



Manuale del Conservatore

di Namirial S.p.A.



EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	02/08/2021	Enrico Giunta	Responsabile della funzione archivistica di conservazione
Verifica	04/08/2021	Davide Coletto	Responsabile del servizio di conservazione
Approvazione	04/08/2021	Massimiliano Pellegrini	Legale rappresentante

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Descrizione	Osservazioni
1.0	28/11/2014	Prima emissione del documento secondo lo schema del manuale AgID per l'accreditamento	Prima versione secondo il modello dell'Agenzia per l'Italia Digitale (AgID)
2.0	22/01/2015	Nuova emissione per revisioni	Variazioni ai paragrafi 2.1, 6.1, 6.2, 6.3, 7.1, 7.2, 7.4 e 7.6
3.0	05/02/2015	Integrazione del manuale per l'accreditamento	Variazioni ai paragrafi 2.1, 6.2, 7, 7.3, 7.4 e 7.6
4.0	22/02/2016	Revisioni varie in tutti i capitoli del manuale	Variazioni in tutti i capitoli
5.0	26/09/2016	Revisione della topologia dei siti di erogazione del servizio, revisione dell'organigramma	Variazioni ai paragrafi 5.1, 8.3
6.0	26/10/2017	Revisioni varie in tutti i capitoli del manuale. In particolare: revisione della topologia dei siti di erogazione del servizio; ristrutturazione e riformulazione dei contenuti; aggiornamento delle specifiche tecniche rispetto all'ultima versione del documento Strongdox SDK	Variazione in tutti i capitoli
6.1	11/10/2018	Aggiornamento glossario e normativa di riferimento; revisione dell'organigramma; aggiornamento tabella dei formati	Variazioni ai paragrafi 2.1, 3.1, 5.1, 6.1



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



Indice del documento

Indice del documento.....	4
1 SCOPO E AMBITO DEL DOCUMENTO	6
2 TERMINOLOGIA	8
2.1 Glossario	8
2.2 Acronimi.....	16
3 NORMATIVA E STANDARD DI RIFERIMENTO.....	17
3.1 Normativa di riferimento	17
3.2 Standard di riferimento	18
4 RUOLI E RESPONSABILITÀ.....	19
5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE.....	27
5.1 Organigramma.....	27
5.2 Strutture organizzative.....	29
6 OGGETTI SOTTOPOSTI A CONSERVAZIONE.....	33
6.1 Oggetti conservati	34
6.2 Formati	35
6.2.1 Valutazione ed indice di interoperabilità	37
6.3 Pacchetto di Versamento.....	38
6.4 Pacchetto di Archiviazione	43
6.5 Pacchetto di Distribuzione	50
7 IL PROCESSO DI CONSERVAZIONE.....	54
7.1 Modalità di acquisizione dei Pacchetti di Versamento per la loro presa in carico	55
7.2 Verifiche effettuate sui Pacchetti di Versamento e sugli oggetti in essi contenuti	56
7.3 Accettazione dei Pacchetti di Versamento e generazione del Rapporto di Versamento	58
7.4 Rifiuto dei Pacchetti di Versamento e modalità di comunicazione delle anomalie	61
7.5 Preparazione e gestione del Pacchetto di Archiviazione	63
7.6 Cifratura degli oggetti di conservazione	64
7.7 Preparazione e gestione del Pacchetto di Distribuzione ai fini dell'esibizione	64
7.8 Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti.....	64
7.9 Scarto dei Pacchetti di Archiviazione	65
7.10 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori	66



8	IL SISTEMA DI CONSERVAZIONE.....	67
8.1	Componenti Logiche	69
8.2	Componenti Tecnologiche	70
8.3	Componenti Fisiche.....	71
8.4	Procedure di gestione e di evoluzione.....	72
8.4.1	Conduzione e manutenzione del Sistema di conservazione.....	72
8.4.2	Gestione e mantenimento dei log	73
8.4.3	Monitoraggio del Sistema di conservazione.....	73
8.4.4	Change management.....	74
8.4.5	Verifica periodica di conformità a normativa e standard di riferimento	74
8.4.6	Gestione della sicurezza e valutazione del rischio.....	75
9	MONITORAGGIO E CONTROLLI	75
9.1	Procedure di monitoraggio.....	75
9.2	Verifica dell'integrità degli archivi	77
9.3	Soluzioni adottate in caso di anomalie	77



1 SCOPO E AMBITO DEL DOCUMENTO

Il presente documento rappresenta il Manuale del Conservatore relativo al servizio Strongdox, erogato e gestito da Namirial S.p.A., ed è adottato secondo le Linee Guida sulla formazione, gestione e conservazione dei documenti informatici emanate da AgID.

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 della conservazione e dal Conservatore in materia di gestione della sicurezza del servizio, dei documenti e delle informazioni trattate nel Sistema di conservazione.

Il presente documento è stato redatto secondo i seguenti principi:

- **Principio di Conformità:** il manuale mira a descrivere un sistema e un processo di conservazione secondo le disposizioni normative vigenti nel tempo;
- **Principio di Trasparenza:** il manuale mira a fornire una chiara spiegazione del Sistema di conservazione documentale e dei processi effettivamente erogati;
- **Ottica di Processo:** il documento mira a descrivere le fasi del processo di conservazione secondo le regole tecniche e il modello di riferimento 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 al modello di riferimento OAIS (Open Archival Information System) standard ISO 14721;
- **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 Soggetto produttore 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, 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. Successivamente, ogni variazione del Servizio su indicazione del Cliente, comporta la necessità di aggiornare la Scheda Servizio.
Richiesta di attivazione (opzionale)	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 e gli eventuali ulteriori documenti rilasciati quali "specifiche forniture del servizio di conservazione" sono custoditi presso la sede del Conservatore Namirial. Il 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 del Conservatore, depositato presso l'Agenzia per l'Italia Digitale, 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]	Accreditamento	Riconoscimento, da parte dell'Agenzia per l'Italia digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza, ad un soggetto pubblico o privato che svolge attività di conservazione o di certificazione del processo di dichiarazione
[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]	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
[6]	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
[7]	Archivio informatico	Archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico
[8]	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
[9]	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
[10]	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
[11]	Base di dati	Collezione di dati correlati e registrati tra loro



N.	Termini	Descrizione
[12]	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)
[13]	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
[14]	Chiave privata	L'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico
[15]	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
[16]	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
[17]	Comunità di riferimento	Un gruppo ben individuato di potenziali Utenti che dovrebbero essere in grado di comprendere l'informazione conservata. Una comunità di riferimento può essere composta anche da più comunità di Utenti
[18]	Conservatore accreditato	Soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
[19]	Conservazione	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 e descritto nel Manuale di conservazione
[20]	Copia analogica del documento informatico	Documento analogico avente contenuto identico a quello del documento informatico da cui è tratto
[21]	Copia di sicurezza	Copia di backup degli archivi del Sistema di conservazione
[22]	Copia informatica di documento analogico	Il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto
[23]	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



N.	Termini	Descrizione
[24]	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
[25]	Destinatario	Identifica il soggetto/sistema al quale il documento informatico è indirizzato
[26]	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
[27]	Documento analogico	La rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti
[28]	Documento informatico	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
[29]	Duplicato informatico	Documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario
[30]	Esibizione	Operazione che consente di visualizzare un documento conservato e di ottenerne copia
[31]	Evidenza informatica	Una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica
[32]	Fascicolo informatico	Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'art. 41 del CAD
[33]	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
[34]	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
[35]	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



N.	Termini	Descrizione
[36]	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
[37]	Formato	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
[38]	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
[39]	FTP Server	Programma che permette di accettare connessioni in entrata e di comunicare in maniera sicura con un Client attraverso il protocollo FTP
[40]	Funzioni archivistiche	Funzioni per la conservazione delle informazioni (acquisizione, archiviazione, gestione dei dati, accesso, distribuzione)
[41]	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
[42]	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
[43]	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
[44]	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
[45]	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



N.	Termini	Descrizione
[46]	Impronta	La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash
[47]	Indice del Pacchetto di Archiviazione	Struttura dell'insieme dei dati a supporto del processo di conservazione, riferita allo standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386)
[48]	Indice del Pacchetto di Versamento	Struttura dell'insieme dei dati a supporto del processo di versamento del Pacchetto di Versamento (PdV), ispirata allo standard internazionale OAIS ISO 14721 e definita nello specifico dal Conservatore in accordo con il Produttore dei documenti
[49]	Indice del Pacchetto di Distribuzione	Struttura dell'insieme dei dati a supporto del processo di distribuzione del Pacchetto di Distribuzione (PdD), ispirata allo standard internazionale OAIS ISO 14721 e definita nello specifico dal Conservatore in accordo con il Produttore dei documenti
[50]	Insieme minimo di metadati del documento informatico	Complesso dei metadati, la cui struttura è descritta nell'allegato 5 delle Linee Guida, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta
[51]	Integrità	Insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo e inalterato
[52]	Interoperabilità	Capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi
[53]	Leggibilità	Insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti
[54]	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
[55a]	Manuale del Conservatore	È il documento analitico, relativo al Sistema di conservazione, redatto dal Conservatore e pubblicato nella sua versione più aggiornata sul sito dell'Agenzia per l'Italia Digitale (in sigla "AgID"), nel quale sono dettagliate le specifiche procedure relative al Servizio, oltre alle politiche generali del Sistema di conservazione dei Documenti informatici.
[55b]	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



N.	Termini	Descrizione
		il contenuto del Manuale del Conservatore, e rinviare, per le parti di competenza, allo stesso.
[56]	Memorizzazione	Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici
[57]	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
[58]	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
[59]	Pacchetto di Archiviazione	Pacchetto informativo composto dalla trasformazione di uno o più Pacchetti di Versamento secondo le specifiche contenute nelle Linee Guida e secondo le modalità riportate nel Manuale del Conservatore
[60]	Pacchetto di Distribuzione	Pacchetto informativo inviato dal Sistema di conservazione all'Utente in risposta ad una sua richiesta
[61]	Pacchetto di Versamento	Pacchetto informativo inviato dal Produttore al Sistema di conservazione secondo un formato predefinito e concordato descritto nel Manuale del Conservatore
[62]	Pacchetto di Scarto	Pacchetto contenente i documenti da scartare dal Sistema di conservazione perché hanno raggiunto il loro termine temporale di conservazione
[63]	Pacchetto informativo	Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare
[64]	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
[65]	Presa in carico	Accettazione da parte del Sistema di conservazione di un Pacchetto di Versamento in quanto conforme alle modalità previste dal Manuale del Conservatore
[66]	Processo di conservazione	Insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 9 delle regole tecniche sul Sistema di conservazione
[67]	Produttore	È il responsabile della generazione del Pacchetto di Versamento e della relativa trasmissione al Conservatore. Nelle pubbliche



N.	Termini	Descrizione
		amministrazioni, tale figura si identifica con il responsabile della gestione documentale
[68]	Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del Sistema di conservazione dei Pacchetti di Versamento inviati dal Produttore
[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 trattamento	Soggetto esterno a cui è affidato il processo di conservazione che assume il ruolo di responsabile del trattamento dei dati, così come previsto dal GDPR e dal Codice in materia di protezione dei dati personali
[71]	Responsabile del servizio di conservazione	Soggetto persona fisica nominato Responsabile del servizio di conservazione <i>Strongdox</i> di Namirial con l'assegnazione delle attività indicate nel documento dell'Agenzia per l'Italia Digitale sui profili professionali richiamati dalla Circolare n. 65/2014 (G.U. n. 89 del 16/04/2014)
[72]	Responsabile della funzione archivistica di conservazione	Soggetto persona fisica nominato responsabile della funzione archivistica di conservazione <i>Strongdox</i> di Namirial con l'assegnazione delle attività indicate nel documento dell'Agenzia per l'Italia Digitale sui profili professionali richiamati dalla Circolare n. 65/2014 (G.U. n. 89 del 16/04/2014)
[73]	Responsabile del trattamento dei dati personali	Soggetto persona fisica nominato responsabile del trattamento dei dati personali del servizio di conservazione <i>Strongdox</i> di Namirial con l'assegnazione delle attività indicate nel documento dell'Agenzia per l'Italia Digitale sui profili professionali richiamati dalla Circolare n. 65/2014 (G.U. n. 89 del 16/04/2014)
[74]	Responsabile della sicurezza dei sistemi per la conservazione	Soggetto persona fisica nominato responsabile della sicurezza dei sistemi per la conservazione <i>Strongdox</i> di Namirial con l'assegnazione delle attività indicate nel documento dell'Agenzia per l'Italia Digitale sui profili professionali richiamati dalla Circolare n. 65/2014 (G.U. n. 89 del 16/04/2014)
[75]	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



N.	Termini	Descrizione
[76]	Scarto	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale
[77]	Service Level Agreement	È l'accordo tra Titolare dell'oggetto di conservazione, Produttore, Responsabile della conservazione e Conservatore sui livelli servizio da garantire
[78]	Sessione di distribuzione	Sessione telematica per la consegna (distribuzione) di uno o più Pacchetti di Distribuzione dal Conservatore al Titolare, sulla base di un modello-dati per i formati e i contenuti definito e concordato tra le parti
[79]	Sessione di ricerca	Una sessione telematica avviata da un Utente di un Sistema di conservazione, durante la quale l'Utente usa gli Strumenti di Ricerca del sistema per individuare e consultare gli oggetti digitali in esso presenti
[80]	Sessione di versamento	Sessione telematica per la consegna (versamento) di uno o più Pacchetti di Versamento dal Produttore al Conservatore, sulla base di un modello-dati per i formati e i contenuti definito e concordato tra le parti
[81]	Sistema di conservazione	Sistema di conservazione dei documenti informatici di cui all'art. 44 del CAD
[82]	Titolare di firma	La persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica
[83]	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
[84]	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
[85]	Versamento agli archivi di stato	Operazione con cui il Responsabile della conservazione di un organo giudiziario o amministrativo dello Stato effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali

[Torna al Sommario](#)



2.2 Acronimi

N.	Acronimi	Descrizione
[1]	AE	Agenzia delle Entrate
[2]	AgID	Agenzia per l'Italia Digitale (già DigitPA e CNIPA)
[3]	CAD	Codice dell'Amministrazione Digitale
[4]	CNIPA	Centro Nazionale per l'Informatica della Pubblica Amministrazione, ora AgID
[5]	FTP	File Transfer Protocol
[6]	IDM	Identity Management
[7]	IPA	Indice delle Pubbliche Amministrazioni
[8]	IPdA	Indice del Pacchetto di Archiviazione
[9]	IPdD	Indice del Pacchetto di Distribuzione (o Rapporto di distribuzione)
[10]	IPdV	Indice del Pacchetto di Versamento
[11]	ISO	International Organization for Standardization
[12]	OAIS	Open Archival Information System, ISO 14721
[13]	PdD	Pacchetto di Distribuzione
[14]	PdS	Pacchetto di Scarto
[13]	PdV	Pacchetto di Versamento
[14]	RdV	Rapporto di Versamento
[15]	SdC	Sistema di Conservazione
[16]	SdI	Sistema d'Interscambio per la fatturazione elettronica per lo scambio delle fatture e delle relative notifiche/ricevute
[17]	SFTP	Protocollo di rete che prevede il trasferimento sicuro dei dati
[18]	SGSI	Sistema di Gestione della Sicurezza delle Informazioni
[19]	SLA	Service Level Agreement
[20]	SOC	Security Operations Center
[21]	TSA	Time Stamping Authority

[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, ordinata secondo il criterio della gerarchia delle fonti:

- **Regolamento del Parlamento europeo e del Consiglio del 27 aprile 2016, n. 679 cd. GDPR** – Regolamento relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
- **Regolamento del Parlamento europeo e del Consiglio 23 luglio 2014, n. 910 cd. eIDAS** – Regolamento in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
- **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, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;
- **AgID, Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, 2020**
- **Circolare AGID 10 aprile 2014, n. 65** - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82;

– [Torna al Sommario](#)



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 14721 OAIS** (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- **ISO/IEC 27001**, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- **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
- **ETSI TS 101 533-1 V1.3.1** Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- **ETSI TR 101 533-2 V1.3.1** Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- **UNI 11386 Standard SinCRO** - Supporto all' Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- **ISO 15836** Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core;
- **ISO 15489-1** Information and documentation - Records management - Part 1: Concepts and principles.

[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 Sistema di conservazione *Strongdox*, gestito dal Conservatore Namirial S.p.A., è basato su un modello organizzativo di riferimento 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 nel documento "Profili professionali" pubblicato da AgID sul proprio sito istituzionale.

Si precisa che il nominativo e i riferimenti del Responsabile della conservazione sono indicati nella Scheda Servizio o, qualora prevista, nella Richiesta di attivazione. Nella Scheda Servizio sono anche riportate le attività affidate al Responsabile del servizio di conservazione.

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo	Eventuali deleghe
Responsabile del servizio di conservazione	Davide Coletto	<ul style="list-style-type: none">- 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	
Responsabile del servizio di conservazione	Luca Romagnoli	<ul style="list-style-type: none">- definizione e attuazione delle politiche complessive del Sistema di conservazione, nonché del governo della gestione del Sistema di conservazione;	Dal 24 novembre 2014 al 22 gennaio 2015	



		<ul style="list-style-type: none">- 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.	
Responsabile della sicurezza dei sistemi per la conservazione	Mario Veltini	<ul style="list-style-type: none">- rispetto e monitoraggio dei requisiti di sicurezza del Sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza;- segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.	Dal 5 luglio 2021
Responsabile della sicurezza dei sistemi per la conservazione	Davide Coletto (interim)	<ul style="list-style-type: none">- rispetto e monitoraggio dei requisiti di sicurezza del Sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza;- segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.	Dal 20 luglio 2018
Responsabile della sicurezza dei sistemi per la conservazione	Andrea Lazzari	<ul style="list-style-type: none">- rispetto e monitoraggio dei requisiti di sicurezza del Sistema di conservazione stabiliti dagli standard, dalle normative e dalle	Dal 24 novembre 2014 al 20 luglio 2018



		<p>politiche e procedure interne di sicurezza;</p> <ul style="list-style-type: none">- segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.	
Responsabile della funzione archivistica di conservazione	Enrico Giunta	<ul style="list-style-type: none">- definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte del Produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato;- definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici;- monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del Sistema di conservazione;- collaborazione con il Produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.	Dal 26 maggio 2021
Responsabile della funzione archivistica di conservazione	Valeria Mocchi	<ul style="list-style-type: none">- 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;	Dal 24 ottobre 2016 al 14 aprile 2021



		<ul style="list-style-type: none">- 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.	
Responsabile della funzione archivistica di conservazione	Matteo Sisti	<ul style="list-style-type: none">- 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 24 novembre 2014 al 24 ottobre 2016
Delegato alla funzione archivistica di conservazione	Enrico Giunta	<ul style="list-style-type: none">- definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte del Produttore, di acquisizione,	Dal 20 aprile 2020 al 25 maggio 2021



		<p>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;</p> <ul style="list-style-type: none">- 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.	
Responsabile del trattamento dei dati personali	Serena Donegani	<ul style="list-style-type: none">- garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali;- garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.	Dal 20 luglio 2018
Responsabile del trattamento dei dati personali	Luca Romagnoli	<ul style="list-style-type: none">- garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali;- garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.	Dal 24 novembre 2014 al 20 luglio 2018
Responsabile dei sistemi informativi per	Mario Veltini	<ul style="list-style-type: none">- gestione dell'esercizio delle componenti hardware e software del Sistema di conservazione;	Dal 5 luglio 2021



la conservazione	<ul style="list-style-type: none">- 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.	
Responsabile dei sistemi informativi per la conservazione	Genesio Di Sabatino <ul style="list-style-type: none">- gestione dell'esercizio delle componenti hardware e software del Sistema di conservazione;- monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con 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.	Dal 24 ottobre 2016
Responsabile dei sistemi informativi per la conservazione	Giuseppe Benedetti <ul style="list-style-type: none">- gestione dell'esercizio delle componenti hardware e software del Sistema di conservazione;- monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con il Soggetto produttore;	Dal 24 novembre 2014 al 24 ottobre 2016



		<ul style="list-style-type: none">- 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.	
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Fabio Didonè	<ul style="list-style-type: none">- coordinamento dello sviluppo e manutenzione delle componenti hardware e software del Sistema di conservazione;- pianificazione e monitoraggio dei progetti di sviluppo del Sistema di conservazione;- monitoraggio degli SLA relativi alla manutenzione del Sistema di conservazione;- interfaccia con il Produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche;- gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.	Dal 5 luglio 2021
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Davide Coletto (interim)	<ul style="list-style-type: none">- coordinamento dello sviluppo e manutenzione delle componenti hardware e software del Sistema di conservazione;	Dal 24 ottobre 2016



		<ul style="list-style-type: none">- pianificazione e monitoraggio dei progetti di sviluppo del Sistema di conservazione;- monitoraggio degli SLA relativi alla manutenzione del Sistema di conservazione;- interfaccia con il Produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche;- gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.	
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Gianluca Cigliano	<ul style="list-style-type: none">- coordinamento dello sviluppo e manutenzione delle componenti hardware e software del Sistema di conservazione;- pianificazione e monitoraggio dei progetti di sviluppo del Sistema di conservazione;- monitoraggio degli SLA relativi alla manutenzione del Sistema di conservazione;- interfaccia con il Produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche;- gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.	Dal 24 novembre 2014 al 24 ottobre 2016

[Torna al Sommario](#)



5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Organigramma

Struttura organizzativa Namirial coinvolta nel servizio di conservazione	Funzioni/macro attività organizzative correlate al servizio in oggetto	Owner Namirial nel servizio di conservazione
Direzione	La Direzione di Namirial è impegnata nel definire gli obiettivi e il piano industriale per lo sviluppo, la messa in atto, il monitoraggio, la manutenzione, la verifica dell'efficacia e il miglioramento continuo del servizio di conservazione.	Direzione
Consiglio di Amministrazione	Pianifica e detta le direttive strategiche e le linee guida in attuazione a quanto stabilito dal piano industriale e dagli obiettivi aziendali nell'ambito del servizio di conservazione.	Amministratore delegato
Area Marketing	È responsabile delle attività di marketing correlate al servizio di conservazione.	Responsabile Marketing
Area Commerciale	È responsabile delle attività di sviluppo commerciale e vendita del servizio di conservazione, nonché della gestione commerciale dei Clienti e della gestione della sottoscrizione dell'accordo contrattuale tra le parti.	Responsabile Commerciale
Area Amministrativa	È responsabile delle attività amministrative e di fatturazione del servizio di conservazione.	Responsabile Amministrazione
Ufficio Legale	È responsabile di garantire il supporto per la gestione degli aspetti contrattuali e legali relativi al servizio di conservazione. È responsabile, inoltre, della gestione e dell'archiviazione della contrattualistica relativa ai Clienti e degli atti di nomina legati al servizio di conservazione.	Responsabile Ufficio Legale
Ufficio Conservazione	È responsabile delle attività del servizio di conservazione; eroga le attività di assistenza e di competenza a supporto delle richieste sia esterne che interne. Supporta l'Area Commerciale nell'attività di analisi dei requisiti del servizio di conservazione.	Responsabile del servizio di conservazione Responsabile della funzione archivistica di conservazione



	<p>Rappresenta il Centro di competenza sui temi normativi e di processo in materia di conservazione di documenti informatici.</p> <p>Contribuisce allo sviluppo in termini di definizione delle funzionalità necessarie all'evoluzione e miglioramento del servizio.</p>	
Area di Produzione	<p>È responsabile delle attività di pianificazione dello sviluppo delle infrastrutture tecnologiche del Sistema di conservazione.</p> <p>È responsabile delle attività di configurazione del servizio ai fini della produzione.</p> <p>È responsabile della gestione delle componenti hardware e software del Sistema di conservazione per l'erogazione del servizio.</p> <p>È responsabile del presidio, controllo, monitoraggio di tutte le componenti del servizio e del soddisfacimento dei livelli di servizio (SLA) verso il Soggetto produttore dei documenti.</p> <p>È responsabile del controllo sui livelli di servizio erogati da terzi (fornitori) verso Namirial.</p> <p>Segnala le eventuali difformità al Responsabile del servizio di conservazione.</p>	Responsabile dei sistemi informativi per la conservazione
Area di Ricerca e Sviluppo	<p>È responsabile delle attività di coordinamento dello sviluppo e manutenzione delle componenti hardware e software del servizio di conservazione.</p> <p>È responsabile della pianificazione e del monitoraggio dei progetti di sviluppo del Sistema di conservazione.</p> <p>È responsabile del controllo degli SLA relativi alla manutenzione del Sistema di conservazione.</p>	Responsabile dello sviluppo e della manutenzione del sistema di conservazione
Audit	<p>È responsabile di eseguire audit periodici sul servizio di conservazione, nonché verifiche ispettive interne e presso fornitori.</p> <p>È responsabile dell'acquisizione delle evidenze per il rilevamento delle eventuali non conformità.</p> <p>È responsabile della redazione del piano di audit e della sua esecuzione.</p> <p>Si occupa della redazione e condivisione dei tableaux de bord con particolare riferimento alle non conformità evidenziate in fase di auditing.</p>	TSP Internal Audit



Il Programma di formazione e sviluppo professionale per il personale coinvolto nel servizio di conservazione e il dettaglio dei compiti sono specificati nella documentazione del sistema di qualità aziendale, del sistema di gestione della sicurezza, delle procedure delle risorse umane e dalla normativa interna legata agli standard di settore.

[Torna al Sommario](#)

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 *Strongdox*, 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 (certificazione **ISO/IEC 27001**), in particolare nel perimetro *"Consulenza, progettazione, sviluppo, distribuzione, supporto e fornitura di servizi gestiti e soluzioni per firma elettronica, firma elettronica avanzata, firma elettronica avanzata basata su un certificato qualificato, firma elettronica avanzata basata su biometria, posta attendibile, servizi di autorità di certificazione, servizi di marcatura temporale e servizi fiduciari come da regolamento europeo eIDAS, servizi SPID come da regolamento italiano. Progettazione di soluzioni ed erogazione di servizi gestiti in modalità SaaS, PaaS e On Premise in Enterprise Content Management e Paperless Business (Business Process Management, Acquisizione e trasmissione documentale, Fatturazione elettronica, Formazione del documento, Gestione della memorizzazione, Archiviazione digitale e Conservazione di documenti elettronici a lungo termine), in conformità con le normative vigenti. Progettazione, sviluppo, manutenzione di software ed erogazione di servizi in modalità SaaS per la gestione delle buste paga, del personale e dell'amministrazione"* ;
- il **Sistema di Gestione della Qualità** secondo la norma **UNI EN ISO 9001**, nel perimetro *"Progettazione, elaborazione ed assistenza post vendita di software, piattaforme gestionali e siti internet. Erogazione di servizi hosting e collocation. Erogazione del servizio di posta elettronica certificata. Certification authority, time stamping, firma automatica, firma remota, firma elettronica semplice e avanzata e personalizzazione smart card, SPID. 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)."*

Il servizio di conservazione *Strongdox* presenta un flusso caratterizzato da tre fasi principali – **attivazione, produzione e post-produzione** – ciascuna delle quali può essere ulteriormente suddivisa in ulteriori attività.



Figura 1 Fasi del servizio di conservazione

Attivazione	Predisposizione e condivisione della Scheda Servizio
	Configurazione del servizio di conservazione
	Collaudo e sua validazione

Figura 2 Attivazione

La fase di **Attivazione** del servizio viene avviata in caso di formale accettazione dell'offerta e delle condizioni contrattuali di servizio da parte del Titolare dell'oggetto di conservazione, inclusi tutti gli allegati e i documenti collegati al contratto.

L'**Area Commerciale** di Namirial, responsabile del processo di vendita del servizio e del completamento dell'accordo tra le parti, comunica l'attivazione all'**Area Amministrativa** per la gestione dell'anagrafica Cliente e all'**Ufficio Legale** per la corretta archiviazione della contrattualistica sottoscritta. Contestualmente invia la richiesta di attivazione operativa del Cliente alle risorse associate a **Ufficio Conservazione** che, presa in carico l'attività, avviano la predisposizione e la messa a disposizione della Scheda Servizio.

In caso di specifica assistenza richiesta dal Titolare dell'oggetto di conservazione relativamente alle modalità di trasferimento dei documenti e dei fascicoli informatici, ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche, le risorse associate a Ufficio Conservazione gestiscono la richiesta con il Cliente e, se necessario, richiedono un intervento di assistenza del **Responsabile dello sviluppo e della manutenzione del servizio di conservazione**, interfacciandosi con il Produttore dei PdV al fine di definire correttamente le specificità da inserire nella Scheda Servizio.

La definizione iniziale dei requisiti del sistema in relazione alle tipologie documentali da conservare e alla normativa di riferimento, nonché l'individuazione degli adempimenti correlati alla conservazione, sono assicurate dall'analisi che precede la predisposizione della Scheda Servizio. Tale documento è sottoposto alla supervisione e alla verifica 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) e deve essere validato dal Cliente.

Successivamente, il processo prevede che ad ogni variazione del Servizio (Change Process), la Scheda Servizio debba essere aggiornata e nuovamente condivisa tra le parti.

Predisposta e condivisa la Scheda Servizio, validata dal Responsabile del servizio di conservazione di Namirial e dal Cliente, vengono avviate le attività di configurazione del servizio nella piattaforma *Strongdox*.



Prima della messa in produzione del servizio è prevista l'effettuazione di un collaudo interno, ossia della verifica interna, della correttezza della configurazione del sistema rispetto a quanto specificato nella Scheda Servizio. Opzionalmente e previa pianificazione può essere eseguito un ulteriore collaudo con il Cliente.

Le modalità dell'eventuale collaudo sono indicate nella Scheda Servizio; a seguito dell'eventuale collaudo e della sua validazione formale da parte del Cliente si procede con la successiva fase di messa in produzione.

Produzione	Acquisizione, verifica e gestione dei Pacchetti di Versamento presi in carico
	Generazione dei Rapporti di Versamento
	Preparazione e gestione dei Pacchetti di Archiviazione
	Erogazione in alta disponibilità, replica geografica dei dati e procedure di backup
	Preparazione e gestione del Pacchetto di Distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta

Figura 3 Produzione

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 di esiti, monitor, report e altri strumenti di controllo.

Inoltre, l'Area di Produzione presidia e gestisce gli asset di infrastruttura e la corretta esecuzione del processo, dalla fase di presa in carico dei Pacchetti di Versamento, ai controlli di coerenza, alla generazione del Rapporto di Versamento, alla preparazione e gestione dei Pacchetti di Archiviazione, fino alla preparazione e gestione del Pacchetto di Distribuzione ai fini dell'esibizione e alla produzione di duplicati e copie informatiche su richiesta dell'Utente.

In particolare, il **Responsabile dei sistemi informativi per la conservazione** è responsabile delle attività di controllo degli asset e del monitoraggio del 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, 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 di conservazione dei documenti per uno specifico cliente, il servizio deve essere mantenuto nel tempo anche nella fase di post-produzione, per tutta la durata contrattuale concordata, garantendo ai documenti e ai pacchetti informativi integrità, autenticità dell'origine, leggibilità, disponibilità e reperibilità, sicurezza e riservatezza.

Post-Produzione	Mantenimento dei documenti in conservazione
	Verifica quinquennale della leggibilità
	Adempimenti normativi
	Gestione dello scarto dei Pacchetti di Archiviazione
	Chiusura del servizio di conservazione

Figura 4 Post-Produzione



Il mantenimento dei documenti e dei pacchetti generati nel processo di conservazione è garantito dalle attività effettuate dall'**Area di Produzione** e dall'**Area di Ricerca e Sviluppo**, 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 Soggetto produttore dei documenti.

Durante la fase di post-produzione la struttura organizzativa di Namirial, in particolare le risorse associate a Ufficio Conservazione e l'Area di Produzione, supportano gli adempimenti previsti dalla normativa.

Scaduto il periodo di conservazione, concordato contrattualmente tra il Soggetto produttore dei documenti, il Responsabile della conservazione e il Conservatore, viene avviata la procedura di scarto condivisa, con la produzione dei Pacchetti di Scarto e la verbalizzazione dello scarto e della chiusura del servizio. Responsabili delle attività sono le risorse associate a Ufficio Conservazione e l'Area di Produzione.

Prima dell'avvio dello scarto e della procedura di chiusura del servizio viene comunicato al Titolare dell'oggetto di conservazione l'avvio dello scarto entro 30 giorni (salvo diversi accordi condivisi col Cliente e specificati nella Scheda Servizio), al fine di fornirgli un periodo transitorio per richiedere formalmente l'estensione (prolungamento) del periodo di conservazione.

Per l'attuazione delle fasi del servizio di conservazione *Strongdox* e, più in generale, per tutte le attività in carico al Conservatore, è necessario garantire la **Gestione dei sistemi informativi e della sicurezza** a supporto del servizio.

Gestione dei sistemi informativi e della sicurezza	Conduzione e manutenzione del Sistema di conservazione
	Monitoraggio del Sistema di conservazione
	Change management
	Verifica periodica di conformità alla normativa e agli standard di riferimento
	Rispetto e monitoraggio dei requisiti di sicurezza del Sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza

Figura 5 Gestione dei sistemi informativi e della sicurezza

Tale obiettivo viene perseguito dall'organizzazione Namirial attraverso la definizione dei compiti, dei ruoli e delle responsabilità descritte nel presente manuale, attraverso verifiche e audit periodici e tramite l'ausilio di strumenti per il controllo e il monitoraggio. Le procedure definite all'interno del sistema di gestione della sicurezza (conforme allo standard ISO 27001) e della qualità aziendale (conforme allo standard ISO 9001) sono gli strumenti primari anche ai fini dell'analisi del rischio, della pianificazione e dell'adozione di misure per la prevenzione, la manutenzione e il miglioramento continuo del servizio.

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

[Torna al Sommario](#)



6 OGGETTI SOTTOPOSTI A CONSERVAZIONE

Il funzionamento del Sistema di conservazione *Strongdox* è conforme alle Linee Guida 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 "pacchetto informativo").

Il versamento dei pacchetti (contenenti documenti e/o dati) al Sistema *Strongdox* 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 (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 Info):

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 *Strongdox* è basato, quindi, su un modello che permette di identificare e comprendere l'oggetto dati e le relative informazioni sulla rappresentazione, che contengono informazioni sia di natura sintattica che semantica.

[Torna al Sommario](#)

6.1 Oggetti conservati

Nella Scheda Servizio concordata tra il Conservatore e il Titolare dell'oggetto, redatta sulla base delle informazioni condivise in fase di analisi, 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 formati (comprensivi della relativa versione) dei file utilizzati;
- l'indicazione dei visualizzatori relativi ai formati gestiti, necessari per garantire la leggibilità nel tempo dei documenti conservati;
- l'elenco e la descrizione dei metadati associati ai documenti;
- il periodo di conservazione;
- le tempistiche del processo di conservazione concordate con il Titolare dell'oggetto;
- altre politiche (regole) che caratterizzano il processo di conservazione.

Le tipologie di documenti che caratterizzano gli oggetti digitali da versare nel Sistema di conservazione *Strongdox* sono definite attraverso le attività di analisi e di classificazione.

La descrizione delle tipologie documentali, con l'indicazione della loro natura, dei formati, dei metadati obbligatori e dei metadati opzionali, delle regole e della durata di conservazione (piano di conservazione e successivo scarto), è riportata nel dettaglio all'interno della Scheda Servizio ed è specifica per ciascun Titolare dell'oggetto e per ciascuna tipologia documentale.

Si riporta di seguito un esempio di draft delle tabelle che definiscono gli aspetti suddetti all'interno della Scheda Servizio:



Tipologia documentale <i>[valore da inserire nel campo LABEL dell'IPdV]</i>	Codice della tipologia nel Sistema di conservazione	Formato	Periodo di riferimento dei documenti con cui si avvia la conservazione <i>(ad esempio periodo di imposta)</i>	Durata di conservazione
.....

Posizione	Denominazione	Descrizione	Obbligatorio	Valore
1	Metadato 1	x	es: Testo
2	Metadato 2	x	es: Data
3

6.2 Formati

I formati dei files contenuti nei Pacchetti di Versamento devono essere conformi all'elenco dei formati previsti dall'Allegato 2 delle Linee Guida e dai formati ammessi dal Sistema di Conservazione qui di seguito elencati. Per quanto riguarda la conservazione di file in formato TXT, non riportato tra i formati indicati da AgID, il Conservatore ha effettuato la valutazione di interoperabilità per il proprio sistema di conservazione secondo quanto indicato al par. 3.1 dell'Allegato 2 delle Linee Guida. La valutazione e il relativo indice di interoperabilità sono riportati nel paragrafo successivo.

I formati associati alla tipologia documentale sottoposta a conservazione sono definiti nella fase di analisi che precede l'attivazione del servizio e dichiarati all'interno della Scheda Servizio.

Il Produttore dei PdV **deve adeguarsi al seguente elenco dei formati ammessi**, che il Sistema di conservazione *Strongdox* verifica nella fase di presa in carico, per l'accettazione e l'individuazione dello specifico Mimetype.

Formato del file	Proprietario	Estensione	Tipo Mime	Visualizzatore	Produttore del visualizzatore
PDF	Adobe Systems - www.adobe.com Ai fini della conservazione, nell'uso di tale formato occorre formare i documenti esclusivamente con caratteri tipografici interoperabili, considerati "standard" da diversi organi di settore, come meglio specificato nel paragrafo 2.8	.pdf	application/pdf	Adobe Reader	Adobe Systems www.adobe.com



	Caratteri tipografici dell'Allegato 2 delle Linee Guida AgID				
PDF/A	Adobe Systems - www.adobe.com	.pdf	application/pdf	Adobe Reader http://www.pdfa.org/doku.php	Adobe Systems www.adobe.com
XML	W3C Ai fini della conservazione, nell'uso di tale formato è obbligatorio per il Titolare mantenere nel tempo anche il file XML Schema .xsd	.xml	application/xml text/xml	Mozilla -Chrome -Internet Explorer	Firefox - Google - Microsoft -
TXT	Ai fini della conservazione nell'uso di tale formato, è importante specificare la codifica del carattere (Character Encoding) adottata	.txt		Mozilla -Chrome -Internet Explorer	Firefox - Google - Microsoft -
TIFF	Aldus Corporation in seguito acquistata da Adobe	.tif, .tiff	image/tiff	Vari visualizzatori di immagini	
JPG	Joint Photographic Experts Group	.jpg, .jpeg	image/jpeg	Vari visualizzatori di immagini	Per maggiori informazioni sul formato www.jpeg.org
EML	Vari	.eml		Client di posta elettronica supportano la visualizzazione di file eml	Vari
OOXML	Microsoft Tale formato deve garantire alcune caratteristiche che lo rendono adatto alla conservazione nel lungo periodo, tra queste l'embedding dei font, la presenza di indicazioni di presentazione del documento, la possibilità di	.docx, .xlsx, .pptx			



	applicare al documento la firma digitale XML. È opportuno utilizzare il profilo <i>Strict</i> che consente di eliminare alcune estensioni "proprietarie" che possono ridurre l'interoperabilità del formato stesso				
ODF	Consorzio OASIS OpenOffice.org	.ods, .odp, .odg, .odt	application/vnd .osis.opendoc ument.text		www.oasis-open.org

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

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

6.2.1 Valutazione ed indice di interoperabilità

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

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

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



Livello di metadati	da 0 a 3	Il formato TXT non consente di incorporare alcun metadato all'interno del file	0
Robustezza	da 0 a 2	Il formato TXT non è binario. Essendo testuale è tra i formati più robusti	2
Indipendenza da dispositivi	da 0 a 4	Il formato TXT è leggibile su qualsiasi ambiente operativo o device.	4
Compatibilità in avanti e all'indietro	non specificato	Il formato TXT appartiene alla categoria file di testo e sono presenti molteplici software di elaborazione testi, installabili su piattaforma di sistema Android, Linux, Mac OS, Windows, Windows Phone, al fine di accedere e visualizzare i file nel formato TXT.	2
Testuale o binario	non specificato	Formato non formattato il cui contenuto è puramente testuale (ASCII)	2
TOTALE			20

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

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

[Torna al Sommario](#)

6.3 Pacchetto di Versamento

Il Pacchetto di Versamento (PdV) del Sistema di conservazione *Strongdox* è costituito da un archivio zip non compresso, composto da:

- i documenti oggetto della conservazione (*Content Information*), eventualmente firmati digitalmente (nello standard di firma CADES ".p7m" o PAdES o XAdES) o eventualmente marcati temporalmente (nello standard di validazione temporale CADES-T, o PAdES-T o XAdES-T);
- un file Indice IPdV (Indice del Pacchetto di Versamento) finalizzato alla descrizione delle *Preservation Description Information* secondo lo standard ISO 14721 OAIS, ossia alla descrizione delle informazioni relative all'oggetto della conservazione, all'identificazione del Titolare dell'oggetto e del Produttore del PdV, ai dati descrittivi e informativi sull'impacchettamento e su ciascun documento contenuto nel pacchetto.

Il file Indice del Pacchetto di Versamento (IPdV) è un file nel formato XML, che in conformità allo standard UNI SINCRO 11386 assicura:

- l'identificazione del soggetto che ha prodotto il Pacchetto di Versamento (Produttore dei PdV);
- 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 e relativi valori, messaggi del Responsabile della conservazione, ecc.

Il file Indice del Pacchetto di Versamento (IPdV) può essere eventualmente firmato digitalmente dal Produttore.



Di seguito la rappresentazione grafica del file XSD dell'Indice del Pacchetto di Versamento del sistema *Strongdox*.

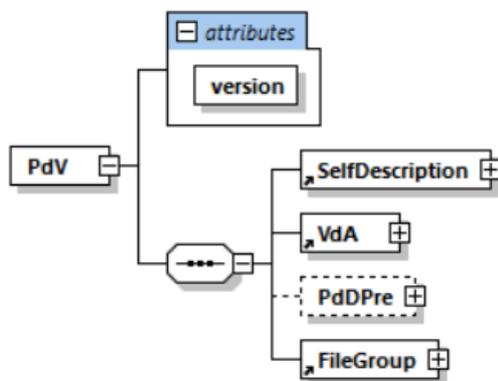
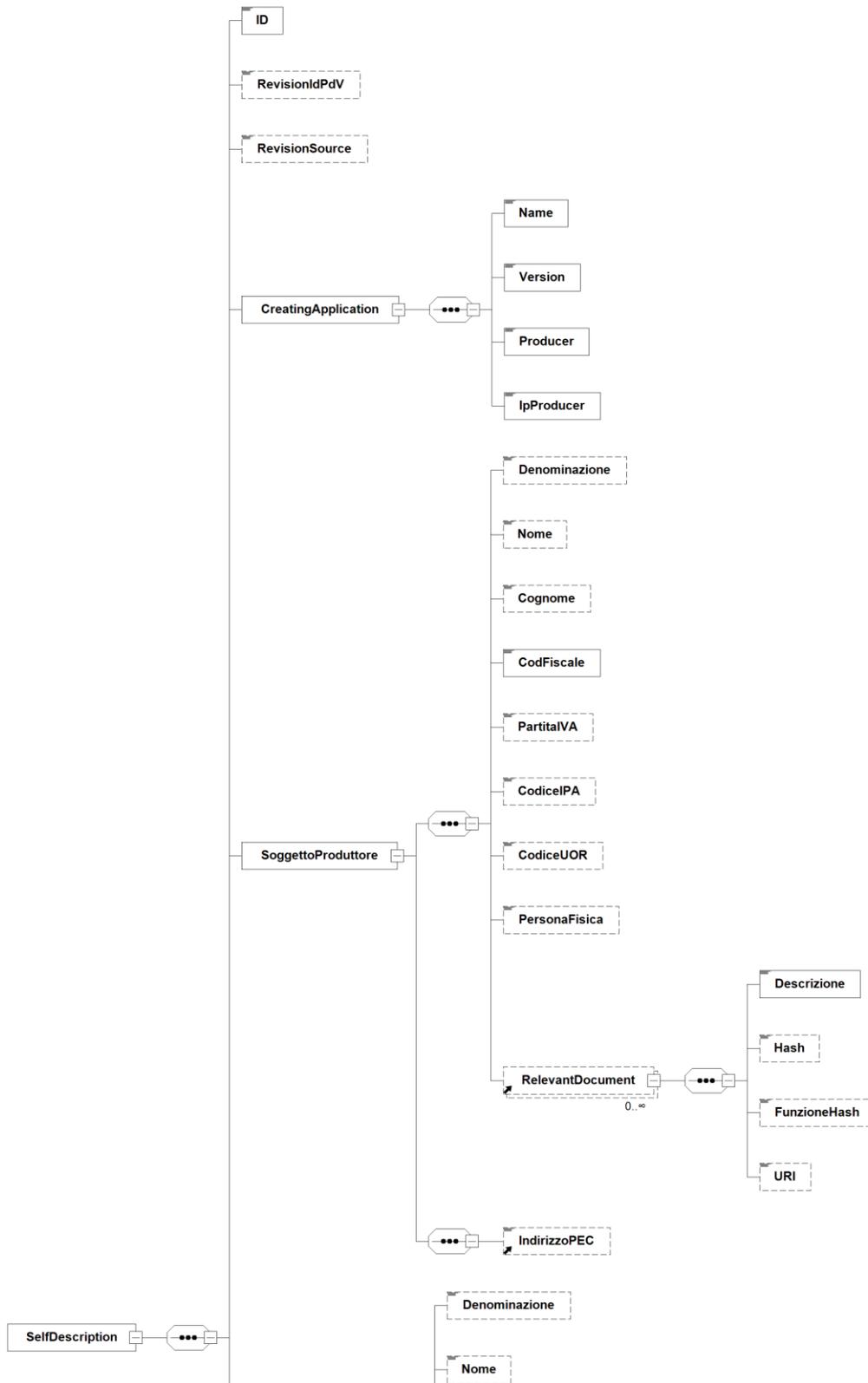


Figura 6 Struttura Indice PdV suddiviso nelle componenti principali



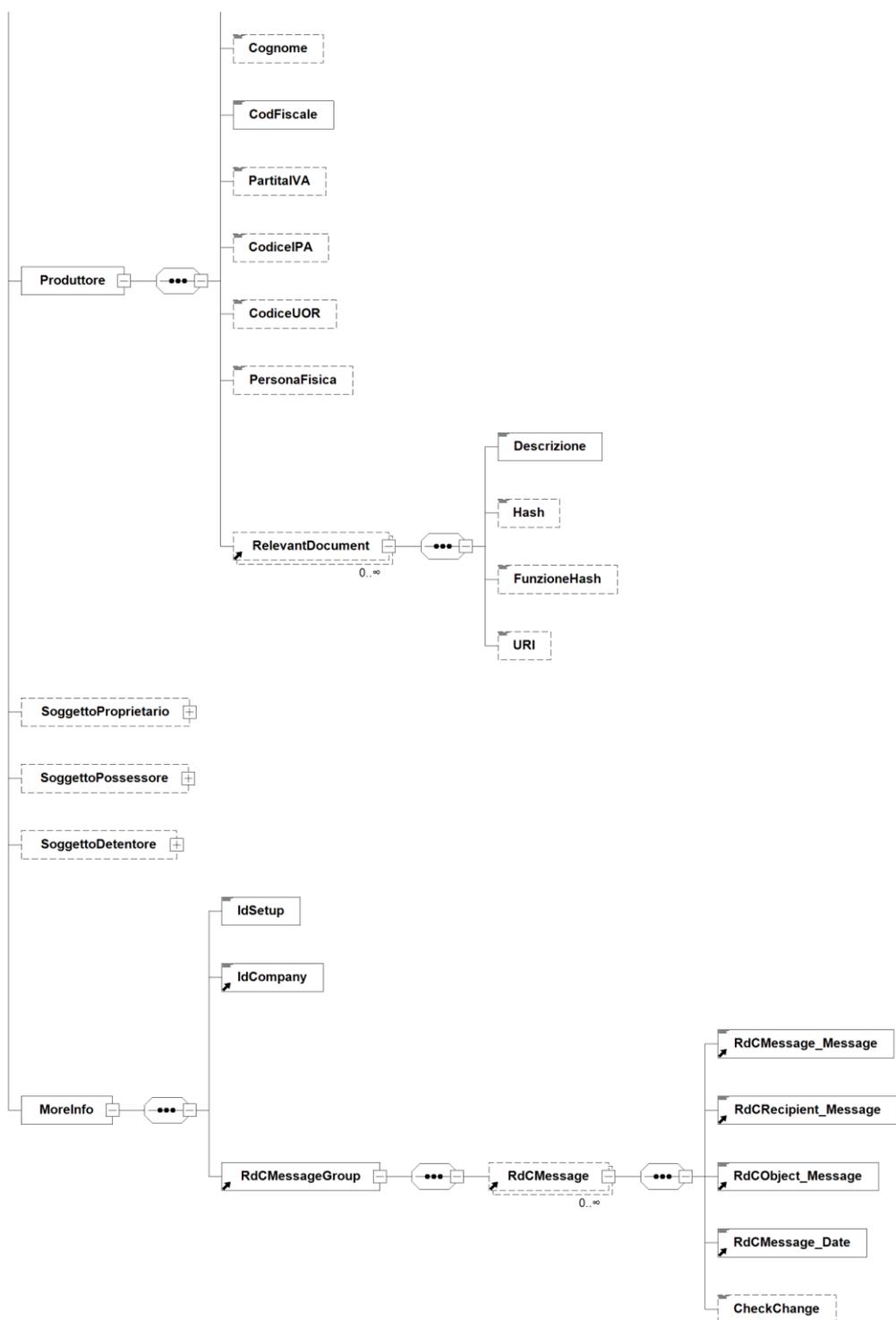


Figura 7 Struttura Indice PdV (Sezione SelfDescription)

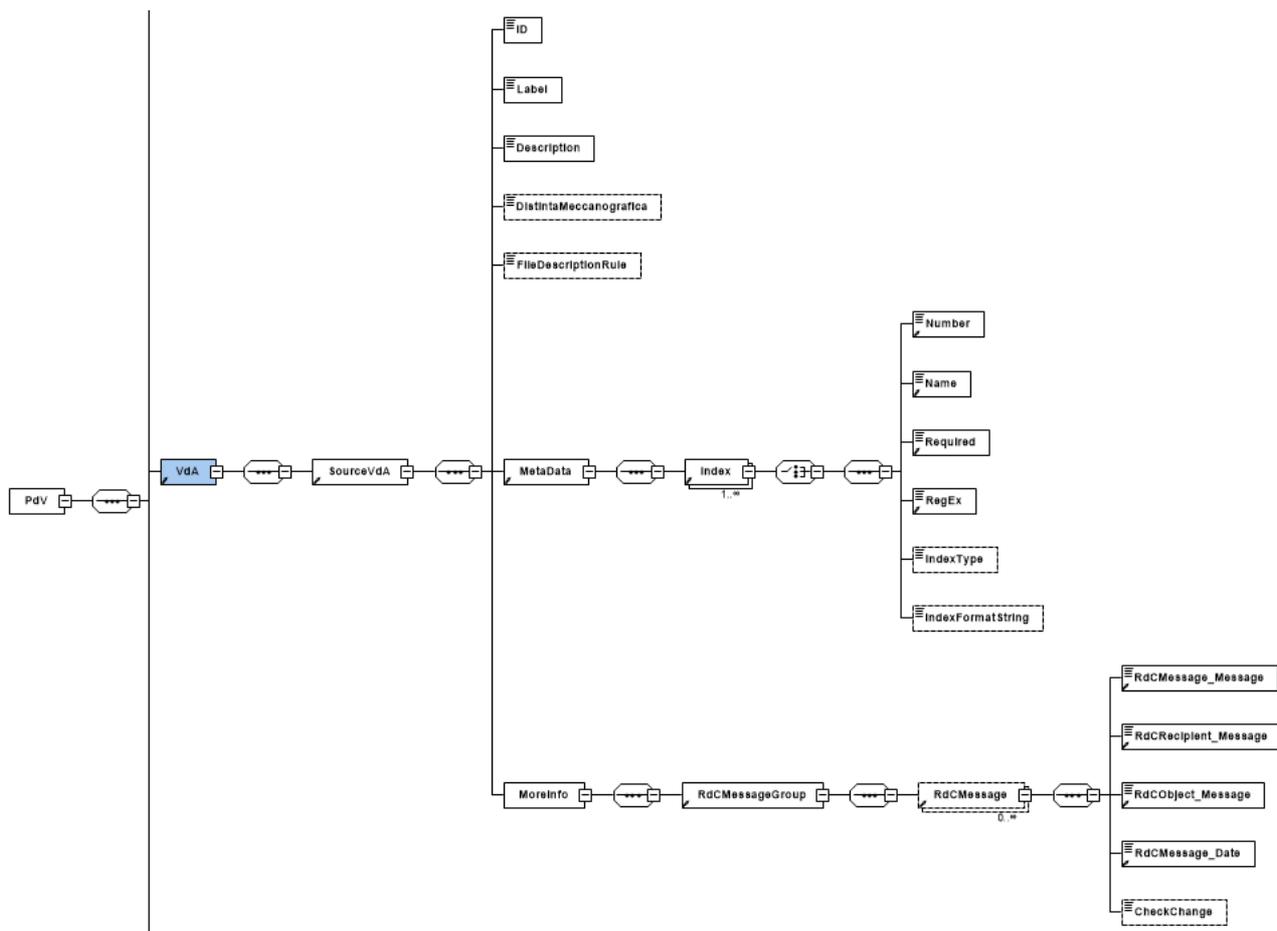


Figura 8 Struttura Indice PdV (Sezione VdA)

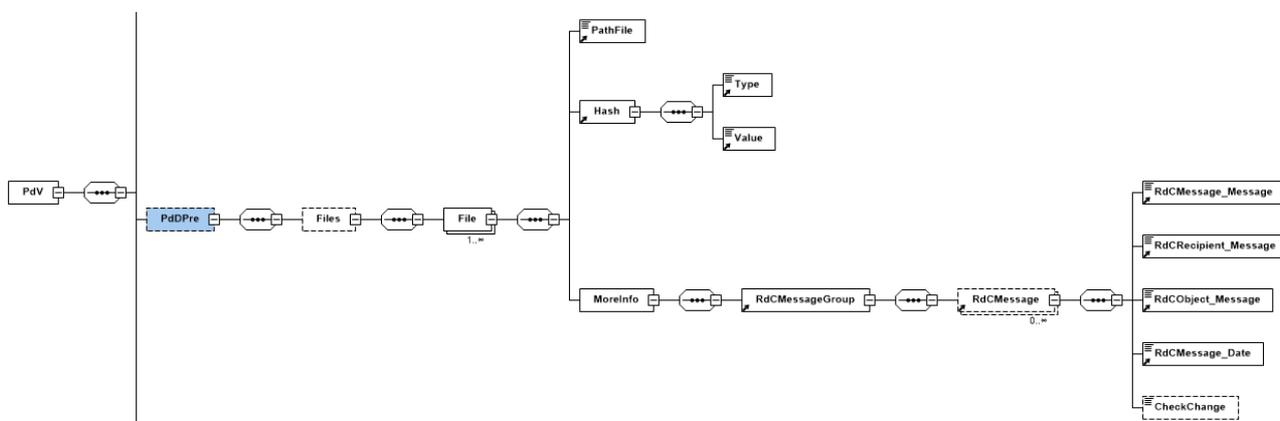
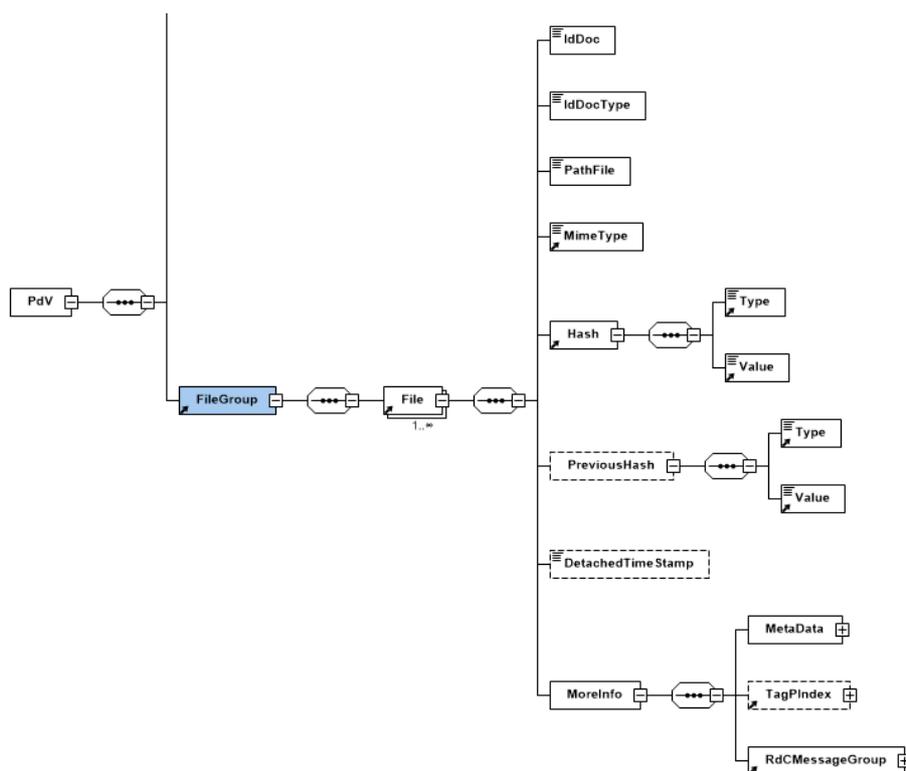


Figura 9 Struttura Indice PdV (Sezione PdDPre)



Il modello-dati del Pacchetto di Versamento e le informazioni di dettaglio sono riportate nella Scheda Servizio.

Figura 10 Struttura Indice PdV (Sezione FileGroup)

[Torna al Sommario](#)

6.4 Pacchetto di Archiviazione

Il Pacchetto di Archiviazione (PdA) generato nel processo di conservazione del sistema *Strongdox* è una specializzazione del Pacchetto Informativo ed è composto dalla trasformazione di uno o più Pacchetti di Versamento secondo le modalità riportate nel presente Manuale.

Un Pacchetto di Archiviazione (PdA) contiene:

- gli oggetti informativi individuati per la conservazione (documenti e/o aggregazioni documentali sottoposti al processo di conservazione a lungo termine);
- un Indice del Pacchetto di Archiviazione (IPdA) che rappresenta le Informazioni sulla Conservazione.

In particolare, la struttura dati dell'IPdA del sistema *Strongdox* fa riferimento allo standard nazionale SInCRO – Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386) – riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione.

L'IPdA è l'evidenza informatica nel formato XML associata ad ogni PdA, contenente un insieme di informazioni descritte nelle regole tecniche in materia, in cui è riportata nel dettaglio la struttura dati prevista. Su ciascun IPdA viene apposta una marca temporale e la firma del Responsabile del Servizio.



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

- **SelfDescription (1)***: Descrizione generale del pacchetto.
 - **ID (1)**: Id univoco del PdA generato dal Sistema di conservazione (Id PdA generato dal database).
 - **CreatingApplication (1)**:
 - **Name (1)**: Sistema di conservazione *Strongdox*.
 - **Version (1)**: Versione ricavata dal Web Service.
 - **Producer (1)**: Produttore del Sistema di conservazione: 2C SOLUTION S.R.L.
 - **PIndexSource (0-n)**
 - **ID (1)**: Id dell'eventuale pacchetto archiviazione (PdA) precedente.
 - **Path (1)**: Percorso relativo all'IPdA (SInCRO) dell'eventuale pacchetto precedente.
 - **Hash (1)**: Valore restituito dalla funzione applicandola al file IPdA dell'eventuale pacchetto precedente; contiene l'attributo "hashFunction" che identifica la funzione di hash utilizzata per il calcolo.
 - **MoreInfo (1)**
 - **EmbeddedMetadata (1)**: Riferimenti del soggetto titolare dei documenti a cui si riferisce il processo di conservazione.
 - **MoreInfoSelfDescription (1)**
 - **IdSetup (1)**: Id installazione per il soggetto titolare dei documenti all'interno di *Strongdox*.
 - **IdAzienda (1)**: Id del soggetto titolare dei documenti all'interno di *Strongdox*.
 - **VersionIPdA (1)**: Versione dell'indice PdA definita dal Conservatore.
- **PVolume (1)**:
 - **ID (1)**: Id univoco del PdA generato dal Sistema di conservazione (Id PdA generato dal database).
 - **Label (0-1)**: Nome dell'aggregazione.
 - **Description (0-1)**: Descrizione dell'aggregazione.
 - **PVolumeSource (0-n)**: Informazioni relative a un volume di conservazione da cui è originato quello in oggetto.
 - **ID (1)**: Identificativo dell'aggregazione.
 - **PIndexID (1)**: Identificativo dell'indice di conservazione associato al precedente volume di conservazione.
 - **PVolumeGroup (0-1)**: Informazioni relative a un'aggregazione cui il volume di conservazione appartiene.
 - **ID (1)**: Identificativo dell'aggregazione.
 - **Label (0-1)**: Nome dell'aggregazione.
 - **Description (0-1)**: Descrizione dell'aggregazione.
 - **MoreInfo (1)**
 - **EmbeddedMetadata (1)**: Elenco dei PdV inclusi all'interno del PdA
 - **MoreInfoPVolume (1)**
 - **PdVGruppo (1)**
 - **PdV (0-n)**



- **IdPdV (1)**: Id del PdV restituito dal Sistema di conservazione al termine della presa in carico.
- **RevisionIdPdV (0-1)**: Id del PdV revisionato (può essere il PdV di origine oppure l'ultima versione pubblicata per il PdV di origine). Il nodo è presente solo se il PdV rappresenta una revisione.
- **RevisionIdPdVOrigin (0-1)**: Id del PdV di origine (PdV iniziale da cui hanno origine tutte le revisioni). Il nodo è presente solo se il PdV rappresenta una revisione.
- **RevisionNumber (0-1)**: Numero della revisione necessario per ordinare la sequenza delle revisioni relative al PdV di origine. Il nodo è presente solo se il PdV rappresenta una revisione.
- **RevisionSource (0-1)**: Definisce la provenienza del pacchetto di revisione. Valori ammessi: RequestProducer o Internal. Il nodo è presente solo se il PdV rappresenta una revisione.
- **FunzioneHash (1)**: Funzione di hash utilizzata per calcolare l'hash dell'IPdV.
- **Hash (1)**: Valore restituito dalla funzione di hash applicata al file IPdV.
- **IdRdV (1)**: Id del RdV restituito dal Sistema di conservazione al momento della generazione.
- **FunzioneHashRdV (1)**: Funzione di hash utilizzata per calcolare l'hash del RdV.
- **HashRdV (1)**: Valore restituito dalla funzione di hash applicata al RdV.
- **DataRdV (1)**: Data di generazione del RdV.
- **RdCMessageGroup (1)**: Eventuali comunicazioni tra il produttore e il Responsabile della conservazione o il suo Delegato relative al PdV.
 - **RdCMessage (0-n)**
 - **RdCMessage_Message**: Testo del messaggio.
 - **RdCRecipient_Message**: Testo del messaggio per chi riceve il pacchetto di Versamento.
 - **RdCObject_Message**: Eventuale file allegato riferito alla comunicazione.
 - **RdCMessage_Date**: Data di inserimento del messaggio.
 - **CheckChange**: Metadato aggiuntivo che consente di specificare la verifica della modifica del documento. Valori ammessi: Rettifica; Integrazione; Annotazione.
- **PdDPre (0-1)**
 - **Files (1)**



- **File (0-n)**
 - **PathFile (1):** Uri del file relativo ad un allegato PdDPre (riversamento da conservatore precedente). Necessario per meglio identificare l'allegato e poter capire in quale PdV si trova il file.
 - **Hash (1)**
 - **Type (1):** Funzione di hash applicata all'allegato PdDPre.
 - **Value (1):** Valore restituito dalla funzione di hash applicata all'allegato PdDPre.
- **RdcMessageGroup (1)**
 - **RdCMessage (0-n):**
 - **RdCMessage_Message:** Testo del messaggio.
 - **RdCRecipient_Message:** Testo del messaggio per chi riceve il pacchetto di Versamento.
 - **RdCObject_Message:** Eventuale file allegato riferito alla comunicazione.
 - **RdCMessage_Date:** Data di inserimento del messaggio.
 - **CheckChange:** Metadato aggiuntivo che consente di specificare la verifica della modifica del documento. Valori ammessi: Rettifica; Integrazione; Annotazione.
- **FileGroup (1-n):**
 - **ID (1):** Id della tipologia documentale alla quale si riferiscono i documenti.
 - **Label (0-1):** Nome della tipologia documentale alla quale si riferiscono i documenti.
 - **Description (0-1):** Descrizione della tipologia documentale alla quale si riferiscono i documenti.
 - **File (1-n):** Definizione del file comprensiva di codifica, estensione e formato (MimeType)
 - **ID (1):** Id del documento assegnato dal Sistema di conservazione (univoco all'interno del Sistema di Conservazione).
 - **Path (1):** Indirizzo logico del file rappresentato da un URI (individua il file all'interno dello storage).
 - **Hash (1):** Funzione di hash utilizzata e valore restituito dalla funzione applicandola al file oggetto della Conservazione.
 - **PreviousHash (1):** Funzione di hash utilizzata e valore restituito dalla funzione applicandola al file oggetto della Conservazione (riferita ad un indice di Conservazione precedente).
 - **MoreInfo:**
 - **EmbeddedMetadata:**



- **MoreInfoFile:** Informazioni relative al documento nel Sistema di conservazione utilizzate per identificare e descrivere il documento all'interno dell'archivio.
 - **File (1)**
 - **IdDoc:** Identificativo univoco del file assegnato dal Produttore (univoco all'interno della tipologia documentale definita per l'azienda).
 - **IdPdV:** Id del PdV associato al documento.
 - **Indici (1)**
 - **Indice (1-n)**
 - **Nome:** Nome del campo indice (metadato).
 - **Valore:** Valore del campo indice (metadato).
 - **AnnoRiferimentoDoc:** Anno di riferimento del documento (ad es. anno del periodo di imposta)
 - **Oggetto:** Metadato funzionale a riassumere brevemente il contenuto del documento o comunque a chiarirne la natura. Viene calcolato in automatico dal sistema, in funzione alle regole definite in fase di versamento.
 - **CheckChange:** Metadato aggiuntivo che consente di specificare la verifica della modifica del documento. Valori ammessi: Rettifica; Integrazione; Annotazione
 - **RdCMessageGroup (1):** Eventuali comunicazioni tra il produttore e il Responsabile della conservazione o il suo Delegato relative al file.
 - **RdCMessage (0-n)**
 - **RdCMessage_Message:** Testo del messaggio.
 - **RdCRecipient_Message:** Testo del messaggio per chi riceve il pacchetto di Versamento.
 - **RdCObject_Message:** Eventuale file allegato riferito alla comunicazione.
 - **RdCMessage_Date:** Data di inserimento del messaggio
 - **DetachedTimeStamp:** Riferimenti ad una eventuale marca temporale detached associata al documento.
 - **AdditionalMetaData:** Metadati aggiuntivi richiesti dalle linee guida AgID.
- **MoreInfo**
 - **EmbeddedMetadata**
 - **MoreInfoFileGroup (1):** Definizione della Tipologia documentale a cui appartiene il documento.
 - **Tipologia (1)**



- **IdTipologia (1):** Id della Tipologia documentale a cui appartiene il documento.
 - **Indici (1)**
 - **Indice (1-n)**
 - **Numero:** Numero indice. Posizione del campo indice (metadato) all'interno della definizione della Tipologia.
 - **Nome:** Nome del campo indice (metadato)
 - **Richiesto:** Indica se il valore dell'indice (metadato) è obbligatorio (possibili valori: True, False).
 - **RegEx:** Eventuale espressione di validazione per il valore dell'indice (metadato).
 - **IndexType:** Tipo di dato del metadato (possibili valori: stringa, intero, data)
 - **IndexFormatString:** Formato del tipo di dato.
- **Process (1)**
- **Submitter (1):** Informazioni relative al soggetto che effettua il trasferimento fisico degli oggetti digitali nel sistema di conservazione.
 - **AgentID:** Identificativo del soggetto sulla base di uno dei tipi di identificazione predefiniti dalla norma ETSI.
 - **AgentName:** Denominazione del soggetto (NameAndSurname oppure FormalName).
 - **NameAndSurname**
 - **FirstName:** Nome del soggetto.
 - **LastName:** Cognome del soggetto.
 - **FormalName:** Denominazione o ragione sociale del soggetto.
 - **RelevantDocument (1-n):** Riferimento ad un documento del soggetto che interviene nel processo di conservazione, rilevante per la comprensione del processo stesso o degli oggetti digitali sottoposti a conservazione.
 - **MoreInfo**
 - **EmbeddedMetadata**
 - **MoreInfoSubmitter**
 - **CodiceIPA (0-1):** Codice IPA definito nel caso il soggetto sia una Pubblica Amministrazione.
 - **CodiceUOR (0-1):** Codice UOR definito nel caso il soggetto sia una Pubblica Amministrazione.
 - **PartitaIVAPF (0-1):** Partita IVA valorizzata (se presente) nel caso in cui il soggetto sia una persona fisica.
 - **Holder (1-n):** Informazioni relative al Titolare dell'oggetto di conservazione (soggetto produttore) o al proprietario, possessore o detentore degli oggetti digitali trasferiti nel sistema di conservazione.
 - **AgentID:** Identificativo del soggetto sulla base di uno dei tipi di identificazione predefiniti dalla norma ETSI.
 - **AgentName:** Denominazione del soggetto (NameAndSurname oppure FormalName).
 - **NameAndSurname**



- **FirstName:** Nome del soggetto.
 - **LastName:** Cognome del soggetto.
 - **FormalName:** Denominazione o ragione sociale del soggetto.
 - **RelevantDocument (1-n):** Riferimento ad un documento del soggetto che interviene nel processo di conservazione, rilevante per la comprensione del processo stesso o degli oggetti digitali sottoposti a conservazione.
 - **MoreInfo**
 - **EmbeddedMetadata**
 - **MoreInfoHolder**
 - **CodiceIPA (0-1):** Codice IPA definito nel caso il soggetto sia una Pubblica Amministrazione.
 - **CodiceUOR (0-1):** Codice UOR definito nel caso il soggetto sia una Pubblica Amministrazione.
 - **AgentIdPdV (1):**
 - **IdPdV (1-n):** Elenco di Id PdV trasferiti dal soggetto.
 - **PartitaIVAPF (0-1):** Partita IVA valorizzata (se presente) nel caso in cui il soggetto sia una persona fisica.
 - **AuthorizedSigner (1-n):** Informazioni relative al soggetto autorizzato ad apporre la firma elettronica (avanzata o qualificata) o il sigillo elettronico (avanzato o qualificato) sull'indice di conservazione, a conclusione del processo di creazione dell'indice.
 - **AgentID:** Identificativo del soggetto sulla base di uno dei tipi di identificazione predefiniti dalla norma ETSI.
 - **AgentName:** Denominazione del soggetto (NameAndSurname oppure FormalName).
 - **NameAndSurname**
 - **FirstName:** Nome del soggetto.
 - **LastName:** Cognome del soggetto.
 - **FormalName:** Denominazione o ragione sociale del soggetto.
 - **RelevantDocument (1-n):** Riferimento ad un documento del soggetto che interviene nel processo di conservazione, rilevante per la comprensione del processo stesso o degli oggetti digitali sottoposti a conservazione.
 - **MoreInfo**
 - **EmbeddedMetadata (1)**
 - **MoreInfoAuthorizedSigner (1):** Informazioni aggiuntive relative al soggetto firmatario designato per la chiusura del processo di Conservazione.
 - **PreservationAgent**
 - **PreservationJobRole:** Descrizione della mansione riferita al soggetto.
 - **CertificateIdentificationCode:** Identificativo del certificato di firma utilizzato nella chiusura del processo di Conservazione.
 - **VATNumberNaturalPerson:** Partita IVA valorizzata (se presente) nel caso in cui il soggetto sia una persona fisica.
 - **Identifier (0-1):** Identificativo del soggetto assegnato dal Sistema di conservazione in fase di definizione del soggetto.
- **TimeReference (1)**



- **TimeInfo (1):** Data in cui è stata prodotto il file indice. Corrisponde entro certi limiti temporali (richiesti dal processo di firma e marca del file) alla data di rilascio della marca temporale.
- **LawAndRegulations (1):** Riferimento alla norma di riferimento: *Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.*
- **MoreInfo**
 - **EmbeddedMetadata**
 - **MoreInfoProcess:** Informazioni aggiuntive relative al processo di Conservazione.
 - **PreservationAgent (0-n)**
 - **AgentID (0-n):** Identificativo del soggetto sulla base di uno dei tipi di identificazione predefiniti dalla norma ETSI.
 - **AgentName (1):** Denominazione del soggetto (NameAndSurname oppure FormalName).
 - **NameAndSurname**
 - **FirstName:** Nome del soggetto.
 - **LastName:** Cognome del soggetto.
 - **FormalName:** Denominazione o ragione sociale
 - **PreservationJobRole (1):** Descrizione della mansione riferita al soggetto.
 - **Identifier (0-1):** Identificativo del soggetto assegnato dal Sistema di conservazione in fase di definizione del soggetto.

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

[Torna al Sommario](#)

6.5 Pacchetto di Distribuzione

Un Pacchetto di Distribuzione (PdD) del sistema *Strongdox*, a garanzia dell'interoperabilità e trasferibilità ad altri conservatori, può essere richiesto dall'utente nelle seguenti modalità:

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

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

- I documenti (oggetti digitali conservati nel sistema) richiesti dall'Utente.



- Uno o più files IPdA firmati dal Responsabile del Servizio e marcati temporalmente associati ai suddetti documenti richiesti dall'Utente.
- File indice del PdD (IPdD): file XML firmato digitalmente dal Responsabile del servizio di conservazione, che contiene l'hash dell'IPdA e l'hash di ogni singolo file (documento richiesto o presente all'interno di un PdV richiesto).

Quest'ultimo contiene al suo interno:

- **Id del PdD**, generato in seguito al salvataggio su Data Base;
- **Data della generazione del PdD** (in formato UTC);
- Soggetto produttore (Titolare dell'oggetto) a cui si riferisce il PdD (Rag. Sociale, Id setup, Id azienda, Cod. Fiscale, Partita IVA);
- Utente che ha richiesto il PdD (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);
- Indirizzo IP da cui è arrivata la richiesta di generazione;
- PdA consegnati (Id PdA, Hash, Funzione di hash utilizzata, Url file nel Sistema di conservazione e nel PdD)
- 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 PdD).

Di seguito viene riportata la struttura dati del Pacchetto di Distribuzione, secondo lo standard SInCRO.

- **DescGenerale**: Informazioni del richiedente, del Responsabile della conservazione e del Sistema di conservazione.
 - **ID**: Id del Pacchetto di Distribuzione (PdD) assegnato dal Sistema di Conservazione.
 - **IdSetup**: Codice Cliente associato al Titolare dell'oggetto di conservazione (soggetto produttore).
 - **IdAzienda**: Id dell'azienda di riferimento nel sistema documentale.
 - **SoggettoProduttore**
 - **Denominazione**: Denominazione del soggetto produttore (Titolare dell'oggetto).
 - **CodFiscale**: Codice fiscale del soggetto produttore (Titolare dell'oggetto).
 - **PartitaIVA**: Partita IVA del soggetto produttore (Titolare dell'oggetto).
 - **CodiceIPA**: Codice IPA del soggetto produttore (nel caso di Pubblica Amministrazione).
 - **PersonaFisica**: Indica se il soggetto produttore (Titolare dell'oggetto) è una persona fisica (true, false).



- **Produttori:** Elenco dei soggetti che hanno effettuato il trasferimento fisico degli oggetti digitali nel Sistema di Conservazione.
 - **Produttore:** soggetto che effettua il trasferimento fisico degli oggetti digitali nel Sistema di Conservazione.
 - **Denominazione:** Denominazione del Produttore.
 - **CodFiscale:** Codice fiscale del Produttore.
 - **PartitaIVA:** Partita IVA del Produttore. **CodiceIPA:** Codice IPA del Produttore(nel caso di Pubblica Amministrazione).
 - **PersonaFisica:** Indica se il Produttore è una persona fisica (true, false).
 - **IPdV_Versati**
 - **IdPdV:** Id del PdV versato nel Sistema di Conservazione.
- **DataGenerazione:** La data in formato UTC riferita alla produzione del PdD.
- **IpAdressClient:** Indirizzo IP da cui è arrivata la richiesta di estrazione del PdD
- **Richiedente:** Dati anagrafici del richiedente del PdD.
 - **Nome:** Nome del richiedente.
 - **Cognome:** Cognome del richiedente.
 - **CodiceFiscale:** Codice fiscale del richiedente.
 - **PartIVA:** Partita IVA del richiedente.
- **SoggettiProcesso,** Dati anagrafici dei soggetti Responsabile della conservazione, Operatore conservatore e Responsabile del servizio di conservazione.
 - **RdC:** Dati anagrafici del responsabile della conservazione (nome e cognome o ragione sociale, ruolo, codice fiscale o Partita IVA).
 - **Operatore:** Dati anagrafici dell'operatore conservatore (nome e cognome o ragione sociale, ruolo, codice fiscale o Partita IVA).
 - **RSdC:** Dati anagrafici del Responsabile del servizio di conservazione (nome e cognome o ragione sociale, ruolo, codice fiscale o Partita IVA).
- **AntiVirus:** Denominazione Software Antivirus e data/ora ultimo aggiornamento.
- **SdC:** Indicazioni anagrafiche del Sistema di conservazione.
 - **Nome:** Denominazione del Sistema di conservazione.
 - **Versione:** Versione del Sistema di conservazione.
- **PdAGruppo:** Descrizione del PdA estratto.
 - **PdA:** Descrizione del Pacchetto di Archiviazione.
 - **Id:** Id del Pacchetto di Archiviazione (identificativo univoco assegnato dal Sistema di Conservazione).
 - **FunzioneHash:** Tipo di funzione di hash usata per calcolare il valore.
 - **Hash:** Valore ricavato applicando la funzione di hash al file associato all'indice del PdA.
 - **UrlFile:** URI del file nel pacchetto.
 - **NumFileInfetti:** Eventuale numero file infetti contenuti nel PdD.
 - **FileGruppo:** Elenco dei file estratti.
 - **File**
 - **Id:** Id del documento assegnato dal Sistema di Conservazione
 - **IdDoc:** Id del documento nel sistema documentale o altro sistema



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

[Torna al Sommario](#)



7 IL PROCESSO DI CONSERVAZIONE

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

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

Di seguito viene rappresentato il processo di conservazione in conformità alle Linee Guida emanate da AgID.

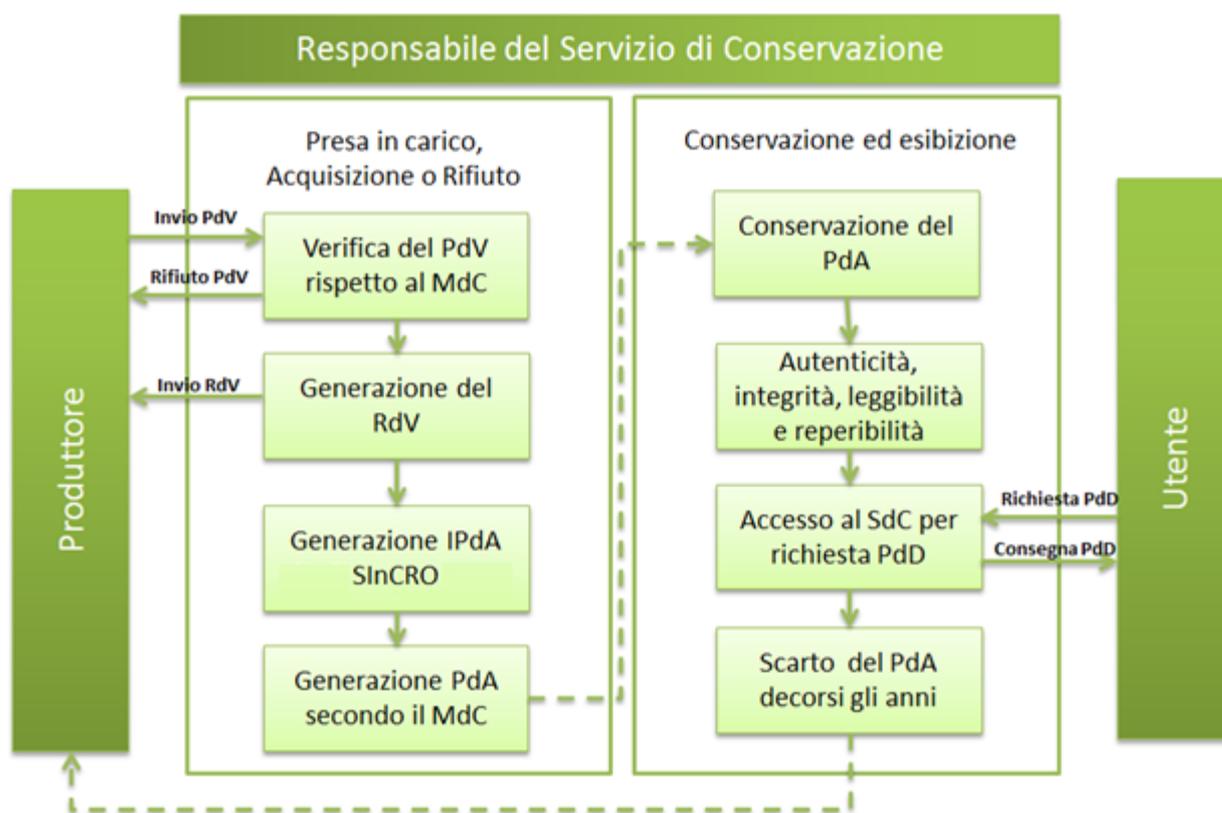


Figura 11 Processo di conservazione in Strongdox



7.1 Modalità di acquisizione dei Pacchetti di Versamento per la loro presa in carico

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

1. Tramite Web Services (processo sincrono)
2. Tramite sFTP e successivo caricamento all'interno di *Strongdox* (processo asincrono)

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

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

Entrambe le modalità di versamento garantiscono la sicurezza e riservatezza dei dati trasmessi grazie alla crittografia del canale adottato (HTTPS o sFTP). Il canale HTTPS integra sul protocollo base HTTP la crittografia di tipo Transport Layer Security (SSL/TLS), questa tecnica aumenta il livello di protezione contro gli attacchi.

Il certificato digitale utilizzato per la connessione HTTPS è fornito e garantito da GeoTrust.

Il protocollo sFTP prevede il trasferimento dei dati usando il protocollo SSH-2, che garantisce la cifratura delle informazioni trasmesse.

Le specifiche e il modello-dati adottati per il PdV sono i medesimi e la presa in carico per entrambe le modalità si conclude con il rilascio da parte del sistema *Strongdox* di:

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

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

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



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

Lo storage che mantiene le copie di backup è costituito da 3 repliche, due sul sito primario e una sul sito DR, questa architettura garantisce l'alta affidabilità e il recupero a seguito di un disastro.

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

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

Ulteriori specifiche concordate tra Produttore e Conservatore Namirial in merito alla sessione di versamento, alla generazione e trasformazione dei PdV, al modello-dati del PdV e alla presa in carico del PdV, sono dettagliate nella Scheda Servizio.

[Torna al Sommario](#)

7.2 Verifiche effettuate sui Pacchetti di Versamento e sugli oggetti in essi contenuti

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

- **(Bloccante)** Verifica che il pacchetto di versamento contenga l'IPdV ed i files. Controllo non effettuato col metodo *checkIndicePdV*.
- **(Bloccante)** Controllo validità del file IPdV con il file XSD.
- **(Bloccante)** Controllo che l'azienda definita nell'IPdV sia presente nel Sistema di Conservazione e che per questa azienda, nel sistema di conservazione sia impostato un soggetto per la firma dei RdV e dei PdA.
- **(Bloccante)** Controllo che il numero di files presenti nel PdV corrisponda al numero di files definiti nell'IPdV, 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'IPdV, abbiano una corrispondenza con i files contenuti nel Pacchetto (PdV). Controllo non effettuato col metodo *checkIndicePdV*.
- **(Bloccante)** Controllo che i nomi dei files presenti nel PdV corrispondano ai files definiti nell'IPdV. Controllo non effettuato col metodo *checkIndicePdV*.



- **(Bloccante)** Controllo che il tipo MIME (MimeType) dei files definito nell'IPdV 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. Controllo non effettuato col metodo *checkIndicePdV*.
- **(Bloccante)** Controllo che i percorsi degli allegati importati da altro Conservatore presenti nel PdV (all'interno della cartella riservata PdDPre) corrispondano agli allegati definiti nell'IPdV (PdDPre). Controllo non effettuato col metodo *checkIndicePdV*.
- **(Bloccante)** Verifica che i formati dei files contenuti nel pacchetto di Versamento siano nei formati previsti (vedere tabella dei formati ammessi).
- **(Bloccante)** Verifica della presenza di files nell'IPdV con Id documento NON specificato.
- **Bloccante: solo per i pacchetti di Revisione):** Verifica dei riferimenti della revisione e delle modifiche apportate dalla revisione per verificare la loro approvazione
- **(Bloccante)** Verifica della presenza di files nell'IPdV con lo stesso Id documento.
- **(Bloccante)** Se l'IPdV è firmato il sistema verifica che la firma sia valida, se non è firmato NON lo verifica. Controllo non effettuato col metodo *checkIndicePdV*.

Per ogni documento definito nell'IPdV si effettuano i seguenti controlli:

- **(Bloccante)** Verifica che la tipologia definita per il documento corrisponda a quella definita per l'IPdV (Vedere: SourceVdA).
- **(Bloccante)** Verifica che il numero di Metadati definiti per il documento corrisponda a quelli definiti all'interno della tipologia (definita nell'IPdV nella sezione SourceVdA).
- **(Bloccante)** Verifica che il nome e l'ordine dei Metadati definiti per il documento corrisponda a quanto definito all'interno della tipologia (definita nell'IPdV nella sezione SourceVdA).
- **(Bloccante)** Verifica della presenza del valore per i Metadati obbligatori, seguendo lo schema dei metadati (inserito nel PdV nella sezione SourceVdA).
- **(Bloccante)** Validazione del valore per i Metadati in base all'eventuale espressione regolare definita, seguendo lo schema dei metadati (inserito nel PdV nella sezione SourceVdA).
- **(Bloccante)** Verifica che non ci siano documenti con lo stesso Id documento, all'interno del Sistema di Conservazione, per la tipologia associata all'azienda
- **(Bloccante)** Se l'IPdV 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 PdV.
- **(Bloccante)** Verifica che l'Hash dei files non corrisponda al Hash del file da 0 byte
- **(Bloccante)** Verifica degli Hash degli allegati importati da altro Conservatore con il valore inserito all'interno della sezione PdDPre (non viene effettuato dal metodo *checkIndicePdV*).



- **(Bloccante)** Verifica della validità della firma sul file. Opzionale il controllo della verifica sui file firmati (non viene effettuato dal metodo checkIndicePdV).
- **(Bloccante)** Verifica dell'anno di riferimento documento: deve essere lo stesso per tutti i documenti (definito dell'IPdV nella sezione FileGroup/File/MoreInfo/MetaData/ReferenceDocYear).
- **(Bloccante)** Verifica della valorizzazione dei metadati aggiuntivi tramite i tag definiti per il documento (definiti nell'IPdV nella sezione: FileGroup/File/MoreInfo/TagPIndex)

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

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

[Torna al Sommario](#)

7.3 Accettazione dei Pacchetti di Versamento e generazione del Rapporto di Versamento

In caso di presa in carico, il Sistema genera il **Rapporto di Versamento** (RdV), quale esito di tutte le verifiche effettuate sul PdV a partire dalla sua ricezione. Il Rapporto di Versamento è previsto dalle Linee Guida ed ha lo scopo di formalizzare l'acquisizione degli oggetti da conservare. Tale rapporto contiene il riferimento ad uno o più Pacchetti di versamento.

La generazione del RdV avviene tramite la schedulazione di un job all'interno dello schedatore integrato nel Sistema di conservazione.

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

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

Il RdV 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 PdV;
- Data di generazione del RdV;
- Dati del Responsabile della conservazione associato al Titolare dell'oggetto;
- Dati del delegato Conservatore;
- Dati del Responsabile del servizio di conservazione;
- Numero di PdV inclusi nel RdV;



- Numero totale dei files contenuti nei PdV inclusi all'interno del RdV
- Informazioni sul tipo di PdV valorizzato (primo versamento, riversamento da altro sistema o revisione)
- Informazioni sull'eventuale versione della revisione o PdV di origine
- La funzione di Hash con cui è stato generato l'hash del IPdV;
- Hash del/i IPdV considerato/i nel RdV;
- L'indirizzo IP della macchina dove è stato generato il PdV
- 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 PdV da parte del Sistema di conservazione.

Di seguito è riportata la struttura del Rapporto di Versamento:

DescGenerale

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

PdVGruppo (1-n), Costituisce il gruppo di PdV considerati dal RdV.

- **PdV**
- **Id**, Id del Pdv incluso nel Rapporto.
- **RevisionIdPdV**, Id del PdV revisionato. (Può essere il PdV di origine oppure l'ultima revisione pubblicata per il PdV di origine). Il nodo è presente solo se il PdV rappresenta una revisione.
- **RevisionIdPdVOrigin**, Id del PdV di origine (PdV iniziale da cui hanno origine tutte le revisioni). Il nodo è presente solo se il PdV rappresenta una revisione.
- **RevisionNumber**, Numero della revisione necessario per ordinare la sequenza delle revisioni relative al PdV di origine. Il nodo è presente solo se il PdV rappresenta una revisione.



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

Inoltre, il Rapporto di Versamento (RdV) contiene il Tag "<DataGenerazione>" quale riferimento temporale in formato UTC (Tempo Universale Coordinato) ed è firmato digitalmente dal Responsabile del servizio di conservazione.

Per quanto riguarda i riferimenti temporali si evidenzia che l'orologio di sistema di tutti gli elaboratori impiegati nel servizio è sincronizzato con il protocollo NTP Time.nist.gov.

Ulteriori specifiche sulla generazione del RdV e il modello dati dello stesso sono dettagliate nella Scheda Servizio.

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

- **attraverso comunicazione via PEC o mail ordinaria**, secondo l'indirizzo di posta elettronica configurato nel Sistema di conservazione Strongdox nella anagrafica del Produttore (servizio configurato su richiesta del Cliente e concordato nella Scheda Servizio o, quando prevista, nella Richiesta di attivazione); la e-mail viene formattata in modo automatico dal Sistema e in allegato viene inserito il RdV firmato dal responsabile del servizio 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, secondo le modalità specificate nel documento Strongdox SDK eventualmente allegato alla Scheda Servizio;
- **tramite accesso alla piattaforma web** del Sistema di conservazione Strongdox da parte di un Utente autorizzato per quel determinato Produttore.

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

[Torna al Sommario](#)

7.4 Rifiuto dei Pacchetti di Versamento e modalità di comunicazione delle anomalie

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

- PdV non contiene l'indice IPdV e i documenti;
- File IPdV 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 PdV si riferisce;
- nel Sistema di conservazione non è configurato il Responsabile della conservazione per il Soggetto produttore a cui il PdV si riferisce;
- Numero di files presenti nel PdV non corrispondente al numero di files dichiarati nell'IPdV;
- Nomi dei files presenti nel PdV non corrispondenti ai nomi files definiti nell'IPdV;
- Esito negativo della verifica del tipo MIME dichiarato nell'IPdV (MimeType tra quelli ammessi per la conservazione dei files);
- Esito negativo della verifica dei formati dichiarati nell'IPdV (formati tra quelli ammessi per la conservazione dei files);
- Presenza di files nell'IPdV con Id documento non specificato;
- Presenza di files nell'IPdV con lo stesso Id documento;
- Esito negativo della verifica di validità della firma digitale (solo se l'IPdV è firmato);
- Esito negativo della verifica di corrispondenza tra la tipologia documentale configurata nel Sistema di conservazione e quella dichiarata nell'IPdV (campo: SourceVdA);
- Esito negativo della verifica di corrispondenza tra i metadati configurati nel Sistema di conservazione per una specifica tipologia documentale e i metadati dichiarati nell'IPdV (campo: SourceVdA);
- Esito negativo della verifica di corrispondenza tra il nome e l'ordine dei metadati configurati nel Sistema di conservazione per una specifica tipologia documentale e quelli dichiarati nell'IPdV (campo: SourceVdA);



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

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

Il Conservatore Namirial consente al Produttore di avere a disposizione gli esiti di presa in carico tramite dialogo applicativo web service o tramite sFTP nella cartella di destinazione "RX".

Si riporta un esempio di generazione del file *Esito di presa in carico* (estensione .esito) messo a disposizione del Produttore:

```
<?xml version="1.0" encoding="utf-8"?>
<EsitoPresalInCarico>
<NomeFile><![CDATA[Files.zip]]></NomeFile>
<DataVersamento>2014-09-11T07:58:01Z</DataVersamento>
<Id>000000001_2014</Id>
<IdPdV>54115609b84ac914886a905b</IdPdV>
<HashIPdV>B6D3163419584386155E39810111ED69BF8D7166FF38502A451371DB42DA0186</HashIPdV>
<FunzioneHashIPdV>SHA-256</FunzioneHashIPdV>
<CodFiscale>COD_FISCALE</CodFiscale>
<PartitaIVA>IT:PARTITA_IVA</PartitaIVA>
<Errori />
</EsitoPresalInCarico>
```

Gli elementi presenti nel file di esito hanno il seguente significato:

- *NomeFile*: Nome file del Pacchetto di Versamento.
- *DataVersamento*: Data e ora in cui l'agent ha preso in carico il PdV.
- *Id*: Progressivo (es.: Guid) generato dal Sistema Documentale, oppure dal sistema che ha prodotto il PdV. Viene inserito all'interno dell'IPdV da parte del Produttore.
- *IdPdV*: Id univoco del PdV assegnato dal Sistema di conservazione.



- *HashIPdV*: Hash del file IPdV.
- *FunzioneHashIPdV*: Funzione di hash con cui è stata calcolato l'hash dell'IPdV.
- *IdSetup*: Id dell'installazione a cui si riferisce il PdV.
- *IdCompany*: Id dell'azienda titolare dei documenti a cui si riferisce il PdV.
- *CodFiscale*: Codice Fiscale del Produttore ricavato dal PdV.
- *PartitaIVA*: Partita Iva del Produttore ricavata dal PdV.
- *Errori*: Lista di eventuali errori verificatisi in fase di acquisizione (vedi esempio sotto)

Si riporta un esempio di possibili errori che possono essere riscontrati dai controlli del Sistema di conservazione *Strongdox*:

<Errori>

```
<Errore><![CDATA[Il file indice PdV contiene 1 files, mentre nel pacchetto sono presenti 2 files.]]></Errore>  
<Errore><![CDATA[Il file NON è presente nel file indice PdV, ma è presente nel pacchetto. Nome file:  
1.pdf]]></Errore></Errori>
```

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

[Torna al Sommario](#)

7.5 Preparazione e gestione del Pacchetto di Archiviazione

La generazione dell'IPdA avviene secondo le specifiche delle Linee Guida emanate da AgID e secondo il modello-dati definito dallo standard SInCRO – Supporto all'interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386).

La generazione dell'IPdA corrisponde alla chiusura definitiva del processo di conservazione a norma. Questa procedura viene avviata nel sistema *Strongdox* tramite un job configurato a sistema, sulla base delle regole di conservazione configurate nel sistema per il Titolare dell'oggetto.

Su ciascun IPdA sono apposti la firma del Responsabile del Servizio e la marca temporale rendendo imm modificabili i Pacchetti di Versamento inclusi nel PdA.

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 PdA, registra i log per la tracciatura delle azioni effettuate sui Pacchetti di Archiviazione.

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

[Torna al Sommario](#)



7.6 Cifratura degli oggetti di conservazione

Gli oggetti informatici vengono crittografati con crittografia lato server e chiavi gestite da Amazon S3 (SSE-S3), servizio fornito da Amazon AWS (Regione italiana), in qualità di datacenter Namirial.

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).

7.7 Preparazione e gestione del Pacchetto di Distribuzione ai fini dell'esibizione

Il Pacchetto di Distribuzione (PdD) può essere richiesto:

- via **interfaccia web** *Strongdox*.
- via interrogazione **web service**.

Una volta che l'Utente richiede un PdD il sistema restituisce tramite canale crittografato (su protocollo HTTPS) il pacchetto in formato di cartella compressa .zip costituito dagli oggetti digitali previsti dalla richiesta di distribuzione. Le tipologie di Pacchetti di Distribuzione e i modelli-dati sono descritti nel paragrafo 6.4 del presente manuale.

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

Lo storage che mantiene i Pacchetti di Archiviazione e dei Pacchetti di Distribuzione è costituito da 3 repliche, due sul sito primario e una sul sito DR: questa architettura garantisce l'alta affidabilità e il recupero dei dati a seguito di corruzione o perdita dei dati.

[Torna al Sommario](#)

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

L'Utente autorizzato ad accedere al Sistema di conservazione *Strongdox* può eseguire le ricerche attraverso un'interfaccia web e tramite l'ausilio di chiavi di ricerca (metadati) predefinite.

Una volta ottenuto l'output della ricerca l'Utente ha la possibilità di richiedere la distribuzione di un PdD o più semplicemente il download dei duplicati dei documenti informatici conservati, per singolo documento o per range di documenti.



La richiesta e l'ottenimento di un duplicato di un documento informatico conservato può essere avanzata anche attraverso chiamate web service.

Inoltre, l'Utente può inoltrare richiesta in merito alla necessità di ricevere duplicati. Il Conservatore Namirial potrà in tal caso mettere a disposizione secondo la modalità concordata in un pacchetto contenitore tutti i duplicati richiesti dall'Utente.

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

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

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

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

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

Questo documento viene posto in conservazione nel sistema come allegato integrativo (collegamento tramite hash tra i PdA) assieme al documento copia conforme e poi entrambi conservati. Tutte le evidenze dell'operazione eseguita vengono mantenute nel tempo dal Conservatore e dal Responsabile del servizio di conservazione.

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

[Torna al Sommario](#)

7.9 Scarto dei Pacchetti di Archiviazione

Superato il periodo di conservazione di pacchetti e documenti concordato tra Conservatore e Titolare, il sistema *Strongdox* deve implementare la procedura di scarto dei Pacchetti di Archiviazione.

Il sistema notifica (via mail/pec) al Titolare, con 30 gg di anticipo (salvo diversi accordi tra Titolare e Conservatore, specificati nella Scheda Servizio condivisa), l'avvio della funzione di scarto per determinati PdA, dandone quindi informativa secondo la normativa vigente e fornendo le informazioni necessarie al Titolare per valutare l'eventuale richiesta di estensione del periodo di conservazione.

In caso di superamento della scadenza prefissata e in assenza di richiesta di estensione, il job della procedura di scarto si attiva e produce dei Pacchetti di Scarto (PdS) in relazione ai PdA oggetto della procedura. L'operazione è tracciata nel sistema e viene prodotto un file Indice del Pacchetto di Scarto (IPdS) firmato



digitalmente dal Responsabile del servizio di conservazione, che grazie al file XSLT può essere visualizzato dal Titolare dei documenti o da altri soggetti interessati, per la verifica della corretta procedura eseguita.

In ultimo, nel sistema *Strongdox* viene registrato se la gestione della procedura di scarto è relativa ad archivi pubblici o privati che rivestono interesse storico particolarmente importante; in tal caso si attiva un alert e la procedura di scarto del Pacchetto di Archiviazione avviene solo previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo, rilasciata al Titolare secondo quanto previsto dalla normativa vigente in materia e secondo gli accordi definiti nella Scheda Servizio.

[Torna al Sommario](#)

7.10 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 il Pacchetto di Archiviazione generato secondo le regole tecniche in materia di Sistema di Conservazione e secondo lo standard nazionale UNI SINCRO 11386.

La sua distribuzione attraverso la richiesta di uno o più Pacchetti di Distribuzione (PdD) tramite diverse funzionalità e modalità (interfaccia web, web service, sFTP, ecc.) messe a disposizione dal servizio *Strongdox* garantisce la corretta trasferibilità da parte del Titolare dell'oggetto ad altro conservatore.

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

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

Il sistema *Strongdox* è in grado di acquisire pacchetti di versamento/pacchetti di archiviazione conformi con la struttura UNI SINCRO 11386 nel caso di subentro su archivi gestiti da altro conservatore che abbia adottato tale standard per la generazione dell'IPdA.

[Torna al Sommario](#)



8 IL SISTEMA DI CONSERVAZIONE

Strongdox è la soluzione del Conservatore Namirial per la conservazione a norma di documenti informatici.

L'infrastruttura di erogazione del servizio *Strongdox* è stata concepita, organizzata e sviluppata in modo che le varie fasi di lavoro risultino atomiche e che il flusso sia modulare.

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

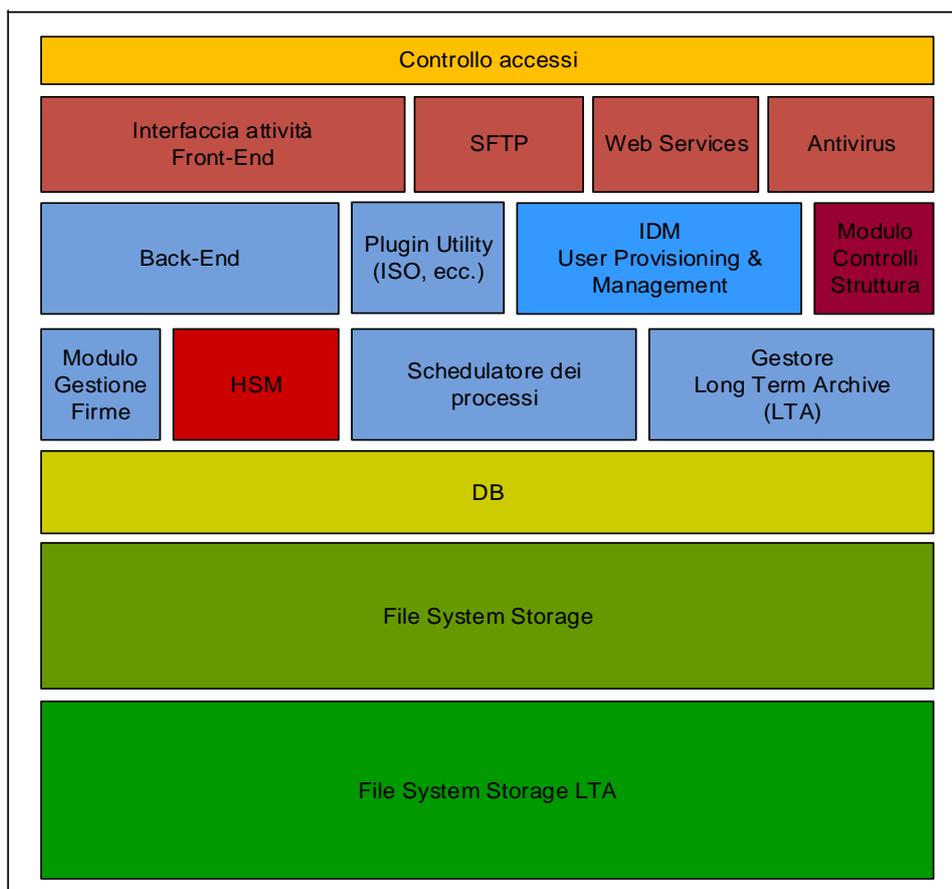


Figura 13 Componenti del Sistema di conservazione Strongdox

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, distribuzione pacchetti, produzione di copie e duplicati, e altre attività eseguibili dagli amministratori.
- Modulo SFTP per il caricamento massivo dei Pacchetti di Versamento (PdV).
- Modulo Web Service per le attività di caricamento e gestione pacchetti e documenti.
- Antivirus.



- Modulo di back end per tutte le attività di interfaccia con il DB e il Filesystem.
- Modulo delle utility (creazione ISO, ecc.).
- Modulo IDM – User Provisioning e Management per la gestione dell'access management.
- Scheduler dei processi. Nello scheduler vengono gestiti i job per:
 - la presa in carico di PdV;
 - l'avvio dei controlli di coerenza;
 - la generazione degli esiti di presa in carico;
 - la generazione e consegna dei RdV;
 - la generazione dei PdA;
 - la generazione e la consegna dei PdD;
 - la generazione dei PdS.
- 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 dell'archivio di lunga durata (LTA).

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

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

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

[Torna al Sommario](#)



8.1 Componenti Logiche

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

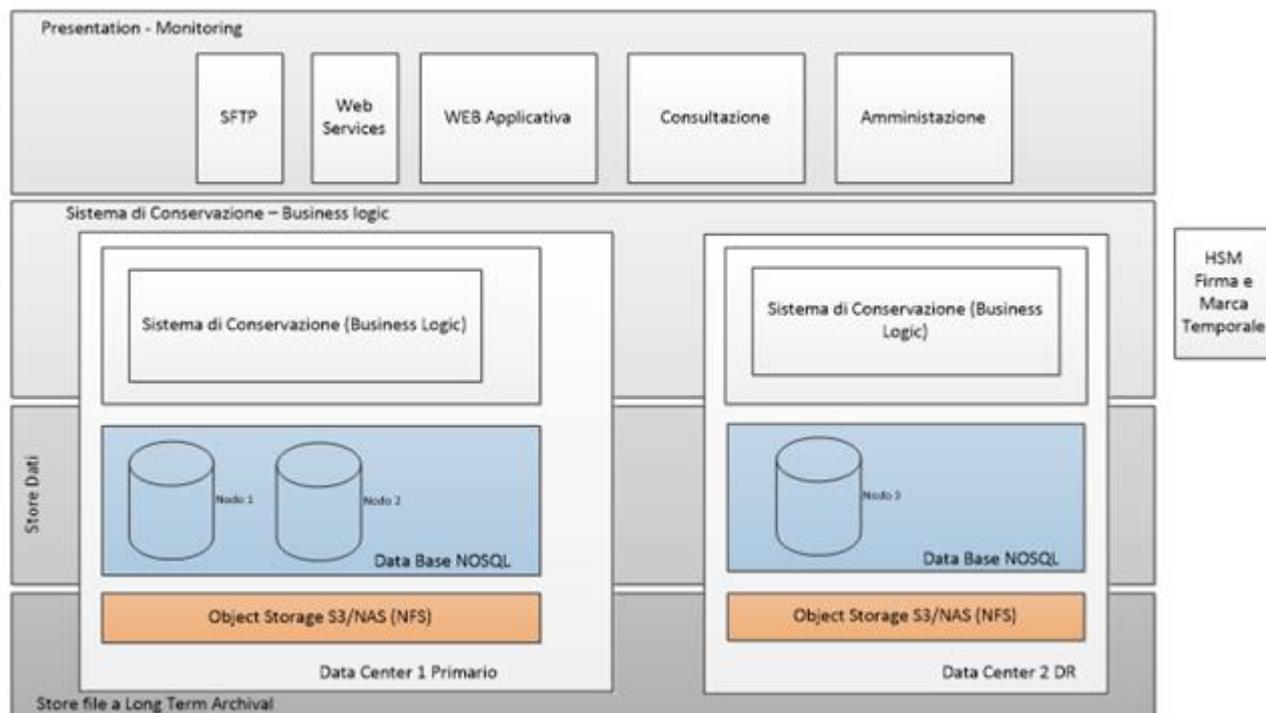


Figura 14 Componenti logiche del Sistema di Conservazione Strongdox

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

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

SdC Web Service: il servizio di conservazione di documenti informatici che espone tutte le funzioni per la gestione applicativa del processo di conservazione.

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

Schedulatore di processi: la sua configurazione permette di definire la sessione di versamento, la predisposizione e gestione dei Pacchetti di Archiviazione, 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 schedatore 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 (Pacchetto di Versamento, Pacchetto di Archiviazione, Pacchetto di Distribuzione, Pacchetto di Scarto).

Database del Sistema di conservazione: *Strongdox* 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/NFS): *Strongdox* supporta lo storage dei file sia su NAS che su sistema Object Storage.

[Torna al Sommario](#)

8.2 Componenti Tecnologiche

L'architettura tecnologica del Sistema di conservazione *Strongdox* può essere suddivisa in 3 livelli:

- Primo livello. La parte di networking che è costituita dagli apparati di rete (router, switch), dal modulo firewall per la protezione del sistema da accessi indesiderati. Dal WAF (Web Application Firewall) e i load balancer che stabilizzano l'applicativo e di suddividono il carico tra le varie macchine che erogano i servizi raggiungibili pubblicamente.
- 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.

- Terzo livello. rappresenta il datastore del sistema e contiene tutti i documenti e tutti i Pacchetti di Archiviazione.

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 *Strongdox* eroga i servizi su data center Amazon AWS.

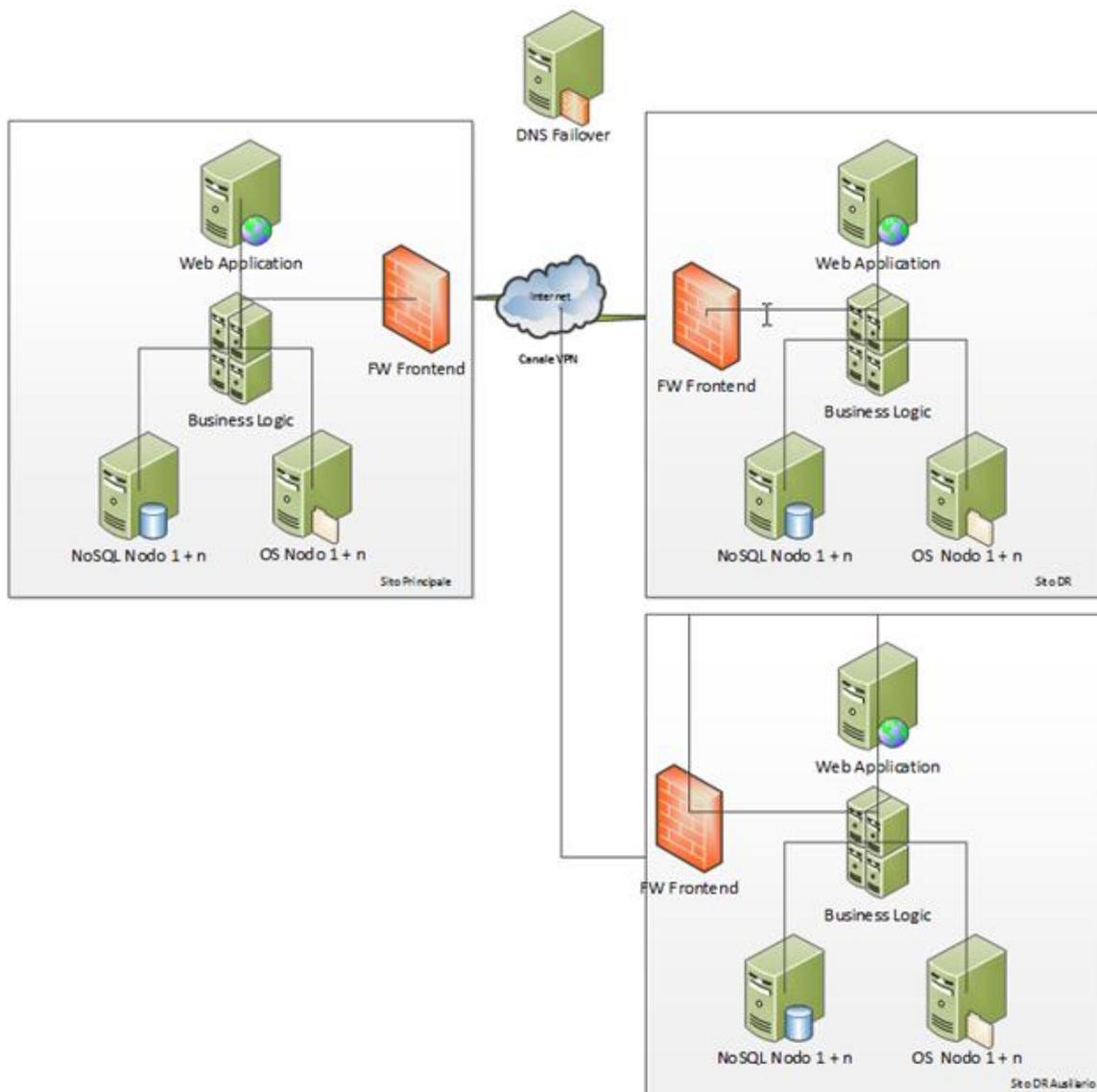


Figura 95 Macro architettura di collegamento dei siti di DR

- Sito Primario, situato su datacenter Amazon AWS nella Region Italiana con tutte le componenti necessarie in HA e collegato tramite connettività descritta sotto.
- Sito DR (Disaster Recovery), situato su data center AWS Amazon sulla Region EU-Central-1 (Francoforte) gestito e amministrato tramite interfaccia di gestione Amazon.

La gestione e l'amministrazione del portale dashboard AWS è in carico al team di Cloud Operation di Namirial tramite account dedicato. Il team è coordinato dal Responsabile dei sistemi.



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

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

La distanza delle Region Primaria e Sito DR sono:

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

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 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.).

8.4.1 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 *Strongdox*, 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.

8.4.2 Gestione e mantenimento dei log

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

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

I log sono mantenuti per oltre dieci anni dal Conservatore.

8.4.3 Monitoraggio del Sistema di conservazione

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

Il sistema di monitoring adottato SysAid è descritto più dettagliatamente nel capitolo 9.



8.4.4 Change management

Il processo di change management sul servizio istanziato dal Cliente, attraverso la piattaforma di ticketing, è gestito dalle risorse associate a Ufficio Conservazione e prevede l'avvio del processo attraverso l'aggiornamento e la condivisione di una nuova versione della Scheda Servizio, che recepisce la modifica richiesta.

Il change management dell'infrastruttura di erogazione del servizio è, invece, gestito e descritto dal Conservatore Namirial in conformità alla certificazione ISO/IEC 27001.

8.4.5 Verifica periodica di conformità a normativa e standard di riferimento

Con periodicità almeno semestrale il Responsabile del servizio di conservazione effettua 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, non esaustivo, 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 qualità e al presente manuale.

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

- verifica delle funzionalità di creazione e mantenimento dei rapporti di versamento, dei Pacchetti di Archiviazione, ecc;
- verifica delle funzionalità di distribuzione 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.

Tali attività di verifica sono riepilogate in un verbale di audit.

8.4.6 Gestione della sicurezza e valutazione del rischio

Per la descrizione della gestione della sicurezza aziendale, dell'analisi dei rischi e della continuità operativa si rimanda a tutta la documentazione relativa al ISMS, certificato ISO/IEC 27001.

[Torna al Sommario](#)

9 MONITORAGGIO E CONTROLLI

La strategia adottata da Namirial prevede che la pianificazione, la struttura organizzativa a supporto e gli strumenti di continuità operativa sviluppati comprendono 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 *Strongdox* 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 SysAid per il ticketing. Nagios al verificarsi di un evento anomalo legato alle risorse hardware o ai servizi applicativi notifica al SOC 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 servizio), deve effettuare le opportune manutenzioni per chiudere l'anomalia. Il sistema inoltre prevede delle policy di escalation verso i supervisor 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.

Gli utenti del sistema di conservazione *Strongdox* usano la piattaforma di ticketing Jira Service Desk per richiedere supporto all'help desk di I livello. I ticket vengono generati riportano le seguenti informazioni:



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

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

SysAid, 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 RdV, PdA, PdD, 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 SysAid 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 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 (IPdA) presenti all'interno del Sistema di conservazione per un determinato Titolare).

Per quanto riguarda la verifica di leggibilità, nel Sistema di conservazione *Strongdox* 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: attraverso il calcolo automatico dell'hash del documento e relativa comparazione con l'hash registrato in fase di creazione del PdA;
- 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. A seguito di ogni operazione di controllo verrà prodotto un Verbale firmato digitalmente dal Responsabile del servizio di conservazione e conservato nel Sistema di conservazione *Strongdox*.

[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 *Strongdox* adotta diversi controlli automatici a garanzia dell'integrità e della coerenza dei dati movimentati dal sistema e durante il processo; i controlli automatici richiedono l'intervento della struttura



organizzativa a supporto del servizio di conservazione solo al verificarsi di anomalie non gestibili in modo automatico.

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

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

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

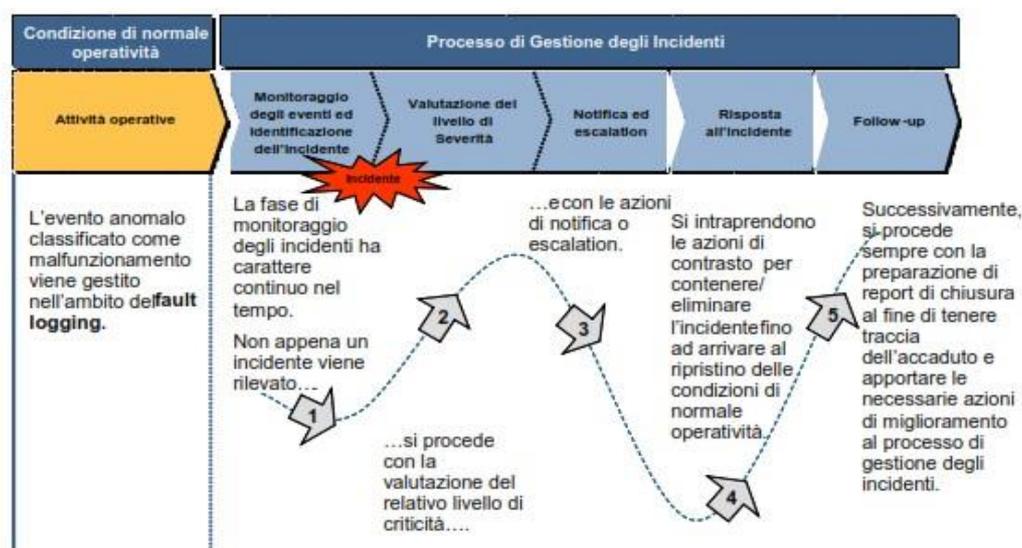


Figura 16 Incident Management

Al verificarsi di malfunzionamenti o situazioni critiche, il sistema di monitoraggio SysAid genera delle notifiche via e-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](#)