso o degli oggetti digitali sottoposti a conservazione.
  - **MoreInfo**
    - **EmbeddedMetadata**
      - **MoreInfoSubmitter**
        - **CodiceIPA (0-1):** Codice IPA definito nel caso il soggetto sia una Pubblica Amministrazione.
        - **CodiceUOR (0-1):** Codice UOR definito nel caso il soggetto sia una Pubblica Amministrazione.
        - **PartitaIVAPF (0-1):** Partita IVA valorizzata (se presente) nel caso in cui il soggetto sia una persona fisica.

- **Holder (1-n):** Informazioni relative al Titolare dell'oggetto di conservazione (soggetto produttore) o al proprietario, possessore o detentore degli oggetti digitali trasferiti nel sistema di conservazione.
  - **AgentID:** Identificativo del soggetto sulla base di uno dei tipi di identificazione predefiniti dalla norma ETSI.
  - **AgentName:** Denominazione del soggetto (NameAndSurname oppure FormalName).
    - **NameAndSurname**
      - **FirstName:** Nome del soggetto.
      - **LastName:** Cognome del soggetto.
    - **FormalName:** Denominazione o ragione sociale del soggetto.
  - **RelevantDocument (1-n):** Riferimento ad un documento del soggetto che interviene nel processo di conservazione, rilevante per la comprensione del processo stesso o degli oggetti digitali sottoposti a conservazione.
  - **MoreInfo**
    - **EmbeddedMetadata**
      - **MoreInfoHolder**
        - **CodiceIPA (0-1):** Codice IPA definito nel caso il soggetto sia una Pubblica Amministrazione.

        - **CodiceUOR (0-1):** Codice UOR definito nel caso il soggetto sia una Pubblica Amministrazione.
        - **AgentIdSIP (1):**
            - **IdSIP (1-n):** Elenco di Id SIP trasferiti dal soggetto.
        - **PartitaIVAPF (0-1):** Partita IVA valorizzata (se presente) nel caso in cui il soggetto sia una persona fisica.
- **AuthorizedSigner (1-n):** Informazioni relative al soggetto autorizzato ad apporre la firma elettronica (avanzata o qualificata) o il sigillo elettronico (avanzato o qualificato) sull'indice di conservazione, a conclusione del processo di creazione dell'indice.
    - **AgentID:** Identificativo del soggetto sulla base di uno dei tipi di identificazione predefiniti dalla norma ETSI.
    - **AgentName:** Denominazione del soggetto (NameAndSurname oppure FormalName).
        - **NameAndSurname**
            - **FirstName:** Nome del soggetto.
            - **LastName:** Cognome del soggetto.
        - **FormalName:** Denominazione o ragione sociale del soggetto.
    - **RelevantDocument (1-n):** Riferimento ad un documento del soggetto che interviene nel processo di conservazione, rilevante per la comprensione del processo stesso o degli oggetti digitali sottoposti a conservazione.
    - **MoreInfo**
        - **EmbeddedMetadata (1)**
            - **MoreInfoAuthorizedSigner (1):** Informazioni aggiuntive relative al soggetto firmatario designato per la chiusura del processo di Conservazione.
                - **PreservationAgent**
                    - **PreservationJobRole:** Descrizione della mansione riferita al soggetto.
                    - **CertificateIdentificationCode:** Identificativo del certificato di firma utilizzato nella chiusura del processo di Conservazione.
                    - **VATNumberNaturalPerson:** Partita IVA valorizzata (se presente) nel caso in cui il soggetto sia una persona fisica.
                    - **Identifier (0-1):** Identificativo del soggetto assegnato dal Sistema di conservazione in fase di definizione del soggetto.
- **TimeReference (1)**
    - **TimeInfo (1):** Data in cui è stata prodotto il file indice. Corrisponde entro certi limiti temporali (richiesti dal processo di firma e marca del file) alla data di rilascio della marca temporale.
- **LawAndRegulations (1):** Riferimento alla norma di riferimento: *Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.*
- **MoreInfo**
    - **EmbeddedMetadata**
        - **MoreInfoProcess:** Informazioni aggiuntive relative al processo di Conservazione.

- **PreservationAgent (0-n)**
  - **AgentID (0-n):** Identificativo del soggetto sulla base di uno dei tipi di identificazione predefiniti dalla norma ETSI.
  - **AgentName (1):** Denominazione del soggetto (NameAndSurname oppure FormalName).
    - **NameAndSurname**
      - **FirstName:** Nome del soggetto.
      - **LastName:** Cognome del soggetto.
    - **FormalName:** Denominazione o ragione sociale
  - **PreservationJobRole (1):** Descrizione della mansione riferita al soggetto.
  - **Identifier (0-1):** Identificativo del soggetto assegnato dal Sistema di conservazione in fase di definizione del soggetto.

*Il numero indicato tra parentesi precisa il numero di ricorrenze che l'elemento può assumere all'interno dell'Indice: ad es. "(1)" specifica che l'elemento può ricorrere una sola volta; "(1-n)" specifica che può ricorrere 1 o più volte.

Torna al Sommario

6.5 Dissemination Information Package

Il Dissemination Information Package (DIP) è generato dal sistema di conservazione a garanzia dell'interoperabilità e trasferibilità ad altri conservatori in conformità alla normativa e agli standard e può essere richiesto dall'utente nelle seguenti modalità:

- **DIP distribuito a seguito di ricerca di un singolo documento**, in risposta alla richiesta dell'Utente;
- **DIP distribuito a seguito di ricerca di più documenti**, anche appartenenti a più AIP, in risposta alla richiesta dell'Utente. Il pacchetto contiene tutti i file richiesti e i relativi file indici degli AIP di tutti i pacchetti;
- **DIP distribuito in risposta alla richiesta di cessazione del servizio**, in tal caso il DIP contiene uno o più AIP, suddivisi per tipologia documentale e anno di riferimento dei documenti.

In tutte le modalità, il DIP è costituito da un archivio zip che contiene i seguenti elementi:

- I documenti (oggetti digitali conservati nel sistema) richiesti dall'Utente.
- L'Indice del SIP relativo ai documenti.
- Uno o più files Indice del AIP firmati dal Responsabile del Servizio di Conservazione e marcati temporalmente, associati ai suddetti documenti richiesti dall'Utente.
- File Indice del DIP: file XML firmato digitalmente dal Responsabile del Servizio di Conservazione, che contiene l'hash dell'Indice del AIP e l'hash di ogni singolo file (documento richiesto o presente all'interno di un pacchetto richiesto).

L'Indice del DIP contiene al suo interno:

- **Id del DIP**, generato in seguito al salvataggio su Data Base;
- **Data della generazione del DIP** (in formato UTC);
- **Soggetto produttore (Titolare dell'oggetto)** a cui si riferisce il DIP (Rag. Sociale, Id setup, Id azienda, Cod. Fiscale, Partita IVA);
- **Id del SIP** relativo ai documenti versati;
- **Utente** che ha richiesto il DIP (Nome, Cognome, Codice Fiscale e/o Partita IVA);
- **Responsabile del Servizio di conservazione** (Nome e cognome, Cod. Fiscale e/o Partita IVA);
- **Operatore** (Nome e cognome/Ragione sociale, Cod. Fiscale e/o Partita IVA del Delegato alla Conservazione);
- **Responsabile della Conservazione** (Nome e cognome, Cod. Fiscale e/o Partita IVA);
- **Indirizzo IP** da cui è arrivata la richiesta di generazione;
- **AIP consegnati** (Id AIP, Hash, Funzione di hash utilizzata, Url file nel Sistema di conservazione e nel DIP)
- **Lista dei file richiesti** (Id documento, Nome file, Anno di riferimento, Hash file, Funzione di hash utilizzata, Url file nel Sistema di conservazione e nel DIP).

Di seguito viene riportata la struttura dati del DIP:

- **DescGenerale**: Informazioni del richiedente, del Responsabile della conservazione e del Sistema di conservazione.
  - **ID**: Id del DIP assegnato dal Sistema di Conservazione.
  - **IdSetup**: Codice Cliente associato al Titolare dell'oggetto di conservazione (soggetto produttore).
  - **IdAzienda**: Id dell'azienda di riferimento nel sistema documentale.
  - **SoggettoProduttore**
    - **Denominazione:** Denominazione del soggetto produttore (Titolare dell'oggetto).
    - **CodFiscale:** Codice fiscale del soggetto produttore (Titolare dell'oggetto).
    - **PartitaIVA:** Partita IVA del soggetto produttore (Titolare dell'oggetto).
    - **CodiceIPA:** Codice IPA del soggetto produttore (nel caso di Pubblica Amministrazione).
    - **PersonaFisica:** Indica se il soggetto produttore (Titolare dell'oggetto) è una persona fisica (true, false).
  - **Produttori:** Elenco dei soggetti che hanno effettuato il trasferimento fisico degli oggetti digitali nel Sistema di Conservazione.
    - **Produttore:** soggetto che effettua il trasferimento fisico degli oggetti digitali nel Sistema di Conservazione.
      - **Denominazione:** Denominazione del Produttore.
      - **CodFiscale:** Codice fiscale del Produttore.
      - **PartitaIVA:** Partita IVA del Produttore.

- **CodiceIPA:** Codice IPA del Produttore (nel caso di Pubblica Amministrazione).
- **PersonaFisica:** Indica se il Produttore è una persona fisica (true, false).
- **Indice SIP_Versati**
  - **IdSIP:** Id del SIP versato nel Sistema di Conservazione.

- **DataGenerazione**: La data in formato UTC riferita alla produzione del DIP.
- **IpAdressClient:** Indirizzo IP da cui è arrivata la richiesta di estrazione del DIP
- **Richiedente**: Dati anagrafici del richiedente del DIP.
  - **Nome**: Nome del richiedente.
  - **Cognome**: Cognome del richiedente.
  - **CodiceFiscale**: Codice fiscale del richiedente.
  - **PartIVA**: Partita IVA del richiedente.
- **SoggettiProcesso**, Dati anagrafici dei soggetti Responsabile della conservazione, Operatore conservatore e Responsabile del servizio di conservazione.
  - **PM**: Dati anagrafici del responsabile della conservazione (nome e cognome o ragione sociale, ruolo, codice fiscale o Partita IVA).
  - **Operatore**: Dati anagrafici dell'operatore conservatore (nome e cognome o ragione sociale, ruolo, codice fiscale o Partita IVA).
  - **PSM**: Dati anagrafici del Responsabile del servizio di conservazione (nome e cognome o ragione sociale, ruolo, codice fiscale o Partita IVA).
- **AntiVirus:** Denominazione Software Antivirus e data/ora ultimo aggiornamento.
- **LTA**: Indicazioni anagrafiche del Sistema di conservazione.
  - **Nome**: Denominazione del Sistema di conservazione.
  - **Versione**: Versione del Sistema di conservazione.

- **AIPGruppo**: Descrizione del AIP estratto.
  - **AIP**: Descrizione dell'Archival Information Package.
    - **Id**: Id del Archival Information Package (identificativo univoco assegnato dal Sistema di Conservazione).
    - **FunzioneHash**: Tipo di funzione di hash usata per calcolare il valore.
    - **Hash**: Valore ricavato applicando la funzione di hash al file associato all'indice del AIP.
    - **UrlFile:** URI del file nel pacchetto.
    - **NumFileInfetti:** Eventuale numero file infetti contenuti nel DIP.
    - **FileGruppo**: Elenco dei file estratti.
      - **File**
        - **Id**: Id del documento assegnato dal Sistema di Conservazione
        - **IdDoc**: Id del documento nel sistema documentale o altro sistema
        - **IdTipologia:** Id della tipologia di riferimento all'interno del sistema di conservazione
        - **Tipologia:** Denominazione della tipologia documentale di riferimento.
        - **IdSIP:** Id del SIP in cui è contenuto il documento.
        - **PathFile**: Nome del file associato al documento.

- **TipoFile:** Tipologia di file (a seconda dell'origine del SIP).
- **AnnoRiferimentoDoc**: Anno di riferimento dell'oggetto conservato.
- **FunzioneHash**: Tipo di funzione di hash usata per calcolare il valore.
- **Hash**: Valore ricavato applicando la funzione di hash al file associato al documento.
- **UrlFile:** URI del file nel DIP.
- **RevisionIdSIP**: Id del SIP revisionato (può corrispondere con il SIP di origine oppure con l'ultima revisione pubblicata per il SIP di origine). Il nodo è presente solo se il SIP rappresenta una revisione.
- **RevisionIdSIPOrigin**: Id del SIP di origine (SIP iniziale da cui hanno origine tutte le revisioni). Il nodo è presente solo se il SIP rappresenta una revisione.
- **RevisionNumber**: Numero della revisione necessario per ordinare la sequenza delle revisioni relative al SIP di origine. Il nodo è presente solo se il SIP rappresenta una revisione.
  RevisionIsLast: Identifica l'ultima versione del file all'interno di una sequenza di revisioni (true or false).

Torna al Sommario

7 IL PROCESSO DI CONSERVAZIONE

Il processo di conservazione implementato dal sistema di conservazione è governato in tutte le sue fasi dall'**entità di Amministrazione del sistema,** che interagisce con le altre entità del Sistema, con il Titolare dell'oggetto di conservazione, con il Produttore dei SIP e con gli Utenti o Gruppi di Utenti (le Comunità di riferimento definite dallo standard OAIS).

Il Responsabile della conservazione, sotto la propria responsabilità, delega il Conservatore, quale prestatore del servizio, affidando le attività previste dal relativo contratto al Conservatore stesso, che attraverso il suo Responsabile del servizio di conservazione, svolgerà le opportune attività.

Di seguito viene rappresentato il processo di conservazione in conformità alla normativa in materia di formazione, gestione e conservazione dei documenti informatici.

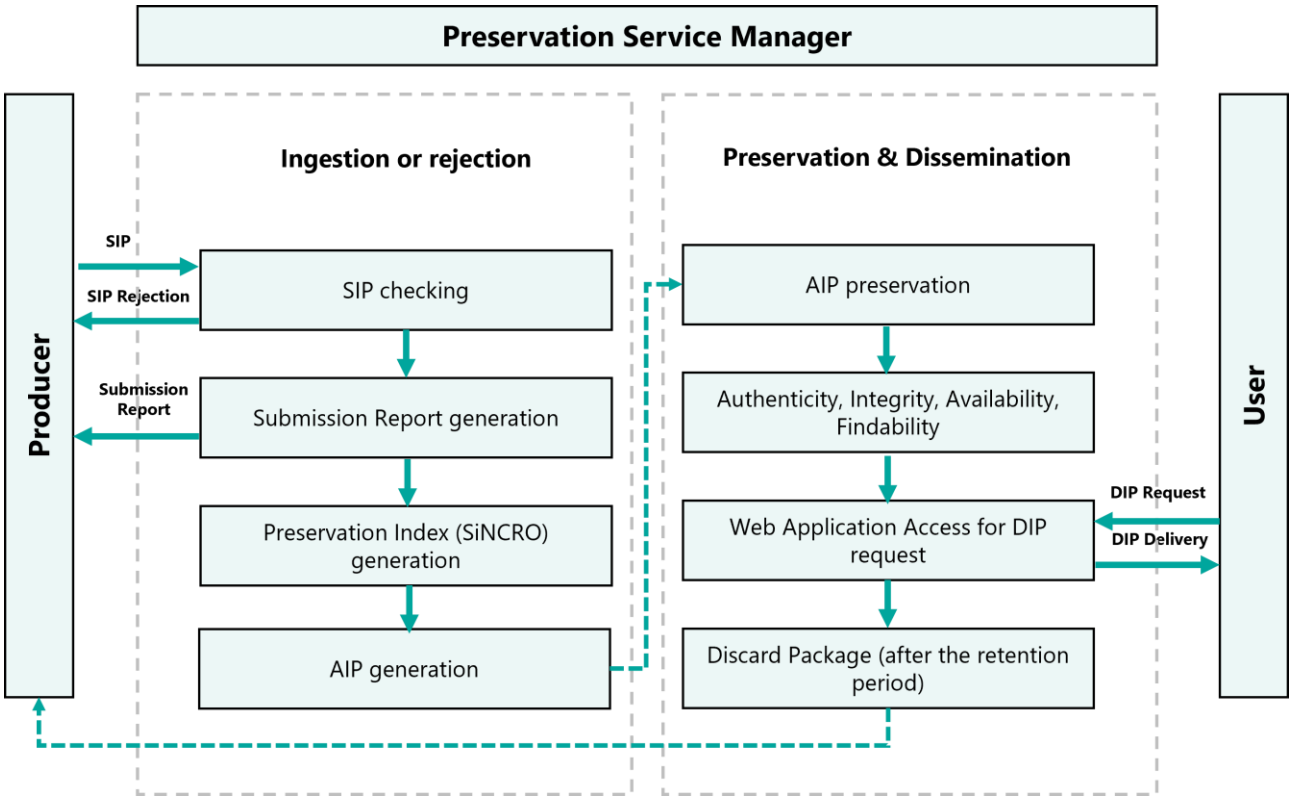


Figura 11 Processo di conservazione

7.1 Modalità di acquisizione dei Submission Information Package per la loro presa in carico

Il sistema prevede le seguenti modalità di trasmissione dei SIP da parte del Produttore al Conservatore:

1. Tramite Web Services (processo sincrono)
    a. utilizzando i servizi web-services e dunque integrando la piattaforma tramite gli opportuni SDK.
    b. attraverso pagina web, mediante il caricamento manuale dei singoli documenti e l'inserimento dei metadati di conservazione;
2. Tramite sFTP e successivo caricamento all'interno del sistema (processo asincrono)

La presa in carico del SIP può avvenire in due modalità:

- Sincrona
    - Trasferimento via web services
    - Check effettuati per il SIP in fase di presa in carico
    - Risposta web services (esito presa in carico).
- Asincrona
    - Trasferimento SIP nella cartella dedicata SFTP
    - Presa in carico da Job Schedulato
    - Inserimento nel Sistema di conservazione
    - Check effettuati per il SIP in fase di presa in carico
    - Creazione del file "Esito di presa in carico".

Entrambe le modalità di versamento garantiscono la sicurezza e riservatezza dei dati trasmessi grazie alla crittografia del canale adottato (HTTPS o sFTP). Il canale HTTPS integra sul protocollo base HTTP la crittografia di tipo Transport Layer Security (SSL/TLS), questa tecnica aumenta il livello di protezione contro gli attacchi.
Il certificato digitale utilizzato per la connessione HTTPS è fornito e garantito da GeoTrust.
Il protocollo sFTP prevede il trasferimento dei dati usando il protocollo SSH-2, che garantisce la cifratura delle informazioni trasmesse.

Le specifiche e il modello-dati adottati per il SIP sono i medesimi e la presa in carico per entrambe le modalità si conclude con il rilascio di:

- un identificativo **Id (GUID) assegnato al SIP** in caso di caricamento con esito positivo in modo da identificarlo in maniera univoca nel Sistema di conservazione in tutto il ciclo di vita del servizio;
- una Eccezione, se si sono verificati degli errori durante il caricamento.

In particolare, nella modalità sFTP l'esito restituito dalla presa in carico è un file testuale che viene depositato in una cartella di output definita e concordata tra Produttore e Conservatore.

I sistemi del Conservatore Namirial per la presa in carico dei SIP sono tutti in alta disponibilità garantendo la ridondanza dei dati.

Inoltre, nel servizio di conservazione sono attive procedure per la generazione di backup dei SIP versati dal Produttore. Le politiche di salvataggio e backup possono essere definite a livello di classe documentale, tale impostazione consente di specificare quanto tempo la copia di sicurezza del SIP debba essere mantenuta nello storage dedicato ai SIP.

Lo storage che mantiene le copie di backup è costituito da tre repliche, due sul sito primario e una sul sito DR, questa architettura garantisce l'alta affidabilità e il recupero a seguito di un disastro.

Tutti le attività di presa in carico dei singoli SIP vengono tracciate tramite il sistema di Log Management integrato nel sistema di conservazione. I log vengono mantenuti per tutto il periodo di conservazione degli oggetti versati.

Pertanto, in caso di necessità di un recupero dei dati dei SIP ancora non trasformati in AIP dal sistema, il recupero in accordo con il Titolare dell'oggetto potrà essere attivato attraverso un ticket di richiesta all'area di Assistenza. La richiesta smistata all'area tecnico-operativa di Namirial permette di attivare il *restore* delle copie dei SIP mantenute nell'area di storage dedicata, al fine di ricreare il processo di acquisizione dei SIP e quindi dare il via ad un nuovo processo di presa in carico.

Torna al Sommario

7.2 Verifiche effettuate sui Submission Information Package e sugli oggetti in essi contenuti

Nel processo di presa in carico dei SIP nel Sistema di conservazione, il servizio effettua una serie di controlli di coerenza su ciascun SIP e sugli oggetti in esso contenuti e genera un **esito di presa in carico**.

- **(Bloccante)** Verifica che il Submission Information Package contenga l'Indice del SIP ed i files.
- **(Bloccante)** Controllo validità del file Indice del SIP con il file XSD.
- **(Bloccante)** Controllo che l'azienda definita nell'Indice del SIP sia presente nel Sistema di Conservazione e che per questa azienda, nel sistema di conservazione sia impostato un soggetto per la firma dei Submission Report e degli AIP.
- **(Bloccante)** Controllo che il numero di files presenti nel SIP corrisponda al numero di files definiti nell'Indice del SIP, se *DistintaMeccanografica* NON valorizzato oppure impostato a False. Se invece il campo *DistintaMeccanografica* è valorizzato a True allora il numero di files presenti nel pacchetto deve coincidere con il numero di documenti che si riferiscono a nomi di files distinti. Il sistema controlla che tutti i documenti indicizzati all'interno dell'Indice del SIP, abbiano una corrispondenza con i files contenuti nel pacchetto.
- **(Bloccante)** Controllo che i nomi dei files presenti nel SIP corrispondano ai files definiti nell'Indice del SIP.
- **(Bloccante)** Controllo che il tipo MIME (MimeType) dei files definito nell' Indice del SIP sia stato specificato.

- **(Bloccante)** Controllo che i nomi delle marche temporali detached (DetachedTimeStamp) corrispondano ai files (.tsr) presenti nella cartella in cui ci sono anche i files oggetto della Conservazione.
- **(Bloccante)** Controllo che i percorsi degli allegati importati da altro Conservatore presenti nel SIP (all'interno della cartella riservata DIPPre) corrispondano agli allegati definiti nell' Indice del SIP (DIPPre).
- **(Bloccante)** Verifica che i formati dei files contenuti nel Submission Information Package siano nei formati previsti.
- **(Bloccante)** Verifica della presenza di files nell' Indice del SIP con Id documento NON specificato.
- **(Bloccante)** Verifica dei riferimenti della revisione e delle modifiche apportate dalla revisione per verificare la loro approvazione (solo per pacchetti di revisione).
- **(Bloccante)** Verifica della presenza di files nell' Indice del SIP con lo stesso Id documento.
- **(Bloccante)** Se l'Indice del SIP è firmato il sistema verifica che la firma sia valida, se non è firmato NON lo verifica.

Per ogni documento definito nell'Indice del SIP si effettuano i seguenti controlli:

- **(Bloccante)** Verifica che la tipologia definita per il documento corrisponda a quella definita per l'Indice del SIP (sezione SourceVdA).
- **(Bloccante)** Verifica che il numero di Metadati definiti per il documento corrisponda a quelli definiti all'interno della tipologia (definita nell' Indice del SIP nella sezione SourceVdA).
- **(Bloccante)** Verifica che il nome e l'ordine dei Metadati definiti per il documento corrisponda a quanto definito all'interno della tipologia (definita nell' Indice del SIP nella sezione SourceVdA).
- **(Bloccante)** Verifica della presenza del valore per i Metadati obbligatori, seguendo lo schema dei metadati (inserito nel SIP nella sezione SourceVdA).
- **(Bloccante)** Validazione del valore per i Metadati in base all'eventuale espressione regolare definita, seguendo lo schema dei metadati (inserito nel SIP nella sezione SourceVdA).
- **(Bloccante)** Verifica che non ci siano documenti con lo stesso Id documento all'interno del Sistema di Conservazione, per la tipologia documentale associata all'azienda
- **(Bloccante)** Se l'Indice del SIP ha versione inferiore a 1.0.5 allora verifica che il nome file rispetti lo standard xs:anyURI
- **(Bloccante)** Verifica degli Hash dei files con il valore inserito nel SIP.
- **(Bloccante)** Verifica che l'Hash dei files non corrisponda al Hash del file da 0 byte
- **(Bloccante)** Verifica degli Hash degli allegati importati da altro Conservatore con il valore inserito all'interno della sezione DIPPre (non viene effettuato dal metodo checkIndiceSIP).
- **(Bloccante)** Verifica della validità della firma sul file. Opzionale il controllo della verifica sui file firmati (non viene effettuato dal metodo checkIndiceSIP).

- **(Bloccante)** Verifica dell'anno di riferimento documento: deve essere lo stesso per tutti i documenti (definito dell'Indice del SIP nella sezione FileGroup/File/MoreInfo/MetaData/ReferenceDocYear).
- **(Bloccante)** Verifica della valorizzazione dei metadati aggiuntivi tramite i tag definiti per il documento (definiti nell'Indice del SIP nella sezione: FileGroup/File/MoreInfo/TagPIndex)

Se le verifiche di coerenza eseguite nella fase di presa in carico sono positive il SIP viene acquisito dal Sistema di conservazione, altrimenti l'esito evidenzia il rifiuto definitivo.

Nella fase di verifica di coerenza del SIP, i risultati dei controlli vengono registrati nel Log Management System con annesso time stamp (riferimento temporale).

Torna al Sommario

7.3 Accettazione dei Submission Information Package e generazione del Submission Report

In caso di presa in carico, il Sistema genera il Submission Report, quale esito di tutte le verifiche effettuate sul SIP a partire dalla sua ricezione. Il Submission Report ha lo scopo di formalizzare l'acquisizione degli oggetti da conservare. Tale rapporto contiene il riferimento ad uno o più SIP.

La generazione del Submission Report avviene tramite la schedulazione di un job all'interno dello schedulatore integrato nel Sistema di conservazione secondo le tempistiche configurate.

Per ogni Titolare dell'oggetto possono essere generati uno o più Submission Report per ogni schedulazione, in quanto:

- ogni Submission Report si riferisce ad una sola tipologia documentale;
- per ogni Titolare è possibile definire il numero massimo di SIP da includere all'interno di un Submission Report.

Il Submission Report è generato in formato XML e riporta le seguenti informazioni:

- Indicazioni della versione del Sistema di conservazione;
- Indicazioni del Titolare dell'oggetto (Soggetto produttore) in riferimento al Sistema di conservazione;
- Riferimenti dell'Utente che ha trasmesso il SIP;
- Data di generazione del Submission Report;
- Dati del Responsabile della conservazione associato al Titolare dell'oggetto;
- Dati del delegato Conservatore;
- Dati del Responsabile del servizio di conservazione;
- Numero di SIP inclusi nel Submission Report;
- Numero totale dei files contenuti nei SIP inclusi all'interno del Submission Report

- Informazioni sul tipo di SIP valorizzato (primo versamento, riversamento da altro sistema o revisione)
- Informazioni sull'eventuale versione della revisione o SIP di origine
- La funzione di Hash con cui è stato generato l'hash dell'Indice del SIP;
- Hash del/i Indice del SIP considerato/i nel Submission Report;
- L'indirizzo IP della macchina dove è stato generato il SIP
- La lista dei messaggi del Responsabile della conservazione o del suo Delegato contenuti nel/nei pacchetto/i di versamento collegato/i al file;
- L'esito dei check una volta ricevuto il SIP da parte del Sistema di conservazione.

Di seguito è riportata la struttura del Submission Report:

DescGenerale
- **IdSetup**, il codice cliente Soggetto produttore.
- **IdAzienda**, L'identificativo univoco assegnato al Titolare/Soggetto produttore
- **RagSociale**, La ragione sociale/denominazione del Soggetto produttore.
- **CodFiscale**, Il codice fiscale del Soggetto produttore.
- **PartitaIVA**, La partita iva del Soggetto produttore rappresentata con il Codice Paese e il numero di partita iva separato da ":" es. IT:04030410288.
- **IdTipologia**, Il codice della tipologia/classe documentale riferita al SIP considerato.
- **Tipologia**, Descrizione della tipologia documentale riferita al SIP considerato.
- **DataGenerazione**, La data di generazione del SubmissionReport in formato UTC.
- **PM**, Dati del Responsabile della conservazione.
    - **Nome e Cognome,** la denominazione del Responsabile della conservazione.
    - **CodFiscale**, Codice Fiscale del Responsabile della conservazione.
    - **PartIVA**, Partita Iva del Responsabile della conservazione.
- **Operatore**, Dati del Delegato alla conservazione.
    - **Nome e Cognome/Ragione sociale,** la denominazione del Delegato alla conservazione.
    - **CodFiscale**, Codice Fiscale del Delegato alla conservazione.
    - **PartIVA**, Partita Iva del Delegato alla conservazione.
- **PSM**, Dati del Responsabile del Servizio di conservazione.
    - **Nome e Cognome,** la denominazione del Responsabile del Servizio di conservazione.
    - **CodFiscale**, Codice Fiscale del Responsabile del Servizio di conservazione.
    - **PartIVA**, Partita Iva del Responsabile del Servizio di conservazione.
- **LTA**, Indicazioni del Sistema di conservazione che ha creato il SubmissionReport
    - **Nome**, Nome commerciale del Sistema di conservazione.
    - **Versione**, Versione del sistema di conservazione.

SIPGruppo (1-n), Costituisce il gruppo di SIP considerati dal SubmissionReport.
- **SIP**
- **Id**, Id del SIP incluso nel Rapporto.
- **RevisionIdSIP**, Id del SIP revisionato. (Può essere il SIP di origine oppure l'ultima revisione pubblicata per il SIP di origine). Il nodo è presente solo se il SIP rappresenta una revisione.
- **RevisionIdSIPOrigin**, Id del SIP di origine (SIP iniziale da cui hanno origine tutte le revisioni). Il nodo è presente solo se il SIP rappresenta una revisione.
- **RevisionNumber**, Numero della revisione necessario per ordinare la sequenza delle revisioni relative al SIP di origine. Il nodo è presente solo se il SIP rappresenta una revisione.

- **RevisionSource**, Definire la provenienza del pacchetto di Revisione. Valori ammessi: RequestProducer, Internal. Il nodo è presente solo se il SIP rappresenta una revisione.
- **Utente**, Dati dell'utente Produttore che versato il SIP.
    - **Nome,** Nome del Produttore.
    - **Cognome,** Cognome del Produttore.
    - **CodFiscale,** Codice Fiscale del Produttore.
    - **PartIVA,** Partita Iva del produttore.
- **NumFiles**, Numero di File inclusi nel Submission Information Package.
- **IpProduttore**, Ip del server/pc dove è stato formato il SIP.
- **Tipo**, Tipologia file a seconda dell'orgine del SIP.
- **AttachmentsDIPImportCounter**
- **Hash** Descrizione della funzione di hash adottata per la generazione dell'impronta informatica.
    - **Tipo,** Tipo di algoritmo (ad es. SHA256).
    - **Valore,** Il valore di HASH del Indice SIP ottenuto in fase di presa in carico.
- **FormatoData**, Descrizione del formato della data es. yyyy-MM-ddTHH:mm:ssK
- **Annullato**, Indica se il Submission Information Package è stato annullato.
- **PMMessageGroup**, In questa sezione vengono raccolti tutti i messaggi del Responsabile della conservazione inseriti sui SIP, oppure derivati dal registro anomalie.
- **FileGroup** (1-n), Il gruppo dei file inclusi nel SIP.
    - **IdDoc,** Id Documento nel sistema documentale.
    - **PathFile,** Nome file oggetto da conservare.
    - **AnnoRiferimentoDoc,** L'anno a cui si riferisce l'oggetto da conservare.
    - **PMMessageGroup,** Messaggi del Responsabile della conservazione riferiti al file considerato.
- **CheckGroup** (1-n)
    - **Descrizione,** Descrizione del tipo di Check effettuato e la descrizione dell'esito.
    - **Esito,** può essere OK o KO.
    - **Data,** La data di esecuzione del check.

Inoltre, il Submission Report contiene il Tag "<DataGenerazione>" quale riferimento temporale in formato UTC (Tempo Universale Coordinato) ed è firmato digitalmente dal Responsabile del servizio di conservazione.
Per quanto riguarda i riferimenti temporali si evidenzia che l'orologio di sistema di tutti gli elaboratori impiegati nel servizio è sincronizzato con il protocollo NTP Time.nist.gov.

Il Conservatore Namirial consente al Produttore di avere a disposizione i Submission Report con le seguenti modalità:

- **attraverso comunicazione via PEC o mail ordinaria**, secondo l'indirizzo di posta elettronica configurato nell'anagrafica del Titolare dell'oggetto di conservazione a sistema (servizio configurato su richiesta del Cliente e concordato a livello contrattuale). L'email viene formattata in modo automatico dal Sistema e in allegato viene inserito il Submission Report firmato dal responsabile del servizio di conservazione e il file non firmato (per una più agevole elaborazione del file da parte di un eventuale sistema di terze parti). Viene inoltre fornito un file XSLT per la visualizzazione agevole tramite browser;
- **tramite chiamata al web service** del Sistema di conservazione;
- **tramite accesso alla piattaforma web** del Sistema di conservazione da parte di un Utente autorizzato

Tutti i Submission Report generati, rimangono sempre a disposizione per la consultazione ed esibizione.

Torna al Sommario

7.4 Rifiuto dei Submission Information Package e modalità di comunicazione delle anomalie

Durante le verifiche di coerenza possono essere riscontrate le seguenti anomalie che generano il rifiuto dei SIP:

- SIP non contiene l'Indice del SIP e i documenti;
- File Indice del SIP non valido rispetto allo schema XSD;
- Identificazione del Soggetto produttore e non corrispondenza con quanto configurato nel Sistema di conservazione; assenza di un Responsabile del Servizio di Conservazione nel Sistema di conservazione per il Soggetto produttore dei documenti a cui il SIP si riferisce;
- nel Sistema di conservazione non è configurato il Responsabile della conservazione per il Soggetto produttore a cui il SIP si riferisce;
- Numero di files presenti nel SIP non corrispondente al numero di files dichiarati nell'Indice del SIP;
- Nomi dei files presenti nel SIP non corrispondenti ai nomi files definiti nell'Indice del SIP;
- Esito negativo della verifica del tipo MIME dichiarato nell'Indice del SIP (MimeType tra quelli ammessi per la conservazione dei files);
- Esito negativo della verifica dei formati dichiarati nell'Indice del SIP (formati tra quelli ammessi per la conservazione dei files);
- Presenza di files nell'Indice del SIP con Id documento non specificato;
- Presenza di files nell'Indice del SIP con lo stesso Id documento;
- Esito negativo della verifica di validità della firma digitale (solo se l'Indice del SIP è firmato);
- Esito negativo della verifica di corrispondenza tra la tipologia documentale configurata nel Sistema di conservazione e quella dichiarata nell'Indice del SIP (campo: SourceVdA);
- Esito negativo della verifica di corrispondenza tra i metadati configurati nel Sistema di conservazione per una specifica tipologia documentale e i metadati dichiarati nel'Indice del SIP (campo: SourceVdA);
- Esito negativo della verifica di corrispondenza tra il nome e l'ordine dei metadati configurati nel Sistema di conservazione per una specifica tipologia documentale e quelli dichiarati nell'Indice del SIP (campo: SourceVdA);
- Esito negativo della verifica della presenza dei metadati dichiarati come obbligatori nell'Indice del SIP (campo: SourceVdA);
- Esito negativo della verifica dell'eventuale espressione regolare dei metadati dichiarati nell'Indice del SIP (campo: SourceVdA);

- Esito negativo della verifica che non ci siano documenti con lo stesso Id documento, all'interno del Sistema di conservazione, per la medesima tipologia documentale associata ad un determinato Soggetto produttore;
- Esito negativo della verifica di corrispondenza tra gli hash (impronte) dei documenti calcolati dal Conservatore e l'hash dichiarato nell' Indice del SIP dal Produttore;
- Esito negativo della verifica di validità della firma sul singolo documento. Il controllo della verifica sui documenti firmati è opzionale e attivabile solo sui documenti firmati.

Si evidenzia che nel Sistema di conservazione è prevista una procedura per permettere al Conservatore di annullare dei SIP già acquisiti solo se non fanno parte di un processo di conservazione già completato (SIP già incluso in un AIP firmato e marcato).

La generazione e la consegna degli esiti di presa in carico sono tutte azioni registrate nel Log management System del Sistema di conservazione con un riferimento temporale.

Torna al Sommario

7.5 Preparazione e gestione dell'Archival Information Package

La generazione dell'Indice del AIP avviene secondo le specifiche della normativa in materia di formazione, gestione e conservazione dei documenti informatici e secondo il modello-dati definito dallo standard SInCRO (UNI 11386).

La generazione dell'Indice del AIP corrisponde alla chiusura definitiva del processo di conservazione a norma. Questa procedura avviene tramite la schedulazione di un job all'interno dello schedulatore integrato nel Sistema di conservazione secondo le tempistiche configurate per il Titolare dell'oggetto. Tali regole consentono di includere uno o più SIP in un AIP. La natura del AIP è descritta nell'apposito paragrafo.

Su ciascun Indice del AIP sono apposti la firma del Responsabile del Servizio e la marca temporale rendendo immodificabili i SIP inclusi nel AIP per tutta la durata della conservazione degli oggetti digitali.

La firma e la marca temporale sono emessi da Namirial in qualità, rispettivamente, di Certification Authority (CA) e di Time Stamping Authority.

Il sistema, anche nel caso della generazione dei AIP, registra i log per la tracciatura delle azioni effettuate sugli AIP.

La procedura di ripristino in caso di corruzione o perdita dei dati dei AIP prevede la gestione dell'incident con livello di priorità massima e il ripristino attraverso l'utilizzo del AIP copia di backup.

Torna al Sommario

7.6 Cifratura degli oggetti di conservazione

Gli oggetti informatici vengono crittografati con crittografia lato server e chiavi gestite da Amazon S3 (SSE-S3), servizio fornito da Amazon AWS, in qualità di datacenter Namirial (al paragrafo relativo alle componenti fisiche sono indicate eventuali variazioni sulla base delle singole Region).

Quando si utilizza la crittografia lato server, Amazon S3 esegue la crittografia di un oggetto prima di salvarlo su disco nei suoi data center e lo decripta al momento della richiesta da parte del Cliente.

La crittografia lato server protegge i dati at rest. Amazon S3 cifra ogni oggetto con una chiave univoca. Come ulteriore protezione, cifra la chiave stessa con una chiave master che ruota regolarmente. La crittografia lato server di Amazon S3 utilizza una delle crittografie a blocchi più potenti disponibili per cifrare i dati, ossia Advanced Encryption Standard a 256 bit (AES-256).

Torna al Sommario

7.7 Gestione di documenti contenenti dati sensibili

In caso di oggetti informatici contenenti dati sensibili che, in accordo alla normativa, necessitano di un particolare trattamento, il servizio implementa delle misure di sicurezza ulteriori.

In particolare, la soluzione prevede l'utilizzo di componenti di crittografia di livello avanzato, insieme a politiche di controllo degli accessi e alla verifica dell'identità dell'utente, come indicato di seguito.

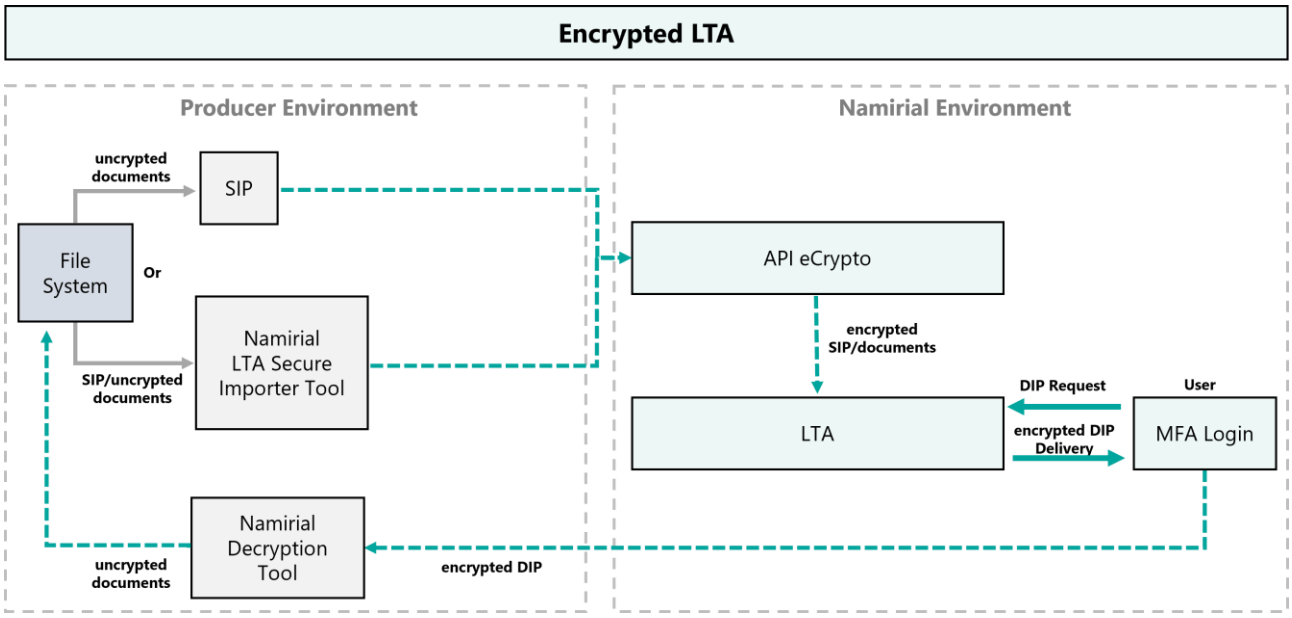


Figura 12 Fasi del processo di gestione di documenti contenenti dati sensibili

Il processo consiste a) nella generazione dei SIP da parte del Produttore o - in alternativa - b) nel deposito di SIP già formati o di documenti corredati di metadati nel tool dedicato e installato nel proprio server. Tramite integrazione web service da parte del Produttore (API dedicate eCrypto e LTA) o via tool con apposita schedulazione, i dati vengono inviati per mezzo di un tunnel criptato. I SIP vengono criptati e inviati al Sistema di Conservazione con il processo descritto nel paragrafo relativo alla gestione dell'Archival Information Package.

L'accesso al portale web per la consultazione dei documenti è protetto da un'autenticazione a due fattori; per la consultazione di uno specifico documento criptato è necessario effettuare il download dello stesso. Il file

scaricato può essere visualizzato attraverso l'utilizzo di uno specifico componente che consente di decriptare i file. Ogni operazione di accesso e richiesta dei documenti è tracciata tramite log.

Torna al Sommario

7.8 Preparazione e gestione del Dissemination Information Package ai fini dell'esibizione

L'Utente può richiedere un DIP durante l'esercizio del servizio o in caso di disattivazione ai fini della migrazione verso un altro sistema.

Alla richiesta del DIP il sistema restituisce tramite canale crittografato (su protocollo HTTPS) il pacchetto in formato di cartella compressa .zip costituito dagli oggetti digitali previsti dalla richiesta di distribuzione. Le tipologie di DIP e i modelli-dati sono descritti nell'apposito paragrafo del presente manuale.

L'Utente può richiedere la generazione di più DIP e ogni azione di richiesta e messa a disposizione del DIP viene tracciata con un identificativo univoco all'interno del sistema di Log Management System con la registrazione di un riferimento temporale.

Lo storage che mantiene gli AIP e i DIP è costituito da tre repliche, due sul sito primario e una sul sito DR: questa architettura garantisce l'alta affidabilità e il recupero dei dati a seguito di corruzione o perdita dei dati.

Torna al Sommario

7.9 Accesso al Sistema

L'accesso web tramite interfaccia consente all'utente di:

- ricercare i propri documenti tramite chiavi univoche (metadati di conservazione);
- verificare l'esito positivo del versamento attraverso la fruizione del Submission Report generato dal Sistema;
- consultare i documenti conservati;
- effettuare il download dei duplicati dei documenti informatici conservati, per singolo documento o per range di documenti;
- effettuare il download dei Dissemination Information Package (DIP) ai fini dell'esibizione delle evidenze di conservazione.

L'utente si autentica mediante l'inserimento delle credenziali (username e password) precedentemente comunicategli da Namirial. Al primo accesso l'utente dovrà cambiare la password secondo le disposizioni vigenti in materia di trattamento dei dati. Ogni utente è responsabile del controllo esclusivo della propria password di accesso che non è recuperabile o visibile al personale Namirial in quanto anonimizzata.

Inoltre, per ragioni di sicurezza, il Sistema di conservazione disattiva temporaneamente le utenze di consultazione inattive da oltre sei mesi.

In caso di oggetti informatici contenenti specifici dati sensibili, l'accesso al portale web per la consultazione dei documenti è protetto da un'autenticazione forte (come indicato nel paragrafo "Gestione di documenti contenenti dati sensibili"), che garantisce un più elevato standard di sicurezza. Per consultare uno specifico documento cifrato è necessario effettuare il download dello stesso. Il file scaricato può essere visualizzato attraverso l'apposito componente Namirial che consente di decifrare i file solo ai soggetti autenticati tramite la chiave di decriptazione assegnata.

Tutte le operazioni di autenticazione, ricerca, consultazione e download degli oggetti digitali fin qui indicate sono implementabili tramite integrazione richiamando il web service del sistema di conservazione.

Le attività relative ad accesso, consultazione ed esibizione vengono tracciate tramite il sistema di Log Management integrato nel sistema di conservazione. I log vengono mantenuti per tutto il periodo di validità del contratto.

Torna al Sommario

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

Vi sono casi in cui è necessaria la produzione di una copia informatica con attestazione di conformità da parte di un pubblico ufficiale:

1. per adeguare il formato del documento all'evoluzione tecnologica attivando un processo di riversamento sostitutivo a seguito dei controlli da parte del Responsabile del Servizio di Conservazione;
2. su esplicita richiesta dell'Utente.

Nel primo caso l'ownership dell'attività è in carico al Conservatore e al Responsabile del Servizio di Conservazione che, secondo un piano preventivo di controlli, esegue le verifiche di integrità, di leggibilità e di adeguatezza della rappresentazione informatica dei documenti all'evoluzione tecnologica.

Il processo, completamente tracciato nei Log Management System, richiede la gestione di un riversamento sostitutivo, ossia del processo che trasferisce uno o più documenti conservati modificando la loro rappresentazione informatica e garantendo l'integrità del contenuto.

Nei casi in cui è previsto l'intervento del pubblico ufficiale, la procedura prevede la messa a disposizione dei documenti originali e dei documenti copia al soggetto incaricato, che una volta verificata l'immodificabilità del contenuto, appone la firma digitale su un file denominato "attestazione di conformità".

Questo documento viene posto in conservazione nel sistema come allegato integrativo (collegamento tramite hash tra gli Archival Information Package) assieme al documento copia conforme e poi entrambi conservati. Tutte le evidenze dell'operazione eseguita vengono mantenute nel tempo.

Si evidenzia che la scelta di formati idonei, previsti e consigliati dalla normativa vigente (ad esempio il formato PDF/A) è indicata al fine di minimizzare i rischi legati all'obsolescenza tecnologica.

Torna al Sommario

7.11 Scarto

Superato il periodo di conservazione di pacchetti e documenti concordato tra Conservatore e Titolare, il sistema di conservazione deve implementare la procedura di scarto degli Archival Information Package.

Il sistema notifica (via mail/pec) al Titolare l'avvio della funzione di scarto per determinati AIP, dandone quindi informativa e fornendo le informazioni necessarie al Titolare per valutare l'eventuale richiesta di estensione del periodo di conservazione.

In caso di superamento della scadenza prefissata e in assenza di richiesta di estensione, il job della procedura di scarto si attiva e produce dei Discard Information Package in relazione agli AIP oggetto della procedura. L'operazione è tracciata nel sistema e viene prodotto un file Indice del Discard Information Package firmato digitalmente dal Responsabile del servizio di conservazione, che grazie al file XSLT può essere visualizzato dal Titolare dei documenti o da altri soggetti interessati, per la verifica della corretta procedura eseguita.

In ultimo, nel sistema viene registrato se la gestione della procedura di scarto è relativa ad archivi pubblici o privati che rivestono interesse storico particolarmente importante; in tal caso si attiva un alert e la procedura di scarto dell'Archival Information Package avviene solo previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo, rilasciata al Titolare secondo quanto previsto dalla normativa vigente in materia.

Torna al Sommario

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

La principale struttura-dati a garanzia dell'interoperabilità per il Conservatore Namirial è l'Archival Information Package generato secondo le regole tecniche in materia di Sistema di Conservazione e secondo lo standard SInCRO (UNI 11386).

La sua distribuzione attraverso la richiesta di uno o più DIP tramite diverse modalità (interfaccia web, web service) messe a disposizione dal servizio garantisce la corretta trasferibilità da parte del Titolare dell'oggetto ad altro conservatore.

Nel caso di riconsegna di tutti gli AIP conservati (ad esempio per la chiusura del servizio o per la cessazione anticipata del servizio secondo quanto concordato contrattualmente), il Titolare potrà richiedere al sistema la distribuzione degli stessi, con le modalità concordate tra il Conservatore e il Titolare stesso.

Ogni DIP contiene un Indice del DIP, firmato dal Responsabile del servizio di conservazione, che rappresenta un rapporto della distribuzione eseguita. Il DIP contiene anche il file XSLT per la corretta visualizzazione dell'Indice del DIP.

Il sistema è in grado di acquisire SIP/AIP conformi con la struttura SInCRO (UNI 11386) nel caso di **subentro/migrazione** di archivi gestiti da altro conservatore che abbia adottato tale standard per la generazione dell'Indice del AIP.

Torna al Sommario

8 IL SISTEMA DI CONSERVAZIONE

L'infrastruttura di erogazione del servizio Namirial di conservazione dei documenti informatici è stata concepita, organizzata e sviluppata in modo che le varie fasi di lavoro risultino atomiche e che il flusso sia modulare. I componenti ad alta affidabilità permettono inoltre l'adattamento del sistema in base al carico corrente. Data la natura critica del servizio, i paradigmi IAC (Infrastructure as code), CI/CD (Continuous integration/Continuous deployment) e Business Continuity sono stati seguiti fin dalla fase di progettazione.

Le principali componenti della soluzione possono essere schematizzate dalla seguente rappresentazione grafica.

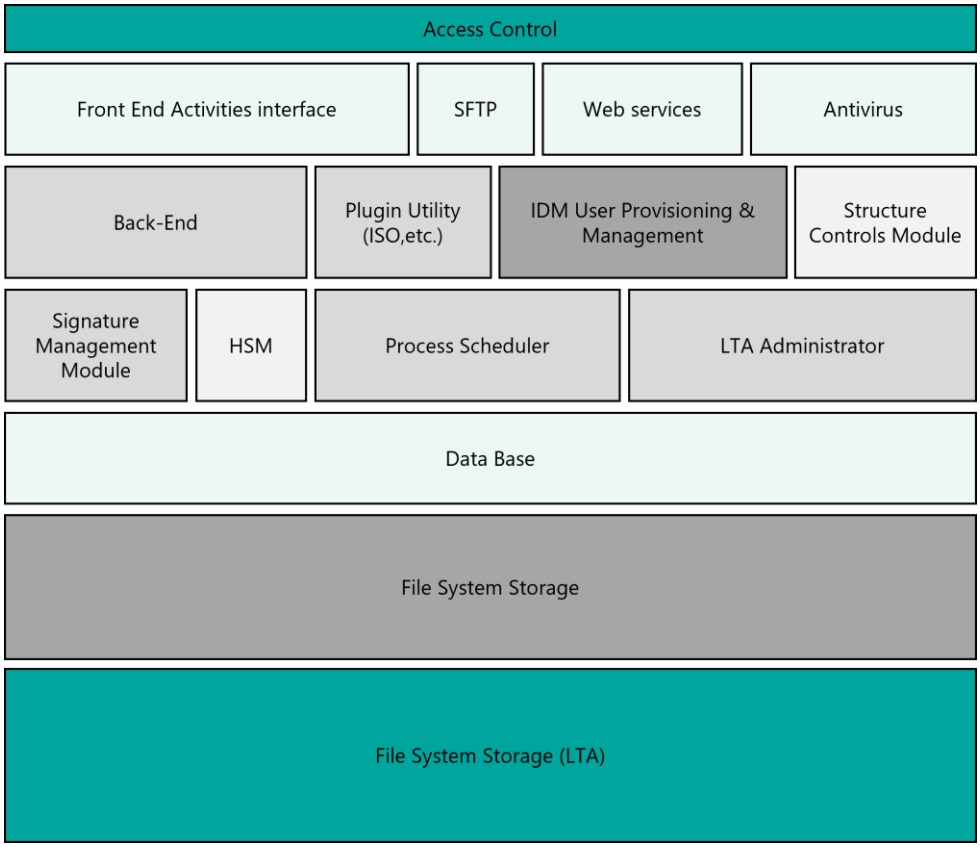


Figura 13 Componenti del Sistema di conservazione

Come rappresentato in figura, la soluzione si sviluppa in moduli organizzati in stack, in cui esiste un nucleo centrale del sistema che si interfaccia con le altre unità logico-funzionali.

Le componenti di soluzione sono:

- Interfaccia delle attività di front-end accessibile agli utenti: versamento manuale di documenti, ricerche, richieste, esibizione, dissemination dei pacchetti, produzione di copie e duplicati e altre attività eseguibili dagli amministratori.
- Modulo Web Service per le attività di caricamento e gestione pacchetti e documenti.
- Modulo SFTP per il caricamento massivo dei SIP.

- Antivirus.
- Modulo di back-end per tutte le attività di interfaccia con il DB e il Filesystem.
- Modulo delle utility (creazione ISO, ecc.).
- Modulo IDM – User Provisioning e Management per la gestione dell'access management.
- Schedulatore dei processi. Nello schedulatore vengono gestiti i job per:
    - la presa in carico di SIP;
    - l'avvio dei controlli di coerenza;
    - la generazione degli esiti di presa in carico;
    - la generazione e consegna dei Submission Report;
    - la generazione degli AIP;
    - la generazione e la consegna dei DIP;
    - la generazione dei Discard Information Package.
- Modulo per il controllo e la pianificazione delle funzionalità dell'intera struttura di servizio (include anche il Sistema di Routing che, in caso di inaccessibilità del Sistema di Conservazione primario, instrada il traffico sui siti secondari di DR);
- Modulo per l'integrazione con i dispositivi per la firma (HSM).
- Modulo per la gestione dello storage.
- Modulo di gestione DB.
- Il modulo per la gestione di Long Term Archiving (LTA).

Sulla base della struttura dei moduli, è previsto che ciascuno di essi abbia tre proprietà fondamentali:

- Identificazione del soggetto logico/fisico che compie l'attività;
- Controllo e gestione dell'attività stessa;
- Espandibilità del modulo (bilanciamento del carico dell'attività, ripartizione e crescita clusterizzabile sulle risorse a disposizione).

Tutte le attività dei moduli sono tracciate nel sistema di Log Management System, descritto nei paragrafi successivi.

Torna al Sommario

8.1 Componenti Logiche

Di seguito si descrivono più nel dettaglio le componenti logiche del Sistema di conservazione.

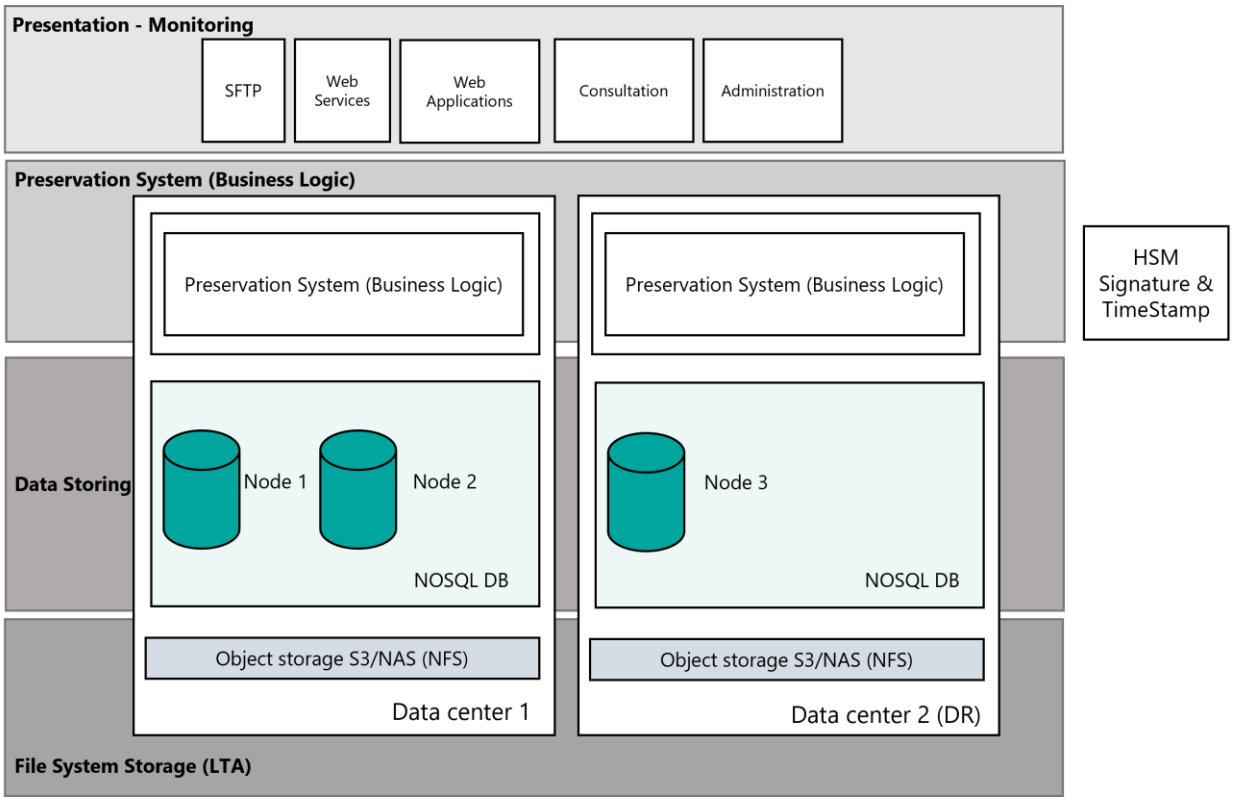


Figura 14 Componenti logiche del Sistema di Conservazione

Front-end applicativa (Web App front-end): è il portale di amministrazione e consultazione del Sistema di conservazione. Il portale web gestisce l'autenticazione e la profilazione degli utenti e permette di configurare tutte le componenti del Sistema di conservazione, le anagrafiche del Titolare dell'oggetto (Aziende), dei soggetti coinvolti nella conservazione con definizione dei ruoli, delle classi documentali, degli utenti, delle regole di amministrazione per la schedulazione dei processi, ecc.

DNS Router: il sistema di Routing che in caso di inaccessibilità del Sistema di conservazione primario, instrada il traffico sui siti DR.

Web Service del Sistema di conservazione: il servizio di conservazione di documenti informatici che espone tutte le funzioni per la gestione applicativa del processo di conservazione. Le API esposte sono di tipo REST e SOAP.

Server SFTP: il servizio per la gestione delle cartelle di ricezione dei SIP da parte del Titolare.

Schedulatore di processi: la sua configurazione permette di definire la sessione di versamento, la predisposizione e gestione degli AIP, la sessione di distribuzione e la sessione di scarto. Permette, inoltre, di definire l'attivazione e la schedulazione di funzioni e servizi per controllare in maniera continuativa le altre entità funzionali del Sistema di conservazione; quindi, interagisce con le altre entità del sistema (pianificazione della conservazione, servizi generali, acquisizione, conservazione, gestione dei dati, accesso).

L'entità logica della pianificazione di conservazione e controllo della struttura lavora e interagisce con lo schedulatore dei processi e definisce le funzioni e i servizi per il controllo dell'intero Sistema di conservazione. Questa entità, gestita dall'amministratore, definisce le policy e i job per mantenere nel sistema l'integrità, la disponibilità, la reperibilità e la leggibilità sia degli archivi che dei documenti, in conformità alla normativa vigente e a tutela dell'obsolescenza tecnologica. Definisce, inoltre, i modelli-dati dei pacchetti informativi (SIP, AIP, DIP, Discard Information Package).

Database del Sistema di conservazione: il sistema salva i dati su un database di tipo NoSQL con una configurazione basata su replica dei set di tre nodi: due sul sito primario e uno sul sito di DR.

MMS Arbiter: il modulo di amministrazione backup e gestione delle repliche dei dati.

Storage File a Lungo Termine (Object Storage S3): il sistema supporta lo storage dei file su sistema Object Storage S3 ed è possibile configurare bucket AWS dedicati al fine di semplificare le operazioni di dismissione/migrazione.

Torna al Sommario

8.2 Componenti Tecnologiche

L'architettura tecnologica del Sistema di conservazione può essere suddivisa in tre livelli:

- Primo livello. Parte di networking costituita dagli apparati di rete (router, switch), dal modulo firewall per la protezione del sistema da accessi indesiderati, dal WAF (Web Application Firewall) e dai load balancer che stabilizzano l'applicativo e suddividono il carico tra le varie macchine che erogano i servizi raggiungibili pubblicamente. Nello specifico: a livello di rete vengono utilizzati VPC (Virtual Private Cloud) dedicati, all'interno dei quali vengono costruiti i vari servizi organizzati nelle diverse sottoreti necessarie per la scalabilità. Ogni sottorete è costruita su una delle tre Availability Zone (AZ) disponibili, in modo da massimizzare la resilienza in caso di incidente su una singola Availability Zone. Ogni VPC è dedicato ad uno specifico servizio che fa parte del sistema ed è isolato dagli altri. Il punto di ingresso del sistema è costituito da un load balancer che distribuisce il lavoro che le macchine back-end svolgono successivamente al passaggio dei controlli delle richieste sul WAF.
- Secondo livello. Rappresenta il Core dell'infrastruttura di conservazione ed è costituito da server fisici che implementano i moduli e le componenti funzionali, dai dispositivi HSM o dalle librerie per la gestione delle firme. In particolare, i dispositivi HSM sono custoditi presso la Certification Authority (CA) Namirial e sono conformi ai requisiti di sicurezza previsti dalla normativa vigente. A questo livello appartengono anche tutte le strutture di controllo antivirus dei pacchetti inviati dagli utenti (ogni documento viene controllato e segnalato al Produttore in caso di elementi riconducibili a malware o virus con un rapporto antivirus dedicato).
- Terzo livello. Rappresenta il Datastore del sistema e contiene tutti i documenti e tutti i AIP.

Dalla struttura di erogazione del servizio (struttura primaria), è previsto un collegamento diretto, cifrato e privato, verso la struttura di Disaster Recovery. Tale struttura è logicamente suddivisa, come la struttura primaria.

Maggiori dettagli sulle componenti tecnologiche sono riportati nella documentazione del Sistema di Gestione della Sicurezza certificato ISO/IEC 27001.

Torna al Sommario

8.3 Componenti Fisiche

Il sistema di conservazione eroga i servizi basandosi su data center Amazon AWS:

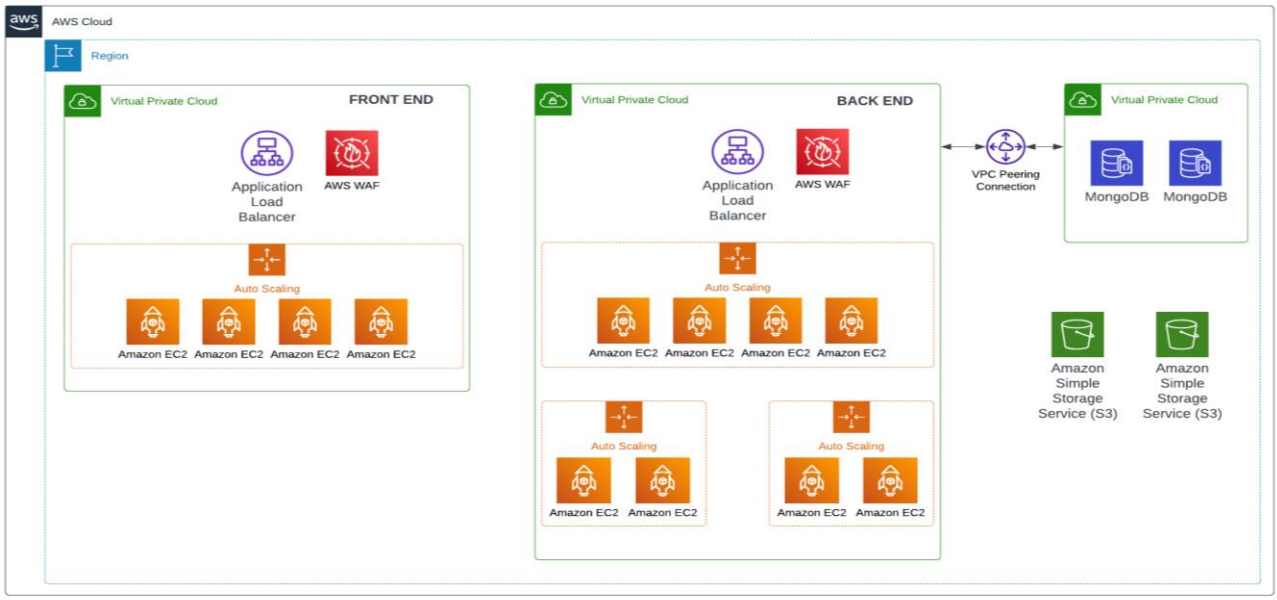


Figura 15 Componenti fisiche

- Sito Primario, situato su datacenter Amazon AWS con tutte le componenti necessarie in HA e collegato tramite connettività descritta sotto.
- Sito DR (Disaster Recovery), situato su data center AWS Amazon gestito e amministrato tramite interfaccia di gestione Amazon.

La gestione e l'amministrazione del cloud AWS è in carico al team Cloud Operation di Namirial che opera seguendo le best practices in termini di gestione dell'organizzazione. Il team, che continua il processo di formazione costantemente, è coordinato dal Cloud Ops Manager.

I data center Amazon AWS sono conformi ai principali standard di sicurezza internazionale ed in particolare implementano un sistema di gestione della sicurezza delle informazioni certificata ISO 27001, 27017 e 27018.

L'architettura di rete di Amazon consente di gestire grandi carichi di lavoro e traffico elevato con una bassa latenza tra i workload. Ogni Region è completamente isolata e comprende varie zone di disponibilità, anch'esse completamente isolate all'interno dell'infrastruttura AWS Amazon. Per meglio isolare ogni problematica e giungere ad una maggiore disponibilità, le istanze dedicate ai workload del sistema di conservazione sono distribuite su più zone di disponibilità all'interno della stessa Region. Inoltre, le zone di disponibilità sono distanti tra loro almeno 70 Km.

8.3.1 Italia

La distanza delle Region Primaria e Sito DR sono:

- Sito Primario: AWS Region Italiana (Milano) -> AWS Region Tedesca (Francoforte) – 600 Km
- Sito Disaster Recovery AWS Region EU-central-1 Francoforte - Distanza in linea d'aria maggiore di 600km.

8.3.2 Francia

- Sito Primario: AWS Region Francese -> AWS Region Italiana (Milano) – 851 Km
- Sito Disaster Recovery AWS Region EU-central-1 Francoforte - Distanza in linea d'aria maggiore di 600km.

8.3.3 Romania

Il Sistema di Conservazione fornisce servizi su data center di GTS Telecom SRL.

- Sito primario, situato nel datacenter di GTS Telecom SRL con tutti i componenti necessari in HA e collegato tramite connettività
- Sito Disaster Recovery, situato nel datacenter di GTS Telecom SRL

*****

Per gli approfondimenti e il dettaglio in relazione alle componenti fisiche e alla continuità operativa si rimanda alla documentazione relativa al sistema di gestione della sicurezza informatica, certificato ISO/IEC 27001.

Torna al Sommario

8.4 Componenti software

Di seguito sono indicati i componenti software utilizzati nel Servizio di Conservazione.

Funzione	*Sistema operativo*	*Licenza*	*Produttore*
WAF	N.A.	AWS provided	AWS
Web service	Windows Server	Datacenter edition	Microsoft
Web Application	Windows Server	Datacenter edition	Microsoft
Scheduler	Windows Server	Datacenter edition	Microsoft
Antivirus	Ubuntu	Open source	Canonical
Server Signature	CentOS	Open source	CentOS
DB Server	Ubuntu	Open source	Canonical

Torna al Sommario

8.5 Procedure di gestione e di evoluzione

Namirial, con il supporto di tutte le strutture aziendali, ciascuna per la parte di propria competenza, ha provveduto ad istituire un sistema di governo e presidio del servizio con lo scopo di:

- garantire la riservatezza, l'integrità, la leggibilità, la reperibilità e la disponibilità dei documenti e dati nel sistema;
- formalizzare e garantire i requisiti del sistema in conformità alla normativa vigente;
- manutenzione del servizio;
- ottimizzare la gestione dell'incident management;
- valutare i livelli di rischio e di continuità operativa;
- monitorare i livelli di sicurezza;
- gestire operativamente le attività di sicurezza (incidenti, prevenzione frodi, gestione della comunicazione in emergenza, ecc.).

8.5.1 Conduzione e manutenzione del Sistema di conservazione

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

Il Conservatore Namirial mantiene un registro cronologico delle componenti della piattaforma software comprensivo di tutte le release. Queste ultime, insieme agli applicativi utilizzati nell'intero processo di conservazione nell'arco degli anni, sono registrate al fine di rendere comunque disponibili e fruibili nel tempo i documenti e i dati relativi al servizio.

La procedura dei rilasci del software segue i requisiti imposti dalla certificazione ISO/IEC 27001.

La predisposizione, la verifica e l'approvazione della documentazione relativa al servizio di conservazione sono gestite all'interno delle Procedure ISMS dell'Organizzazione Namirial.

In ultimo, Namirial mette a disposizione sia internamente che per i soggetti esterni (clienti, fornitori, ecc.) un servizio di assistenza specifico e di competenza, istanziato da parte dell'Utente autorizzato attraverso il sistema di ticketing e strutturato come segue:

- Help Desk 1° Livello: è composto dagli operatori che ricevono il primo contatto da parte dell'Utente in caso di necessità e che riescono a dare supporto su tematiche relative all'utilizzo della piattaforma, al processo, al servizio, ecc.
- Help Desk 2° Livello: a seconda dei casi può gestire le richieste tecniche del primo livello e provvede alla gestione e alla risoluzione della problematica.

8.5.2 Gestione e mantenimento dei log

Il Sistema di conservazione integra applicativamente la tracciatura tramite un sistema di log di tutte le chiamate/eventi sul sistema. I dati tracciati sono:

- Livello LOG: indica il tipo di informazione tracciata, Debug, Warning, Info.
- Messaggio: informazioni descrittive dell'operazione eseguita.
- Note: i parametri applicativi inviati per l'operazione considerata.
- Operazione: la descrizione dell'evento applicativo eseguito.
- Utente: il nome dell'Utente che ha richiesto l'operazione.
- Indirizzo IP: l'eventuale indirizzo IP da dove proviene la richiesta.
- Data Creazione: la data di creazione del Log.

I log sono conservati in conformità alle disposizioni vigenti attuando meccanismi e controlli per la protezione da modifiche non autorizzate o problemi operativi, al fine di evitare:

- la disattivazione degli strumenti di log;
- le alterazioni ai messaggi registrati;
- editing e modifiche ai record di log;
- l'esaurimento dello spazio disponibile con conseguente perdita delle registrazioni
- la perdita di riservatezza delle informazioni.

Viene effettuato un backup giornaliero e i log vengono conservati nel Sistema di Conservazione per il periodo relativo alla conservazione degli oggetti conservati.

8.5.3 Monitoraggio del Sistema di conservazione

Tutte le operazioni eseguite da ciascun componente del sistema vengono tracciate tramite log al fine di mantenere evidenza delle attività e facilitare la diagnosi di eventuali anomalie e/o incident.

Il sistema di monitoring adottato è descritto più dettagliatamente nel capitolo dedicato al monitoraggio e ai controlli.

8.5.4 Change management

Il processo di change management sul servizio è istanziato dal Cliente attraverso la piattaforma di ticketing, e gestito da team dedicati attraverso l'eventuale aggiornamento contrattuale. Il Contratto recepisce le specifiche di change di servizio, e solo se espressamente accettato e condiviso tramite mail dal Titolare degli oggetti di conservazione, permette di attivare la successiva fase implementativa del change (dal collaudo fino alla messa in produzione).

Il change management dell'infrastruttura di erogazione del servizio, invece, è gestito e descritto dal Conservatore secondo la proceduta definita dallo standard ISO/IEC 27001.

8.5.5 Verifica periodica di conformità a normativa e standard di riferimento

Il Responsabile del servizio di conservazione effettua periodicamente un riesame generale del servizio insieme ai soggetti incaricati nell'organigramma per la conservazione, al fine di accertare la conformità del sistema al livello di servizio atteso, analizzare le cause di eventuali incidenti o disservizi e promuovere attività di prevenzione o miglioramento.

Qualora necessario, una riunione di riesame può essere indetta a fronte di particolari eventi (ad esempio, cambi tecnologici, normativi o di requisiti funzionali, stagionalità di carico elaborativo, ecc.).

Con periodicità almeno annuale, in accordo con le funzioni interne, il Responsabile del servizio di conservazione pianifica processi di audit che coinvolgono aspetti normativi, di processo, organizzazione, tecnologici e logistici, anche con l'intervento di consulenze specifiche.

L'obiettivo è accertare la conformità del sistema alle leggi, ai regolamenti, al contratto con i Titolari degli oggetti, alla documentazione generale del servizio, ai principi che ispirano il sistema di qualità e al presente manuale.

Periodicamente sono, inoltre, eseguite delle verifiche di audit sulle funzionalità del Sistema di conservazione, principalmente su:

- verifica delle funzionalità di creazione e mantenimento dei Submission Report, degli AIP, etc;
- verifica delle funzionalità di dissemination di pacchetti e documenti ai fini di esibizione e produzione delle copie;
- mantenimento e disponibilità di un archivio del software dei programmi in gestione nelle eventuali diverse versioni, per permettere il ripristino;
- verifica della corretta configurazione delle varie anagrafiche (Titolare dell'oggetto, Responsabile della conservazione, altri soggetti, classi documentali, metadati, privilegi utenti, ecc.);
- verifica del corretto funzionamento delle procedure di sicurezza utilizzate per garantire l'apposizione della firma digitale e della validazione temporale;
- verifica della corretta predisposizione e mantenimento della documentazione relativa alla conservazione, anche a fronte di variazione delle condizioni di servizio o a eventi di cui si deve tenere traccia, quali adeguamenti normativi, evoluzioni tecnologiche, subentro di personale in attività previste dalla conservazione, evoluzioni tecnologiche e software, ecc.

8.5.6 Gestione della sicurezza e valutazione del rischio

Per la descrizione della gestione della sicurezza aziendale, dell'analisi dei rischi e della continuità operativa si rimanda a tutta la documentazione relativa al ISMS, certificato ISO/IEC 27001 e per lo specifico Servizio di Conservazione - Long Term Archiving (LTA) al Piano della Sicurezza LTA.

Torna al Sommario

9 MONITORAGGIO E CONTROLLI

Nell'ambito delle certificazioni 27001 ed estensioni vengono effettuati dei controlli per accertare la conformità agli standard di implementazione della sicurezza, secondo quanto previsto nell'ambito del processo di miglioramento continuo del sistema di gestione per la sicurezza delle informazioni. La verifica della conformità tecnica comporta la verifica dei sistemi operativi per garantire che le contromisure e i controlli hardware e software siano stati implementati correttamente. Le verifiche di conformità tecnica includono anche test di **Vulnerability Assessment** e **Penetration Test**.

La strategia adottata da Namirial prevede che la pianificazione, la struttura organizzativa a supporto e gli strumenti di continuità operativa sviluppati comprendano tutte le misure funzionali, tecnologiche, organizzative e infrastrutturali necessarie per assicurare qualità, sicurezza e affidabilità ai servizi erogati per il Titolare dell'oggetto di conservazione.

Per il raggiungimento di questo obiettivo le procedure e gli strumenti di monitoraggio e controllo descritti nel seguito sono essenziali.

Torna al Sommario

9.1 Procedure di monitoraggio

Il servizio di conservazione viene costantemente controllato da un sistema di monitoring che rileva malfunzionamenti, anomalie ma anche situazioni critiche che rischiano di causare problemi di funzionamento del sistema.

Le aree organizzative di Produzione e di Sviluppo Software di Namirial effettuano il monitoring on-line e le attività di controllo delle componenti applicative e di impianto con cui vengono erogati i servizi, tramite gli indicatori e i controlli identificati sul Sistema di Gestione della Sicurezza delle Informazioni ISMS.

In particolare, il Conservatore Namirial effettua le attività di controllo avvalendosi della **piattaforma Nagios** (sistema di asset management) e pagina dedicata per il ticketing. Nagios al verificarsi di un evento anomalo legato alle risorse hardware o ai servizi applicativi notifica al SOC (Security Operations Center) l'anomalia, il quale, previo controllo, crea un ticket e lo assegna al Responsabile dei sistemi informativi o altro operatore deputato, che entro un tempo prestabilito (SLA – Service Level Agreement), deve effettuare le opportune manutenzioni per chiudere l'anomalia. Il sistema inoltre prevede delle policy di escalation verso i supervisori nel caso in cui il ticket non venga preso in carico nei tempi prestabiliti. Il ticket una volta lavorato viene chiuso dall'operatore inserendo le attività effettuate per risolvere l'incidente. Tutti i ticket gestiti rimangono storicizzati nel sistema e costituiscono la base per la creazione dei report di monitoraggio e controllo.

Namirial è inoltre dotata di un software per il monitoraggio degli eventi di sicurezza e continuità operativa sui servizi essenziali del sistema di conservazione, tale software **QRadar** di IBM viene utilizzato dal SOC operato dalla società Yarix di Montebelluna che monitora 24h ore al giorno 365 gg anno e al verificarsi di eventuali eventi critici contatta il personale preposto per mitigare eventuali problemi di sicurezza e continuità operativa.

Gli utenti del sistema di conservazione usano la piattaforma di ticketing **Namirial ServiceDesk** raggiungibile all'indirizzo servicedesk.namirial.com per richiedere supporto all'help desk di I livello. I ticket generati riportano le seguenti informazioni:

- presa in carico della richiesta
- assegnazione
- messaggi scambiati con l'operatore
- chiusura del ticket
- attività effettuate.

Gli utenti possono inoltre monitorare in autonomia lo stato del Servizio tramite la **Status page** di Namirial (status.namirial.com), costantemente aggiornata.

Gli utenti amministratori del Sistema di Conservazione possono a loro volta aprire internamente dei ticket attraverso la piattaforma **Jira** qualora la richiesta debba essere smistata a livelli di assistenza superiori al primo.

Il sistema di ticketing, inoltre, tiene traccia di data e ora di gestione dei ticket. In particolare, vengono controllati costantemente:

- processi e web services;
- esposizione del servizio all'utente;
- processi di acquisizione dei documenti;
- servizio sFTP;
- servizi di scheduling (es. processi generazione Submission Report, AIP, DIP, ecc.);
- servizi di supporto (es. antivirus, servizio di firma, servizio di time stamping);
- occupazione, latenza e performance storage;
- processi, transazioni e performance DB;
- log del sistema di gestione delle repliche del DB;
- servizio di pubblicazione web;
- log servizio di pubblicazione web;
- log di sistema e funzionalità risorse;
- log di procedura e consistenza;
- servizio di rotazione legale dei log;
- processi backup, replica geografica e DR;
- funzionamento sistema di backup e DR;
- funzionamento e performance HSM;

Il sistema di gestione degli asset e log management rileva, grazie all'installazione di un agent sulle macchine di produzione del servizio di conservazione, i seguenti dati:

- accesso amministratori di sistema;
- hardware e software installato sul server;

- uso della CPU, RAM, SPAZIO disco monitorato con intervalli di 5 minuti.

Ulteriori ed eventuali procedure aggiuntive di monitoraggio e controllo richieste dal Titolare dell'oggetto sono concordate tra il Conservatore e lo stesso Titolare.

Torna al Sommario

9.2 Verifica dell'integrità degli archivi

Il processo di verifica dell'integrità dei pacchetti informativi e dei documenti nell'ambito del servizio prevede:

- la verifica di corrispondenza sul numero dei documenti (verifica tra il numero di documenti effettivi presenti nel Sistema di conservazione e il numero dei records presenti all'interno della struttura del DB per un determinato Titolare);
- il controllo dell'integrità degli strumenti di validazione apposti sui documenti e sugli Indici dei pacchetti (verifica della firma e della marca temporale su una percentuale prescelta rispetto al totale dei documenti e indici XML del AIP presenti all'interno del Sistema di conservazione per un determinato Titolare).

Per quanto riguarda la verifica di leggibilità, nel Sistema di conservazione sono attivi degli automatismi che entro il termine quinquennale effettuano una serie di controlli su base campionaria estratta tramite un algoritmo pseudocasuale, considerando l'insieme degli Id presenti nella totalità dei documenti conservati:

- verifica di integrità, effettuata attraverso il calcolo automatico dell'hash del documento e relativa comparazione con l'hash registrato in fase di creazione del AIP;
- verifica di leggibilità, sull'insieme dei documenti estratti per la verifica di integrità verrà ulteriormente creato un sottoinsieme di documenti al fine di verificarne la leggibilità e a seguito di ogni operazione di controllo verrà prodotto un verbale firmato digitalmente dal Responsabile del servizio di conservazione e conservato nel Sistema.

Torna al Sommario

9.3 Soluzioni adottate in caso di anomalie

La gestione degli incidenti nell'erogazione del servizio e nella conduzione del Sistema di conservazione è governata da Namirial attraverso l'adozione di:

- idonei strumenti di rilevazione;
- sistemi formalizzati di reazione agli eventi inattesi, riconosciuti come incidenti;
- adeguati processi di comunicazione;
- efficienti contromisure di sicurezza e di ripristino delle funzionalità del Sistema di conservazione o in caso di perdita dei dati.

Il sistema adotta controlli automatici a garanzia dell'integrità e della coerenza dei dati movimentati dal sistema e durante il processo; i controlli automatici richiedono l'intervento della struttura organizzativa a supporto del servizio di conservazione solo al verificarsi di anomalie non gestibili in modo automatico.

Qualora si verificasse un incidente di sistema o di processo, le operazioni di rilevamento e ripristino delle funzionalità seguono una procedura definita e documentata, come previsto anche dal sistema di gestione ISMS certificato ISO/IEC 27001.

Nell'ambito della gestione degli incidenti, Namirial segue una procedura che rispetta le seguenti fasi:

- Fase 1: Monitoraggio e identificazione dell'incidente;
- Fase 2: Tracciamento dell'incidente;
- Fase 3: Classificazione dell'incidente;
- Fase 4: Notifica ed escalation;
- Fase 5: Risposta all'incidente;
- Fase 6: Follow-up.

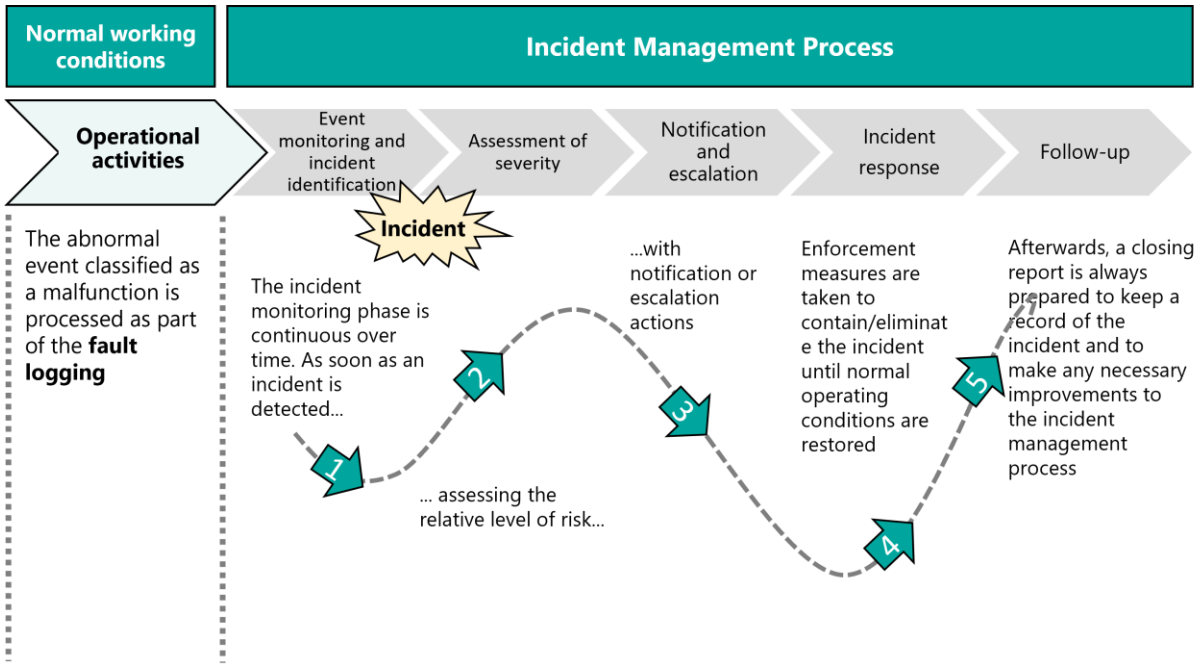


Figura 16 Incident Management

Al verificarsi di malfunzionamenti o situazioni critiche, il sistema di monitoraggio genera delle notifiche via mail al personale reperibile che si attiverà per risolvere il problema secondo quanto stabilito dagli SLA concordati con il Titolare dell'oggetto e secondo le procedure interne di gestione degli incidenti.

Per una trattazione più dettagliata dell'argomento, si rimanda ai documenti aziendali specifici in ambito di Incident management oggetto di certificazione ISO/IEC 27001.

Torna al Sommario

10 ANNEX

Integrano il presente Manuale una serie di documenti aziendali relativi a specifici aspetti connessi al Servizio di Conservazione - Long Term Archiving (LTA) di Namirial.

Di seguito si riporta l'elenco di tali documenti disponibili per la consultazione se di natura pubblica.

All'interno dei documenti elencati è possibile trovare rimandi ad ulteriori documenti e policy di gruppo Namirial.

N.	*Nome*	*Nota di riservatezza*
1.	Namirial - LTA - Qualified electronic signatures and seals preservation policy	Documento pubblico
2.	Namirial - LTA - Piano della Sicurezza	Documento interno
3.	Namirial - LTA - Piano di Cessazione	Documento interno
4.	Namirial - LTA - Risk Assessment	Documento interno

Torna al Sommario