



# Manuale di Conservazione

**di NAMIRIAL S.p.A.**

**EMISSIONE DEL DOCUMENTO**

<b>Azione</b>	<b>Data</b>	<b>Nominativo</b>	<b>Funzione</b>
<i>Redazione</i>	12/02/2016	Davide Coletto	Responsabile del servizio di conservazione
<i>Verifica</i>	17/02/2016	Matteo Sisti - Andrea Lazzari	Responsabile della funzione archivistica di conservazione - Responsabile della sicurezza dei sistemi per la conservazione
<i>Approvazione</i>	22/02/2016	Davide Coletto - Paolo Giacometti	Responsabile del servizio di Conservazione - Legale rappresentante

**REGISTRO DELLE VERSIONI**

<b>N°Ver/Rev/Bozza</b>	<b>Data emissione</b>	<b>Descrizione</b>	<b>Osservazioni</b>
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

## INDICE DEL DOCUMENTO

<b>1</b>	<b>SCOPO E AMBITO DEL DOCUMENTO .....</b>	<b>5</b>
<b>2</b>	<b>TERMINOLOGIA .....</b>	<b>7</b>
2.1	Glossario .....	7
2.2	Acronimi .....	13
<b>3</b>	<b>NORMATIVA E STANDARD DI RIFERIMENTO .....</b>	<b>15</b>
3.1	Normativa di riferimento .....	15
3.2	Standard di riferimento .....	16
<b>4</b>	<b>RUOLI E RESPONSABILITÀ .....</b>	<b>17</b>
<b>5</b>	<b>STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE .....</b>	<b>21</b>
5.1	Organigramma .....	21
5.2	Strutture organizzative .....	23
<b>6</b>	<b>OGGETTI SOTTOPOSTI A CONSERVAZIONE .....</b>	<b>28</b>
6.1	Oggetti conservati .....	29
6.2	Pacchetto di versamento .....	32
6.3	Pacchetto di archiviazione .....	36
6.4	Pacchetto di distribuzione .....	39
<b>7</b>	<b>IL PROCESSO DI CONSERVAZIONE .....</b>	<b>42</b>
7.1	Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico .....	44
7.2	Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti .....	45
7.3	Accettazione dei pacchetti di versamento e generazione del rapporto di versamento .....	48
7.4	Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie .....	49
7.5	Preparazione e gestione del pacchetto di archiviazione .....	53
7.6	Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione .....	54
7.7	Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti .....	54
7.8	Scarto dei pacchetti di archiviazione .....	56
7.9	Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori .....	56
<b>8</b>	<b>IL SISTEMA DI CONSERVAZIONE .....</b>	<b>58</b>
8.1	Componenti Logiche .....	60
8.2	Componenti Tecnologiche .....	61
8.3	Componenti Fisiche .....	62
8.4	Procedure di gestione e di evoluzione .....	64
<b>9</b>	<b>MONITORAGGIO E CONTROLLI .....</b>	<b>68</b>

9.1	Procedure di monitoraggio .....	68
9.2	Verifica dell'integrità degli archivi .....	70
9.3	Soluzioni adottate in caso di anomalie .....	70

## 1 SCOPO E AMBITO DEL DOCUMENTO

Il presente documento rappresenta il Manuale della Conservazione del servizio *Strongdox*, erogato e gestito da Namirial S.p.A., ed è adottato secondo le disposizioni dell'art. 8 del DPCM 3 dicembre 2013.

Il presente Manuale ha lo scopo di illustrare dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, la comunità di riferimento, 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 il disposto dell'art. 8 del DPCM 3 dicembre 2013.

Il Manuale, inoltre, descrive tutte le procedure e le prassi seguite dal Responsabile della Conservazione e 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 ed 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 ed il modello di riferimento OAIS (Open Archival Information System) standard ISO 14721:2012;
- **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 per un produttore dei documenti ben identificato, con il quale preventivamente sono stati concordati tutti gli aspetti connessi alla conservazione ed alla fruizione del patrimonio informativo digitale, in conformità al modello di riferimento OAIS (Open Archival Information System) standard ISO 14721:2012;
- **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 ed uno studio preliminare delle esigenze del produttore dei documenti e degli utenti del sistema, in conformità al modello di riferimento OAIS (Open Archival Information System) standard ISO 14721:2012, ed è riportata come *addendum* al presente manuale, parte integrante e sostanziale dello stesso.

Il presente Manuale della Conservazione è collegato ai documenti riportati nella successiva tabella, che entrano più nel dettaglio in diversi aspetti del sistema di conservazione e costituiscono parti integranti e sostanziali del Manuale della Conservazione.

Documenti collegati	
<b><i>Specificità del Contratto</i></b>	<p>È un documento disciplinare che contiene le specifiche forniture del servizio di conservazione (SPECIFICITÀ DEL CONTRATTO) per i titolari e i produttori dei documenti. Può essere denominato Scheda Servizio o Richiesta/Modulo di Attivazione.</p> <p>È parte integrante del contratto di servizi sottoscritto tra le parti e del Manuale di conservazione, redatto dal Conservatore sulla base delle informazioni condivise con il produttore dei documenti (Cliente), contenente i requisiti essenziali del Servizio, le relative specifiche tecnico-funzionali e procedurali per le varie fase del servizio (attivazione, versamento, conservazione, post-produzione, distribuzione) oltre ai livelli di Servizio (SLA); tale documento è redatto in fase di analisi, prima del primo processo di conservazione. Ogni variazione delle modalità di erogazione del Servizio, dovuta a richieste del Cliente o a evoluzioni del Sistema di conservazione, comporta la necessità di aggiornare la Scheda Servizio Cliente – Specificità del Contratto.</p>
<b><i>Piano per la Sicurezza</i></b>	<p>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</p>

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 della Conservazione, 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.	Glossario dei termini	
[1]	<b>Accesso</b>	Operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici
[2]	<b>Accreditamento</b>	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]	<b>Affidabilità</b>	Caratteristica che esprime il livello di fiducia che l'utente ripone nel documento
[4]	<b>Aggregazione documentale informatica</b>	Aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente
[5]	<b>Archiviazione</b>	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]	<b>Archivio</b>	Complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività
[7]	<b>Archivio informatico</b>	Archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico
[8]	<b>Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico</b>	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico
[9]	<b>Autenticazione del documento informatico</b>	La validazione del documento informatico attraverso l'associazione di dati informatici relativi all'autore o alle circostanze, anche temporali, della redazione
[10]	<b>Autenticità</b>	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]	<b>Base di dati</b>	Collezione di dati correlati e registrati tra loro
[12]	<b>Certificato qualificato</b>	Il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva
[13]	<b>Certification authority (CA)</b>	Il soggetto che secondo quanto disposto dall'art. 27 del CAD presta servizi di certificazione delle firme elettroniche qualificate o che fornisce altri servizi connessi con queste ultime, quali ad esempio quello delle marche temporali

N.	Glossario dei termini	
[14]	<b>Chiave privata</b>	L'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico
[15]	<b>Chiave pubblica</b>	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]	<b>Ciclo di gestione</b>	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]	<b>Comunità di riferimento</b>	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]	<b>Conservatore accreditato</b>	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, dall'Agenzia per l'Italia digitale
[19]	<b>Conservazione</b>	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione
[20]	<b>Copia analogica del documento informatico</b>	Documento analogico avente contenuto identico a quello del documento informatico da cui è tratto
[21]	<b>Copia di sicurezza</b>	Copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell'art. 12 del DPCM 3 dicembre 2013
[22]	<b>Copia informatica di documento analogico</b>	Il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto
[23]	<b>Copia informatica di documento informatico</b>	Il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari
[24]	<b>Copia per immagine su supporto informatico di documento analogico</b>	Il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto
[25]	<b>Destinatario</b>	Identifica il soggetto/sistema al quale il documento informatico è indirizzato
[26]	<b>Dispositivo sicuro per la creazione della firma:</b>	I dispositivi sicuri per la generazione della firma qualificata che devono essere dotati di certificazione di sicurezza secondo l'art. 35 del CAD
[27]	<b>Documento analogico</b>	La rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti
[28]	<b>Documento informatico</b>	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
[29]	<b>Duplicato informatico</b>	Documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario

N.	Glossario dei termini	
[30]	<b>Esibizione</b>	Operazione che consente di visualizzare un documento conservato e di ottenerne copia
[31]	<b>Evidenza informatica</b>	Una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica
[32]	<b>Fascicolo informatico</b>	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 Codice dell'Amministrazione Digitale (D. Lgs. 7 marzo 2005, n. 82 e successive modifiche ed integrazioni)
[33]	<b>Firma elettronica</b>	L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica
[34]	<b>Firma elettronica avanzata</b>	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]	<b>Firma elettronica qualificata</b>	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
[36]	<b>Firma digitale</b>	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]	<b>Formato</b>	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
[38]	<b>Formazione</b>	Il processo atto ad assicurare l'autenticità dell'origine e l'integrità del contenuto dei documenti informatici, con apposizione della firma digitale su ciascun singolo documento e/o della marca temporale ai fini di associare una data certa elettronica ove richiesto
[39]	<b>FTP Server</b>	Programma che permette di accettare connessioni in entrata e di comunicare in maniera sicura con un Client attraverso il protocollo FTP
[40]	<b>Funzioni archivistiche</b>	Funzioni per la conservazione delle informazioni (acquisizione, archiviazione, gestione dei dati, accesso, distribuzione)
[41]	<b>Funzione di hash</b>	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

N.	Glossario dei termini	
[42]	<b>Identificativo univoco</b>	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]	<b>Identificazione informatica</b>	La validazione dell'insieme di dati attribuiti in modo esclusivo ed 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]	<b>IDM</b>	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]	<b>Immodificabilità</b>	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
[46]	<b>Impronta</b>	La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash
[47]	<b>Indice del Pacchetto di Archiviazione</b>	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 11386:2010)
[48]	<b>Indice del Pacchetto di Versamento</b>	Struttura dell'insieme dei dati a supporto del processo di versamento del pacchetto di versamento (PdV), ispirata allo standard internazionale OAIS ISO 14721:2012 e definita nello specifico dal Conservatore in accordo con il produttore dei documenti
[49]	<b>Indice del Pacchetto di Distribuzione</b>	Struttura dell'insieme dei dati a supporto del processo di distribuzione del pacchetto di distribuzione (PdD), ispirata allo standard internazionale OAIS ISO 14721:2012 e definita nello specifico dal Conservatore in accordo con il produttore dei documenti
[50]	<b>Insieme minimo di metadati del documento informatico</b>	Complesso dei metadati, la cui struttura è descritta nell'allegato 5 del DPCM 3 dicembre 2013, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta
[51]	<b>Integrità</b>	Insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato
[52]	<b>Interoperabilità</b>	Capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi
[53]	<b>Leggibilità</b>	Insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti
[54]	<b>Log di sistema</b>	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
[55]	<b>Manuale di conservazione</b>	Strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'art. 8 del DPCM 3 dicembre 2013, regole tecniche in materia di sistema di conservazione.

N.	Glossario dei termini	
[56]	<b>Memorizzazione</b>	Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici
[57]	<b>Metadati</b>	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; tale insieme è descritto nell'allegato 5 del DPCM 3 dicembre 2013
[58]	<b>Originali non unici</b>	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]	<b>Pacchetto di archiviazione</b>	Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del DPCM 3 dicembre 2013 e secondo le modalità riportate nel manuale di conservazione
[60]	<b>Pacchetto di distribuzione</b>	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta
[61]	<b>Pacchetto di versamento</b>	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione
[62]	<b>Pacchetto di scarto</b>	Pacchetto contenente i documenti da scartare dal Sistema di conservazione perché hanno raggiunto il loro termine temporale di conservazione
[63]	<b>Pacchetto informativo</b>	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]	<b>Piano per la sicurezza</b>	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]	<b>Presa in carico</b>	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione
[66]	<b>Processo di conservazione</b>	Insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 9 delle regole tecniche sul sistema di conservazione
[67]	<b>Produttore</b>	Persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale
[68]	<b>Rapporto di versamento</b>	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore
[69]	<b>Responsabile della conservazione</b>	Soggetto, individuato dall'art. 44 del CAD e dall'art. 6, c. 5, del DPCM 3 Dicembre 2013, i cui compiti generali sono quelli di definire

N.	Glossario dei termini	
		e attuare le politiche complessive del sistema di conservazione e di governarne la gestione con piena responsabilità ed autonomia, in relazione al modello organizzativo della conservazione adottato. I compiti ed il ruolo del responsabile della conservazione, che è persona fisica inserita stabilmente nell'organico del soggetto produttore dei documenti, sono stabiliti dall'art. 7, c. 1, del DPCM 3 dicembre 2013. Ai sensi dell'art. 7, c. 3, del DPCM 3 Dicembre 2013, nelle pubbliche amministrazioni il ruolo del responsabile della conservazione è svolto da un dirigente o da un funzionario formalmente designato
[70]	<b>Responsabile del trattamento dei dati</b>	Soggetto esterno a cui è affidato il processo di conservazione che assume il ruolo di responsabile del trattamento dei dati, così come previsto dal Codice in materia di protezione dei dati personali ed espressamente richiamato dall'art. 6, punto 8) del DPCM 3 Dicembre 2013
[71]	<b>Responsabile del servizio di conservazione</b>	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]	<b>Responsabile della funzione archivistica di conservazione</b>	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]	<b>Responsabile del trattamento dei dati personali</b>	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]	<b>Responsabile della sicurezza dei sistemi per la conservazione</b>	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]	<b>Riferimento temporale</b>	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
[76]	<b>Scarto</b>	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale
[77]	<b>Service Level Agreement</b>	È l'accordo tra produttore, responsabile della conservazione e conservatore sui livelli servizio da garantire ed indica i giorni entro cui devono essere conservati i documenti nel Sistema di conservazione
[78]	<b>Sessione di distribuzione</b>	Sessione telematica per la consegna (distribuzione) di uno o più Pacchetti di Distribuzione dall'Ente Conservatore all'Ente Produttore,

N.	Glossario dei termini	
		sulla base di un modello-dati per i formati ed i contenuti definito e concordato tra le parti
[79]	<b>Sessione di ricerca</b>	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]	<b>Sessione di versamento</b>	Sessione telematica per la consegna (versamento) di uno o più pacchetti di Versamento dall'Ente Produttore all'Ente Conservatore, sulla base di un modello-dati per i formati ed i contenuti definito e concordato tra le parti
[81]	<b>Sistema di conservazione</b>	Sistema di conservazione dei documenti informatici di cui all'art. 44 del Codice dell'Amministrazione Digitale (D. Lgs. 7 marzo 2005, n. 82 e successive modifiche ed integrazioni)
[82]	<b>Titolare</b>	La persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica
[83]	<b>Utente</b>	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]	<b>Validazione temporale</b>	Il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi
[85]	<b>Versamento agli archivi di stato</b>	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	
[1]	<b>AE</b>	Agenzia delle Entrate
[2]	<b>AgID</b>	Agenzia per l'Italia Digitale (già DigitPA e CNIPA)
[3]	<b>CAD</b>	Codice dell'Amministrazione Digitale
[4]	<b>CNIPA</b>	Centro Nazionale per l'Informatica della Pubblica Amministrazione, ora AgID
[5]	<b>FTP</b>	File Transfer Protocol
[6]	<b>IDM</b>	Identity Management
[7]	<b>IPA</b>	Indice delle Pubbliche Amministrazioni

N.	Acronimi	
[8]	<b>IPdA</b>	Indice del Pacchetto di Archiviazione
[9]	<b>IPdD</b>	Indice del Pacchetto di Distribuzione (o Rapporto di distribuzione)
[10]	<b>IPdV</b>	Indice del Pacchetto di Versamento
[11]	<b>ISO</b>	International Organization for Standardization
[12]	<b>OAIS</b>	Open Archival Information System, ISO 14721:2012
[13]	<b>PdD</b>	Pacchetto di Distribuzione
[14]	<b>PdS</b>	Pacchetto di Scarto
[13]	<b>PdV</b>	Pacchetto di Versamento
[14]	<b>RdV</b>	Rapporto di Versamento
[15]	<b>SdC</b>	Sistema di Conservazione
[16]	<b>SdI</b>	Sistema d'Interscambio per la fatturazione elettronica PA per lo scambio delle fatture e delle relative notifiche/ricevute ai sensi del DM 3 aprile 2013, n. 55
[17]	<b>SGSI</b>	Sistema di Gestione della Sicurezza delle Informazioni
[18]	<b>SLA</b>	Service Level Agreement
[19]	<b>TSA</b>	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:

- **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 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;
- **Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013** - 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, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- **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;
- **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;

- **Regolamento europeo eIDAS 910/2014/EC del 24 luglio 2014** – Regolamento in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
- **Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014** - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

La normativa specifica relativa alle diverse tipologie di documenti riguardanti il contratto di erogazione del servizio di conservazione è riportata nel documento “Specificità del Contratto”.

[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, elencati nell'allegato 3 delle Regole Tecniche in materia di Sistema di conservazione con indicazione delle versioni aggiornate al 1° ottobre 2014, come indicato nelle regole tecniche di cui al DPCM 3 Dicembre 2013.

- **ISO 14721:2012 OAIS** (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- **ISO/IEC 27001:2013**, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- **ETSI TS 101 533-1 V1.3.1 (2012-04)** Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- **ETSI TR 101 533-2 V1.3.1 (2012-04)** Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- **UNI 11386:2010 Standard SInCRO** - Supporto all' Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;

- **ISO 15836:2009** Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

[Torna al Sommario](#)

## 4 RUOLI E RESPONSABILITÀ

Il sistema di conservazione descritto nel presente manuale, come prescritto dall'art. 5 del DPCM 3 dicembre 2013, definisce ed 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 ed i riferimenti del Responsabile della conservazione sono indicati nel documento "Specificità del contratto" nel quale sono anche riportate le attività affidate al Responsabile del servizio di conservazione.

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo	Eventuali deleghe
<b>Responsabile del servizio di conservazione</b>	Davide Coletto	<ul style="list-style-type: none"> <li>– definizione ed attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione;</li> <li>– definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente;</li> <li>– corretta erogazione del servizio di conservazione all'ente produttore;</li> <li>– 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.</li> </ul>	Dal 22 gennaio 2015	

<b>Responsabile del servizio di conservazione</b>	Luca Romagnoli	<ul style="list-style-type: none"> <li>- definizione ed attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione;</li> <li>- definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente;</li> <li>- corretta erogazione del servizio di conservazione all'ente produttore;</li> <li>- 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.</li> </ul>	Dal 24 novembre 2014 al 22 gennaio 2015	
<b>Responsabile della sicurezza dei sistemi per la conservazione</b>	Andrea Lazzari	<ul style="list-style-type: none"> <li>- rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza;</li> <li>- segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.</li> </ul>	Dal 24 novembre 2014	
<b>Responsabile della funzione archivistica di conservazione</b>	Matteo Sisti	<ul style="list-style-type: none"> <li>- definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato;</li> <li>- definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici;</li> <li>- monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione;</li> <li>- collaborazione con l'ente produttore ai fini del trasferimento in</li> </ul>	Dal 24 novembre 2014	

		conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.		
<b>Responsabile del trattamento dei dati personali</b>	Luca Romagnoli	<ul style="list-style-type: none"> <li>- garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali;</li> <li>- 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.</li> </ul>	Dal 24 novembre 2014	
<b>Responsabile dei sistemi informativi per la conservazione</b>	Giuseppe Benedetti	<ul style="list-style-type: none"> <li>- gestione dell'esercizio delle componenti hardware e software del sistema di conservazione;</li> <li>- monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore;</li> <li>- segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive;</li> <li>- pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione;</li> <li>- controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.</li> </ul>	Dal 24 novembre 2014	
<b>Responsabile dello sviluppo e della manutenzione del sistema di conservazione</b>	Gianluca Cigliano	<ul style="list-style-type: none"> <li>- coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione;</li> <li>- pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione;</li> <li>- monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione;</li> <li>- interfaccia con l'ente produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare,</li> </ul>	Dal 24 novembre 2014	

		<p>all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche;</p> <ul style="list-style-type: none"><li>- gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.</li></ul>		
--	--	---	--	--

[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
<b>Direzione</b>	La Direzione di Namirial è impegnata nel definire gli obiettivi ed il piano industriale per lo sviluppo, la messa in atto, il monitoraggio, la manutenzione, la verifica dell'efficacia ed il miglioramento continuo del servizio di conservazione dei documenti informatici.	<b>Direzione</b>
<b>Comitato Strategico</b>	Pianifica e detta le direttive strategiche e le linee guida in attuazione a quanto stabilito dal piano industriale e dagli obiettivi aziendali in ambito del servizio di conservazione di documenti informatici.	<b>Comitato Strategico</b>
<b>Area Marketing</b>	È owner delle attività di marketing correlate al servizio di conservazione.	<b>Responsabile Marketing</b>
<b>Area Commerciale</b>	È responsabile delle attività di sviluppo commerciale e vendita del servizio di conservazione.  È responsabile della gestione commerciale dei Clienti e della gestione della sottoscrizione dell'accordo contrattuale tra le parti.	<b>Responsabile Commerciale</b>
<b>Area Amministrativa</b>	È responsabile delle attività amministrativa e di fatturazione del servizio di conservazione.	<b>Responsabile Amministrazione</b>
<b>Ufficio Legale</b>	È responsabile di garantire il supporto per la gestione degli aspetti contrattuali e legali relativi al servizio e alle attività del Responsabile della conservazione e del soggetto conservatore delegato Namirial Spa.  È owner della gestione ed archiviazione della contrattualistica Clienti e degli atti di nomina legati al servizio di conservazione.	<b>Responsabile Ufficio Legale</b>
<b>Area Assistenza Dematerializzazione e Sicurezza Digitale</b>	È owner delle attività tipiche del demand e quindi eroga le attività di assistenza e di	<b>Responsabile del servizio di conservazione</b>

	<p>competenza a supporto delle richieste sia esterne che interne.</p> <p>Supporta il sales nell'attività di analisi dei requisiti del servizio di conservazione.</p> <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>	<p><b>Responsabile della funzione archivistica di conservazione</b></p>
<p><b>Area di Produzione</b></p>	<p>È owner delle attività di pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione.</p> <p>È owner delle attività di configurazione del servizio ai fini della produzione.</p> <p>È owner della gestione delle componenti hardware e software del sistema di conservazione per l'erogazione del servizio.</p> <p>È owner del presidio, controllo, monitoraggio di tutte le componenti del servizio e del soddisfacimento dei livelli di servizio (SLA) verso il produttore dei documenti.</p> <p>È owner del controllo sui livelli di servizio erogati da terzi (fornitori) verso Namirial.</p> <p>Segnalazione delle eventuali difformità al Responsabile del servizio di conservazione</p>	<p><b>Responsabile dei sistemi informativi per la conservazione</b></p>
<p><b>Area di Ricerca e Sviluppo</b></p>	<p>È owner delle attività di coordinamento dello sviluppo e manutenzione delle componenti hardware e software del servizio di conservazione.</p> <p>È owner della pianificazione e del monitoraggio dei progetti di sviluppo del sistema di conservazione.</p> <p>È owner del controllo degli SLA relativi alla manutenzione del sistema di conservazione.</p>	<p><b>Responsabile dello sviluppo e della manutenzione del sistema di conservazione</b></p>
<p><b>Audit</b></p>	<p>È owner di eseguire audit periodici sul servizio di conservazione</p>	<p><b>Responsabile del servizio di conservazione</b></p>

	<p>Verifiche ispettive interne e presso fornitori</p> <p>Acquisizione delle check evidence per l'identificazione delle non conformità</p> <p>Redazione del piano di audit</p> <p>Esecuzione del piano di audit</p> <p>Redazione e condivisione dei tableaux de board con particolare riferimento alla non conformità evidenziate in fase ispettiva</p>	<p><b>Responsabile della sicurezza dei sistemi per la conservazione</b></p> <p><b>Responsabile del trattamento dei dati personali</b></p>
--	--	---

Il Programma di formazione e sviluppo professionale per il personale coinvolto nel servizio di conservazione e il dettaglio dei compiti nello svolgimento delle attività è riportato nella documentazione e nelle attività del sistema di qualità aziendale norma UNI EN ISO 9001:2008, nelle lettere di incarico e nel sistema di gestione della sicurezza aziendale.

[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 *Strongdox* di conservazione di documenti informatici, Namirial ha certificato:

- il proprio sistema di gestione della sicurezza delle informazioni nel dominio logico, fisico e organizzativo nel quale viene realizzato il processo di conservazione (certificazione **ISO/IEC 27001:2013**), in particolare nel perimetro “*Progettazione ed erogazione di servizi gestiti in modalità Saas, Paas e on premise in ambito Enterprise Content Management e paperless business (Business Process Management, acquisizione e trasmissione dei documenti, fatturazione elettronica, formazione documenti, gestione archiviazione e conservazione a Norma di documenti informatici)*”;
- il **Sistema di Gestione della Qualità** secondo la norma **UNI EN ISO 9001:2008**, che comprende anche il perimetro predetto.

Il servizio di conservazione *Strongdox* di Namirial presenta un ciclo di vita caratterizzato da tre fasi principali: **attivazione, produzione e post-produzione**.



Figura 1 Fasi del servizio di conservazione

In ciascuna fase del servizio sono previste delle sotto fasi principali:

<b>Attivazione</b>	Predisposizione e condivisione della “Scheda Servizio Cliente Specificità di Contratto” per la definizione dei requisiti di servizio Cliente
	Configurazione 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/Produttore dei documenti, inclusi tutti gli allegati e i documenti collegati al Contratto.

L’**Area Commerciale** di Namirial, owner del processo di vendita del servizio e del completamento dell’accordo tra le parti, comunica l’attivazione all’**Area Amministrazione** per la gestione dell’anagrafica Cliente e l’**Ufficio Legale** per la corretta archiviazione della contrattualistica sottoscritta. Contestualmente, invia tramite sistema aziendale la richiesta di attivazione operativa del Cliente all’**Area Assistenza** di Namirial che, presa in carico l’attività, avvia la predisposizione ovvero la messa a disposizione del documento di “*Specificità del Contratto*”. Questo documento è fondamentale e basilico per l’erogazione del servizio ad un determinato Cliente (titolare/produttore dei documenti) ed è parte integrante del contratto di servizi e del manuale, redatto dal Conservatore sulla base delle informazioni condivise con il produttore dei documenti (Cliente) e contenente i requisiti essenziali del Servizio, le relative specifiche tecnico-funzionali e procedurali per le varie fasi in cui si articola (attivazione, versamento, conservazione, post-produzione, distribuzione) oltre ai livelli di Servizio (SLA) ed alla pianificazione della fase di messa in produzione; tale documento è redatto in fase di analisi, prima del primo processo produttivo di conservazione.

In caso di specifica assistenza richiesta dal produttore dei documenti 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, l’Area di Assistenza di Namirial gestisce la richiesta con il Cliente e richiede un intervento di assistenza del **Responsabile dello sviluppo e della manutenzione del servizio di**

**conservazione**, che pertanto s’interfaccia con l’ente produttore al fine di definire correttamente la modalità da inserire nel documento di “*Specificità del Contratto*”..

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

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

Predisposto e condiviso il documento di “*Specificità del Contratto*”, validato dal Responsabile del servizio di conservazione di Namirial e dal Cliente, l’area di Assistenza ingaggia l’**Area di Produzione** che avvia le attività di configurazione del servizio nella piattaforma *Strongdox*.

Prima viene eseguito un collaudo interno (verifica interna dell’Area di Produzione delle configurazioni eseguite in coerenza con quanto concordato nel documento di *Specificità del Contratto*) e poi si esegue opzionalmente, previa pianificazione, il collaudo con il Cliente.

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

<b>Produzione</b>	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 ed 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, al controllo di coerenza, dalla 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 della produzione di duplicati e copie informatiche su richiesta dell'utente.

In particolare, il **Responsabile dei sistemi informativi per la conservazione** ha l'ownership delle attività di controllo degli asset e di monitorare il corretto svolgimento del servizio. In caso di riscontro di incident viene attivato il processo di gestione e risoluzione dell'incident attraverso la creazione di un ticket 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 27001:2013.

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

<b>Post - Produzione</b>	Mantenimento dei documenti in conservazione
	Verifica quinquennale della leggibilità
	Adempimenti normativi (es. dichiarazione art. 52 comma 10, DPR 633/72)
	Gestione dello scarto dei pacchetti di archiviazione
	Chiusura del servizio di conservazione (al termine di un contratto)

Figura 4 Post-Produzione

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

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

Infine, scaduto il periodo di conservazione, concordato contrattualmente tra produttore dei documenti, responsabile della conservazione e Conservatore, viene avviata la procedura di Scarto

concordata, con la produzione del Pacchetti di Scarto e la verbalizzazione dello scarto e della chiusura del servizio. Owner di queste attività sono l'Area di Assistenza e Produzione.

Prima dell'avvio dello scarto e della procedura di chiusura del Servizio, che si conclude con una verbalizzazione dell'attività, viene comunicato al produttore l'avvio dello scarto entro 30 gg al fine di fornirgli un periodo transitorio per richiedere formalmente l'estensione (prolungamento) del periodo di conservazione.

Infine, in tutte le predette fasi del servizio di conservazione *Strongdox* ed in generale in tutte le attività in carico ad un Conservatore è necessario garantire la **Gestione dei sistemi informativi e della sicurezza a supporto del servizio.**

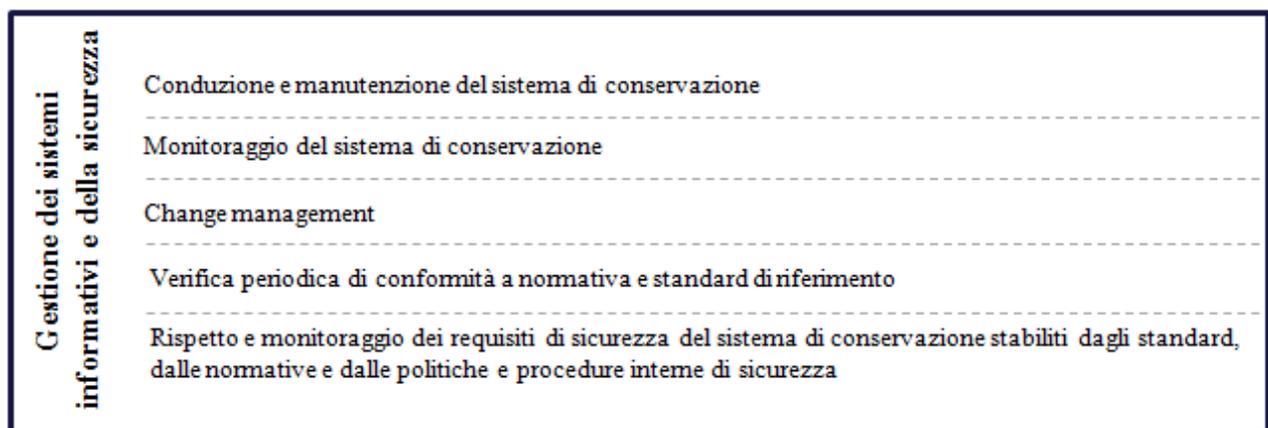


Figura 5 Gestione dei sistemi informativi e della sicurezza

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

[Torna al Sommario](#)

## 6 OGGETTI SOTTOPOSTI A CONSERVAZIONE

Il funzionamento del sistema di conservazione *Strongdox* è basato sulla *compliance* alle regole tecniche di cui al DPCM 3 dicembre 2013 ed allo standard ISO 14721:2012 OAIS (Open Archival Information System), modello di riferimento di sistema informativo per l'archiviazione e la conservazione degli oggetti digitali.

Alla base del funzionamento del predetto modello OAIS e quindi delle regole tecniche vigenti vi è il concetto di informazione da conservare e quindi di *pacchetto informativo*.

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

Il Conservatore Namirial, ispirandosi ai principi dello standard OAIS, ha quindi implementato nel Sistema di Conservazione e nella fasi fondamentali del processo i pacchetti informativi intesi come contenitori astratti contenente due tipologie di informazioni:

- Contenuto informativo;
- Informazioni sulla Conservazione (PDI).

### Contenuto informativo

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

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

### Informazioni sulla Conservazione (PDI Preservation Description Info):

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* (informazioni che garantiscono che il Contenuto informativo non sia stato alterato senza una documentazione dell'evento);

- *Informazioni sul contesto* (informazioni che 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* (informazioni che 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 ed identificabili mediante le Informazioni sull'Impacchettamento, ovvero informazioni usate per collegare ed identificare le componenti di un pacchetto informativo (Contenuto informativo e Informazioni sulla conservazione).

Il pacchetto informativo, infine, può essere trovato nel sistema di conservazione tramite le informazioni descrittive ovvero 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

Nel documento “Specificità del Contratto” concordato tra Ente Conservatore Namirial e Ente Produttore sono elencate e descritte le tipologie di documenti sottoposte a conservazione per un determinato Produttore e le relative politiche di conservazione.

In particolare, le predette politiche di conservazione relative agli oggetti conservati riguardano per ciascuna tipologia documentale:

- 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;
- i livelli di servizio (SLA) concordati con l'ente produttore;
- 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 documentale nella fase di prevendita ed attivazione del servizio.

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) sono riportate nel dettaglio in una tabella per ciascuna tipologia nel documento allegato "Specificità del Contratto" e sono peculiari di ciascun produttore dei documenti e di ciascuna tipologia documentale.

Di seguito si riporta un esempio di draft della tabella da compilare nella "Specificità del Contratto" del Servizio Strongdox:

<b>1</b>	<b>TIPOLOGIA DOCUMENTALE</b>		.....
<b>1.1</b>	<b>Codice della tipologia nel Sistema di conservazione Strongdox</b>		.....
<b>1.2</b>	<b>Natura di documento informatico amministrativo</b>		Sì o No
<b>1.3</b>	<b>Apposizione della firma digitale su ciascun singolo documento eseguita da Strongdox (nella fase di formazione)</b>		Sì o No
<b>1.4</b>	<b>Apposizione della marca temporale su ciascun singolo documento eseguita da Strongdox (nella fase di formazione)</b>		Sì o No
<b>1.5</b>	<b>Metadati</b>	<p><i>In questa sezione della tabella sono inseriti tutti i metadati associati alla specifica tipologia documentale, indicandone la loro descrizione ed il loro valore (stringa, numero, data).</i></p> <p><i>Per ciascun metadato si dichiara se è un metadato "obbligatorio" in quanto richiesto dalla normativa vigente a seconda della natura della tipologia documentale ovvero in quanto richiesto dall'accordo tra ente produttore ed ente conservatore.</i></p>	
<b>1.6</b>	<b>Presenza di fascicolo informatico o aggregazione documentale</b>		Sì o No
<b>1.7</b>	<b>Periodo di riferimento dei documenti con cui si avvia la conservazione digitale</b>		.....
<b>1.8</b>	<b>Durata di conservazione prevista</b>		Esempio: 10 anni
<b>1.9</b>	<b>Formato del file</b>		...

I formati dei files contenuti nei Pacchetti di Versamento devono essere conformi all'elenco dei formati previsti dall'Allegato 2 del DPCM 3 Dicembre 2013.

I formati associati alla tipologia documentale sottoposta a conservazione sono dichiarati nella tabella precedente nella fase di analisi antecedente l'attivazione del servizio Strongdox.

Il produttore dei documenti 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.

<b>Formato del file</b>	<b>Proprietario</b>	<b>Estensione</b>	<b>Standard</b>	<b>Tipo Mime</b>	<b>Visualizzatore</b>	<b>Produttore del visualizzatore</b>
<b>PDF</b>	Adobe Systems - <a href="http://www.adobe.com">www.adobe.com</a>	.pdf	ISO32000-1	application/pdf	Adobe Reader	Adobe Systems - <a href="http://www.adobe.com">www.adobe.com</a>

<b>PDF/A</b>	Adobe Systems - <a href="http://www.adobe.com">www.adobe.com</a>	.pdf	ISO 19005-1:2005 (vers. PDF 1.4) ISO 19005-2:2011 (vers. PDF 1.7)	application/pdf	Adobe Reader <a href="http://www.pdfa.org/doku.php">http://www.pdfa.org/doku.php</a>	Adobe Systems - <a href="http://www.adobe.com">www.adobe.com</a>
<b>XML</b>	W3C	.xml		application/xml text/xml	Mozilla - Chrome - Internet Explorer	Firefox - Google - Microsoft -
<b>TXT</b>	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 -
<b>TIFF</b>	Aldus Corporation in seguito acquistata da Adobe	.tif		image/tiff	Vari visualizzatori di immagini	
<b>JPG</b>	Joint Photographic Experts Group	.jpg, .jpeg	ISO/IEC 10918:1	image/jpeg	Vari visualizzatori di immagini	Per maggiori informazioni sul formato <a href="http://www.jpeg.org">www.jpeg.org</a>
<b>EML</b>	Vari	.eml	RFC2822		Client di posta elettronica supportano la visualizzazione di file eml	Vari
<b>OOXML</b>	Microsoft	.docx, .xlsx, .pptx	ISO/IEC DIS 29500:2008			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 applicare al documento la firma digitale XML
<b>ODF</b>	Consorzio OASIS OpenOffice.org	.ods, .odp, .odg, .odb	ISO/IEC 26300:2006	application/vnd.oasis.opendocument.text		<a href="http://www.oasis-open.org">www.oasis-open.org</a>

In tutti i casi riportati in tabella, il produttore dei documenti s’impegna a versare al sistema di conservazione Strongdox documenti privi di codici eseguibili o macro istruzioni o privi di qualsiasi causa, anche non visibile all’utente, che ne possa alterare il contenuto.

Infine, gli oggetti da conservare sono versati al sistema di conservazione dall’Ente Produttore all’interno di Pacchetti Informativi denominati Pacchetti di Versamento e descritti nel paragrafo successivo.

[Torna al Sommario](#)

## 6.2 Pacchetto di versamento

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

- i documenti oggetti da conservare (*Content Information*), eventualmente firmati digitalmente (nello standard di firma CADES “.p7m” ovvero nello standard PAdES ovvero XAdES) o eventualmente marcati temporalmente (nello standard di validazione temporale CADES-T ovvero nello standard PAdES-T ovvero XAdES-T);
- un file Indice IPdV (Indice del Pacchetto di Versamento) finalizzato alla descrizione delle *Preservation Description Information* secondo lo standard ISO 14721:2012 OAIS, ovvero alla descrizione delle informazioni relative all’oggetto della conservazione, all’identificazione del produttore, ai dati descrittivi ed 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 11386:2010 assicura:

- o l’identificazione del soggetto che ha prodotto il Pacchetto di Versamento (produttore dei documenti);
- o l’identificazione dell’applicativo che lo ha prodotto;
- o la definizione della tipologia documentale (a cui appartengono i documenti inclusi nel pacchetto) ed eventuali messaggi del Responsabile della Conservazione;
- o 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 dei documenti.

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

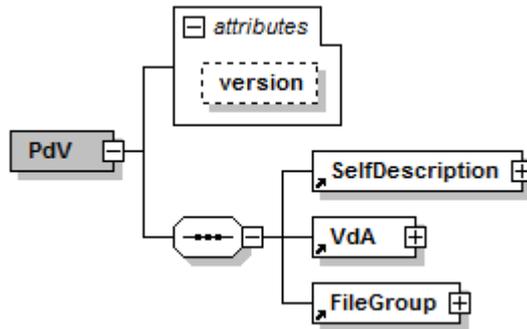


Figura 6 Struttura Indice PdV: suddiviso in SelfDescription, VdA e FileGroup

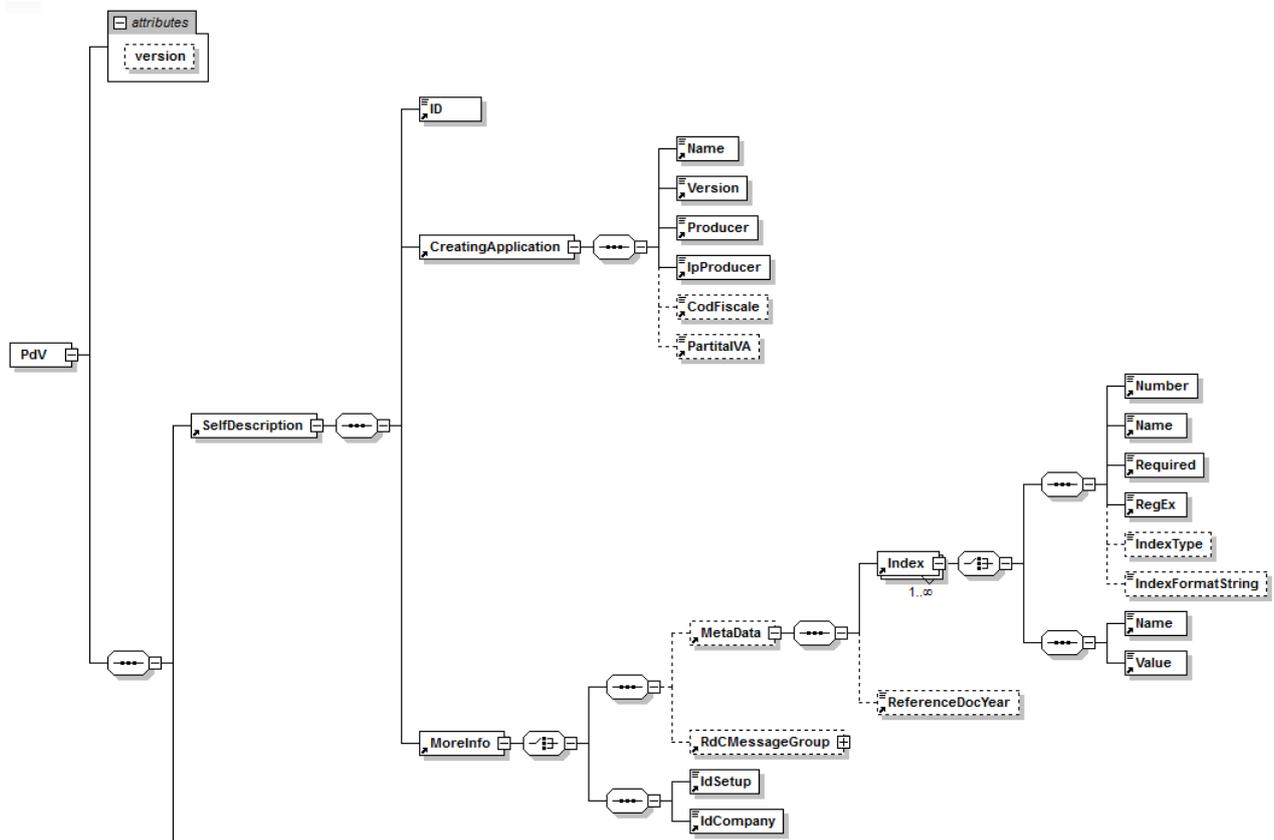


Figura 7 Struttura Indice PdV (Sezione SelfDescription)

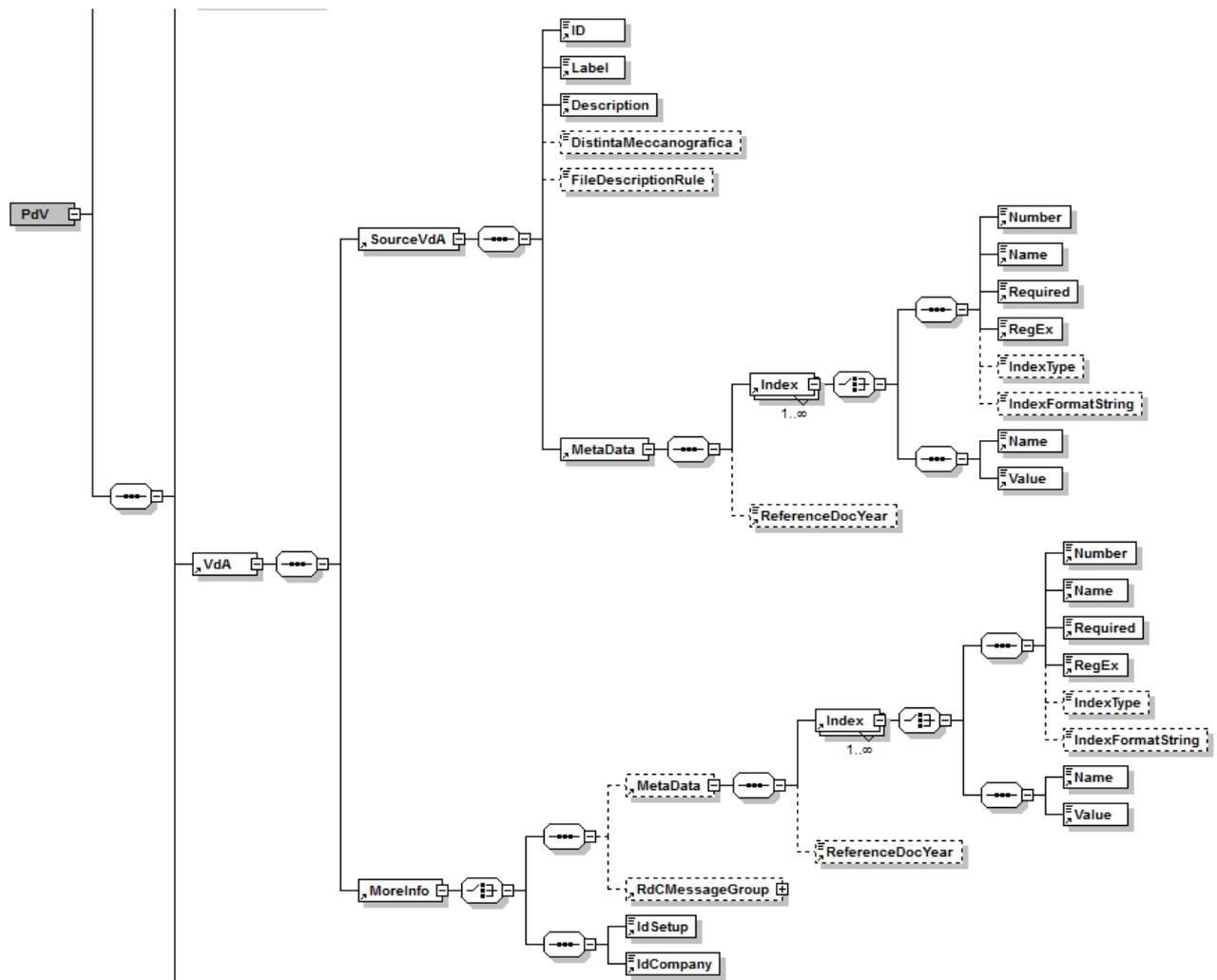


Figura 8 Struttura Indice PdV (Sezione VdA)

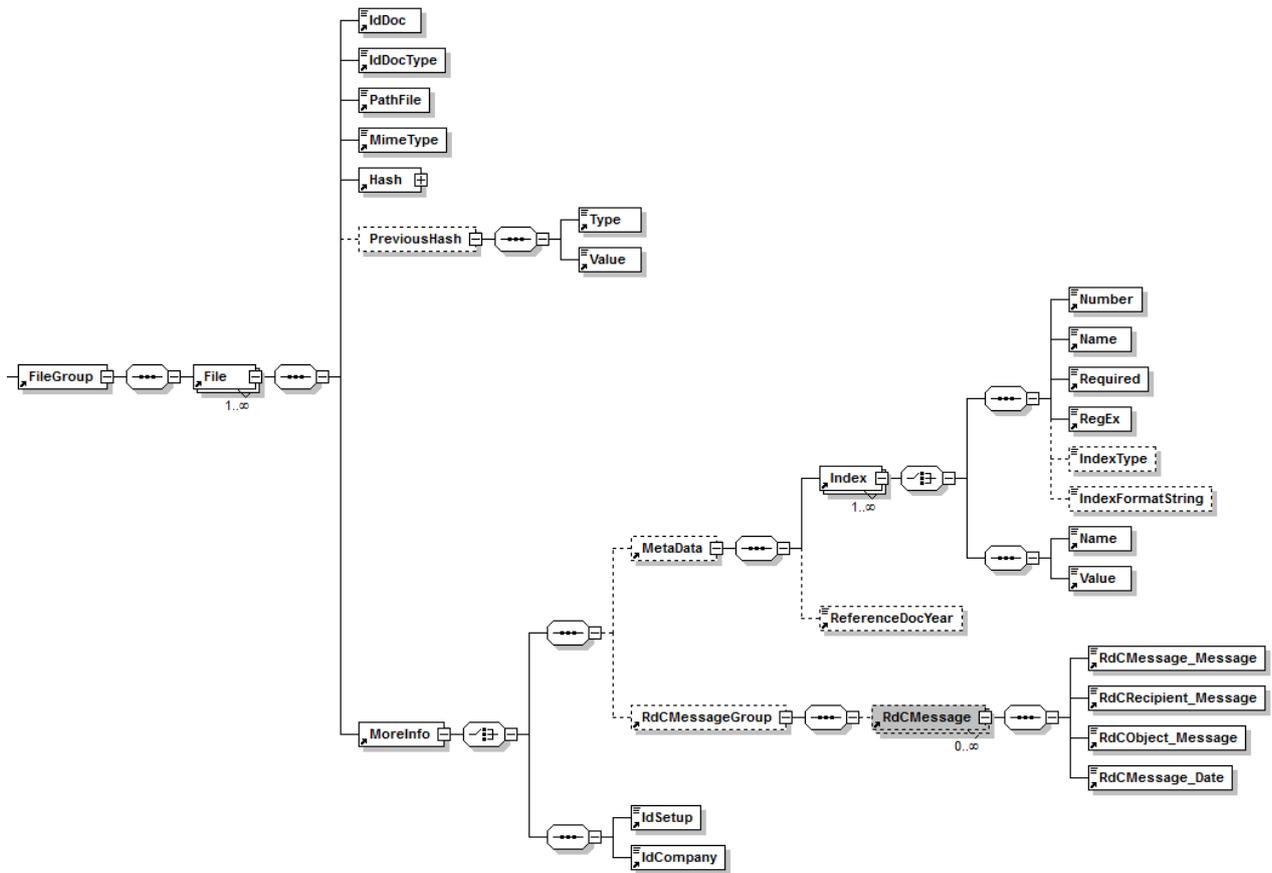


Figura 9 Struttura Indice PdV (Sezione FileGroup)

Il modello-dati del Pacchetto di Versamento e le informazioni di dettaglio sono riportate nel documento di “Specificità del Contratto”.

Tra gli oggetti sottoposti a conservazione si menziona, inoltre, il Rapporto di Versamento (RdV), il quale rappresenta l’esito della verifica di coerenza eseguita dal Sistema di Conservazione sui pacchetti di versamento ricevuti. Il rapporto di versamento del sistema *Strongdox* è un file XML generato secondo lo standard UNI SInCRO 11386:2010 che formalizza il buon esito o meno del versamento dei pacchetti da parte del Produttore dei documenti.

Maggiori informazioni sulla fase di generazione del Rapporto di Versamento sono riportate nel paragrafo 7.3.

Il modello-dati del Rapporto di Versamento e le informazioni di dettaglio sono riportate nel documento di “Specificità del Contratto”.

Le eventuali personalizzazioni sul Pacchetto di Versamento e sulla sessione di versamento sono descritte e concordate tra le parti nel documento di “Specificità del contratto”.

[Torna al Sommario](#)

### 6.3 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 di conservazione.

Un Pacchetto di Archiviazione (PdA) è un contenitore informativo che contiene:

- gli oggetti informativi individuati per la conservazione (quindi i documenti, i fascicoli elettronici o le 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 11386:2010), standard 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 digitale del Responsabile del servizio di conservazione.

La struttura dati del PdA del sistema *Strongdox* completa delle ulteriori strutture collegate ai diversi elementi "MoreInfo" previsti dallo standard SInCRO.

\*\*\*\*\*

- **SelfDescription (1)\*:** Descrizione generale del pacchetto
  - **Id:** Identificativo univoco del PdA generato dal Sistema di conservazione (Id PdA generato dal database)
  - **CreatingApplication (1):**
    - **Name:** Sistema di conservazione *Strongdox*
    - **Version:** Versione ricavata dal Web Service
    - **Producer:** Produttore del Sistema di Conservazione: 2C SOLUTION SRL
  - **SourceIdC (0-n)**
    - **ID:** Id del pacchetto di archiviazione (PdA) precedente
    - **Path:** Percorso relativo dell'IPdA (SInCRO) del pacchetto precedente
    - **Hash:** Valore restituito dalla funzione applicandola al file IPdA del pacchetto precedente, contiene l'attributo "function" che identifica la funzione di Hash utilizzata per il calcolo.

- **Moreinfo (1)**
  - **EmbeddedMetadata:** Riferimenti dell'azienda a cui si riferisce il processo di Conservazione
    - **SoggettoProduttore**
      - **IdSetup:** Id Cliente (Es.: Codice Cliente)
      - **IdAzienda:** Id soggetto produttore all'interno di *Strongdox*
      - **Denominazione:** Ragione Sociale del soggetto produttore
      - **CodFiscale:** Codice Fiscale del soggetto produttore
      - **PartitaIVA:** Partita IVA del soggetto produttore
      - **VersionIPdA:** **Versione dell'Indice del Pacchetto di Archiviazione generato dal Sistema di conservazione.**
- **VdC (1):**
  - **ID:** Identificativo univoco del PdA generato dal Sistema di conservazione (Id PdA generato da database)
  - **MoreInfo (1)**
    - **EmbeddedMetadata:**
      - **PdVGruppo:** Elenco dei PdV inclusi all'interno del PdA
        - **PdV**
          - **IdPdV:** Id del PdV restituito dal Sistema di conservazione al termine della presa in carico
          - **FunzioneHash:** Funzione di hash utilizzata per calcolare hash dell'IPdV
          - **Hash:** Valore restituito dalla funzione di hash applicata al file IPdV
          - **RdCMessageGroup:** Eventuali comunicazioni tra il produttore ed il Responsabile della Conservazione o il suo Delegato relative al PdV.
- **FileGroup (1-n):**
  - **Label:** Nome della tipologia documentale
    - **File:** Definizione del file comprensiva di codifica, estensione e formato (MimeType)
      - **ID:** Id del documento assegnato dal Sistema di conservazione
      - **Path:** Indirizzo logico del file rappresentato da un URI (individua il file all'interno dello storage)
      - **Hash:** Funzione di hash utilizzata e valore restituito dalla funzione applicandola al file oggetto della Conservazione
      - **MoreInfo:**
        - **EmbeddedMetadata**
          - **File (1)**
            - **IdDoc:** Identificativo univoco del file valorizzato dal produttore (univoco all'interno della tipologia documentale definita per l'azienda)
            - **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
  - **RdCMessageGroup:** Eventuali comunicazioni tra il produttore ed il Responsabile della Conservazione o il suo Delegato relative al file.
  - **MoreInfo**
    - **EmbeddedMetadata**
      - **Tipologia (1)**
        - **IdTipologia:** 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)**
  - **Agent (1-n):** Definizione dei soggetti che fanno parte del processo di Conservazione (vedere l'Allegato 4 delle Regole tecniche in materia di sistema di conservazione: Specifiche tecniche del Pacchetto di Archiviazione)
    - **AgentName**
      - **NameAndSurname** oppure **FormalName.**
        - **FirstName:** Nome
        - **LastName:** Cognome
        - **FormalName:** Denominazione o ragione sociale
      - **Agent\_ID (1-n):** Id univoco del soggetto che interviene nel processo di produzione del pacchetto di Archiviazione (Cod. Fiscale o Partita IVA). Se il soggetto appone la firma, allora uno di questi campi riporta l'Id del certificato digitale del soggetto.
    - **MoreInfo (0-n)**
      - **EmbeddedMetadata**
        - **Soggetto (1-n)**
          - **Mansione:** Descrizione della mansione riferita al soggetto
  - **TimeReference (1)**
    - **TimeInfo:** 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:** 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, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

\*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](#)

\*\*\*\*\*

## 6.4 Pacchetto di distribuzione

Un Pacchetto di Distribuzione (PdD) del sistema *Strongdox* può essere delle seguenti tipologie:

- **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.

In entrambe le tipologie, il PdD è costituito da un contenitore compresso (ad esempio zip) che contiene i seguenti elementi:

- ✓ **I documenti** (oggetti digitali conservati nel sistema) richiesti dall'Utente.
- ✓ **Uno o più files IPdA** firmati digitalmente dal Responsabile del servizio di conservazione e marcati temporalmente associati ai predetti documenti richiesti dall'Utente.
- ✓ **File indice del PdD (IPdD)**: file XML ispirato allo standard UNI SINCRO 11386:2010 e firmato digitalmente dal Responsabile del servizio di conservazione, che contiene l'hash dell'IPdA, l'hash di ogni singolo file (documento richiesto o presente all'interno di un PdV richiesto), Super Impronta (se presente).
- ✓ La **Super Impronta** (opzionale, se presente) generata per il produttore (Azienda) a cui si riferiscono i documenti.  
[ad esempio presente per tutti i documenti con rilevanza tributaria oggetto di conservazione, propedeutica alla comunicazione dell'impronta dell'Archivio secondo il Provvedimento Attuativo Agenzia delle Entrate n. 2010/143663 del 25 ottobre 2010, abrogato con l'entrata in vigore del DM 17 Giugno 2014].

Per ogni PdD generato viene archiviato il file indice (IPdD) all'interno del Sistema di conservazione, per la tracciatura formale delle richieste di documenti da *Strongdox*. Questo file indice contiene al suo interno:

- Id del PdD, generato in seguito al salvataggio su Data Base

- Data della generazione del PdD (in formato UTC)
- Azienda a cui si riferisce il PdD (Rag. Sociale, Id setup, Id azienda, Cod. Fiscale, Partita IVA)
- L'utente che ha richiesto il PdD (Nome, Cognome, Codice Fiscale e/o Partita IVA)
- Responsabile della conservazione
- Operatore conservatore delegato della conservazione
- Responsabile del servizio di conservazione
- L'indirizzo IP da cui è arrivata la richiesta di generazione
- PdA consegnati (Id PdA, Hash, Funzione di hash utilizzata, Uri file nel Sistema di conservazione e nel PdD)
- La lista dei file richiesti (Id documento, Id tipologia, Nome tipologia, Nome file, Hash file, Funzione di hash utilizzata, Uri 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 documento estratto dal Sistema di conservazione
  - **IdSetup**, Il codice Cliente associato al produttore
  - **IdAzienda**, L'id dell'azienda di riferimento nel sistema documentale
  - **RagSociale**, La ragione sociale del produttore dei documenti
  - **CodFiscale**, Il codice fiscale del produttore dei documenti
  - **PartitaIVA**, La partita Iva del produttore dei documenti
  - **DataGenerazione**, La data in formato UTC riferita alla produzione del PdD
  - **Richiedente**, Dati anagrafici del richiedente
    - **Nome**, Il nome del richiedente
    - **Cognome**, Il cognome del richiedente
    - **CodiceFiscale**, Il codice fiscale del richiedente
    - **PartIVA**, La partita IVA del richiedente
  - **Soggetti**, Dati anagrafici dei soggetti Responsabile della conservazione, Operatore conservatore e Responsabile del servizio di conservazione
    - **RdC**, Dati anagrafici del responsabile delle conservazione
    - **Operatore**, Dati anagrafici dell'operatore conservatore
    - **RSdC**, Dati anagrafici del responsabile del servizio di conservazione
  - **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 del data base)
- **FunzioneHash**, il tipo di algoritmo usato per calcolare l'hash
- **Hash**, Il valore di hash ottenuto dal PdA
- **FileGruppo**, descrizione dei file estratti
  - File
    - **IdDoc**, id del documento nel sistema documentale o altro sistema
    - **PathFile**, Il nome file
    - **AnnoRiferimentoDoc**, anno di riferimento dell'oggetto conservato
    - **FunzioneHash**, il tipo di funzione di hash usata per calcolare il valore
    - **Hash**, Il valore hash del file considerato

\*\*\*\*\*

Le eventuali personalizzazioni di tali pacchetti, specifiche di un contratto, sono descritte nel documento “*Specificità del contratto*”.

[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 Produttore dei documenti e con gli Utenti e le eventuali Comunità di riferimento (Gruppi di Utenti).

Il Responsabile della conservazione, sotto la propria responsabilità, affida a Namirial, quale prestatore del servizio di conservazione digitale dei documenti informatici, il servizio di conservazione digitale dei documenti informatici del Cliente, affidando le attività previste dal relativo contratto di servizio a Namirial stessa, che attraverso il suo Responsabile del servizio di conservazione, svolgerà le opportune attività ad essa affidate dal Cliente.

Nel seguito viene graficato il processo di conservazione implementato nel sistema di conservazione *Strongdox* in conformità all'art. 8 del DPCM 3 Dicembre 2013.

Per ciascuna delle seguenti fasi del processo viene riportata una descrizione esaustiva:

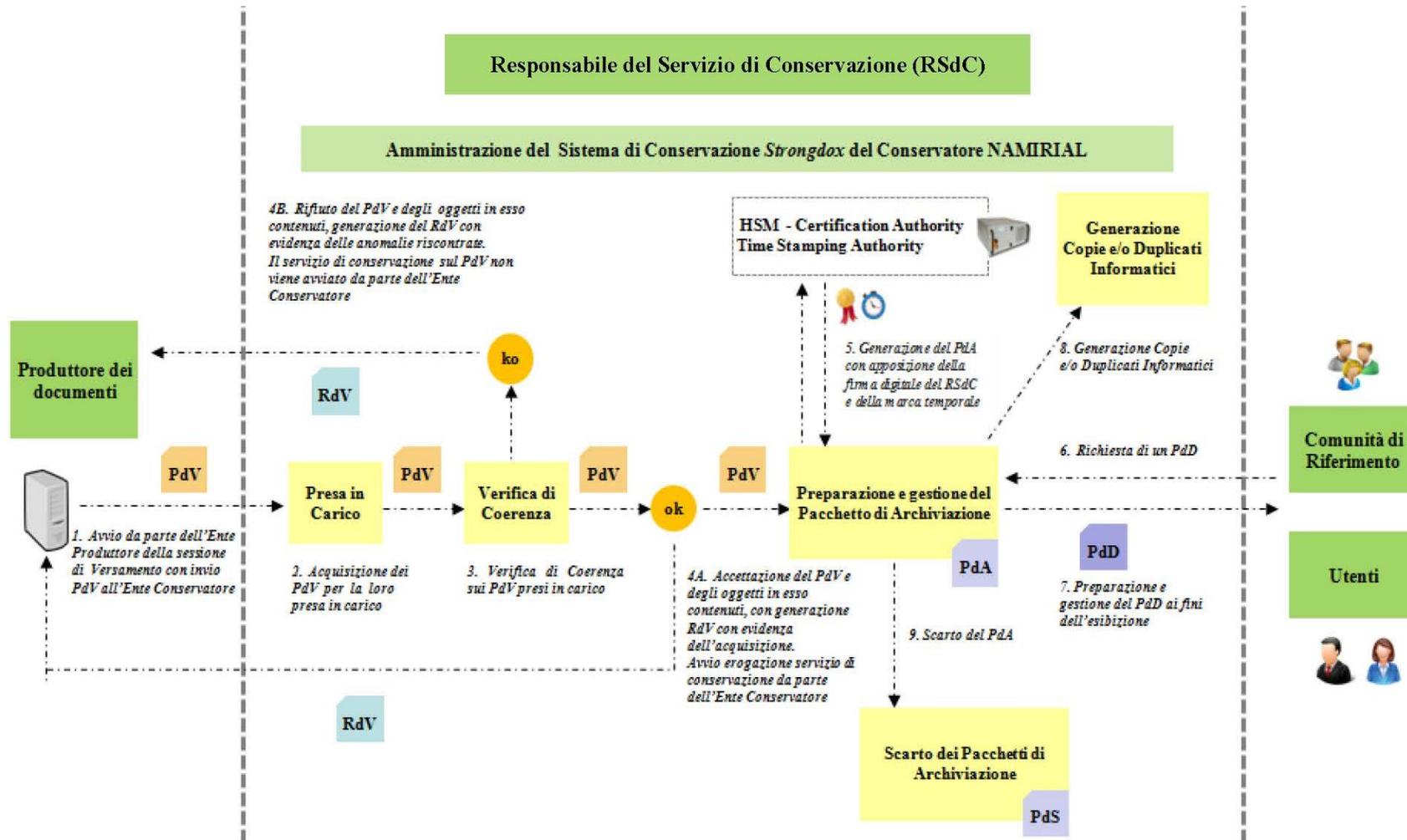


Figura 10 Processo di conservazione in Strongdox

[Torna al Sommario](#)

## 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 dell'Ente Produttore verso l'Ente 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
  - o Trasferimento via web services
  - o Check effettuati per il PdV in fase di presa in carico
  - o Risposta web services (esito presa in carico).
- Asincrona
  - o Trasferimento PdV nella cartella dedicata SFTP
  - o Presa in carico da Job Schedulato
  - o Inserimento nel Sistema di conservazione
  - o Check effettuati per il PdV in fase di presa in carico
  - o 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 e sFTP); le specifiche ed 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 file "Esito di presa in carico" contenente:

- 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.

Pertanto in caso di necessità di un recupero dei dati dei PdV ancora non trasformati in PdA dal sistema, il recupero in accordo con l'Ente Produttore 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 nel documento di "Specificità del Contratto".

[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**.

I controlli eseguiti dal Sistema sui PdV trasmessi sono i seguenti:

- **(Bloccante)** Verifica che il pacchetto di versamento contenga l'IPdV ed i files (non viene effettuato dal metodo web services checkIndicePdV);
- **(Bloccante)** Controllo validità del file IPdV con il file schema XSD;
- **(Bloccante)** Controllo che il soggetto titolare dei documenti (azienda) definito nell'IPdV sia presente e configurato nel Sistema di Conservazione e che sia impostato nel SdC 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 dichiarati nell'IPdV (il predetto controllo non viene effettuato dal metodo web services checkIndicePdV).

Nel caso specifico della tipologia documentale distinta meccanografica, il numero di files presenti nell'IPdV deve coincidere con il numero di documenti presenti nel singolo documento Distinta contenuto nel PdV. Il sistema controlla che tutti i files indicizzati all'interno dell'IPdV abbiano una corrispondenza con i documenti contenuti nella Distinta;

- **(Bloccante)** Controllo che i nomi dei files presenti nel PdV corrisponda ai files definiti nell'IPdV (il predetto controllo non viene effettuato dal metodo web services checkIndicePdV);
- **(Bloccante)** Controllo che il MimeType dei files definito nell'IPdV sia stato specificato;

Tipo file	Tipo MIME	Codifica	Note
PDF, PDF/A	application/pdf, application/x-pdf, application/x-bzpdf, application/x-gzpdf	Binario	
TIFF	image/tiff, image/tiff-fx	Binario	
JPG-JPEG	image/jpeg	Binario	
TXT	text/plain	8 bit	
EML (Messaggio di Posta elettronica)	RFC 2822/MIME (text/plain, message/rfc822, multipart/alternative, text/html)	8 bit	
XML	application/xml, text/xml	8 bit	
ODT	application/vnd.oasis.opendocument.text	Binario	
FODT	application/vnd.oasis.opendocument.text	Binario	
DOCX	application/vnd.openxmlformats-officedocument.wordprocessingml.document	Binario	
ODS	application/vnd.oasis.opendocument.spreadsheet	Binario	
FODS	application/vnd.oasis.opendocument.spreadsheet	Binario	
XLSX	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	Binario	
ODP	application/vnd.oasis.opendocument.presentation	Binario	
FODP	application/vnd.oasis.opendocument.presentation	Binario	
PPTX	application/vnd.openxmlformats-officedocument.presentationml.presentation	Binario	
ODG	application/vnd.oasis.opendocument.graphics	Binario	
FODG	application/vnd.oasis.opendocument.graphics	Binario	

- **(Bloccante)** Verifica che i formati dei files contenuti nel PdV siano nei formati previsti dall'Allegato 2 del DPCM 3 Dicembre 2013 e dalla tabella di seguito riportata
- **(Bloccante)** Verifica della presenza di files nell'IPdV con Id documento NON specificato;
- **(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 (il predetto controllo non viene effettuato dal metodo web services 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 (campo: SourceVdA);
- **(Bloccante)** Verifica che il numero di metadati definiti per il documento corrisponda a quelli definiti all'interno della tipologia configurata nel SdC (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 configurata nel SdC (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)** Verifica degli Hash dei file con il valore inserito nel PdV (Il predetto controllo non viene effettuato dal metodo web services checkIndicePdV);
- **(Bloccante)** Verifica della validità della firma sul file (opzionale); il predetto controllo non viene effettuato dal metodo web services 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).

Ulteriori personalizzazioni sui controlli eseguiti sono riportati nel documento “Specificità del Contratto”.

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

In caso di presa in carico, il sistema di conservazione *Strongdox* esegue, con una schedulazione periodica il cui timing è configurabile per ciascun produttore dei documenti, eventuali ulteriori controlli di continuità (se previsti nella presente Scheda Servizio) e genera un rapporto, il **Rapporto di Versamento** (RdV), quale esito di tutte le verifiche effettuate sul PdV a partire dalla sua ricezione.

Nella fase di verifica di coerenza del PdV, i risultati dei predetti controlli vengono tutti registrati all'interno della funzionalità di LOG Management System del Sistema con la registrazione di un time stamp (riferimento temporale).

Inoltre, l'esito di presa in carico generato dal sistema di conservazione *Strongdox* contiene un riferimento temporale e, come meglio specificato nel paragrafo successivo, il Rapporto di Versamento (RdV) generato dal sistema contiene il Tag “<DataGenerazione>” ed è anche firmato digitalmente dal Responsabile del servizio di conservazione. Il riferimento temporale associato al rapporto di versamento, rappresenta quindi un'informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC) che identifica la data di formazione del RdV.

Per quanto riguarda i riferimenti temporali si evidenzia che l'orologio di sistema di tutti gli elaboratori impiegati nel servizio di conservazione di documenti informatici sono sincronizzati con i segnali di tempo campione generati dall'Istituto Nazionale di Ricerca Metrologica (INRIM) in Torino ([www.inrim.it](http://www.inrim.it)). Questo permette al server di firma massiva di mantenere un tempo di sistema che si discosta dal tempo campione dell'istituto metrologico primario INRIM con un errore sicuramente inferiore al minuto.

[Torna al Sommario](#)

### 7.3 Accettazione dei pacchetti di versamento e generazione del rapporto di versamento

In caso di presa in carico con esito positivo, il sistema di conservazione *Strongdox* esegue, con una schedulazione periodica il cui timing è configurabile per ciascun produttore dei documenti, eventuali ulteriori controlli di continuità (se previsti nella Scheda Servizio Cliente – Specificità del Contratto) e genera un rapporto, il **Rapporto di Versamento (RdV)**, quale esito di tutte le verifiche effettuate sul PdV dalla sua ricezione.

Il Rapporto di Versamento previsto dalle regole tecniche (DPCM 3 Dicembre 2013) ha lo scopo di formalizzare l'acquisizione degli oggetti da conservare inviati tramite un PdV dal Produttore dei documenti. Tale rapporto, come previsto dalla normativa, viene generato anche automaticamente dal sistema *Strongdox* e può contenere uno o più pacchetti di versamento.

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

Per ogni Ente Produttore possono essere generati uno o più RdV per ogni schedulazione, in quanto:

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

Il RdV è generato nel formato XML secondo lo standard UNI SInCRO 11386:2010, dove all'interno vengono riportate le seguenti informazioni:

- ✓ Indicazioni della versione del Sistema di conservazione
- ✓ Indicazioni ed autenticazione del produttore dei documenti in riferimento al sistema di Conservazione
- ✓ Riferimenti dell'utente che ha trasmesso il PdV
- ✓ Data di generazione del RdV
- ✓ Dati del responsabile della conservazione
- ✓ 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
- ✓ 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 RdC ovvero 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

Il rapporto di versamento, viene firmato digitalmente dal responsabile del servizio di conservazione. Alla firma digitale è associato un riferimento temporale che, rappresenta quindi un'informazione contenente la data e l'ora che identifica la data di formazione del documento informatico RdV. Il predetto riferimento temporale è riferito al Tempo Universale Coordinato (UTC) con i segnali di tempo campione generati dall'Istituto Nazionale di Ricerca Metrologica (INRIM) in Torino.

I rapporti di versamento sono conservati digitalmente a norma nel sistema *Strongdox* periodicamente per ciascun Produttore dei documenti. I rapporti di versamento sono sempre consultabili dall'utente autorizzato e possono essere, inoltre, scaricati attraverso specifica funzionalità nella schermata delle proprietà del documento e del pacchetto di versamento, come indicato nella seguente immagine:

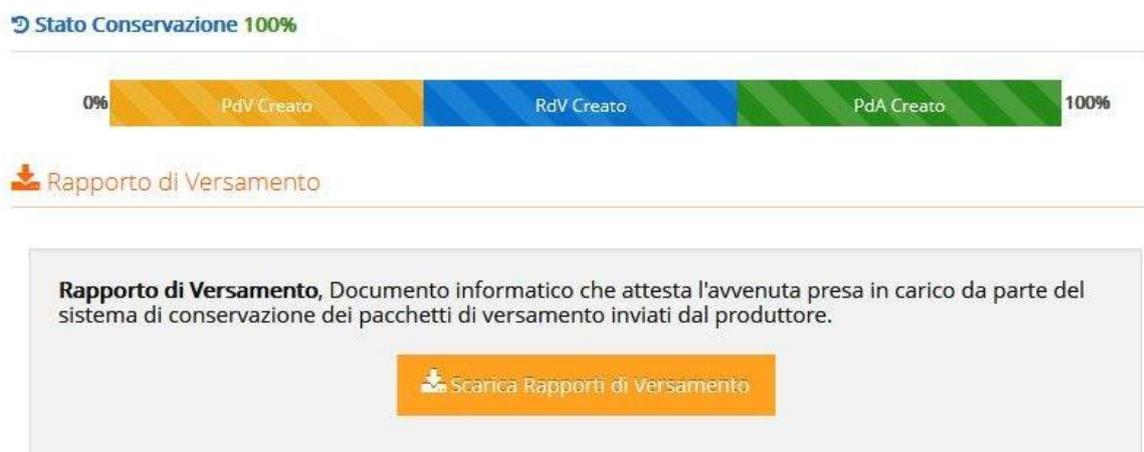


Figura 11 Rapporto di versamento in Strongdox

Ulteriori specifiche sulla generazione del RdV ed il modello dati dello stesso sono dettagliate nel documento di “Specificità del Contratto.”

[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 ed i documenti;
- File IPdV non valido rispetto allo schema XSD;

- Identificazione del produttore dei documenti e non corrispondenza con quanto configurato nel sistema di conservazione;
- nel sistema di conservazione non è configurato il responsabile della conservazione per il produttore dei documenti 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;
- Verifica tipo MIME dichiarato nell'IPdV (MimeType tra quelli ammessi per la conservazione dei files);
- Verifica 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;
- Verifica della validità della firma digitale solo se l'IPdV è firmato;
- Verifica che la tipologia documento nel sistema di conservazione corrisponda a quella definita per l'IPdV (campo: SourceVdA);
- Verifica che la tipologia documentale configurata nel Sistema di conservazione corrisponda a quella dichiarata nell'IPdV (campo: SourceVdA);
- Verifica che i metadati configurati per quella tipologia documentale nel sistema di conservazione corrispondano a quelli dichiarati nell'IPdV (campo: SourceVdA);
- Verifica che il nome e l'ordine dei metadati configurati per quella tipologia documentale nel sistema di conservazione corrispondano a quelli dichiarati nell'IPdV (campo: SourceVdA);
- Verifica della presenza dei metadati settati come obbligatori nell'IPdV (campo: SourceVdA);
- Verifica dell'eventuale espressione regolare dei metadati dichiarati nell'IPdV (campo: SourceVdA);
- 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 produttore dei documenti;
- Verifica della corrispondenza degli hash (impronte) dei documenti calcolati dall'ente conservatore con l'hash dichiarato nell'IPdV dall'ente produttore;
- Verifica della validità della firma sul singolo documento. Il controllo della verifica sui documenti firmati è opzionale ed attivabile solo sui documenti firmati.

Ulteriori controlli possono essere eseguiti in merito al rispetto della continuità della numerazione o all'ordinamento cronologico, eventualmente generando ulteriori anomalie riportate nel Rapporto di Versamento, ma ciò è concordato tra produttore, responsabile della conservazione e Conservatore nel documento di "Specificità del Contratto".

Il sistema di conservazione, successivamente alla sua generazione, prevede la possibilità di inoltrare al produttore dei documenti del RdV tramite e-mail ovvero tramite chiamata web service.

La modalità di consegna del RdV dal sistema di conservazione al produttore prevede la creazione di un pacchetto contenitore, contenente il file RdV firmato dal responsabile del servizio di

conservazione, il file RdV non firmato per una più agevole elaborazione del file da un eventuale sistema informativo ed un file XSLT per la semplice visualizzazione tramite browser.

É inoltre possibile richiedere il RdV direttamente accedendo dall'interfaccia web di consultazione in *Strongdox* da parte di un utente autorizzato dal produttore dei documenti.

Periodicamente il Sistema di Conservazione conserva in conformità alla normativa vigente tutti i RdV generati, che rimangono sempre a disposizione per la consultazione ed esibizione. 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).

L'annullamento dei PdV avviene tramite interfaccia Web attraverso una specifica funzionalità e tramite la condivisione con il produttore dei documenti. Tali pacchetti se annullati attraverso l'interfaccia web resteranno comunque salvati e disponibili nel Sistema di conservazione ma nello stato annullato e quindi non potranno più essere selezionati per la successiva fase di generazione dell'IPdA.

L'operazione di annullamento dal processo di conservazione di un PdV viene comunicata al produttore dei documenti all'interno del successivo RdV per esso generato.

In conclusione, nel presente paragrafo e nel paragrafo 7.2 sono stati descritti i controlli eseguiti dal servizio *Strongdox* sui PdV ricevuti in cui si è descritto che le anomalie rilevate sui PdV vengono tracciate negli esiti di presa in carico e nel rapporto di versamento (RdV).

La comunicazione al Produttore delle anomalie riscontrate dai predetti controlli avviene, pertanto, attraverso la consegna o messa a disposizione degli esiti di presa in carico e dei rapporti di versamento.

Il Conservatore Namirial consente all'Ente Produttore di avere a disposizione gli esiti di presa in carico tramite dialogo applicativo web services o tramite sFTP nella cartella di destinazione "RX" definita tra le parti nel documento di "Specificità del Contratto".

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"?>
<EsitoPresaInCarico>
<NomeFile><![CDATA[Files.zip]]></NomeFile>
<DataVersamento>2014-09-11T07:58:01Z</DataVersamento>
<Id>000000001_2014</Id>
<IdPdV>54115609b84ac914886a905b</IdPdV>
<HashIPdV>B6D3163419584386155E39810111ED69BF8D7166FF38502A451371DB42
DA0186</HashIPdV>
<FunzioneHashIPdV>SHA-256</FunzioneHashIPdV>
<CodFiscale>COD_FISCALE</CodFiscale>
```

```
<PartitaIVA>IT:PARTITA_IVA</PartitaIVA>  
<Errori />  
</EsitoPresaInCarico>
```

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

- *NomeFile*: Nome file del pacchetto di versamento (Archivio Zip o Non Zip).
- *DataRicezione*: Data e ora in cui è stato ricevuto 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.
- *CodFiscale*: Codice Fiscale del produttore ricavato dal PdV.
- *PartitaIVA*: Partita Iva del produttore ricavata dal PdV.

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.

Il Conservatore Namirial consente all'Ente 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 nel documento "Specificità del Contratto"); 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 webservice del sistema di conservazione**, secondo le modalità specificate nel documento *Strongdox* SDK eventualmente allegato al documento di "Specificità del Contratto";
- tramite **accesso alla piattaforma web del Sistema di conservazione *Strongdox*** da parte di un utente autorizzato per quel determinato Produttore.

Anche in questo caso tutte le azioni sono tracciate 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 dell'Allegato 4 del DPCM 3 Dicembre 2013 e secondo il modello-dati definito dallo standard SInCRO – Supporto all'interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010), che è lo standard nazionale riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione.

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 all'interno dell'entità funzionale schedulatore del processi presente nel sistema, sulla base delle regole di conservazione configurate nel sistema per il produttore dei documenti.

Una volta generato l'IPdA viene apposto su di esso la firma digitale del Responsabile del Servizio di Conservazione ed una marca temporale, quindi i Pacchetti di Versamento inclusi nel PdA non potranno più essere modificati.

La firma digitale e la marca temporale sono emesse, in conformità alla normativa vigente, da Namirial, rispettivamente in qualità di Certification Authority (CA) e di Time Stamping Authority, in conformità alla normativa vigente.

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 ed il ripristino attraverso l'utilizzo del PdA copia di backup da parte del team preposto, secondo il piano operativo esposto nella documentazione sulla continuità operativa gestita per la certificazione ISO/IEC 27001:2013.

Specifici casi in cui è necessario adottare metodi di crittografia per proteggere i dati conservati nei PdA sono descritti nel documento "Specificità del contratto", che rappresenta l'accordo sulle condizioni di servizio specifiche tra Ente Conservatore ed Ente Produttore.

[Torna al Sommario](#)

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

In risposta ad un ordinativo (richiesta dell'Utente) tramite l'interfaccia di ricerca documenti di *Strongdox*, il sistema di conservazione fornisce all'Utente richiedente tutto o parte o una raccolta di Pacchetti di Archiviazione, sotto forma di Pacchetto di Distribuzione (PdD).

L'Utente può ricercare da interfaccia web, attraverso l'inserimento di apposite chiavi di ricerca, i documenti come output della ricerca, su cui poi richiedere la distribuzione del relativo PdD attraverso un pulsante "Genera Pacchetto di Distribuzione"; in alternativa un'utenza applicativa autorizzata può richiedere un PdD tramite chiamata web service. Il PdD distribuito dal sistema *Strongdox* contiene tutte le evidenze di un singolo documento o quelle di un sottoinsieme di documenti conservati, a seconda della tipologia di PdD richiesta.

Una volta che l'utente richiede un PdD il sistema restituisce tramite canale crittografato (su protocollo HTTPS utilizzando TLSv1.2 crittografato in AES 128 ed autenticato mediante Diffie Helman RSA) il pacchetto PdD in formato di cartella compressa .zip costituito dagli oggetti digitali previsti dalla richiesta di distribuzione. Le tipologie di Pacchetti di Distribuzione ed 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.

Ulteriori informazioni di dettaglio, concordate con il soggetto Produttore, sono descritte nel documento "Specificità del Contratto".

[Torna al Sommario](#)

## **7.7 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* tramite le sue credenziali può eseguire le ricerche attraverso una interfaccia web e tramite l'ausilio di una serie 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 può eseguire la richiesta di 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 da un utente autorizzato.

Inoltre, attraverso il sistema di ticketing aziendale e secondo quanto concordato nel documento "Specificità del Contratto", 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 (ad esempio sFTP) 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 in quanto concordato nel documento di Specificità del Contratto.

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 e presidiato operativamente dall'Area di Assistenza Dematerializzazione e Sicurezza Digitale di Namirial, richiede la gestione di un riversamento sostitutivo, ovvero il processo che trasferisce uno o più documenti conservati da un supporto di memorizzazione ad un altro, modificando la loro rappresentazione informatica, garantendo il mantenimento dell'integrità del contenuto.

Proprio per la garanzia della conformità del contenuto nel passaggio da una rappresentazione informatica ad un'altra rappresentazione, più aggiornata tecnologicamente, è necessario nel processo l'intervento del pubblico ufficiale. La procedura prevede la messa a disposizione dei documenti originali e dei documenti copia al pubblico ufficiale, 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 *Strongdox* 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) da parte del Responsabile della Conservazione, del Conservatore Namirial e del Produttore dei documenti è la scelta perseguita come prevenzione e minimizzazione dei rischi legati all'obsolescenza tecnologica.

[Torna al Sommario](#)

## **7.8 Scarto dei pacchetti di archiviazione**

Superato il periodo di conservazione di pacchetti e documenti concordato tra Ente Conservatore e Ente Produttore, il sistema *Strongdox* deve implementare la procedura di scarto dei pacchetti di archiviazione.

Il sistema notifica (via mail/pec) al produttore con 30 gg di anticipo l'avvio della funzione di scarto per determinati PdA dandone quindi informativa secondo la normativa vigente e fornendo le informazioni necessarie al produttore per valutare l'eventuale richiesta di estensione del periodo di conservazione.

In caso di superamento della scadenza prefissata ed 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) nel formato UNI SInCRO 11386:2010 firmato digitalmente dal Responsabile del Servizio di Conservazione che grazie al file XSLT può essere visualizzato dal Produttore dei documenti o 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 questo 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 produttore secondo quanto previsto dalla normativa vigente in materia e secondo gli accordi definiti nel documento di "Specificità del Contratto".

[Torna al Sommario](#)

## **7.9 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 11386:2010.

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 produttore 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 produttore dei documenti (utente) potrà richiedere la loro distribuzione al sistema *Strongdox*, selezionando la richiesta tramite dei filtri da interfaccia web e l'apposita funzionalità.

Ogni PdD contiene un Indice del PdD, generato secondo lo standard UNI SInCRO 11386:2010 e firmato dal Responsabile del Servizio di Conservazione, che rappresenta un rapporto (verbale) della distribuzione eseguita. Il PdD contiene anche il file XSLT per la corretta visualizzazione dell'IPdD.

Se il Produttore dei documenti volesse richiedere una personalizzazione del servizio di distribuzione con l'esecuzione di attività aggiuntive per la migrazione o per l'interfacciamento diretto di Namirial con altri Conservatori ai fini della trasferibilità, le attività saranno eseguite da Namirial sulla base di quanto concordato nel documento "Specificità del Contratto" con il produttore stesso.

[Torna al Sommario](#)

## 8 IL SISTEMA DI CONSERVAZIONE

*Strongdox* è la soluzione informatica del Conservatore Namirial per la gestione del servizio di conservazione dei documenti informatici a norma di legge.

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

Le principali componenti della soluzione di conservazione di documenti informatici possono essere schematizzate dalla seguente rappresentazione grafica.

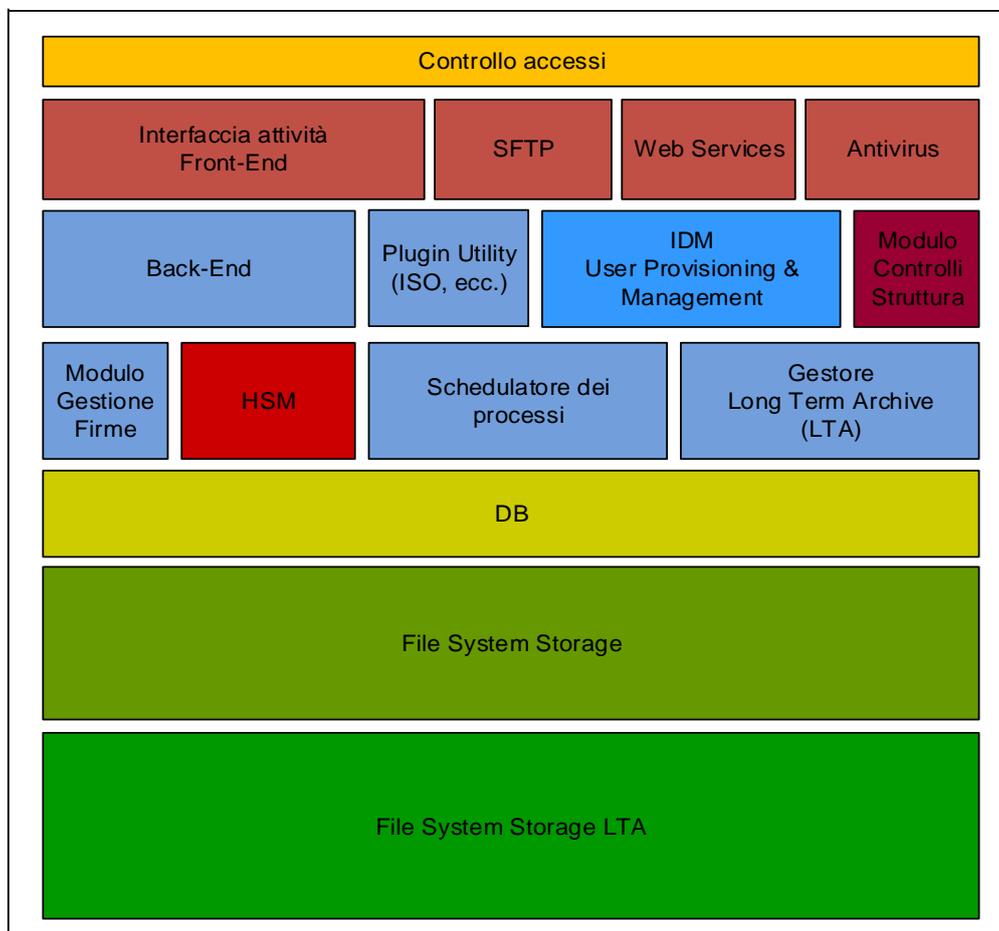


Figura 12 Componenti del sistema di conservazione Strongdox

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:

- L'interfaccia delle attività di front end che si incarica dell'esposizione delle funzioni di interattività con gli utenti (versamento manuale di documenti, ricerche, richieste, esibizione, distribuzione pacchetti, produzione di copie e duplicati, ecc.) ma anche della configurazione amministratore di tutti le funzionalità e servizi.
- Il modulo SFTP per il caricamento massivo dei pacchetti di versamento (PdV).
- Il modulo Web Services per le attività di caricamento e gestione pacchetti e documenti.
- L'antivirus.
- Il modulo di back end per tutte le attività di interfaccia con il DB ed il Filesystem. Il modulo delle utility (creazione ISO, ecc.).
- Modulo IDM – User Provisioning e Management per la gestione dell'access management.
- Scheduler dei processi: componente fondamentale per l'amministrazione del servizio di conservazione, per la gestione nel sistema dei produttori dei documenti, degli utenti, delle classi documentali, delle regole e lavori di conservazione, processi di verifica e controllo e delle comunicazioni email-pec per messaggistica. 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.
- Il 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 sul sito secondario di DR);
- Il modulo per l'integrazione con i dispositivi per la firma (HSM).
- Il modulo per la gestione dello storage.
- Il modulo di gestione DB.
- Il modulo per la gestione dell'archivio di lunga durata, solo se concordato nel documento di "Specificità del Contratto".

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 SysAid di Log Management System di *Strongdox*, descritto nei paragrafi successivi.

[Torna al Sommario](#)

## 8.1 Componenti Logiche

Nel seguito si descrivono più nel dettaglio le componenti logiche del Sistema di Conservazione *Strongdox*.

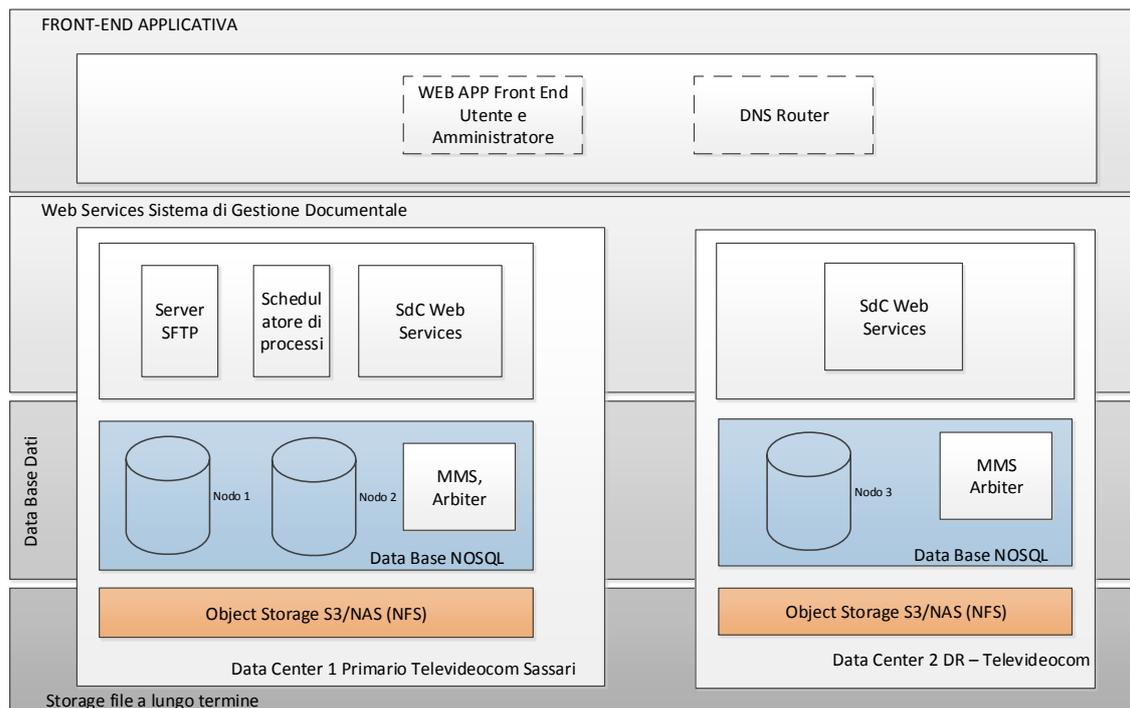


Figura 13 Componenti logiche del sistema di conservazione Strongdox

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 produttore dei documenti (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 sul sito di DR.

SdC Web Services: 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 produttore.

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. Inoltre, permette 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 ed interagisce con lo schedulatore dei processi e definisce le funzioni ed i servizi per il controllo dell'intero sistema di conservazione. Questa entità, gestita dall'amministratore, definisce le policy ed 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).

Base dati del Sistema di conservazione: *Strongdox* salva i dati su un data base 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) ed i load balancer che si occuperanno di proteggere l'applicativo e di suddividere il carico tra le varie macchine che erogheranno le funzionalità pubbliche.

- Secondo livello. Il secondo livello rappresenta il core dell'infrastruttura di conservazione e sarà costituito da server fisici che implementano i moduli e le componenti funzionali nonché dai dispositivi HSM o dalle librerie per la gestione delle firme.

In particolare i dispositivi HSM sono custoditi presso il certificatore accreditato (CA) Namirial S.p.A. e sono conformi ai requisiti di sicurezza previsti dalla normativa vigente.

- Terzo livello. Il 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 27001:2013.

[Torna al Sommario](#)

### **8.3 Componenti Fisiche**

Il sistema di conservazione *Strongdox* è installato ed eroga i servizi su data center Televideocom.

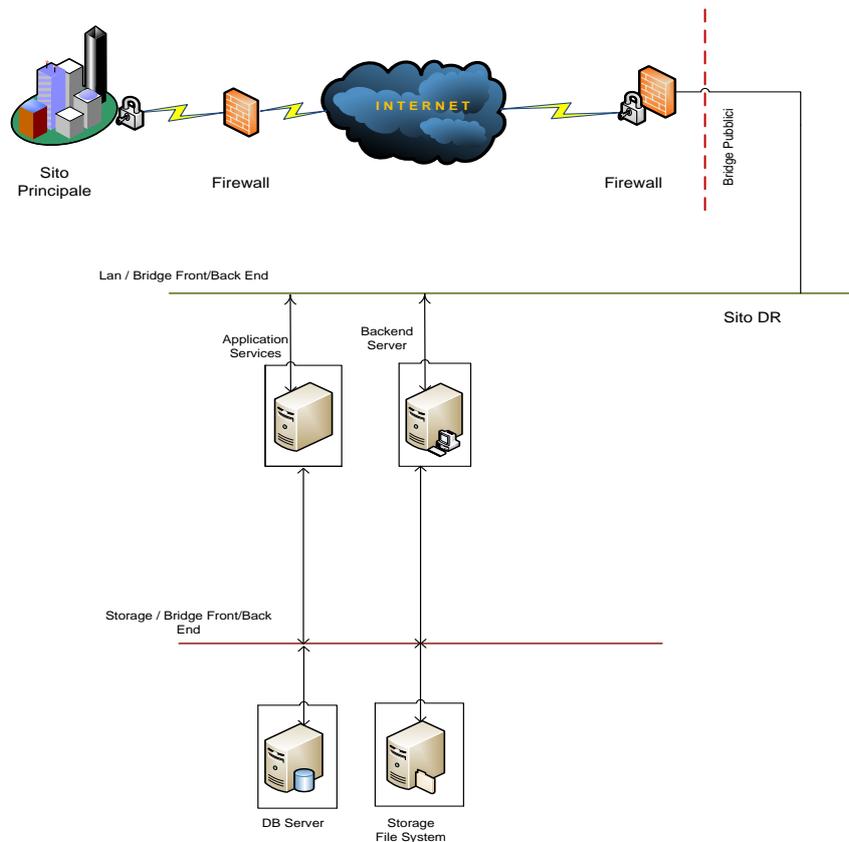


Figura 14 Macro architettura di collegamento del sito di DR

L'architettura di rete che compone il sistema informativo di Namirial è strutturata secondo lo schema "Network Fully Connected / Any to Any" completamente ridondato. L'infrastruttura di telecomunicazioni è affidata agli outsourcer Fastweb (FB) e Telecom (TC), che in qualità di "Full Contractor" gestiscono per conto del gruppo Namirial tutti i diversi fornitori di servizio utili al mantenimento della infrastruttura di comunicazione in essere. I principali fornitori coinvolti nel mantenimento e nella gestione della infrastruttura di rete per il gruppo Namirial sono:

- FB – main carrier
- TC – carrier per il networking WAN tra le sedi

La valutazione della distanza dei siti elaborativi Sassari (SS) e Pomezia (RM), i quali erogano i servizi informatici di produzione per il business di Namirial spa, evidenzia quanto segue:

- Distanza in linea d'aria
  - Sassari (Produzione) – Pomezia (Disaster Recovery) → **350 km**
  - Namirial (Esercizio) – Sassari (Produzione) → **500 km**
- Raggiungibilità
  - Namirial (Esercizio) – Pomezia (Disaster Recovery)

- 360 km / 3,5h circa in automobile via Teramo-L'Aquila o 1h circa di aereo via Falconara (AN)

Per gli approfondimenti ed il dettaglio in relazione alle componenti fisiche ed alla continuità operativa si rimanda alla documentazione relativa al sistema di gestione della sicurezza informatica, certificato ISO/IEC 27001:2013.

[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.).

##### – *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 del sistema di gestione della sicurezza.

Il Conservatore Namirial mantiene un registro cronologico delle componenti della piattaforma software *Strongdox*, comprensivo di tutte le release, inoltre registra le diverse release di sistema operativo e di applicativi utilizzati nell'intero processo di conservazione nell'arco degli anni al fine di rendere comunque disponibili e fruibili nel tempo i documenti ed i dati relativi al servizio.

La procedura dei rilasci del software è una procedura che segue i requisiti imposti dalla certificazione ISO/IEC 27001:2013.

La predisposizione, la verifica e l'approvazione della documentazione relativa al servizio di conservazione sono gestiti all'interno della Procedure del Sistema di gestione per la Qualità e Sicurezza delle Informazioni 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 nel seguente modo:

- **Help Desk 1° Livello**, sono gli operatori che ricevono il primo contatto da parte dell'Utente in caso di necessità, riescono a dare supporto su tematiche relative all'utilizzo della piattaforma, al processo, al servizio, ecc.  
Se il supporto non riesce a soddisfare la richiesta viene ingaggiato l'Help Desk di 2° Livello, che a seconda della catalogazione del ticket è rappresentato dall'Area di Assistenza Dematerializzazione e Sicurezza Digitale, dall'Area di Sviluppo software o dall'Area di Produzione;
- **Help Desk 2° Livello**, prende in carico la richiesta dall'Help Desk di primo livello e provvedono alla gestione della problematica secondo la propria competenza ed eventualmente in team con altre competenza multidisciplinari.

– 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.

– monitoraggio del sistema di conservazione

Il sistema di conservazione *Strongdox* implementa numerosi sotto processi dediti al controllo e al monitoraggio del corretto svolgimento dei processi, segnalando eventuali errori o anomalie al personale incaricato dal Responsabile della Conservazione ovvero dal suo Delegato.

Tutte le componenti del sistema sono dotate di un proprio file di log nel quale sono tracciate tutte le operazioni eseguite dal componente e le altre informazioni che permettono di tenere traccia delle attività svolte e facilitare la diagnosi di eventuali anomalie e/o incident.

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

– change management:

Il processo di change management sul servizio istanziato dal Cliente, attraverso la piattaforma di ticketing, è gestito dall'Area di Assistenza Dematerializzazione e Sicurezza Digitale e prevede l'avvio del processo attraverso l'aggiornamento e la condivisione di una nuova versione del documento "Specificità del Contratto" che appunto deve recepire il change di servizio e che attiva la successiva fase implementativa del change.

Il change management dell'infrastruttura di erogazione del servizio, invece, è gestito e descritto dal conservatore Namirial secondo la procedura definita dal SGSI ISO/IEC 27001:2013.

– 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 produttori dei documenti, 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 funzionalità di creazione e mantenimento dei rapporti di versamento, dei pacchetti di archiviazione, ecc;
- verifica 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 (produttore, 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 sulla 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.

Le predette attività di verifica sono riepilogate in un verbale di audit.

– *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 SGSI, certificato ISO/IEC 27001:2013.

[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 produttore dei documenti.

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 di documenti informatici *Strongdox* viene costantemente controllato da un sistema di monitoring che rileva malfunzionamenti, anomalie ma anche situazioni critiche che rischiano di degenerare e causare problemi di funzionamento dei moduli che compongono l'intero sistema.

L'area organizzativa di Produzione e di Sviluppo Software di Namirial sono responsabili dell'infrastruttura e dei sistemi, pertanto 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.

In particolare, il conservatore Namirial effettua le attività di controllo avvalendosi della **piattaforma SySAid** sistema di asset management e ticketing, il quale al verificarsi di un evento anomalo legato alle risorse hardware o ai servizi applicativi crea un ticket in automatico e lo assegna al Responsabile dei sistemi informativi o altro operatore deputato, il quale entro un tempo prestabilito (SLA servizio) deve effettuare le opportune manutenzioni per chiudere l'anomalia. Il ticket viene chiuso dall'operatore inserendo le attività effettuate per chiudere l'incidente.

Gli utenti del sistema di conservazione *Strongdox* usano la stessa piattaforma per aprire i ticket per richiedere supporto al help desk del servizio. Tali ticket riportano tutte le fasi di gestione del ticket nel seguito descritto:

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

Il sistema, inoltre, tiene traccia delle date e ore di gestione dei ticket e mantiene i ticket salvati nel proprio data base almeno per 10 anni.

In particolare, attraverso il sistema di **SysAid**, vengono controllati costantemente:

- processi e web services
- l'esposizione del servizio all'utente
- processi di acquisizione documentali
- 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.

Il sistema inoltre genera in automatico dei report inviati periodicamente al Responsabile dei sistemi informativi e al responsabile della sicurezza. Il dettaglio degli indicatori è riportato nella documentazione del SGSI ISO/IEC 27001:2013.

Ulteriori ed eventuali procedure aggiuntive di monitoraggio e controllo richieste dal soggetto Produttore sono descritte nel documento "Specificità del contratto".

[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 produttore);
- 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 ed indici XML (IPdA) presenti all'interno del sistema di conservazione per un determinato produttore dei documenti).

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 nell'insieme dei documenti conservati. Il campione prodotto da sottoporre a verifica è pari al 5% dei documenti totali conservati per ciascun produttore dei documenti. I controlli eseguiti su questi documenti sono i seguenti:

- 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 human-readable: sull'insieme dei documenti estratti per la verifica di integrità verrà ulteriormente creato un sottoinsieme di documenti nella percentuale del 1% visualizzati da un operatore delegato che verificherà se il documento è correttamente leggibile ad occhio umano.

A seguito di ogni operazione di controllo verrà prodotto un Verbale di controllo firmato digitalmente dal Responsabile del servizio di conservazione e conservato nel sistema di conservazione *Strongdox*.

Ulteriori ed eventuali procedure aggiuntive richieste dal soggetto Produttore sono descritte nel documento di "Specificità del contratto".

[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 eventi anomali 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, secondo quanto previsto anche dal sistema di gestione SGSI certificato ISO/IEC 27001:2013.

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

- Fase 1: Monitoraggio ed 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.

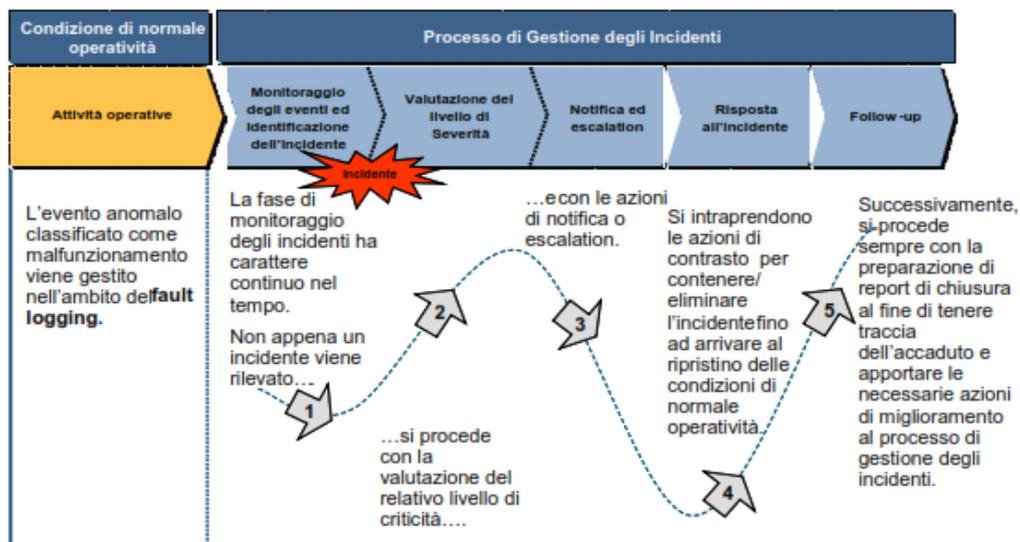


Figura 15 Incident Management

Al verificarsi di malfunzionamenti o situazioni critiche, il sistema di monitoraggio SysAid genera delle notifiche via sms e via email al personale reperibile che si attiverà per risolvere il problema

secondo quanto stabilito dagli SLA concordati con il produttore 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 27001:2013 (in particolare ai documenti Namirial “Piano della Sicurezza” e “BCP – Business Impact Analysis & Risk analysis”). Eventuali ulteriori accordi specifici concordati con il soggetto Produttore sono descritti nel documento di “Specificità del contratto”.

[Torna al Sommario](#)