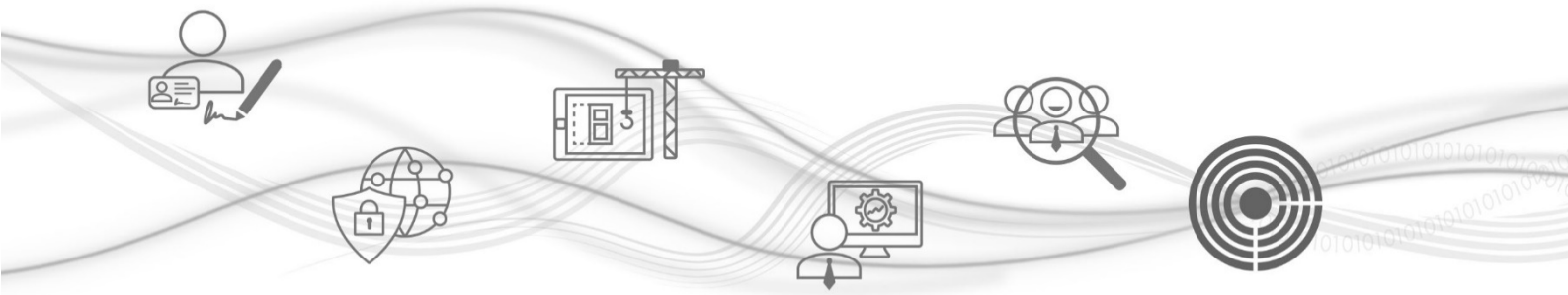
Manuale del Conservatore

NamirialArchive

Servizio 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	**11.4**	**Massimiliano Pellegrini**
Approvato da	**Massimiliano Pellegrini**	Data di emissione	**02/12/2025**	_____

MASSIMILIANO PELLEGRINI
18/12/2025 12:11:19 UTC+0100

Indice del documento

Indice del documento 2
Registro delle versioni 5
1 SCOPO E AMBITO DEL DOCUMENTO 9
2 TERMINOLOGIA 11
2.1 Glossario 11
2.2 Acronimi 18
3 NORMATIVA E STANDARD DI RIFERIMENTO 19
3.1 Normativa di riferimento 19
3.1.1 Unione Europea 19
3.1.2 Italia 19
3.1.3 Romania 20
3.1.4 Francia 20
3.2 Standard di riferimento 21
4 RUOLI E RESPONSABILITÀ 22
4.1 Deleghe 26
4.2 Obblighi delle parti esterne 26
5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE 28
5.1 Organigramma 28
5.2 Strutture organizzative 28
6 OGGETTI SOTTOPOSTI A CONSERVAZIONE 32
6.1 Identificativi univoci 33
6.2 Oggetti conservati 33
6.3 Formati 34
6.3.1 Valutazione ed indice di interoperabilità 35
6.3.2 Eventuale obsolescenza dei formati 36
6.4 Submission Information Package (SIP) 36
6.4.1 Pre-pacchetto 42
6.4.2 Revision Package 42
6.5 Archival Information Package (AIP) 43
6.6 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 50
7.2 Verifiche effettuate sui Submission Information Package e sugli oggetti in essi contenuti 51
7.3 Signature Report 53
7.4 Accettazione dei Submission Information Package e generazione del Submission Report 53
7.5 Rifiuto dei Submission Information Package e modalità di comunicazione delle anomalie 56
7.6 Antivirus Report 57
7.7 Preparazione e gestione dell'Archival Information Package 58
7.8 Cifratura degli oggetti di conservazione 58
7.9 Gestione di documenti contenenti dati sensibili 59
7.10 Preparazione e gestione del Dissemination Information Package ai fini dell'esibizione 60
7.11 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori 60
7.12 Interazioni con il servizio 61
7.13 Scarto (Deletion) 61
7.13.1 Periodo di conservazione 63
7.14 Utilizzo del Servizio Qualificato di Conservazione di Firme e Sigilli Elettronici 63
8 IL SISTEMA DI CONSERVAZIONE 64
8.1 Componenti Logiche 66
8.2 Componenti Tecnologiche 67
8.3 Componenti Fisiche 68
8.3.1 Italia 69
8.3.2 Francia 69
8.3.3 Spagna 69
8.3.4 Romania 69
8.3.5 LATAM 69
8.4 Componenti software 70
8.5 Procedure di gestione e di evoluzione 70
8.5.1 Conduzione e manutenzione del Sistema di conservazione 70
8.5.2 Log 71
8.5.3 Change management 71
8.5.4 Verifica periodica di conformità a normativa e standard di riferimento 71
8.5.5 Gestione della sicurezza e valutazione del rischio 72
9 MONITORAGGIO E CONTROLLI 73

9.1 Procedure di monitoraggio 73
9.2 Verifica dell'integrità degli archivi 75
9.3 Soluzioni adottate in caso di anomalie 75
10 ALLEGATI 77

Registro delle versioni

N°Ver/Rev/Bozza	Data emissione	Descrizione
1.0	28/11/2014	Prima emissione del documento secondo lo schema del manuale AgID per l'accreditamento
2.0	22/01/2015	Nuova emissione per revisioni
3.0	05/02/2015	Integrazione del manuale per l'accreditamento
4.0	22/02/2016	Revisioni varie in tutti i capitoli del manuale
5.0	26/09/2016	Revisione della topologia dei siti di erogazione del servizio, revisione dell'organigramma
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
6.1	11/10/2018	Aggiornamento glossario e normativa di riferimento; revisione dell'organigramma; aggiornamento tabella dei formati
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
8.0	04/06/2020	Aggiornamento Ruoli e Responsabilità
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) -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
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)
10.2	27/02/2023	Aggiornamento dei seguenti capitoli: -Aggiornamento componenti fisiche (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
11.1	15/05/2024	-Aggiornamento paragrafo 1 Aggiunto paragrafo 4.2 "Obblighi delle parti esterne" -Aggiornamento paragrafo 8.3 con intervallo massimo di configurazione di sistema -Aggiunto paragrafo 6.1 "Identificativi univoci" -Aggiornamento paragrafo 7.11 "Scarto" -Aggiunto paragrafo 7.13 "Utilizzo del Servizio Qualificato di Conservazione di Firme e Sigilli Elettronici"
11.2	10/09/2024	Modifiche minori
11.3	20/12/2024	-Aggiornamento della struttura e degli schemi dei pacchetti informativi -Aggiornamento e revisione del paragrafo 7.13 relativo allo scarto (Deletion) -Revisioni minori in tutti i paragrafi
11.4	02/12/2025	- Aggiornamenti nel paragrafo dei riferimenti normativi e standard - Aggiornamento paragrafo 2.1 "Glossario" - Aggiornamento paragrafo 4 "Ruoli e Responsabilità"

		- Aggiornamento contenuto del DIP al paragrafo 6.6 “Dissemination Information Package” - Aggiornamenti formati ed estensioni ammessi al paragrafo 6.3 “Formati”

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 Manuale copre il servizio LTA e, nell'Allegato 1, comprende la practice statement per un servizio Qualificato di Conservazione di Firme e Sigilli Elettronici, utilizzato dal servizio LTA per garantire l'integrità dei dati archiviati e conservare le firme e i sigilli elettronici qualificati. Il servizio Qualificato di Conservazione di Firme e Sigilli Elettronici è progettato per soddisfare i requisiti del Regolamento (UE) n. 910/2014 (Regolamento eIDAS) come servizio di conservazione qualificato per firme e sigilli elettronici qualificati, ovvero conforme ai requisiti degli articoli 34 e 40, ed è sottoposto ad audit da parte di un Organismo di Valutazione della Conformità (CAB) Accreditato e sotto vigilanza. Il Servizio LTA implementa un servizio di archiviazione elettronica non qualificato come definito nell'articolo 3(16)(m) del Regolamento eIDAS, come rivisto dal Regolamento (UE) 2024/1183.

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	Agenzia per l'Italia Digitale
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.	Deletion Package	Pacchetto generato dal servizio a seguito dell'esecuzione di un processo di eliminazione di oggetti.
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.	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
36.	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
37.	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
38.	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
39.	Formato	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
40.	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
41.	FTP Server	Programma che permette di accettare connessioni in entrata e di comunicare in maniera sicura con un Client attraverso il protocollo FTP
42.	Funzioni archivistiche	Funzioni per la conservazione delle informazioni (acquisizione, archiviazione, gestione dei dati, accesso, distribuzione)
43.	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
44.	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
45.	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
46.	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
47.	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
48.	Impronta	La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash
49.	Incremento delle evidenze della conservazione (preservation evidence augmentation)	Incremento di dati rispetto a un'evidenza di conservazione esistente per estendere il periodo di validità di tale evidenza.
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). Rappresenta la preservation evidence - evidenza di conservazione
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 Deletion Package	Indice del Deletion Package, struttura dell'insieme dei dati a supporto del processo di eliminazione dei documenti informatici e definita nello specifico dal Conservatore
54.	Information Package	Pacchetto Informativo, contenitore che racchiude uno o più oggetti da conservare insieme ai metadati riferiti agli oggetti
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.	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
63.	Presa in carico	Accettazione da parte del Sistema di conservazione di un SIP in quanto conforme alle modalità previste dal Manuale del Conservatore
64.	Preservation evidence	Evidenze prodotte dal servizio di conservazione che possono essere utilizzate per dimostrare che uno o più obiettivi di conservazione sono stati raggiunti per un determinato oggetto di conservazione.
65.	Preservation profile	Un profilo di conservazione identifica un insieme di dettagli di implementazione che specificano come vengono generate e convalidate le evidenze di conservazione e che sono pertinenti a un modello di conservazione e a uno o più obiettivi di conservazione.
66.	Processo di conservazione	Insieme delle attività finalizzate alla conservazione dei documenti informatici
67.	Produttore	È il responsabile della generazione del SIP e della relativa trasmissione al Conservatore
68.	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
69.	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
70.	Responsabile del servizio di conservazione (Preservation Service Manager)	Soggetto persona fisica nominato Responsabile del servizio di conservazione di Namirial
71.	Responsabile della funzione archivistica di conservazione (Archival Manager)	Soggetto persona fisica nominato Responsabile della funzione archivistica di conservazione di Namirial
72.	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

73.	Revision Package	Pacchetto informativo inviato al Sistema di conservazione secondo un formato predefinito al fine di apportare una revisione ai dati precedentemente conservati dal Sistema
74.	Scarto	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti che hanno raggiunto il termine di durata di conservazione previsto
75.	Service Level Agreement (SLA)	È l'accordo tra il Titolare dell'oggetto di conservazione, Produttore, Responsabile della conservazione e Conservatore sui livelli servizio da garantire
76.	Sessione di distribuzione	Sessione per la consegna (distribuzione) di uno o più DIP dal Conservatore al Titolare
77.	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
78.	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
79.	Signature Report (or Validation Report)	Documento informatico esito della verifica della firma qualificata o del sigillo qualificato, contenente dati riferiti al certificato qualificato utilizzato per l'apposizione della firma/sigillo e conservato insieme alle evidenze di conservazione come elemento di prova.
80.	Sistema di conservazione/Long Term Archiving System (LTA)	Sistema di conservazione dei documenti informatici
81.	Submission Information Package (SIP)	Pacchetto informativo inviato dal Produttore al Sistema di conservazione secondo un formato predefinito
82.	Submission Report	Oggetto digitale che attesta l'avvenuta presa in carico da parte del Sistema di conservazione dei SIP inviati dal Produttore
83.	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.
84.	Titolare di firma	La persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica
85.	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
86.	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.	LTA	Long Term Archiving
2.	OAIS	Open Archival Information System, ISO 14721
3.	AIP	Archival Information Package
4.	DIP	Dissemination Information Package
5.	SiNCRO	Support for Interoperability in Preservation and Recovery of Digital Objects - Supporto all'interoperabilità nella conservazione e recupero degli oggetti digitali (UNI 11386)
6.	SIP	Submission Information Package
7.	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**)
- **Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024** amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework

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**, **dicembre 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
- **Ordin nr. 20717 din 9 Mai 2024** pentru aprobarea Normelor tehnice privind procedura de acreditare a administratorilor de arhivă electronică și procedura de avizare a sistemelor electronice de arhivare și pentru abrogarea Ordinului ministrului comunicațiilor și societății informaționale nr. 493/2009 privind normele tehnice și metodologice pentru aplicarea Legii nr. 135/2007 privind arhivarea documentelor în formă electronică.

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;
- **NF Z42-013** Archivage électronique - Recommandations et exigences
- **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;
- **ETSI TS 119 172-4** Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists; **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.
- **ISO/TS 7538 Functional requirements for disposition of records**

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)	**Eleonora Luzi**	– 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 27 novembre 2025	

	Enrico Giunta	Come sopra	Dal 26 maggio 2021 al 27 novembre 2025	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	**Mario Veltini**	– gestione dell'esercizio delle componenti hardware e software del Sistema di conservazione;	Dal 5 luglio 2021	

la conservazione (Information System Manager)		– 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; – 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)	**Nicola Bruni**	– 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	Dal 3 settembre 2024	

		verso nuove piattaforme tecnologiche; – gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.		
	Fabio Didonè	Come sopra	Dal 5 luglio 2021 al 15 maggio 2024	
	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)	**Luigi Enrico Tomasini**	– revisione periodica e completa dell'aderenza del servizio a tutte le leggi, i regolamenti e gli standard applicabili	Dal 30 agosto 2025	
	Federica Marti	come sopra	Dal 31 luglio 2023 al 29 agosto 2025	
	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

4.2 Obblighi delle parti esterne

Gli obblighi di terzi a supporto dei servizi offerti devono fornire, in generale, le seguenti garanzie:

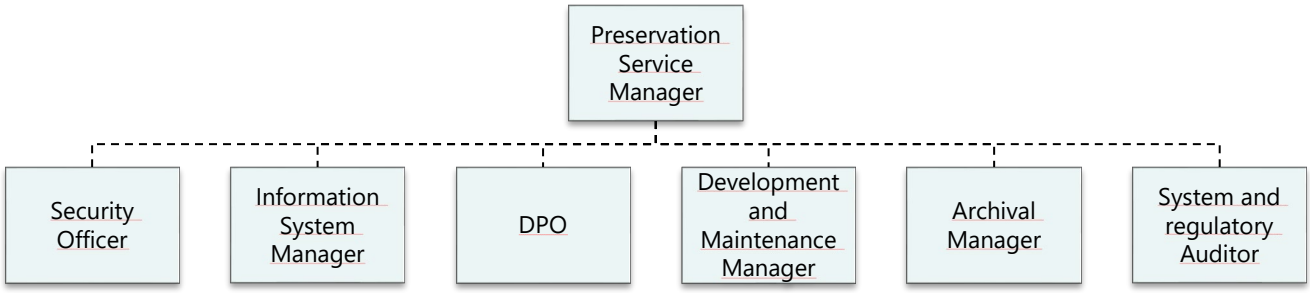
- conoscere e seguire quanto stabilito nel presente documento e nelle politiche di conservazione;
- osservare e facilitare il rispetto di tutto ciò che è stabilito in questo documento e nelle politiche di conservazione;
- informare di tutte le modifiche che verranno apportate all'infrastruttura o alle procedure al fine di garantire il mantenimento delle condizioni previste dai requisiti di certificazione del servizio. In ogni caso, tali modifiche devono garantire quanto previsto dal presente documento e dalle politiche di conservazione;
- sottoscrivere un contratto con Namirial;
- utilizzare i servizi in conformità alle procedure stabilite da Namirial;
- notificare qualsiasi incidente o evento che riguardi i servizi in oggetto

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:



Organigramma del servizio

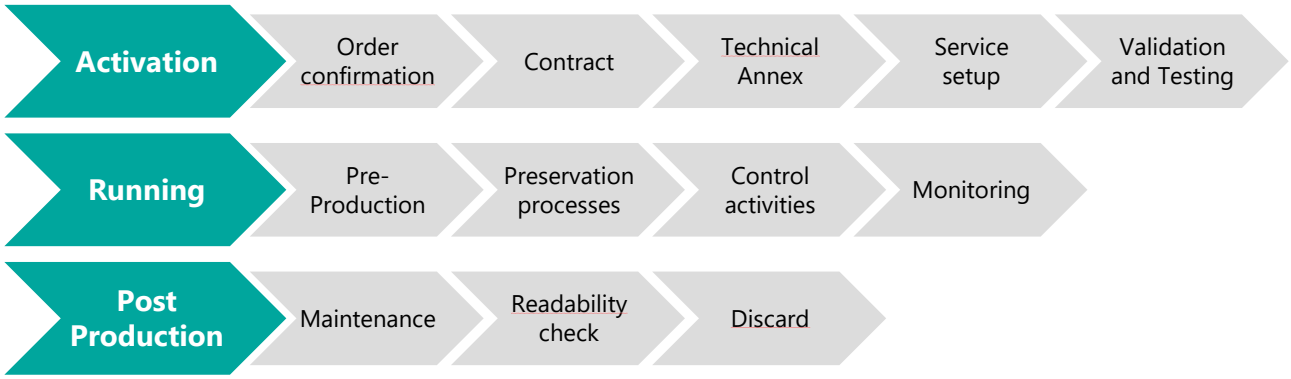
5.2 Strutture organizzative

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).

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



Ciclo di vita del Servizio di Conservazione

In ciascuna fase del servizio sono presenti sotto fasi.

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.

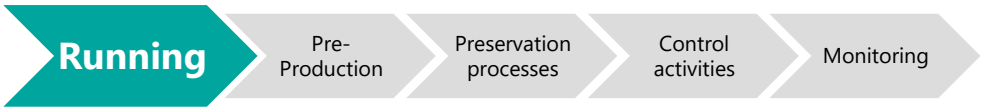
La predisposizione della corretta definizione iniziale dei requisiti e quindi la conformità alla normativa vigente in materia di sistemi di conservazione, con anche l'individuazione degli adempimenti correlati, è assicurata in fase di analisi dalla predisposizione del documento "Specificità del contratto - 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.



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, 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.

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.

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/IEC 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 Identificativi univoci

Il servizio di conservazione è identificato tramite appositi identificativi indicati di seguito:

- **System OID** (identificativo univoco del sistema): **1.3.6.1.4.1.36203.7.1.0**
- **Process OID WST** (identificativo del profilo di conservazione basato sullo standard OAIS e sul modello WST): **1.3.6.1.4.1.36203.7.1.1**
- **Process OID WTS** (identificativo del profilo di conservazione basato sullo standard OAIS e sul modello WTS): **1.3.6.1.4.1.36203.7.1.2**

6.2 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 modulo 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 ;
- 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 modulo da attivare.

6.3 Formati

Il Sistema di Conservazione accetta tutti i formati ritenuti adatti alla conservazione secondo l'Allegato 2 delle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici:

- PDF. PDF/A (.pdf)
- Office Open XML (.dccx, .dotx, .xlsx, .pptx . . xltx . . ppsx, .potx)
- Open Document Format (.odt. .ods, .odp . . odg, .fods, .fodp, .fodg, .odi . . odf, .fodt)
- Markup Language (.html. .htm, .xhtml. .css, .md, .mml)
- XML (.xml. .xslt, .xsd . . xsl)
- TIFF (.tif . . tiff)
- JPG (.jpg ..j peg)
- PNG (.png)
- Scalable Vector Graphics (.svg, .svgz)
- MAIL (.emi, .mbox)
- TXT (.txt)
- Structured data (.csv, .json, .jsonld, .sql)
- Academy Color Encoding System (.exr, .mxf, .amf . . clf)
- Autodesk® (.dwg, .dwt, .fbx)
- Font (.otf, .ttf, .woff, .woff2)
- Audio (.wav, .bwf, .rf64, .flac . . pcm, .raw, .sam, .musicxml. .mid, .midi)
- Video (.mp4, .m4a, .m4v)
- Timed Text Markup Language (.ttml. .dfxp)
- Compress archive (.tar, .jar, .zip)
- ISO (.iso)
- VMDK (.vmdk)

Ulteriori formati potranno essere aggiunti in accordo a specifici standard, linee guida o richieste di Produttori con motivate esigenze. Nello specifico il sistema accetta anche:

- MP3 (.mp3)
- EDI (.edi)
- Digital model (ifc, .dwg, .dxf)

- XFIR (container based on asic standard)

Valutazione e relativa interoperabilità del formato andranno opportunamente valutati. Nel caso in cui la richiesta provenga dal cliente, quest'ultimo è responsabile di tale valutazione.
Per quanto riguarda la conservazione di file in formato TXT, non riportato tra i formati indicati nell'Allegato 2, 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 indice di interoperabilità sono riportati nel paragrafo successivo.

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 o un sigillo elettronico nei formati standard di firma CAdES (.p7m), PAdES (.pdf) e XAdES (.xml) e/o una marca temporale.

6.3.1 Valutazione ed indice di interoperabilità

Il Sistema di Conservazione supporta il formato TXT, 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

6.3.2 Eventuale obsolescenza dei formati

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, tuttavia, qualora l'evoluzione tecnologica o nuovi standard e normative dovessero far emergere l'esigenza di utilizzare nuovi formati considerati maggiormente idonei, è possibile valutare un eventuale processo volto all'adeguamento del formato del documento. A seguito di un piano preventivo di controlli mirati ad eseguire le necessarie verifiche di integrità, di leggibilità e di adeguatezza della rappresentazione informatica dei documenti, può essere pianificato un processo di riversamento interno. Tale processo trasferisce uno o più documenti conservati modificando la loro rappresentazione informatica, ma garantendo l'integrità del contenuto.

Torna al Sommario

6.4 Submission Information Package (SIP)

Il Submission Information Package (SIP) è costituito da un oggetto in formato zip , composto da:

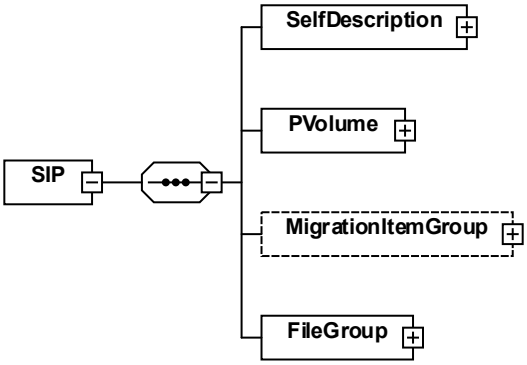
- i documenti oggetto della conservazione (*Content Information*), eventualmente firmati digitalmente (nello standard di firma CAdES ".p7m" o PAdES o XAdES) o eventualmente marcati temporalmente (nello standard di validazione temporale CAdES-T, o PAdES-T o XAdES-T);
- un file SIP Index (SIPindex) finalizzato 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:

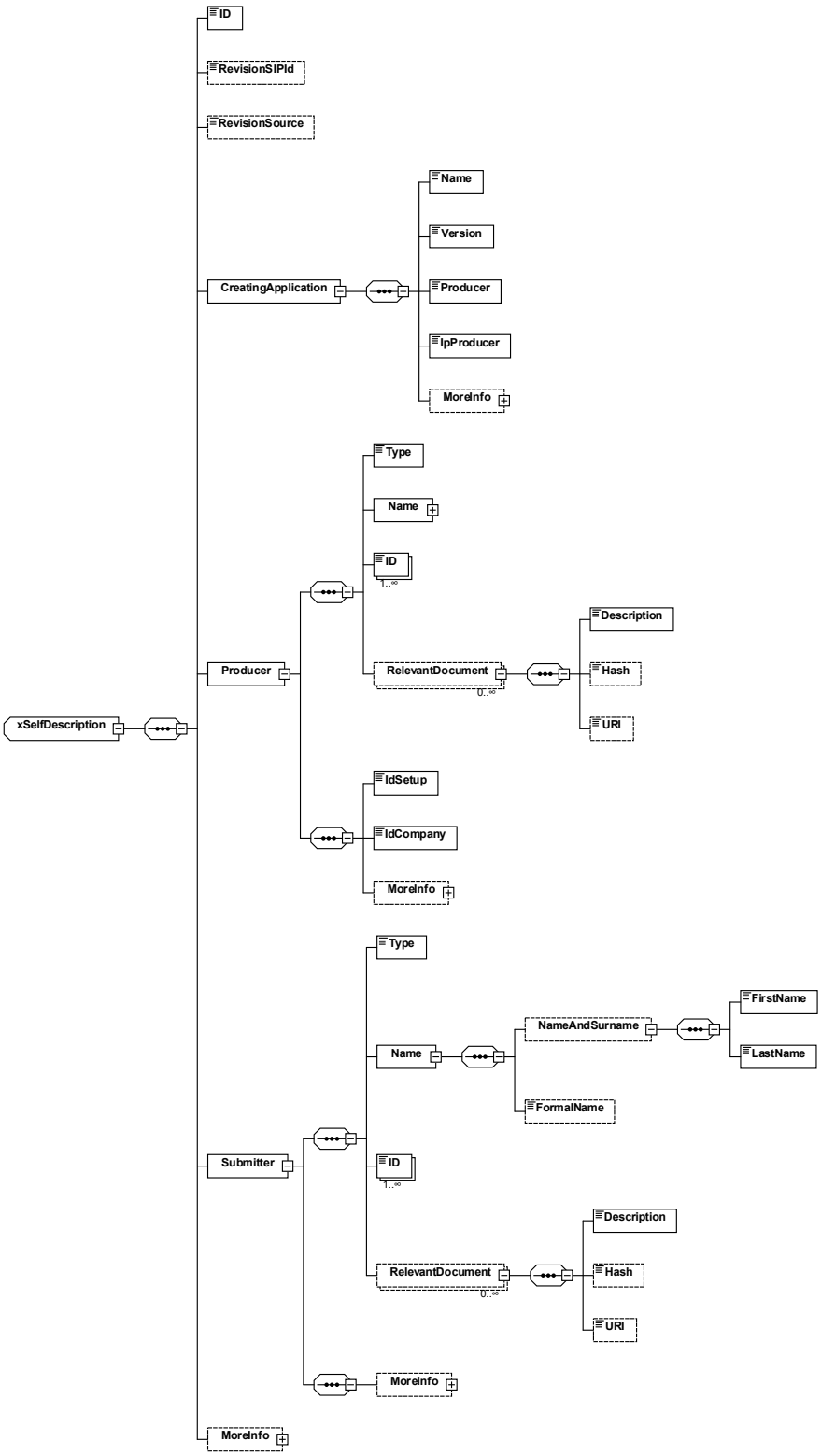
- l'identificazione del soggetto che ha prodotto il SIP (Producer);
- l'identificazione dell'applicativo che lo ha prodotto;
- la definizione della tipologia documentale a cui appartengono i documenti inclusi nel pacchetto ed eventuali messaggi del Responsabile della conservazione;
- la definizione dei 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.

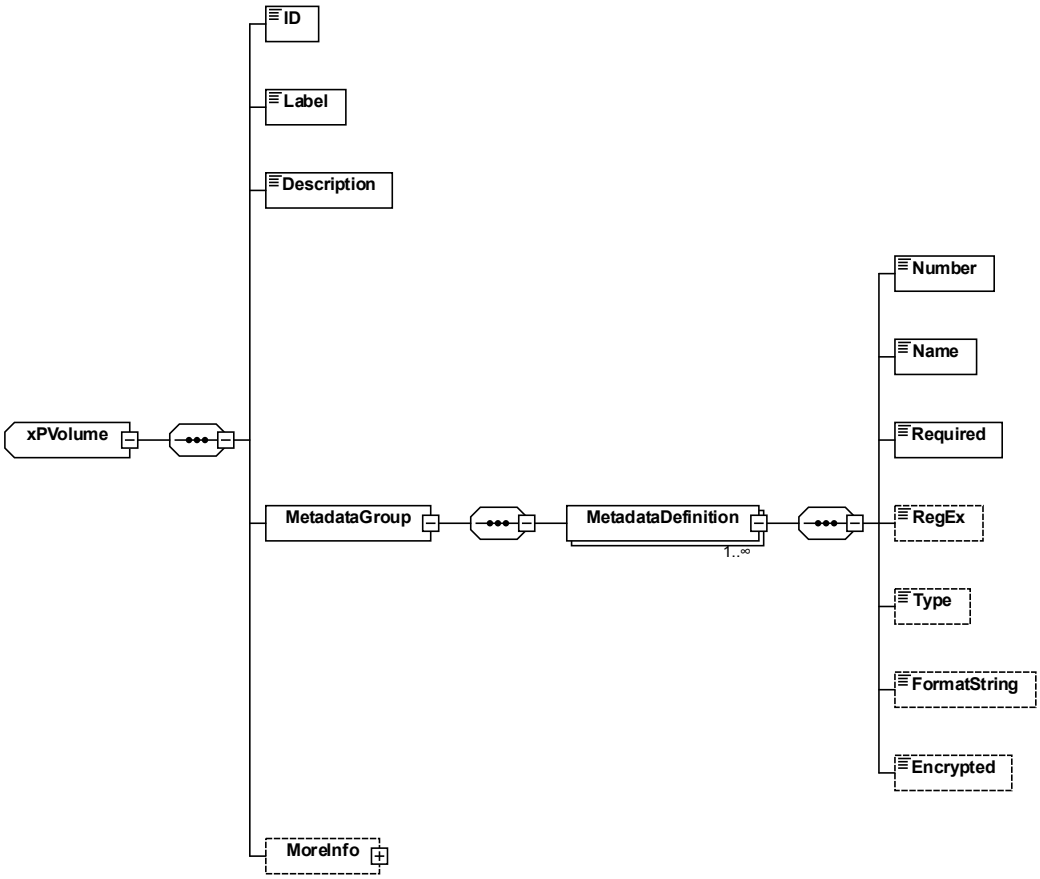
Di seguito la rappresentazione grafica del file XSD dell'Indice del SIP:



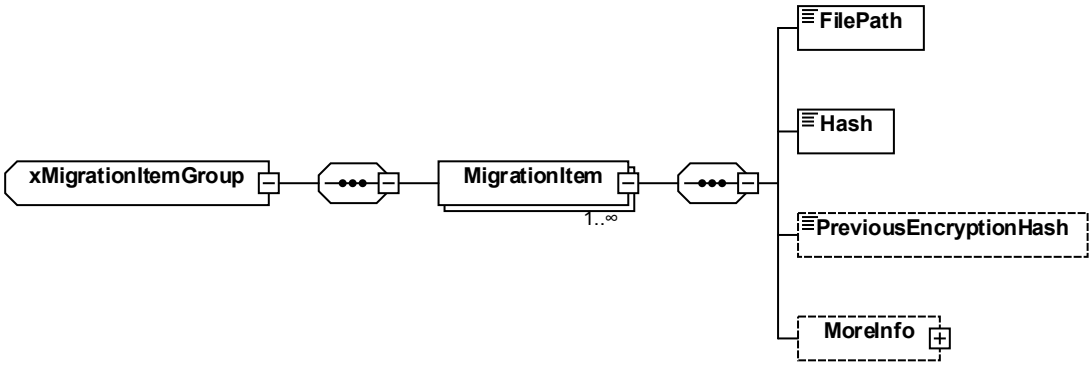
SIP Index Structure



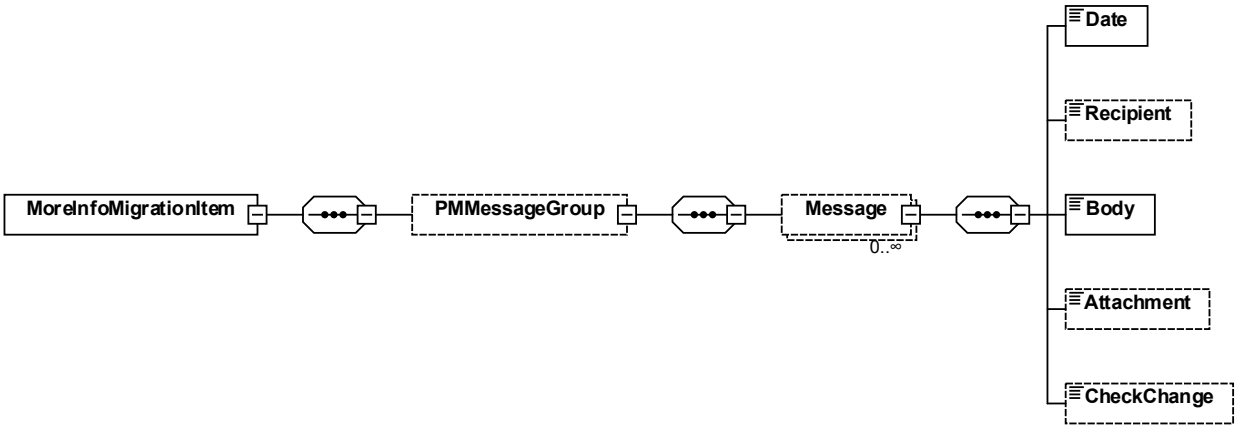
SelfDescription



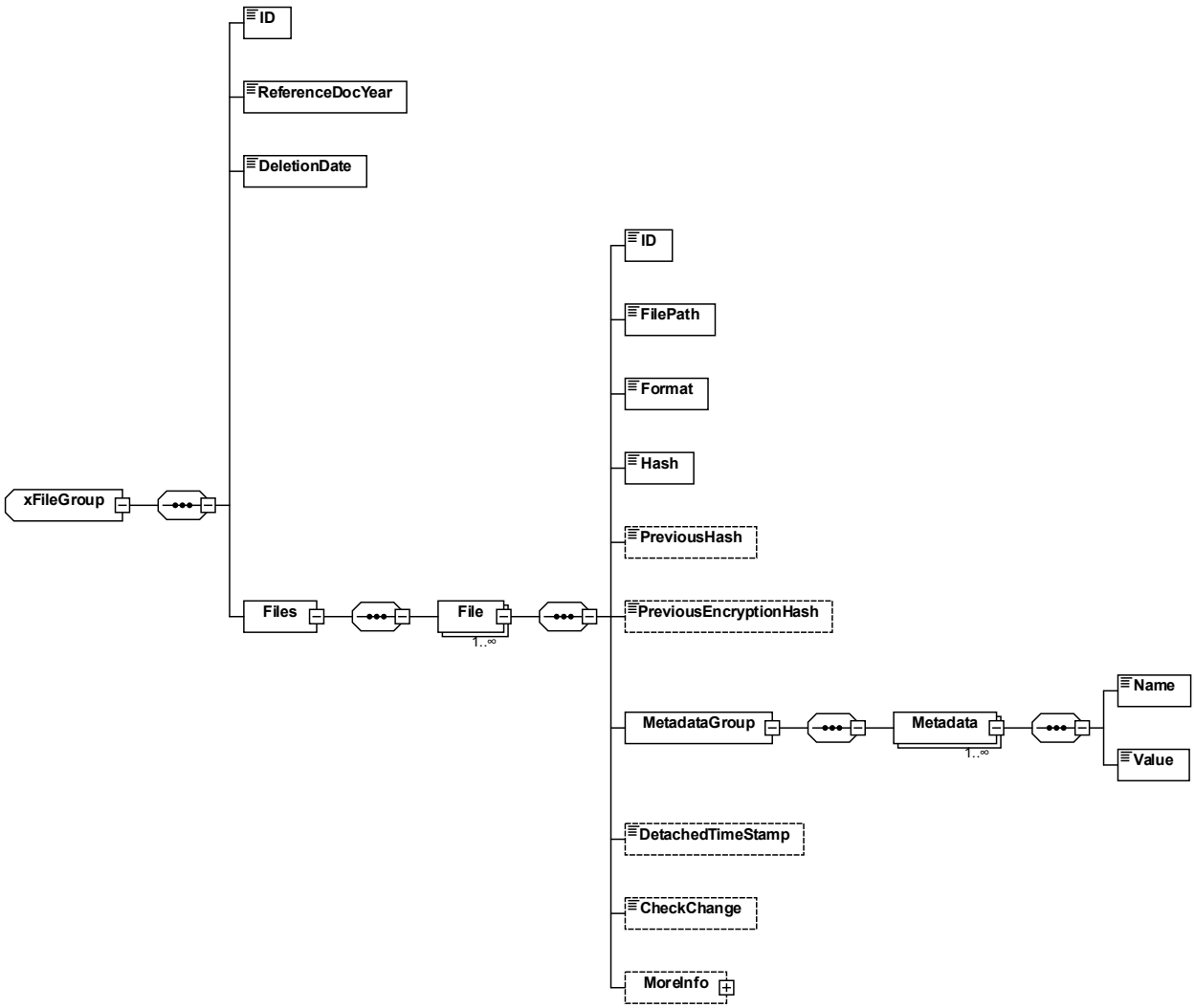
PVolume



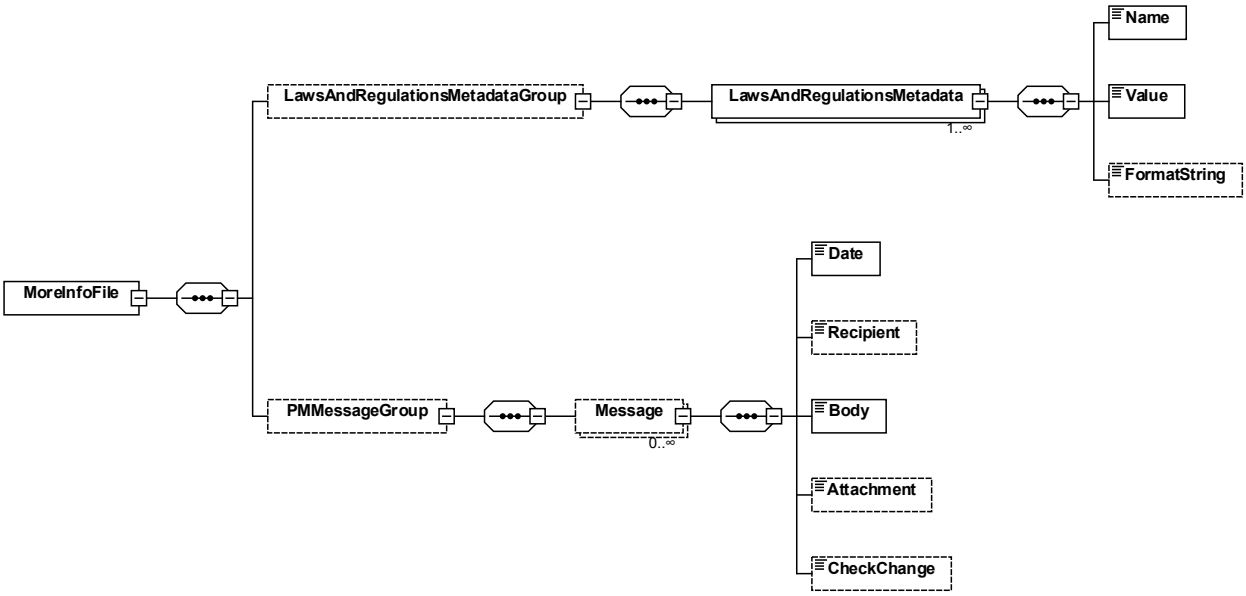
MigrationItem



MoreInfoMigrationItem


ID
ReferenceDocYear
DeletionDate
xFileGroup
Files
File
1..∞
ID
FilePath
Format
Hash
PreviousHash
PreviousEncryptionHash
MetadataGroup
Metadata
1..∞
Name
Value
DetachedTimeStamp
CheckChange
MoreInfo

FileGroup



MoreInfoFile

6.4.1 Pre-pacchetto

In caso di versamento di file non firmati o non 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.

6.4.2 Revision Package

Un pacchetto di revisione consente all'utente o al sistema di aggiornare e aggiungere informazioni a un oggetto precedentemente inviato in conservazione, tramite il versamento al servizio di un nuovo SIP contenente il riferimento univoco (Id) del SIP originario.
Una volta acquisito il nuovo SIP, il servizio crea una nuova evidenza di conservazione – generando un nuovo AIP – che riporta al suo interno un riferimento univoco all'evidenza di conservazione del precedente AIP.
Per poter essere accettato dal sistema, un pacchetto di revisione deve contenere il tipo di modifica richiesta, che può essere:

- Rettifica: intervento volto alla correzione di elementi presenti nel SIP originario;
- Integrazione: intervento volto ad aggiungere informazioni al SIP originario;

- Annotazione: intervento volto ad apporre una registrazione sintetica al contenuto del SIP originario.

L'incremento dei dati (augmentation) rispetto a un'evidenza di conservazione esistente (PIndex AIP) avviene tramite l'utilizzo del Revision Package. Prima dello scadere della validità del certificato di marca temporale apposto sull'indice del AIP, il sistema utilizza tale processo al fine di estendere il periodo di validità di tale evidenza.

Torna al Sommario

6.5 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 dell'AIP (PIndex – Preservation Index) completa delle ulteriori strutture collegate ai diversi elementi "MoreInfo" previsti dallo standard SInCRO (PIndex).

- **SelfDescription (1)***: AIP description.
  - **ID (1)**: AIP unique identifier
  - **CreatingApplication (1)**:
    - **Name (1)**: Name of the application that created the AIP.
    - **Version (1)**: Application version
    - **Producer (1)**: Application producer
  - **MoreInfo (1)**
    - **EmbeddedMetadata (1)**: References of the Company to which the preservation process refers.
      - **MoreInfoSelfDescription (1)**

- **IdSetup (1):** Activation Id of the Company
- **IdCompany (1):** Id of the Company
- **PIndexVersion (1):** Version of the PreservationIndex
- **SystemOID (1):** Unique system identifier
- **EnvironmentId (1)** Name and country of the environment

- **PVolume (1):**
  - **ID (1)**: AIP unique identifier
  - **MoreInfo (1)**
    - **EmbeddedMetadata**
      - **MoreInfoPVolume**
        - **SIPGroup (1)**
          - **SIP (1 -n)**
            - **SIPId (1):** Id of the Submission Information Package to which the AIP refers
            - **Hash (1):** Hash of the SIP
            - **SRId (1):** Id of the Submission Report
            - **SRHash (1):** Hash of the Submission Report
            - **SRCreationDate (1):** Date of generation of the SR
            - **MigrationItemGroup (1-n):** Info about migrated objects (if any)
- **FileGroup (1-n)**:
  - **ID (1)**: Id of the Document type to which the documents refer.
  - **Label (0-1):** Document type name
  - **Description (0-1):** Document type description
  - **File (1-n)**:
    - **ID (1)**: Unique document identifier assigned by the System
    - **Path (1)**: Logical address of the file represented by a URI (locates the file within the storage).
    - **Hash (1)**: Hash function used, and value returned for the object
    - **PreviousHash (0-1)**: Hash function used, and value returned for the object (referring to a previous Preservation Index, if any) **MoreInfo**: info about PIndex XSD schema
      - **EmbeddedMetadata**
        - **MoreInfoFile:** Information about the document in the Preservation System used to identify and describe the document
          - **File (1-n)**
            - **IdDoc**: Unique document identifier assigned by the Producer in the Submission phase
            - **SIPId**: Id of the Submission Information Package
            - **PreviousEncryptionHash**: hash of the unsigned object (only in case of pre-SIP)
            - **MetadataGroup:** list of the metadata associated with the object
              - **Metadata (0-n)**
                - **Name:** Name of the index
                - **Value:** Value of the index
            - **ReferenceDocYear:** Year to which the object refers

- **LawsAndRegulationsMetadata:** metadata required by specific laws or regulations (if any)
- **DeletionDate:** DeletionDate associated to the object

- **MoreInfoFileGroup (1)**
  - **PVolume**
    - **ID (1):** Id of the Document type to which the documents refer
    - **MetadataGroup:** list of the metadata associated with the object
      - **MetadataDefinition (0-n):** description of the structure of the metadata associated with the Document type
        - **Number:** Number of the index
        - **Name:** Name of the index
        - **Required:** Required index (true/false)
        - **RegEx:** RegularExpression
        - **Type:** Type of index (String, date, number, ..)
        - **FormatString:** Format of the string

➢ **Process (1)**

- **Submitter (1):** Information about the entity performing the physical transfer of digital objects into the preservation system.
  - **AgentID:** Submitter identifier
  - **AgentName**
    - **NameAndSurname:** Name and Surname of the Submitter
    - **FormalName:** Formal Name of the Submitter
  - **RelevantDocument (1-n):** Reference to a document from the entity involved in the preservation process that is relevant to understanding the process itself or the digital objects submitted for preservation.
  - **MoreInfo**
    - **EmbeddedMetadata**
      - **MoreInfoSubmitter**

- **Holder (1-n):** Information about the Preservation Object Owner or possessor, or holder of the digital objects transferred to the preservation system.
  - **AgentID:** Holder identifier
  - **AgentName**
    - **NameAndSurname:** Name and Surname of the Holder
    - **FormalName:** Formal Name of the Holder
  - **RelevantDocument (1-n):** Reference to a document from the entity involved in the preservation process that is relevant to understanding the process itself or the digital objects submitted for preservation.
  - **MoreInfo**
    - **EmbeddedMetadata**
    - **MoreInfoHolder**
- **AuthorizedSigner (1-n):** Information about the person authorized to sign with an electronic signature (advanced or qualified) or with an electronic seal (advanced or qualified) the preservation index at the conclusion of the index creation process.
  - **AgentName**
    - **NameAndSurname:** Name and Surname of the **AuthorizedSigner**
    - **FormalName:** Formal Name of the **AuthorizedSigner**

- **RelevantDocument (1-n):** Reference to a document from the entity involved in the preservation process that is relevant to understanding the process itself or the digital objects submitted for preservation.
- **MoreInfo**
  - **EmbeddedMetadata**
  - **MoreInfo AuthorizedSigner**
    - **PreservationAgent**
      - **PreservationJobRole:** Job description related to the subject.
      - **CertificateIdentificationCode:** Identifier of the signing certificate used in closing the Preservation process.
      - **Identifier (0-1):** Subject identifier assigned by the Preservation System

- **TimeReference (1)**
  - **TimeInfo (1):** Date on which the Index file was produced. Corresponds within certain time limits (required by the file signing and time-stamping process) to the date the time stamp was applied.
- **LawAndRegulations (1):** Reference standard for the generation of the PIndex.
- **MoreInfo**
  - **EmbeddedMetadata**
    - **MoreInfoProcess:** Additional information related to the Preservation process.
      - **PreservationAgent**
        - **AgentName (1)**
          - **NameAndSurname**
            - **FirstName:** Name of the Agent
            - **LastName:** Surname of the Agent
        - **PreservationJobRole (1):** Job description related to the subject.
        - **Identifier:** Subject identifier assigned by the Preservation System
      - **ProcessOID:** Preservation profile identifier based on the OAIS standard

*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

6.6 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.
- Il Submission Report (SR)
- Il Signature Report (presente solo qualora la componente del Servizio Qualificato di Conservazione di Firme e Sigilli Elettronici sia attivo)
- 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. Per i termini già precedentemente utilizzati si veda la struttura descrittiva dell'AIP.

- **Summary:** Info related to the DIP
  - **ID:** Identifier of the DIP assigned by the System.
  - **Producer**
    - **Type**
    - **Name**
      - **NameAndSurname**
      - **FormalName**
    - **ID**
    - **IdSetup**
    - **IdCompany**
    - **MoreInfo**
  - **Submitter**
    - **Type**
    - **Name**
      - **NameAndSurname**
      - **FormalName**
    - **ID**
    - **SIPGroup**
    - **MoreInfo**
  - **CreationDate:**
  - **IpAddressClient**
  - **Applicant:** Info related to the subject who requested the dip
    - **Type**
    - **Name**
      - **NameAndSurname**
      - **FormalName**
    - **ID**
    - **MoreInfo**
  - **Subjects:** Info related to the subjects involved in the process of the creation of the DIP
    - **Subject (0-n)**
      - **Type**
      - **Name**
        - **NameAndSurname**
        - **FormalName**
      - **ID**
      - **Role**
      - **MoreInfo**
  - **Antivirus:** Name of the Antivirus software used in the process
  - **LTA:** Info about the LTA System
    - **Name**

        - **Version**
        - **EnvironmentId**
- **AIPGroup:** Info related to the AIPs to which the DIP refers.
    - **AIP (1-n)**
        - **ID**
        - **Hash**
        - **FileUrl**
        - **InfectedFilesCount**
        - **FileGroup**
            - **File (1-n)**
                - **ID**
                - **IdDoc**
                - **PVolume**
                - **ID**
                - **Label**
                - **SIPId**
                - **FileType**
                - **FilePath**
                - **FileUrl**
                - **Hash**
                - **PreviousEncryptionHash**
                - **ReferenceDocYear**
                - **RevisionSIPIdOrigin**
                - **RevisionNumber**
                - **RevisionIsLast**
                - **CheckChange**
                - **VirusName**
                - **MoreInfo**
        - **MoreInfo**

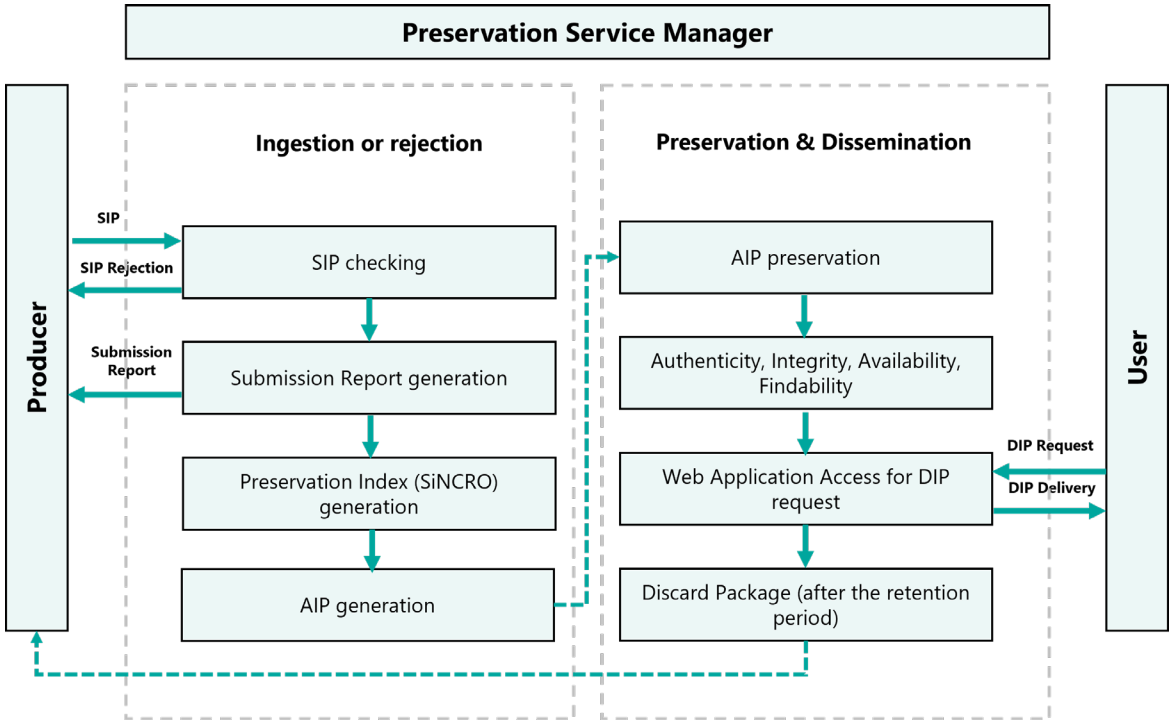
Torna al Sommario

7 IL PROCESSO DI CONSERVAZIONE

Il processo di conservazione è gestito in tutte le sue fasi dal modulo LTA che interagisce con i diversi soggetti 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 Titolare dell'oggetto di 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, garantisce lo svolgersi del corretto processo di conservazione.

Di seguito viene rappresentato il processo di conservazione.



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, 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).
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.

Tutti le attività di presa in carico dei singoli SIP vengono tracciate tramite il sistema di Log Management integrato nel sistema di conservazione.

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 corrispondano agli allegati definiti nell' Indice del SIP.
- **(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.
- **(Bloccante)** Verifica che il numero di Metadati definiti per il documento corrisponda a quelli definiti all'interno della tipologia.
- **(Bloccante)** Verifica che il nome e l'ordine dei Metadati definiti per il documento corrisponda a quanto definito all'interno della tipologia.
- **(Bloccante)** Verifica della presenza del valore per i Metadati obbligatori, seguendo lo schema dei metadati.

- **(Bloccante)** Validazione del valore per i Metadati in base all'eventuale espressione regolare definita, seguendo lo schema dei metadati.
- **(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.
- **(Bloccante)** Verifica della validità della firma sui file firmati.
- **(Bloccante)** Verifica dell'anno di riferimento documento.

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 riferimento temporale.

Torna al Sommario

7.3 Signature Report

Qualora sia attivo il componente del Servizio Qualificato di Conservazione di Firme e Sigilli Elettronici, il servizio effettua un'analisi dedicata ai certificati qualificati, generando un apposito Signature Report, quale esito della verifica delle firme qualificate e/o dei sigilli qualificati. Tale report in formato XML o JSON è firmato digitalmente dal servizio (modello WST) e anche marcato temporalmente (modello WST). Al suo interno vengono riportati i dati riferiti ai certificati qualificati utilizzati per l'apposizione delle firme/sigilli e viene mantenuto insieme alle evidenze di conservazione come elemento di prova. Il Signature Report è recuperabile dall'utente tramite richiesta del Dissemination Information Package (DIP).
Per ulteriori informazioni si rimanda all'Allegato 1 che include la Practice Statement per il servizio Qualificato di Conservazione di Firme e Sigilli Elettronici qualificati.

Torna al Sommario

7.4 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 a cui un Submission Report fa riferimento.

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. Per i termini già precedentemente utilizzati si veda la struttura descrittiva dei pacchetti.

- **Summary:** Info related to the SR
    - **Producer**
        - **Type**
        - **Name**
            - **NameAndSurname**
            - **FormalName**
        - **ID**
        - **IdSetup**
        - **IdCompany**
        - **MoreInfo**

- **PVolume**
  - **ID**
  - **Label**
- **CreationDate**
- **Subjects:** Info related to the subjects involved in the process of the creation of the SR
  - **Subject**
    - **Type**
    - **Name**
      - **NameAndSurname**
      - **FormalName**
    - **ID**
    - **Role**
    - **MoreInfo**
- **LTA:** Info about the LTA System
  - **Name**
  - **Version**
  - **EnvironmentId**

- **SIPGroup:** Info related to the SIPs to which the SR refers.
  - **SIP (1-n)**
    - **ID**
    - **RevisionSIPId**
    - **RevisionSIPIdOrigin**
    - **RevisionNumber**
    - **RevisionSource**
    - **User**
    - **DocumentsCount**
    - **SubmitterIp**
    - **Type**
    - **MigrationItemsCount**
    - **Hash**
    - **DateFormat**
    - **Cancelled**
    - **PMMessageGroup:** Message of the Preservation Manager
      - **Message (1-n)**
        - **Date**
        - **Recipient**
        - **Body**
        - **Attachment**
        - **CheckChange**
    - **FileGroup**
      - **File (1-n)**
        - **IdDoc**
        - **FilePath**
        - **ReferenceDocYear**
        - **PMMessageGroup**
          - **Message (1-n)**
            - **Date**
            - **Recipient**

- **Body**
- **Attachment**
- **CheckChange**

- **CheckChange:** List of checks performed by the System on the SIPs
  - **Check (1-n)**
    - **Description:** Description of the type of check
    - **Result**
    - **Date**
- **MoreInfo**

Inoltre, il Submission Report contiene un 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

7.5 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 corrispondenza tra la tipologia documentale configurata nel Sistema di conservazione e quella dichiarata nell'Indice del SIP;
- 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;
- 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;
- Esito negativo della verifica della presenza dei metadati dichiarati come obbligatori nell'Indice del SIP;
- Esito negativo della verifica dell'eventuale espressione regolare dei metadati dichiarati nell'Indice del SIP;
- 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;
- Esito negativo della verifica di validità della firma digitale in caso di Indice del SIP firmato (opzionale).

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

7.6 Antivirus Report

Nel processo è attiva una specifica funzione di scansione antivirus per gli oggetti inviati al sistema. Questa funzione notifica all'utente le eventuali minacce che si possono nascondere in un SIP inviato. La presenza di eventuali virus non blocca il processo di conservazione, a garanzia del contenuto originario inviato in fase di versamento.

La scansione viene effettuata dopo l'invio e, se viene rilevato un virus, viene prodotto un rapporto antivirus (AR) che presenta una struttura XML basata sul Submission Report.

I rapporti antivirus sono generati da un processo schedulato che considera ogni pacchetto SIP. Dopo l'esecuzione di una scansione, il rapporto viene generato se il pacchetto SIP contiene almeno un virus.

Una scansione antivirus viene eseguita anche quando un utente richiede un DIP.

Torna al Sommario

7.7 Preparazione e gestione dell'Archival Information Package

La generazione dell'Indice dell'AIP avviene secondo le specifiche tecniche di riferimento, in particolare del 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 generazione degli AIP avviene in modo tale da garantire univocità e segregazione dei dati per ogni Titolare a cui viene associata un'azienda. 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

7.8 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.

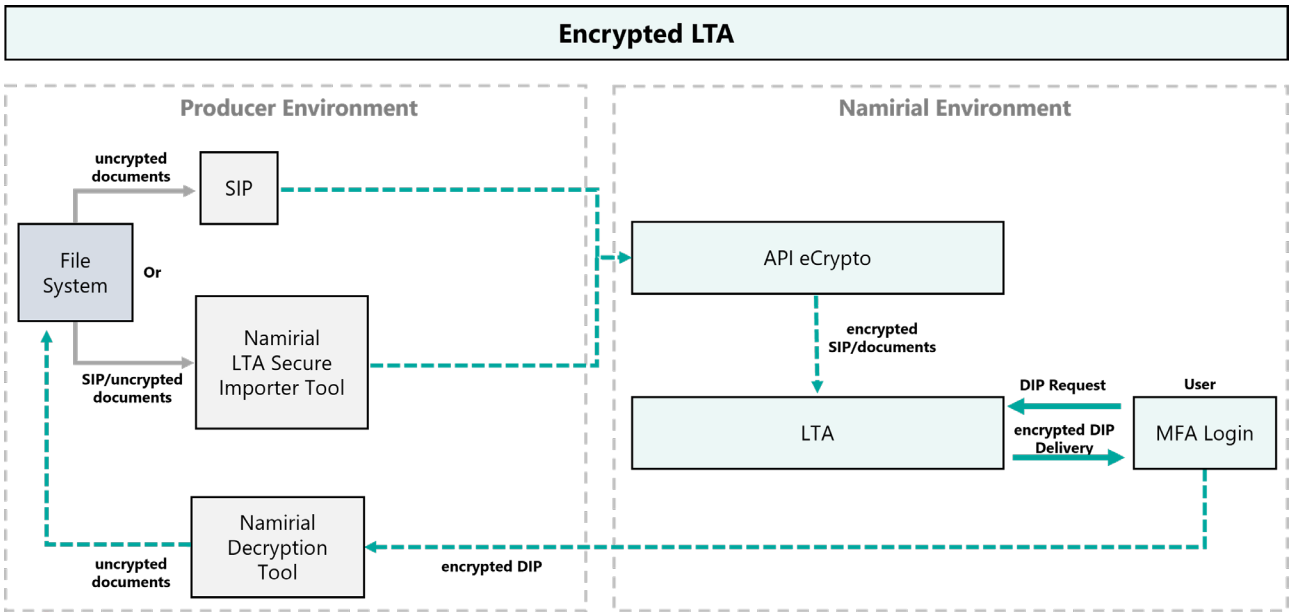
La crittografia lato server protegge i dati at rest. Amazon S3 cifra ogni oggetto con una chiave univoca. Come ulteriore protezione, cifra la chiave stessa con una chiave master che ruota regolarmente. La crittografia lato server di Amazon S3 utilizza una delle crittografie a blocchi più potenti disponibili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

Torna al Sommario

7.9 Gestione di documenti contenenti dati sensibili

In caso di oggetti informatici contenenti dati sensibili che possono necessitare di una securizzazione specifica, 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.



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 solo ai soggetti autenticati tramite la chiave di decriptazione assegnata.

Ogni operazione di accesso e richiesta dei documenti è tracciata tramite log.

Torna al Sommario

7.10 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.

Al Titolare dell'oggetto viene comunicato un apposito indirizzo sicuro di una pagina web dedicata alla restituzione degli oggetti conservati contenuti nei DIP generati. L'interazione dell'utente con la pagina viene tracciata ai fini della registrazione dell'operazione di ricezione. La pagina rimane attiva per consentire all'utente di recuperare gli oggetti e per un tempo indicato a livello contrattuale.

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.

Ogni DIP contiene un Indice del DIP, firmato dal Responsabile del servizio di conservazione, che rappresenta un rapporto della distribuzione eseguita.

Al termine delle operazioni di restituzione e, dopo che il Titolare ha recuperato gli oggetti, viene condivisa una dichiarazione di ricezione approvata dal Titolare per avere conferma dell'effettiva restituzione conclusa positivamente.

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 eventuale corruzione o perdita dei dati.

Torna al Sommario

7.11 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 secondo lo standard SInCRO (UNI 11386).

La sua distribuzione attraverso la richiesta di uno o più DIP 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, tramite DIP, con le modalità concordate tra il Conservatore e il Titolare stesso.

Il sistema è in grado di acquisire oggetti precedentemente conservati nel caso di **subentro/migrazione** di archivi gestiti da altro conservatore.

Torna al Sommario

7.12 Interazioni con il servizio

L'interazione col servizio da parte dell'utente può avvenire tramite integrazione informatica e accesso web tramite interfaccia. Entrambe le modalità consentono di:

- inviare oggetti al servizio;
- verificare l'esito positivo del versamento attraverso la fruizione del Submission Report generato dal servizio;
- ricercare i propri oggetti tramite chiavi univoche (metadati);
- consultare gli oggetti conservati;
- effettuare il download degli oggetti conservati;
- effettuare il download dei Dissemination Information Package (DIP) ai fini dell'esibizione delle evidenze di conservazione.

L'organizzazione di riferimento degli utenti, all'interno del contratto (Richiesta di attivazione o Allegato alla Scheda Servizio), indica i soggetti abilitati ad accedere alla piattaforma (utenti), cui Namirial fornisce delle credenziali univoche. Tali credenziali sono di tipo username e password o basate su un doppio fattore di autenticazione. In caso di necessità di aggiungere nuovi utenti, i soggetti indicati dall'organizzazione in sede contrattuale possono richiedere l'attivazione di nuovi utenti tramite servizio di ticketing tracciato tramite o aggiornamento dell'allegato alla Scheda Servizio. Tali soggetti hanno la facoltà di richiedere anche la revoca delle credenziali. Nel caso dell'interfaccia web, 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 motivi di sicurezza, il servizio disattiva temporaneamente gli utenti di consultazione che sono rimasti inattivi per più di sei mesi. Per riattivare l'utente, è necessario procedere con la procedura di rinnovo della password accessibile dalla pagina di login.

Le attività relative ad accesso, consultazione ed esibizione vengono tracciate tramite il sistema di Log Management integrato nel sistema.

Torna al Sommario

7.13 Scarto (Deletion)

L'eliminazione degli oggetti consiste nell'operazione con cui si pone termine alla conservazione degli stessi, rimuovendoli dal servizio. Tale processo viene avviato:

- al termine del periodo di conservazione degli oggetti;
- su richiesta del cliente per specifici pacchetti/oggetti;
- in caso di disdetta del servizio da parte del cliente.

L'utente ha la facoltà di confermare la proposta di eliminazione; qualora non confermi, ha la facoltà di richiedere l'estensione del periodo di conservazione.

In caso di disdetta, successivamente alla consegna verso l'utente degli oggetti conservati, il sistema procede con la cancellazione.

Tali operazioni vengono gestite in maniera automatica, tramite job e schedulazioni che avviano il processo di verifica del periodo di conservazione, delle proposte di eliminazione, delle autorizzazioni e dell'eliminazione degli oggetti.

Quale esito dell'avvenuta procedura di eliminazione, il servizio genera un Deletion package.

Si elencano di seguito gli oggetti generati durante il processo di scarto (deletion process) e il loro contenuto:

1. Deletion Request:
    - Lista degli AIP associati alla richiesta
    - Soggetto che ha effettuato la richiesta
    - Motivo della richiesta
2. Deletion Provider Report:
    - Lista dei documenti associati alla richiesta generato in formato csv per il Provider e contenente indicazioni minimali relative ai file (id del documento, hash del documento)
    - Indici dei SIP
3. Deletion Producer Report:
    - Lista dei documenti associati alla richiesta generato in formato XML e firmato dal Provider, inviato esclusivamente al Titolare quale attestazione della consistenza degli oggetti da eliminare e contenente indicazioni relative ai file (id del documento, hash del documento, filename, metadati associati ai documenti)
    - Indici dei SIP
4. Deletion Proposal:
    - Deletion Proposal Index
    - Deletion Provider Report
5. Deletion Package:
    - Deletion Proposal Index
    - Deletion Provider Report
    - Deletion Package
    - Eventuali allegati autorizzativi
6. Deletion Report:
    - Notifica dell'avvenuta eliminazione

Il Deletion Package contiene:

- la proposta di eliminazione;
- un report con l'elenco degli oggetti, con indicazioni di codifiche minimali quali traccia degli stessi (Id oggetto, hash), in conformità al trattamento dati;

- l'Indice del Deletion package, contenente – tra le varie informazioni - l'esito dell'accettazione della proposta (*approved* o *rejected*) e l'elenco delle fasi. Tale indice viene sottoscritto digitalmente sia dal Responsabile del Servizio di Conservazione sia dall'utente operatore dello scarto per approvazione.
- eventuali allegati del processo autorizzativo come ad esempio autorizzazioni di enti amministrativi

La cancellazione effettiva degli oggetti conservati viene notificata al Titolare tramite il Deletion report, che attesta la rimozione irreversibile dei documenti dal sistema.

Durante le fasi del processo, il Titolare interagisce con il sistema esclusivamente tramite l'utente operatore dello scarto preventivamente autorizzato all'accesso alla dashboard dedicata, e/o tramite utente tecnico autorizzato.

Tutte le fasi del processo sono tracciate.

7.13.1 Periodo di conservazione

Il periodo di conservazione è la durata in cui il servizio di conservazione conserva gli oggetti. Il periodo di conservazione, nell'ambito del servizio, è definito associando al SIP una data (*deletion date*) che indica il termine di conservazione dopo il quale viene avviato il processo di eliminazione dell'oggetto e delle evidenze associate. Tale data può:

- essere fornita dall'utente nella fase di generazione e invio del SIP;
- associata agli oggetti conservati in maniera automatica dal sistema.

Durante questo periodo, il servizio di conservazione crea e incrementa – qualora necessario - le evidenze di conservazione per raggiungere l'obiettivo di conservazione.

Torna al Sommario

7.14 Utilizzo del Servizio Qualificato di Conservazione di Firme e Sigilli Elettronici

Il servizio LTA del Conservatore Namirial fornisce le evidenze di conservazione per un servizio qualificato di Conservazione di Firme e Sigilli Elettronici Qualificati conforme al TS 119 511 "Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques". Ogni evidenza di conservazione, in conformità allo standard italiano UNI SInCRO, è protetta da una firma elettronica qualificata o da un sigillo e da una marca temporale qualificata per garantire l'integrità dell'evidenza.

Il servizio Qualificato di Conservazione di Firme e Sigilli Elettronici è un Servizio Fiduciario Qualificato conforme agli Articoli 34 e 40 del Regolamento eIDAS. La conformità di Namirial come fornitore di detto Servizio Fiduciario Qualificato e del Servizio Fiduciario Qualificato prestato ai requisiti eIDAS è confermata dall'audit di un Organismo di Valutazione della Conformità accreditato e dalla supervisione di AGID, l'organismo di vigilanza italiano, come stabilito dal regolamento eIDAS per i servizi fiduciari qualificati. Ciò supporta

l'affidabilità del servizio LTA e la sua conformità ai requisiti di un servizio fiduciario di archiviazione elettronica secondo il Regolamento (UE) 2024/1183.

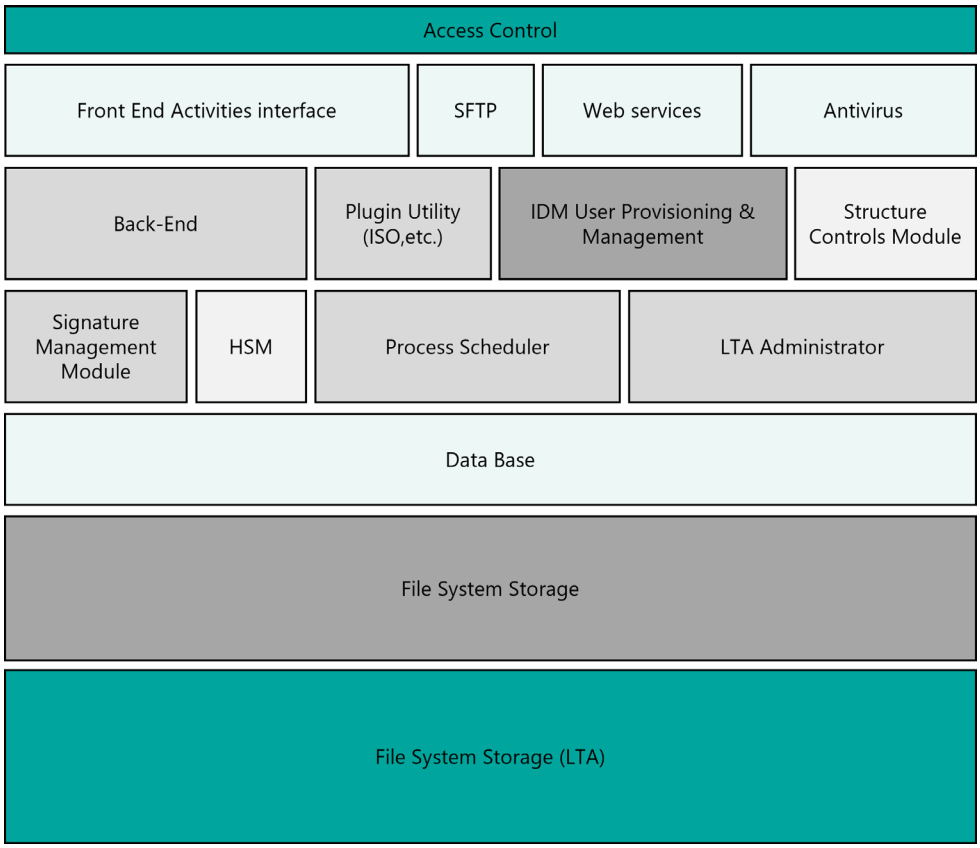
L'Allegato 1 include la Practice Statement per il servizio Qualificato di Conservazione di Firme e Sigilli Elettronici qualificati.

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 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.



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 dei SIP.
- Antivirus.
- Modulo di back-end per tutte le attività di interfacciamento 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;
    - Deletion process
- 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:

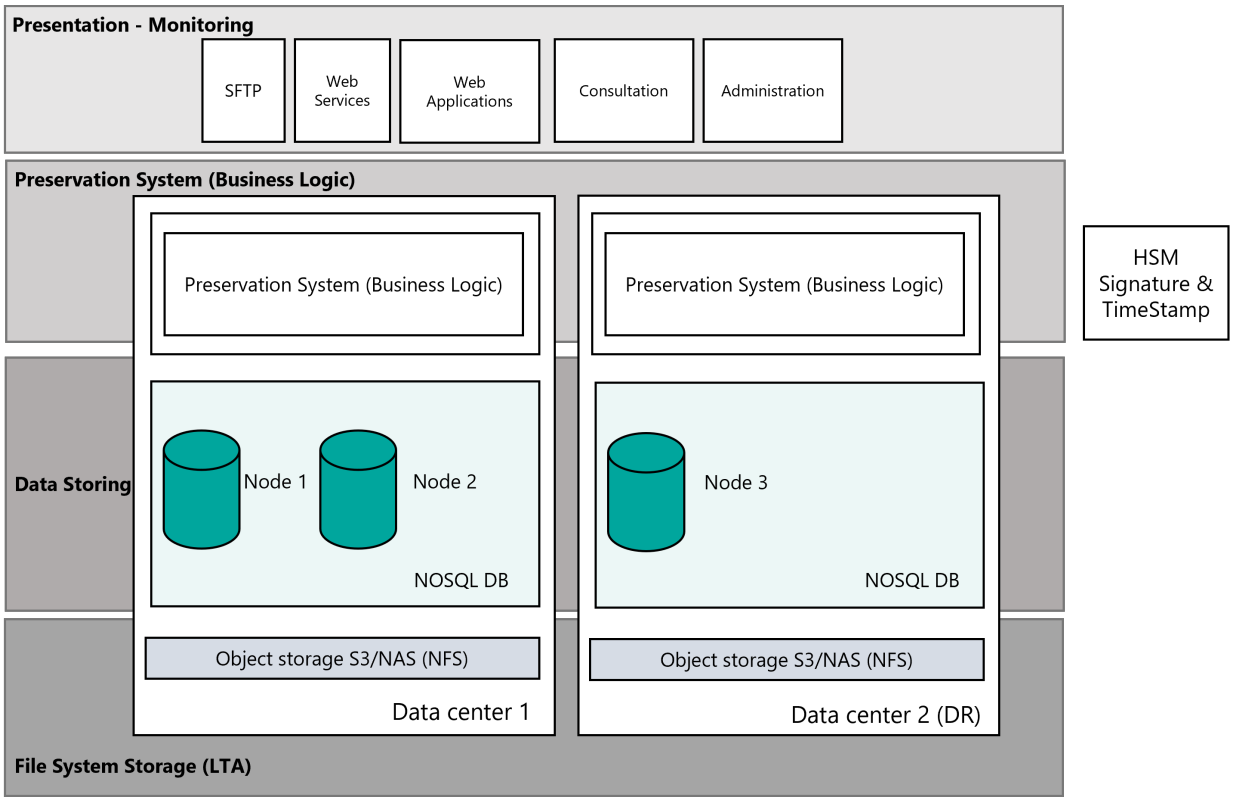
- Identificazione del soggetto logico/fisico che compie l'attività;
- Controllo e gestione dell'attività stessa;
- Espandibilità del modulo (bilanciamento del carico dell'attività, ripartizione e crescita clusterizzabile sulle risorse a disposizione).

Tutte le attività dei moduli sono tracciate nel sistema di Log Management System.

Torna al Sommario

8.1 Componenti Logiche

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



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 tipologie 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, Deletion 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 gli AIP.

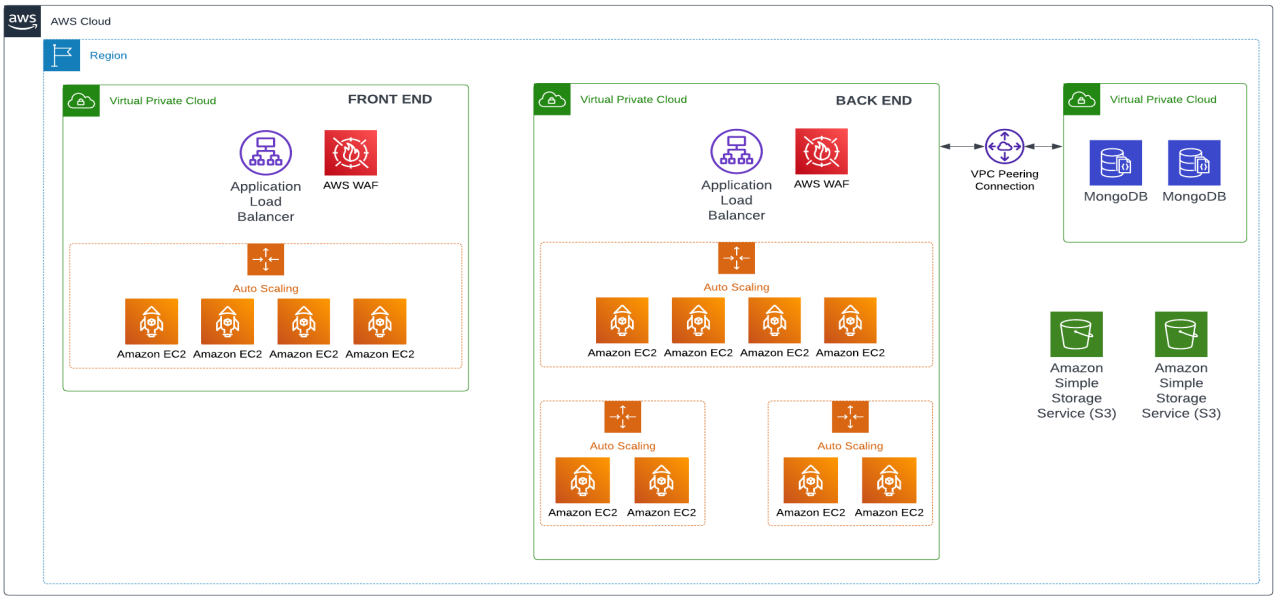
Dalla struttura di erogazione del servizio (struttura primaria), è previsto un collegamento diretto, cifrato e privato, verso la struttura di Disaster Recovery. Tale struttura è logicamente suddivisa, come la struttura primaria.

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:



Rappresentazione del servizio AWS

- 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 dall'Head of Cloud Ops.

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/IEC 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 circoscrivere 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.

L'intervallo massimo tra due controlli (configurazione dei sistemi TSP) viene eseguito ogni 24 ore.

8.3.1 Italia

Il Sistema di Conservazione e Conservazione di firme e sigilli elettronici qualificati fornisce servizi su data center AWS:

- Sito Primario: AWS Italian Region (Milan)
- Sito Disaster Recovery AWS Region EU-central-1 Frankfurt

8.3.2 Francia

Il Sistema di Conservazione e Conservazione di firme e sigilli elettronici qualificati fornisce servizi su data center AWS:

- Sito Primario: AWS French Region (Paris)
- Sito Disaster Recovery AWS Region EU-central-1 Frankfurt

Il Sistema di Conservazione e Conservazione di firme e sigilli elettronici qualificati fornisce servizi anche su data center OutScale nella Region cloudgouv-eu-west-1, così ridondata:

- SEC1 (Pantin, France)
- SEC2 (Magny-les-Hameaux, France)
- SEC3 (Aubergenville, France)

8.3.3 Spagna

Il Sistema di Conservazione e Conservazione di firme e sigilli elettronici qualificati fornisce servizi su data center AWS:

- Sito Primario: AWS Spanish Region (Aragon);
- Sito Disaster Recovery AWS Region EU-central-1 Frankfurt.

8.3.4 Romania

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

- Sito primario, situato nel datacenter di GTS Telecom SRL (Bucarest)
- Sito Disaster Recovery, situato nel datacenter di GTS Telecom SRL (Cluji)

8.3.5 LATAM

Il Sistema di Conservazione fornisce servizi su data center AWS:

- Sito Primario: AWS South America Region (Sao Paolo);
- Sito Disaster Recovery AWS US East (Northern Virginia) Region

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 Log

Gli eventi generati dal Sistema di conservazione durante le fasi del processo producono dei log al fine di tracciare le diverse operazioni generate dal servizio durante i processi automatici e di interazione con l'utente e facilitare la diagnosi di eventuali anomalie e/o incident.

Ogni log riporta un riferimento temporale e la descrizione che consente di individuarne la natura e l'origine.

Tali file vengono mantenuti e conservati dal sistema.

La natura dei dati tracciati, i tipi di log, le modalità di invio in conservazione, sono dettagliate nel documento interno Piano della Sicurezza del servizio.

8.5.3 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.

8.5.4 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 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.

8.5.5 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 Long Term Archiving (LTA) al Piano della Sicurezza.

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:

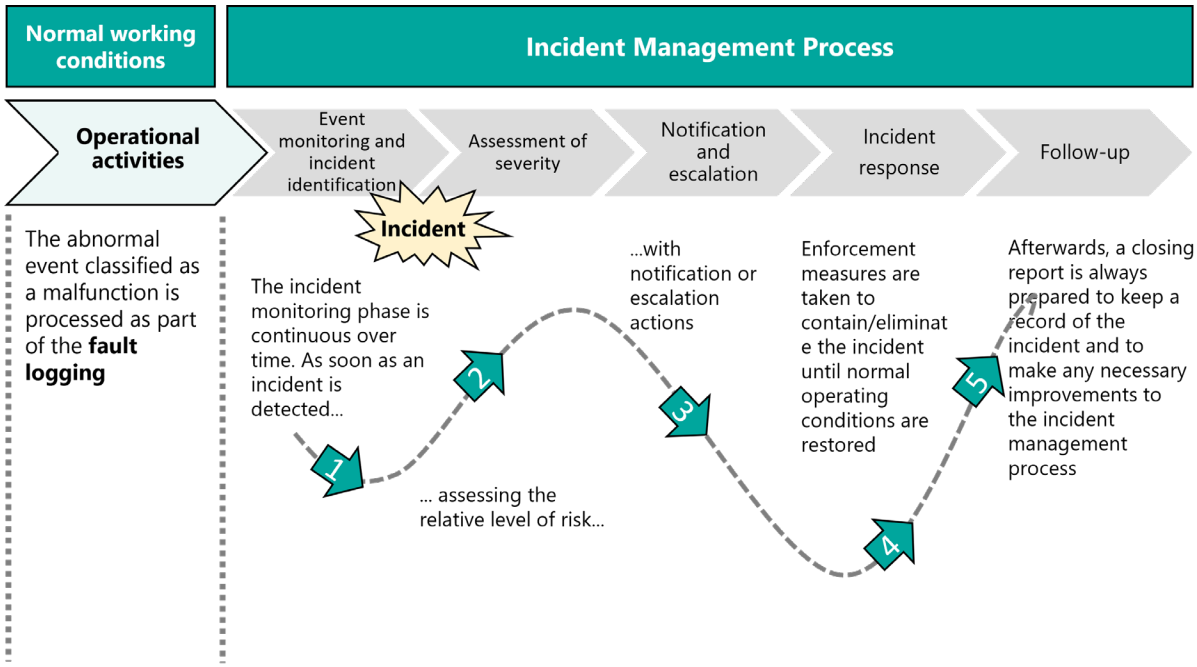
- idonei strumenti di rilevazione;
- sistemi formalizzati di reazione agli eventi inattesi, riconosciuti come incidenti;
- adeguati processi di comunicazione;
- efficienti contromisure di sicurezza e di ripristino delle funzionalità del Sistema di conservazione o in caso di perdita dei dati.

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.



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 ALLEGATI

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***
Allegato 1.	Namirial - Policy e Practice Statement del Servizio qualificato di conservazione di firme elettroniche qualificate e sigilli elettronici qualificati (Qpres)	Documento pubblico
Allegato 2.	Namirial – LTA e Qpres - Piano della Sicurezza	Documento interno
Allegato 3.	Namirial - LTA e Qpres - Piano di Cessazione	Documento interno
Allegato 4.	Namirial - LTA e Qpres - Risk Assessment	Documento interno

Torna al Sommario