



Servizio conservazione digitale (E-DK)

Manuale della conservazione

Scopo del documento:	Descrivere l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.
Redatto da:	Silvia Loffi – Digital Corporate Banking Products Data: 13/06/2025
Verificato da:	Armando Mirabella - Catia Principe – CIO – Doc Archiving
Approvato da:	Luca Terzaghi – DCB – DCB Marketing & Products
Codice documento:	0000012567
Classificazione:	esterna
Dominio di applicazione:	Servizio di conservazione E-DK

SOMMARIO

SCOPO E AMBITO DEL DOCUMENTO	4
1. TERMINOLOGIA	5
1.1 Glossario e Acronimi.....	5
2. NORMATIVA E STANDARD DI RIFERIMENTO	15
2.1 Normativa di riferimento	15
2.2 Abrogazione e norme transitorie	16
2.3 I principali riferimenti normativi	17
2.4 Standard di riferimento	18
2.5 Certificazioni	18
3. RUOLI E RESPONSABILITA'	19
3.1 Titolare dell'oggetto della conservazione	19
3.2 Produttore dei PdV	19
3.3 Utente abilitato	19
3.4 Responsabile della conservazione	19
3.5 Conservatore.....	19
3.6 Ruoli Interni al sistema di conservazione	20
4. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE	22
5. OGGETTI SOTTOPOSTI A CONSERVAZIONE	25
5.1 Oggetti conservati	25
5.2 Pacchetto di Versamento	28
5.3 Pacchetto di archiviazione.....	29
5.4 Pacchetto di distribuzione	30
6. IL PROCESSO DI CONSERVAZIONE	32
6.1 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti.....	33
6.1.1 Verifiche relative all'Ente soggetto Produttore.....	33
6.1.2 Verifiche in fase di versamento dei formati dei documenti	33
6.1.3 Verifiche in fase di versamento dei metadati minimi.....	33
6.1.4 Verifiche in fase di versamento della firma del documento.....	33
6.1.5 Verifiche in fase di versamento di documenti singoli	34
6.1.6 Verifiche in fase di versamento dei gruppi di caricamento	34
6.2 Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico.....	34
6.2.1 Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie.....	34
6.3 Preparazione e gestione del pacchetto di archiviazione	36
6.4 Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione.....	36

6.5 Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico Ufficiale nei casi previsti.....	37
7.8 Scarto dei pacchetti di archiviazione.....	38
7.9 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori ..	38
8. IL SISTEMA DI CONSERVAZIONE.....	39
8.1 Componenti Logiche	39
8.2 Componenti Fisiche	40
8.3 Procedure di gestione e di evoluzione	42
9. MONITORAGGIO E CONTROLLI	43
9.1 Procedure di monitoraggio.....	43
9.2 Verifica dell'integrità degli archivi.....	43
9.3 Soluzioni adottate in caso di anomalie.....	44
10. IMPIANTO CONTRATTUALE DEL SERVIZIO (SPECIFICITA' DEL CONTRATTO)	44
INFORMAZIONI GENERALI.....	45
Storia delle modifiche apportate.....	Errore. Il segnalibro non è definito.
Riferimenti procedure interne	46
INDICE DELLE FIGURE	47

SCOPO E AMBITO DEL DOCUMENTO

Il presente Manuale della conservazione digitale di Nexi Payments S.p.A., di seguito Nexi, ha lo scopo di illustrare dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione. in qualità di Conservatore, in ottemperanza alle "Linee Guida sulla formazione, gestione e conservazione dei documenti" di AgID, di seguito Linee Guida.

Con efficacia dal 1° gennaio 2022 si è perfezionata la fusione per incorporazione di SIA S.p.A. in Nexi S.p.A. e nella stessa data si è perfezionata altresì la cessione a Nexi del ramo di azienda costituito dal complesso di beni, materiali e immateriali, funzionalmente organizzati da SIA S.p.A. per l'esercizio della propria attività e comprendente le attività, le passività, nonché tutti i rapporti contrattuali originariamente in capo a SIA S.p.A..

Lo scopo di questo documento è quello di dettagliare le modalità di erogazione del servizio di "conservazione digitale", attraverso la piattaforma proprietaria E-Document Keeper (e-DK) installata nella propria server farm, in modalità SaaS (Software as a service) su Private Cloud.

Il processo di conservazione, qui presentato in dettaglio e secondo le indicazioni fornite dalla norma, mostra una struttura e un'organizzazione, nonché una politica gestionale, atte a garantirne l'aderenza alla normativa vigente in materia di conservazione digitale. Il Responsabile del servizio di conservazione, insieme alle altre figure professionali individuate ed elencate in questo manuale, ha definito l'operatività e le attività di conservazione coerentemente con le politiche di efficienza gestionale e di risorse Nexi Payments per far in modo che tutte le attività siano organizzate per produrre massima efficienza nell'ambito del processo globale di conservazione digitale.

[Torna al sommario](#)

1. TERMINOLOGIA

1.1 Glossario e Acronimi

Il glossario adottato nella stesura del presente Manuale e dei contratti di servizio fa riferimento a quanto riportato nell' allegato 1 delle "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici".

TERMINE	DEFINIZIONE
Accesso	Operazione che consente di prendere visione dei documenti informatici.
Affidabilità	Caratteristica che, con riferimento a un sistema di gestione documentale o conservazione, esprime il livello di fiducia che l'utente ripone nel sistema stesso, mentre con riferimento al documento informatico esprime la credibilità e l'accuratezza della rappresentazione di atti e fatti in esso contenuta.
Aggregazione documentale informatica	Insieme di documenti informatici o insieme di fascicoli informatici riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente.
Archivio	Complesso dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività.
Archivio informatico	Archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche.
Area Organizzativa Omogenea	Un insieme di funzioni e di uffici individuati dall'ente al fine di gestire i documenti in modo unitario e coordinato, secondo quanto disposto dall'art. 50 comma 4 del D.P.R. 28 dicembre 2000, n. 445. Essa rappresenta il canale ufficiale per l'invio di istanze e l'avvio di procedimenti amministrativi.

TERMINE	DEFINIZIONE
Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.
Autenticità	Caratteristica in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto un oggetto è autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze.
Certificazione	Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi.
Cloud della PA	Ambiente virtuale che consente alle Pubbliche Amministrazioni di erogare servizi digitali ai cittadini e alle imprese nel rispetto di requisiti minimi di sicurezza e affidabilità.
Codec	Algoritmo di codifica e decodifica che consente di generare flussi binari, eventualmente imbustarli in un file o in un wrapper (codifica), così come di estrarli da esso (decodifica).
Conservatore	Soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici.
Conservazione	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti
Convenzioni di denominazione del file	Insieme di regole sintattiche che definisce il nome dei file all'interno di un file system o pacchetto.
Destinatario	Soggetto o sistema al quale il documento informatico è indirizzato.

TERMINE	DEFINIZIONE
Digest	Vedi Impronta crittografica.
Documento amministrativo informatico	Ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa
Documento elettronico	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva
Documento informatico	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Duplicato informatico	Vedi art. 1, comma 1, lett) i quinquies del CAD.
eSeal	Vedi sigillo elettronico.
Esibizione	L'operazione che consente di visualizzare un documento conservato
eSignature	Vedi firma elettronica.
Estratto di documento informatico	Parte del documento tratto dal documento originale
Fascicolo informatico	Aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento.
File	Insieme di informazioni, dati o comandi logicamente correlati, raccolti sotto un unico nome e registrati, per mezzo di un programma di elaborazione o di scrittura, nella memoria di un computer.

TERMINE	DEFINIZIONE
Filesystem	Sistema di gestione dei file, strutturato mediante una o più gerarchie ad albero, che determina le modalità di assegnazione dei nomi, memorizzazione e organizzazione all'interno di uno storage.
Firma elettronica	Vedi articolo 3 del Regolamento eIDAS.
Firma elettronica avanzata	Vedi articoli 3 e 26 del Regolamento eIDAS.
Firma elettronica qualificata	Vedi articolo 3 del Regolamento eIDAS.
Formato del documento informatico	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
Formato "deprecato"	Formato in passato considerato ufficiale il cui uso è attualmente sconsigliato a favore di una versione più recente.
Funzione di hash crittografica	Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o digest (vedi) in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
Gestione Documentale	Processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta, uso, selezione e conservazione dei documenti.
hash	Termine inglese usato, impropriamente, come sinonimo d'uso di "impronta crittografica" o "digest" (vedi).

TERMINE	DEFINIZIONE
Identificativo univoco	Sequenza di numeri o caratteri alfanumerici associata in modo univoco e persistente ad un'entità all'interno di uno specifico ambito di applicazione.
Impronta crittografica	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di hash crittografica a un'evidenza informatica.
Integrità	Caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità.
Interoperabilità	Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi.
Leggibilità	Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica.
Manuale di conservazione	Documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture.
Manuale di gestione	Documento informatico che descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

TERMINE	DEFINIZIONE
Metadati	Dati associati a un o documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017.
Naming convention	Vedi Convenzioni di denominazione
Oggetto di conservazione	Oggetto digitale versato in un sistema di conservazione.
Oggetto digitale	Oggetto informativo digitale, che può assumere varie forme tra le quali quelle di documento informatico, fascicolo informatico, aggregazione documentale informatica o archivio informatico.
Pacchetto di archiviazione	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel manuale di conservazione.
Pacchetto di distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione.
Pacchetto di file (file package)	Insieme finito di più file (possibilmente organizzati in una struttura di sottoalbero all'interno di un file system) che costituiscono, collettivamente oltre che individualmente, un contenuto informativo unitario e auto-consistente.
Pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione.
Pacchetto informativo	Contenitore logico che racchiude uno o più oggetti di conservazione con i relativi metadati, oppure anche i soli metadati riferiti agli oggetti di conservazione.

TERMINE	DEFINIZIONE
Path	Percorso (vedi).
Pathname	Concatenazione ordinata del percorso di un file e del suo nome.
Percorso	Informazioni relative alla localizzazione virtuale del file all'interno del file system espressa come concatenazione ordinata del nome dei nodi del percorso.
Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi.
Piano della sicurezza del sistema di gestione Informatica dei documenti	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi.
Piano di classificazione (Titolario)	Struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata.
Piano di conservazione	Documento, allegato al manuale di gestione e integrato con il sistema di classificazione, in cui sono definiti i criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445.
Piano generale della sicurezza	Documento che pianifica le attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza.
Presa in carico	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione e, in caso di affidamento del servizio all'esterno, dagli accordi stipulati tra il titolare dell'oggetto di conservazione e il responsabile del servizio di conservazione.

TERMINE	DEFINIZIONE
Processo	Insieme di attività correlate o interagenti che trasformano elementi in ingresso in elementi in uscita.
Produttore dei PdV	Persona fisica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con il responsabile della gestione documentale.
QSeal	Sigillo elettronico qualificato, come da art. 35 del Regolamento eIDAS.
qSignature	Firma elettronica qualificata, come da art.25 del Regolamento eIDAS.
Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.
Regolamento eIDAS	Electronic IDentification Authentication and Signature, Regolamento (UE) № 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
Responsabile del servizio di conservazione	soggetto che coordina il processo di conservazione all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Responsabile della conservazione	Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.
Responsabile della funzione archivistica di conservazione	soggetto che coordina il processo di conservazione dal punto di vista archivistico all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID

TERMINE	DEFINIZIONE
Responsabile della gestione documentale	Soggetto responsabile della gestione del sistema documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445.
Responsabile della protezione dei dati	Persona con conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, in grado di assolvere i compiti di cui all'articolo 39 del Regolamento (UE) 2016/679.
Responsabile della sicurezza dei sistemi di conservazione	soggetto che assicura il rispetto dei requisiti di sicurezza all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	soggetto che assicura lo sviluppo e la manutenzione del sistema all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Riferimento temporale	Insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC).
Riversamento	Procedura mediante la quale uno o più documenti informatici sono convertiti da un formato di file (ovvero di busta, ovvero di pacchetto di file) ad un altro, lasciandone invariato il contenuto per quanto possibilmente permesso dalle caratteristiche tecniche del formato (ovvero dei formati) dei file e delle codifiche di destinazione.
Scarto	Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storicoculturale.
Sidecar (file)	File-manifesto (vedi).
Sigillo elettronico	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi.

TERMINE	DEFINIZIONE
Sistema di conservazione	Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, comma 1, del CAD.
Sistema di gestione informatica dei documenti	Insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle organizzazioni per la gestione dei documenti. Nell'ambito
	della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445
Timeline	Linea temporale virtuale su cui sono disposti degli eventi relativi ad un sistema informativo o a un documento informatico. Costituiscono esempi molto diversi di timeline un file di log di sistema, un flusso multimediale contenente essenze audio/video sincronizzate.
Titolare dell'oggetto di conservazione	Soggetto produttore degli oggetti di conservazione.
Trasferimento	Passaggio di custodia dei documenti da una persona o un ente ad un'altra persona o un altro ente.
TUDA	Testo Unico della Documentazione Amministrativa, Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni e integrazioni.
Ufficio	Riferito ad un'area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico.
Utente abilitato	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.

TERMINE	DEFINIZIONE
Versamento	Passaggio di custodia, di proprietà e/o di responsabilità dei documenti. Nel caso di un organo giudiziario e amministrativo dello Stato operazione con la quale il responsabile della conservazione trasferisce agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali.

ACRONIMO	DESCRIZIONE
AGID	Agenzia per l'Italia digitale
CAD	Codice dell'Amministrazione Digitale - Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni.
eIDAS	Regolamento (UE) № 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
FEA	Vedi firma elettronica avanzata.
FEQ	Vedi firma elettronica qualifica.
GDPR	Regolamento (UE) № 679/2016 del Parlamento Europeo e del Consiglio, del 27 aprile 2016 ("General Data Protection Regulation"), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.
PdA (AiP)	Pacchetto di Archiviazione.
PdD (DiP)	Pacchetto di Distribuzione.
PdV (SiP)	Pacchetto di Versamento.
UOR	Unità Organizzativa Responsabile

[Torna al sommario](#)

2. NORMATIVA E STANDARD DI RIFERIMENTO

Si elencano, di seguito, le principali normative e standard in ambito conservazione digitale.

2.1 Normativa di riferimento

Le Linee Guida contengono le regole tecniche sugli ambiti disciplinati dalle seguenti disposizioni del CAD:

- Art. 20, *Validità ed efficacia probatoria dei documenti informatici*, fatte salve le norme in materia di generazione, apposizione e verifica di qualsiasi tipo di firma elettronica
- Art. 20, *Validità ed efficacia probatoria dei documenti informatici*, fatte salve le norme in materia di generazione, apposizione e verifica di qualsiasi tipo di firma elettronica
- Art. 21, *Ulteriori disposizioni relative ai documenti informatici, sottoscritti con firma elettronica avanzata, qualificata o digitale*
- Art. 22, commi 2 e 3, *Copie informatiche di documenti analogici*
- Art. 23, *Copie analogiche di documenti informatici*
- Art. 23-bis, *Duplicati e copie informatiche di documenti informatici*

- Art. 23-ter, *Documenti amministrativi informatici*
- Art. 23-quater, *Riproduzioni informatiche*
- Art. 34, *Norme particolari per le Pubbliche Amministrazioni*
- Art. 40, *Formazione di documenti informatici*
- Art. 40-bis, *Protocollo informatico*
- Art. 41, *Procedimento e fascicolo informatico*
- Art. 42, *Dematerializzazione dei documenti delle Pubbliche Amministrazioni*
- Art. 43, *Conservazione ed esibizione dei documenti*
- Art. 44, *Requisiti per la conservazione dei documenti informatici*
- Art. 45, *Valore giuridico della trasmissione*
- Art. 46, *Dati particolari contenuti nei documenti trasmessi*
- Art. 47, *Trasmissione dei documenti tra le Pubbliche Amministrazioni*
- Art. 49, *Segretezza della corrispondenza trasmessa per via telematica*
- Art. 50, *Disponibilità dei dati delle Pubbliche Amministrazioni*
- Art. 51, *Sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture delle Pubbliche Amministrazioni*
- Art. 64-bis, *Accesso telematico ai servizi della Pubblica Amministrazione*
- Art. 65, *Istanze e dichiarazioni presentate alle Pubbliche Amministrazioni per via telematica*

[Torna al sommario](#)

2.2 Abrogazione e norme transitorie

Le presenti Linee Guida entrano in vigore dal 1 gennaio 2022.

A partire da questo termine i soggetti di cui all' art. 2 commi 2 e 3 del CAD formano i loro documenti esclusivamente in conformità alle presenti Linee Guida.

A partire da tale data, sono abrogati:

- il DPCM 13 novembre 2014, contenente “Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici”;
- il DPCM 3 dicembre 2013, contenente “Regole tecniche in materia di sistema di conservazione”.

Per quanto concerne il DPCM 3 dicembre 2013, contenente “Regole tecniche per il protocollo informatico”, a partire dalla data di applicazione delle presenti Linee guida sono abrogate tutte le disposizioni fatte salve le seguenti:

- art. 2 comma 1, *Oggetto e ambito di applicazione*;
- art. 6, *Funzionalità*;
- art. 9, *Formato della segnatrice di protocollo*;
- art. 18 commi 1 e 5, *Modalità di registrazione dei documenti informatici*; • art. 20, *Segnatrice di protocollo dei documenti trasmessi*;
- art. 21, *Informazioni da includere nella segnatrice*.

Sempre a far data dalla data di applicazione delle presenti Linee guida, la circolare n. 60 del 23 gennaio 2013 dell'AgID in materia di “Formato e definizione dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le Pubbliche Amministrazioni” è abrogata e sostituita dall'allegato 6 “Comunicazione tra AOO di documenti amministrativi protocollati” del presente documento.

[Torna al sommario](#)

2.3I principali riferimenti normativi

I principali riferimenti normativi sono i seguenti:

- a) RD 1163/1911, *Regolamento per gli archivi di Stato*;
- b) DPR 1409/1963, *Norme relative all'ordinamento ed al personale degli archivi di Stato*;
- c) DPR 854/1975, *Attribuzioni del Ministero dell'interno in materia di documenti archivistici non ammessi alla libera consultabilità*;
- d) Legge 241/1990, *Nuove norme sul procedimento amministrativo*;
- e) DPR 445/2000, *Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*;
- f) DPR 37/2001, *Regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli uffici dello Stato*;
- g) D.lgs 196/2003 recante il *Codice in materia di protezione dei dati personali*;
- h) D.lgs 42/2004, *Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137*;
- i) Legge 9 gennaio 2004, n. 4 aggiornata dal decreto legislativo 10 agosto 2018, n. 106, *Disposizioni per favorire e semplificare l'accesso degli Utenti abilitati e, in particolare, delle persone con disabilità agli strumenti informatici*;
- j) D.lgs 82/2005 e ss.mm.ii., *Codice dell'amministrazione digitale*;
- k) D.lgs 33/2013, *Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*;
- l) DPCM 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*;
- m) DPCM 21 marzo 2013, *Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere Utenti abilitati da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni*;
- n) Reg. UE 910/2014, *in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE - Regolamento eIDAS*;
- o) Circolare 40 e 41 del 14 dicembre 2015 della Direzione generale degli archivi, *Autorizzazione alla distruzione di originali analogici riprodotti secondo le regole tecniche di cui al DPCM 13.11.2014 e conservati secondo le regole tecniche di cui al DPCM 13.12.2013*;
- p) Reg. UE 679/2016 (GDPR), *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*;
- q) Circolare 18 aprile 2017, n. 2/2017 dell'Agenzia per l'Italia Digitale, *recante le misure minime di sicurezza ICT per le pubbliche amministrazioni*;
- r) Circolare n. 2 del 9 aprile 2018, *recante i criteri per la qualificazione dei Cloud Service Provider per la PA*;
- s) Circolare n. 3 del 9 aprile 2018, *recante i criteri per la qualificazione di servizi SaaS per il Cloud della PA*;
- t) Reg. UE 2018/1807, *relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea*;
- u) DPCM 19 giugno 2019, n. 76, *Regolamento di organizzazione del Ministero per i beni e le attività culturali, degli uffici di diretta*.

[Torna al sommario](#)

2.4 Standard di riferimento

Si riportano di seguito gli standard di riferimento:

- ISO 14721:2012 OAIS, (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- REFERENCE MODEL FOR AN OPEN ARCHIVAL INFORMATION SYSTEM (OAIS) 02/2025
- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- 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 TS 101 533-1 V1.3.1 (2012-04), Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- UNI 11386:2020 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

2.5 Certificazioni

Nexi ha implementato un Sistema di Gestione della Qualità conforme alla norma ISO 9001:2015 per i seguenti campi di attività “Ideazione, progettazione, realizzazione, gestione e relativa assistenza di soluzioni di pagamento digitali (pagamento e accettazione) dedicate a Consumatori, Esercenti, Aziende e Istituzioni Pubbliche, in collaborazione con le Banche partner. Ideazione, progettazione, realizzazione, gestione e relativa assistenza di infrastrutture e servizi tecnologici, di soluzioni software e di servizi informatici e di outsourcing tecnologico e applicativo dedicati a Banche Centrali, Clearing House, associazioni e consorzi bancari, Pubblica Amministrazione, nei settori dei Clienti Privati ed Esercenti, dei Pagamenti Digitali, dei Servizi di Rete, dei Mercati dei Capitali, delle Grandi Basi Dati e della Conservazione di Documenti Digitali.”.

Inoltre, Nexi ha implementato un Sistema di Gestione della Sicurezza delle Informazioni conforme alla norma ISO 27001:2013 per i seguenti campi di attività: “Erogazione del servizio di Conservazione Digitale. Progettazione, sviluppo e manutenzione di software per la Conservazione Digitale.

Nexi è in possesso delle certificazioni presenti su questa pagina:

<https://www.nexi.it/chi-siamo/brand/certificazioni.html>.

[Torna al sommario](#)

3. RUOLI E RESPONSABILTA'

3.1 Titolare dell'oggetto della conservazione

È il soggetto produttore degli oggetti di conservazione (definizione dell'Allegato 1 al documento "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici"), ossia il Cliente che ha sottoscritto un contratto con la società Nexi, avente come oggetto la fornitura del servizio di conservazione digitale dei documenti informatici.

Nell'ambito di tale contratto il Cliente ha nominato la società Nexi Conservatore dei propri documenti informatici.

3.2 Produttore dei PdV

Persona fisica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione (definizione dell'Allegato 1 al documento "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici"). Nelle pubbliche amministrazioni, tale figura si identifica con il responsabile della gestione documentale.

Ricevendo dal cliente/produttore le informazioni documentali secondo un tracciato concordato, tramite il proprio sistema documentale, crea i pacchetti di versamento destinati ad essere acquisiti dal sistema di Conservazione rispettando tempi e modalità previste dal contratto.

3.3 Utente abilitato

Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse (definizione dell'Allegato 1 al documento "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici").

Le Utenze con tali privilegi di "esibizione a norma" sono concordate con il soggetto titolare dei contenuti e, generalmente, laddove non diversamente specificato, sono costituite dal personale amministrativo e gestionale del soggetto Titolare delle informazioni conservate.

[Torna al sommario](#)

3.4 Responsabile della conservazione

Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia (definizione dell'Allegato 1 al documento "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici").

Per le Pubbliche amministrazioni è un ruolo previsto dall'organigramma del Titolare dell'oggetto di conservazione, per i soggetti diversi dalla Pubblica Amministrazione, il ruolo del responsabile della conservazione può essere svolto da un soggetto esterno all'organizzazione, in possesso di idonee competenze giuridiche, informatiche ed archivistiche, purché terzo rispetto al Conservatore al fine di garantire la funzione del Titolare dell'oggetto di conservazione rispetto al sistema di conservazione.

3.5 Conservatore

Nexi è la PayTech Europea con la scala, le capacità e la vicinanza territoriale per fornire le soluzioni di pagamento più semplici, veloci e sicure a Persone, Aziende e Istituzioni Finanziarie.

Nasce dall'unione di Nexi, Nets e Sia, tre dei maggiori player europei nel mercato dei pagamenti e siamo presenti in più di 25 Paesi. Nexi svolge il ruolo di Conservatore, ed eroga e svolge in modalità full outsourcing il processo di conservazione dei documenti informatici.

Inoltre offre la soluzione di conservazione digitale in continuità con il servizio di conservazione erogato da SIA S.p.A.

[Torna al sommario](#)

Di seguito i dati societari:

DENOMINAZIONE SOCIALE	Nexi Payments S.p.A.
SEDE LEGALE E DIREZIONE GENERALE	Corso Sempione 55, 20149 Milano Tel. +39 02 3488.1 (Centralino - No Servizio Clienti) Fax +39 02 3488.4180
SITO WEB	https://www.nexigroup.com/
CODICE FISCALE/ PARTITA IVA	Reg. Imprese Milano, Monza Brianza e Lodi, C.F. 04107060966 Membro del Gruppo IVA Nexi P.IVA 10542790968 REA Milano n. 1725898

[Torna al sommario](#)

3.6 Ruoli Interni al sistema di conservazione

La tabella seguente riporta la descrizione di tutti i nominativi che partecipano al processo di Conservazione Digitale di Nexi.

Con un provvedimento interno la società Nexi ha provveduto a individuare nel proprio organigramma le persone che per competenza ed esperienza garantiranno la corretta esecuzione delle operazioni ad esse affidate.

[Torna al sommario](#)

RUOLI	ATTIVITÀ DI COMPETENZA	DATA NOMINA
Responsabile del servizio di conservazione (RSdC) Silvia Loffi	- la definizione e attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione; - la definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente; - la corretta erogazione del servizio di conservazione all'ente produttore; - la gestione delle convenzioni, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione	Dal 2019 e confermato ruolo nel 2022 post fusione.
Responsabile funzione archivistica di conservazione (RFAC) Silvia Loffi	- la 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; - la definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici; - il monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione; - la collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.	DAL 2022

Il Responsabile del servizio di Conservazione è stato incaricato espressamente e nominalmente dalla direzione DCB (Digital Corporate Banking) di Nexi.

[Torna al sommario](#)

4. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

La struttura organizzativa in cui è inserito il Conservatore e il Responsabile funzione archivistica di conservazione è la struttura di Digital Corporate Banking, nella figura di Silvia Loffi, in particolare la struttura DCB Marketing & Products.

Le strutture organizzative coinvolte nell'erogazione e gestione del servizio sono presenti nelle aree:

- DCB – Digital Corporate and Open Banking
- Operations - Operations Digital Banking & Corporate Solutions
- CIO – Core Infrastructures & Platforms
- CIO – Payments Platforms
- CIO – IT Governance, Architecture & Cybersecurity
- CIO – Core Infrastructures & Platforms
- CISO - Chief Information Security Officer
- Compliance – IT & Data Protection Compliance
- Risk Management –Servicing customers risks and Int'l Markets

[Torna al sommario](#)

Lo schema che segue illustra attraverso una matrice di responsabilità O (Opera), R (Responsabile) V (Verifica) rispetto alle fasi di erogazione e le attività del Servizio di conservazione:

RESPONSABILITÀ	CONSERVATORE- RESPONSABILE DEL SERVIZIO DI CONSERVAZIONE	RESPONSABILE DELLA FUNZIONE ARCHIVISTICA DI CONSERVA	RESPONSABILE DELLA CONSERVAZIONE
Attivazione del servizio (A seguito della sottoscrizione del contratto)	O R	V	R
Acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento	O R	V	V
Preparazione e gestione del pacchetto di archiviazione	O R	V	V
Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta;	O R	V	V
Scarto dei pacchetti di archiviazione	R	R	R
Chiusura del Servizio (al termine di un contratto di servizio)	OR	V	R

[Torna al sommario](#)

Lo schema che segue illustra attraverso una matrice di responsabilità O (Opera), R (Responsabile) V (Verifica) rispetto alle responsabilità rispetto al ciclo di vita del Servizio e le attività proprie di gestione dei sistemi informativi:

RESPONSABILITÀ	CONSERVATORE - RESPONSABILE DEL SERVIZIO DI CONSERVAZIONE	RESPONSABILE DELLA FUNZIONE ARCHIVISTICA DI CONSERVAZIONE	RESPONSABILE DELLA CONSERVAZIONE
Conduzione e manutenzione del sistema di conservazione	O R	V	V
Monitoraggio del sistema di conservazione	O R	V	V
Change management	O R	V	
Verifica periodica di conformità a normativa standard di riferimento	O R	V	V

[Torna al sommario](#)

5. OGGETTI SOTTOPOSTI A CONSERVAZIONE

Il servizio di conservazione E-DK (Electronic- Document Keeper) conserva molteplici tipologie documentali come descritto nelle Specifiche tecniche allegato al contratto concordato tra il Conservatore e il Responsabile della conservazione.

5.1 Oggetti conservati

La gestione delle tipologie documentarie viene effettuata dal Responsabile della funzione archivistica di conservazione e dai suoi collaboratori, che per ciascuna tipologia documentaria provvedono a definire i metadati standard, in linea con l'allegato 5 "Metadati" delle LLGG Agid.

Per la descrizione e l'applicazione dei nuovi metadati si fa riferimento al "Gestione Metadati Allegato 5_e-DK".

Di seguito si elencano i parametri di controllo del servizio di conservazione:

- firma digitale su ciascun documento (opzionale in base alla tipologia documentale): i documenti informatici da conservare sono pronti per essere inseriti in pacchetti di archiviazione oppure si necessita di uno step di firma su ciascun documento prima della creazione dei pacchetti di archiviazione;
- firma digitale sull'indice dei pacchetti di archiviazione da parte del responsabile del servizio di conservazione;
- marca temporale sull'indice dei pacchetti di archiviazione;
- periodo di conservazione (Retention Time);
- parametri di servizio per la procedura di trattamento dei documenti;
- regole per l'estrazione dei documenti dal sistema alimentante per la conservazione;
- frequenza di estrazione dei documenti dal sistema alimentante;
- tempistica di conservazione;
- frequenza delle attività di controllo periodiche;
- dimensionamento del flusso dei documenti da conservare;
- sistema alimentante;
- provider del sistema alimentante: esterno o interno;
- formato dei documenti standard in base a quanto descritto nell'allegato 2 delle Linee Guida o proprietario. Nel caso di formato proprietario occorre che vengano compiute le attività di aggiornamento della libreria dei visualizzatori, come descritto nel documento "Specificità del contratto";
- metadati specifici della tipologia di documenti.

Le principali tipologie documentarie trattate dal Servizio sono descritte nel documento "Specifiche tecniche" del servizio, dove per ogni tipologia documentaria vengono identificati i metadati standard compliance con le LLGG Agid.

Tutti i formati gestiti sono coerenti con quelli elencati e descritti in un registro interno al Servizio.

I formati gestiti dal servizio per la conservazione di specifiche tipologie documentarie sono concordati con il Produttore ed esplicitati anch'essi all'interno degli accordi contrattuali, che definiscono anche le eventuali modalità di aggiornamento concordato dei formati gestiti.

[Torna al sommario](#)

I PRINCIPALI FORMATI PREVISTI PER I DOCUMENTI SONO ELENCATI NELL'ALLEGATO 2. FORMATO	TIPO FILE (MIME)	ESTENSIONE	VISUALIZZATORE	STANDARD
PFA/PDFA/PDFB	Application/pdf	.pdf	Adobe Reader	ISO/IEC 32000; ISO/IEC 19005
ODT	Application/vnd.oasis .opendocument.text	.odt	Writer, LibreOffice	ISO/IEC 26300
XML	Application/xml	.xml	Browser, Editor di testo	www.w3.org/standards/xml
XSD	Application/xml	.xsd	Browser, Editor di testo	W3C Recommendation XLS
XSL	Text/xls	.xsl	Browser, Editor di testo	W3C Working Draft XSL
XSLT	Application/xslt+xml, text/xml	.xslt	Browser, Editor di testo	W3C Recommendation XSL Transformation
CSS	Text/css	.css	Browser, Editor di testo	W3C Recommendation CSS
MathML	Text/mathml	.mml, .xml	Browser, Editor di testo	ISO/IEC 40314 W3C Recommendation MathML
SQL	Application/sql	.sql	Microsoft SQL	ISO/IEC 9075
JSON	Application/json	.json	JavaScript	ISO/IEC 8825
JSON-LD	Application/ld+Jason	.jsonld	JavaScript	W3C Recommendation JSONLD
CSV	Text/csv	.csv		
OOXML		.docx, .xlsx, .pptx	Microsoft Office	ISO/IEC 29500
EML	Application/eml	.eml	Microsoft Outlook	RFC 5322 RFC 2822
Mbox	Application/mbox	.mbox		RFC 4155
Excel	application/vnd.open xmlformatofficedocument.spread sheetml.sheet	.xlsx	Microsoft Excel	RFC 2822

I PRINCIPALI FORMATI PREVISTI PER I DOCUMENTI SONO ELENCATI NELL'ALLEGATO 2. FORMATO	TIPO FILE (MIME)	ESTENSIONE	VISUALIZZATORE	STANDARD
PowerPoint	application/vnd.openxmlformats-officedocument.presentationml.presentation	.pptx, .ppsx, .potx	Microsoft PowerPoint	
PNG	Image/png	.png	ACME	ISO/IEC 15948
JPEG	Image/jpg, image/jpeg	.jpg, .jpeg		www.jpeg.org/jpeg
TIFF	Image/tiff	.tiff, .tif	Imaging	ISO/IEC 12234
WAV	Audio/wave	.wav, .bmf, .rf64	IBM, Microsoft	RFC 2361
MP4	Video/mp4, audio/mp4	.mp4, .m4a, .m4v	QuickTime	ISO/IEC 14496
ZIP	Application/zip	.zip, .zipx	ZIP	ISO/IEC 21320

Il Produttore si impegna a versare nel Sistema di Conservazione documenti privi di codici eseguibili o macro istruzioni o privi di qualsiasi causa, anche non visibile all'utente, che ne possa alterare il contenuto; si impegna inoltre a versare documenti nei formati ammessi.

Il Sistema di Conservazione conserva degli oggetti, ovvero dei pacchetti informativi contenenti a loro volta uno o più oggetti da trattare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche, metadati riferiti agli oggetti da conservare o conservati) comprensivi delle informazioni per la loro consultazione.

Per tutta la durata della conservazione, i pacchetti di archiviazione possono essere richiesti dagli Utenti abilitati, nel formato di pacchetto di distribuzione. Il pacchetto di distribuzione si presenta in una forma idonea alle specifiche esigenze di utilizzo delle tipologie documentarie conservate e delle evidenze informatiche generate dal sistema nel corso del processo di conservazione.

I pacchetti sono distinti in tre tipologie:

Pacchetto di Versamento (PdV)

È il pacchetto con cui il Soggetto Produttore trasferisce gli oggetti da conservare al Sistema di Conservazione.

Il Sistema di Conservazione in seguito al versamento di un PdV genera, un rapporto di versamento che attesta l'avvenuta presa in carico da parte del Sistema di Conservazione del PdV inviato dal Produttore.

Il rapporto di versamento, univocamente identificato, firmato e conservato, certifica che i documenti inviati dal Produttore coincidano con quelli acquisiti dal Sistema di Conservazione.

Pacchetto di Archiviazione (PdA)

È il pacchetto informativo con cui il Sistema di Conservazione conserva i dati con garanzia di integrità e reperibilità nel tempo.

Il Pacchetto di Archiviazione viene formato in seguito alla acquisizione del PdV. Il pacchetto di archiviazione viene riepilogato nell'Indice del Pacchetto di Archiviazione.

Pacchetto di Distribuzione (PdD)

È il pacchetto informativo con cui i dati conservati sono resi disponibili agli Utenti abilitati per la consultazione.

Nei paragrafi seguenti viene descritto l'intero processo implementato da Nexi per la conservazione a norma dei documenti e quindi dalla ricezione del PdV, alla generazione del PdA, fino alla creazione del PdD.

I metadati di ricerca utilizzati nel Sistema di Conservazione, sono concordati con il Produttore, oltre a quelli minimi obbligatori indicati e definiti nell'Allegato 5 delle Linee Guida.

[Torna al sommario](#)

5.2 Pacchetto di Versamento

Il pacchetto di versamento (*Submission Information Package*, SIP) è creato in conformità allo standard OAIS. Ogni tipologia di pacchetto di versamento utilizza la struttura dati definita da un set di metadati obbligatori e un set opzionale.

Le eventuali personalizzazioni di tali pacchetti, specifiche di un contratto, sono descritte nell'allegato "Specificità del contratto".

In fase di analisi previa attivazione del servizio si definiscono tutte le tipologie documentali e tutte le rispettive caratteristiche insieme al Produttore.

Conservatore e Produttore si accordano sulle modalità di versamento e, ove necessario, redigono un apposito accordo di versamento (*submission agreement*) nel quale vengono indicati i formati, le caratteristiche e le dimensioni massime dei documenti da versare, le relative modalità e i tempi di versamento e ogni altra indicazione necessaria a garantire il corretto versamento dei documenti al sistema di conservazione.

Il file Indice del Pacchetto di Versamento (IpdV/distinta di caricamento) contiene, quindi, i seguenti elementi:

- l'identificazione del soggetto Titolare dei dati presenti nel Pacchetto di Versamento;
- la definizione della tipologia documentale (a cui appartengono i documenti inclusi nel pacchetto);
- la definizione dei documenti inclusi nel pacchetto, con le relative informazioni quali: nome file, indici (tag) e relativi valori (metadati), ecc.

Nel dettaglio il pacchetto di versamento contiene le seguenti informazioni:

- Codice-azienda (Titolare del dato);
- Tipologia-Documentale;
- N° documenti;
- Tag dei metadati specifici di ogni singolo documento presente nel PdV.

Il file Indice del Pacchetto di Versamento (IpdV/distinta di caricamento) può essere eventualmente firmato digitalmente dal Produttore dei documenti.

[Torna al sommario](#)

5.3 Pacchetto di archiviazione

I pacchetti di archiviazione (Archival Information Package, AIP), sono creati secondo lo standard OAIS, e sono composti dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nella rappresentazione grafica SInCRO UNI 11386:2020.

Pertanto l'identificativo univoco dell'PIndex è identico all'identificativo numerico univoco del PdA.

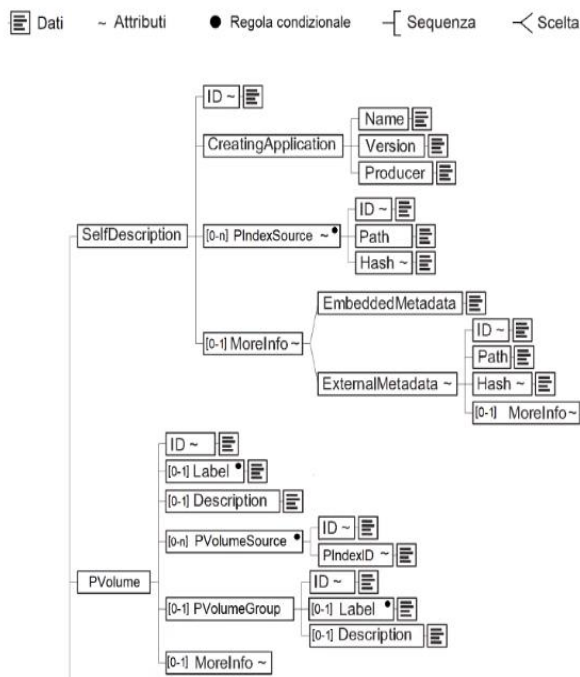
Il PdA è rappresentato da un file compresso contenente i seguenti files:

- Schema XSD PVolume;
- Schema XSD del file indice contenente i metadati associati ai files contenuti nel FileGroup;
- Xml PIndex firmato e marcato;
- Xml del file indice contenente i metadati associati ai files contenuti nel PIndex;
- Marca Temporale in formato .tsr.
- Documenti.

Per assicurare l'interoperabilità nel tempo dei sistemi di conservazione, PIndex viene formato secondo le regole tecniche definite nella norma UNI 11386:2020 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.

La norma UNI 11386:2020 definisce la struttura ed il contenuto del PIndex. Il principale contenuto del PIndex è relativo a:

- Informazioni relative al Sistema di Conservazione stesso (ovvero versione, produttore, identificativo);
- Informazioni relative al Volume di Conservazione (identificativo, pacchetti di archiviazione, ... - Standard OAIS - PDI Reference);
- Informazioni relative ai files (Hash, id, percorso, ... - Standard OAIS - PDI Fixity);
- Informazioni relative ai Metadati di Archiviazione dei Documenti (Standard OAIS - PDI Context);



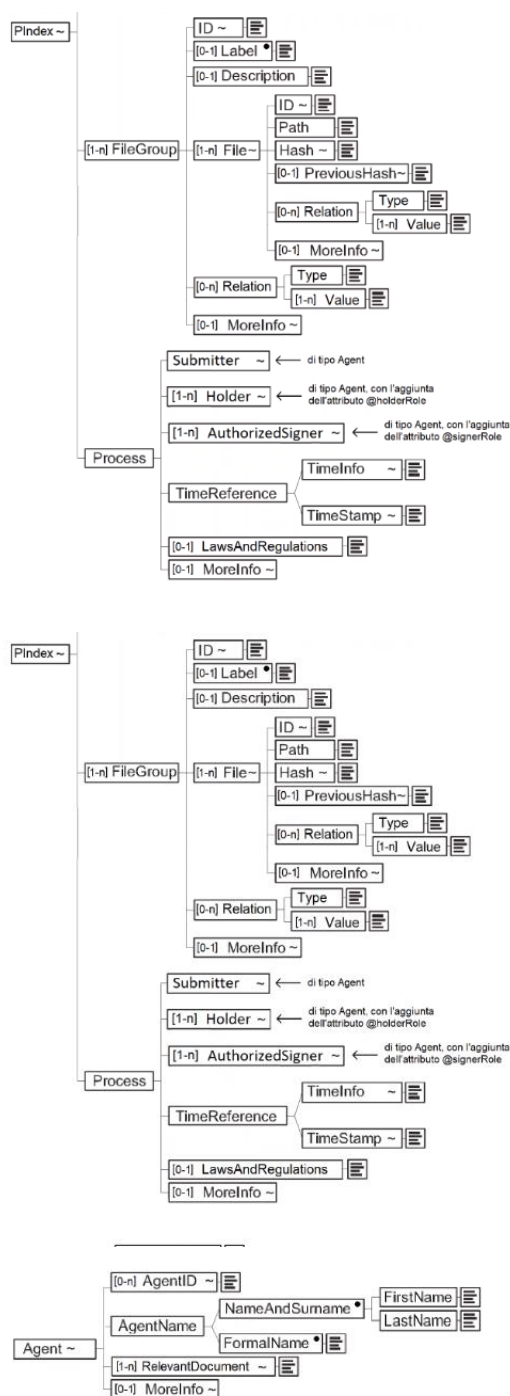


Figura 1 Struttura dati del pacchetto di archiviazione secondo standard UNI 11386:2020 Standard SInCRO

[Torna al sommario](#)

5.4 Pacchetto di distribuzione

Il pacchetto di distribuzione (*Dissemination Information Package*, DIP), creato secondo lo standard OAIS, è inviato dal Servizio all'Utente in risposta ad una sua richiesta di esibizione o ricerca.

Il pacchetto è ricercabile tramite opportune funzioni web, in particolare tramite interfacce user friendly, messe a disposizione dal Servizio che permettono di valorizzare, quale criterio per la ricerca, ciascuno dei metadati caratteristici del pacchetto.

È quindi disponibile al Conservatore e all'Utente la funzionalità di esportazione di pacchetti e relativi indici, attraverso la quale è possibile scaricare un file .zip contenente il file indice dei pacchetti, i documenti conservati e le evidenze della conservazione (firme e marche temporali). Inoltre sono disponibili le interfacce applicative per poter operare l'estrazione di file .zip contenenti file indici dei pacchetti, i documenti conservati e le evidenze della conservazione (firme e marche temporali) tramite applicazione esterna e in modalità massiva automatica, in base a specifiche concordate in fase contrattuale.

Il pacchetto di distribuzione è il pacchetto informativo inviato dal sistema di conservazione all'utente abilitato che ne effettua la richiesta.

Il PdD è un file in formato compresso che disporrà dei seguenti elementi:

- I documenti richiesti dall'Utente (funzione esportazione pacchetti di distribuzione selettivi, solo da front end web);
- I rispettivi PdA anch'essi in formato compresso e contenenti quindi i files PIndex firmati digitalmente dal Responsabile del Servizio di Conservazione associati ai documenti richiesti, le marche temporali associate e i rispettivi files di metadati e i file Xsd con i rispettivi schemi;
- Il file indice del PdD (PIndex): file ispirato allo standard UNI SINCRO 11386:2020.

Ogni PdD generato viene archiviato nel Sistema di conservazione e contiene i seguenti ulteriori metadati:

- Identificativo Univoco del PdD;
- Ragione Sociale Cliente titolare della documentazione;
- Utente richiedente;
- Riferimenti temporali della generazione.

[Torna al sommario](#)

6. IL PROCESSO DI CONSERVAZIONE

Il processo di conservazione segue le seguenti fasi, che di seguito si schematizzano:

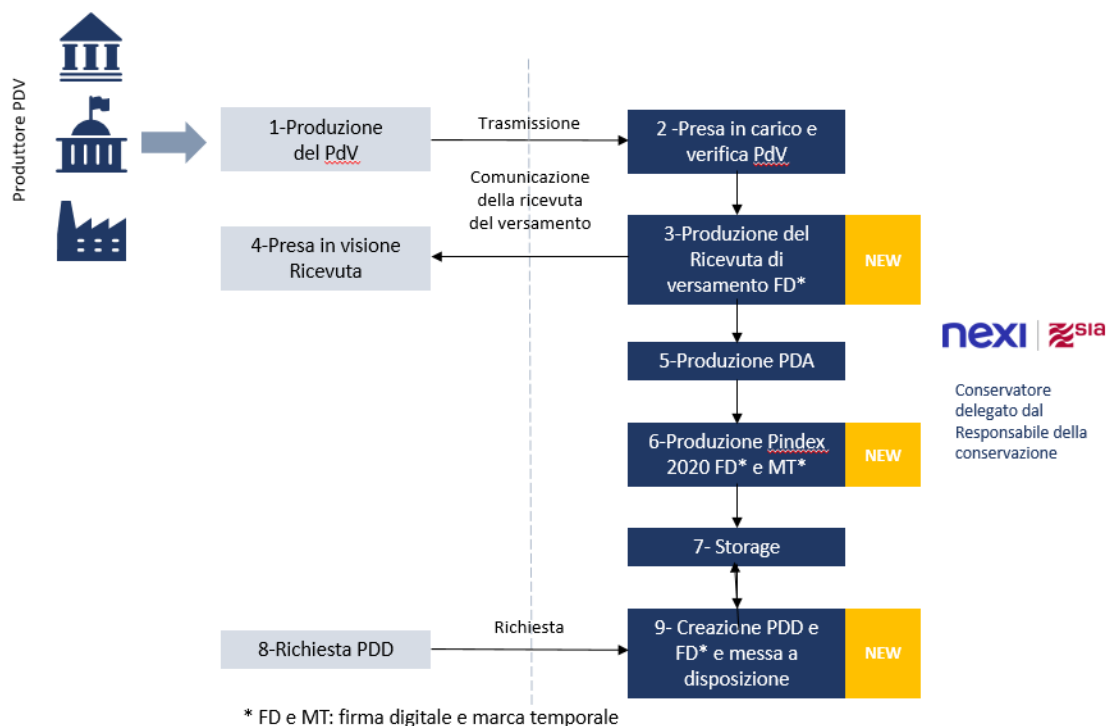


Figura 2 Processo conservazione

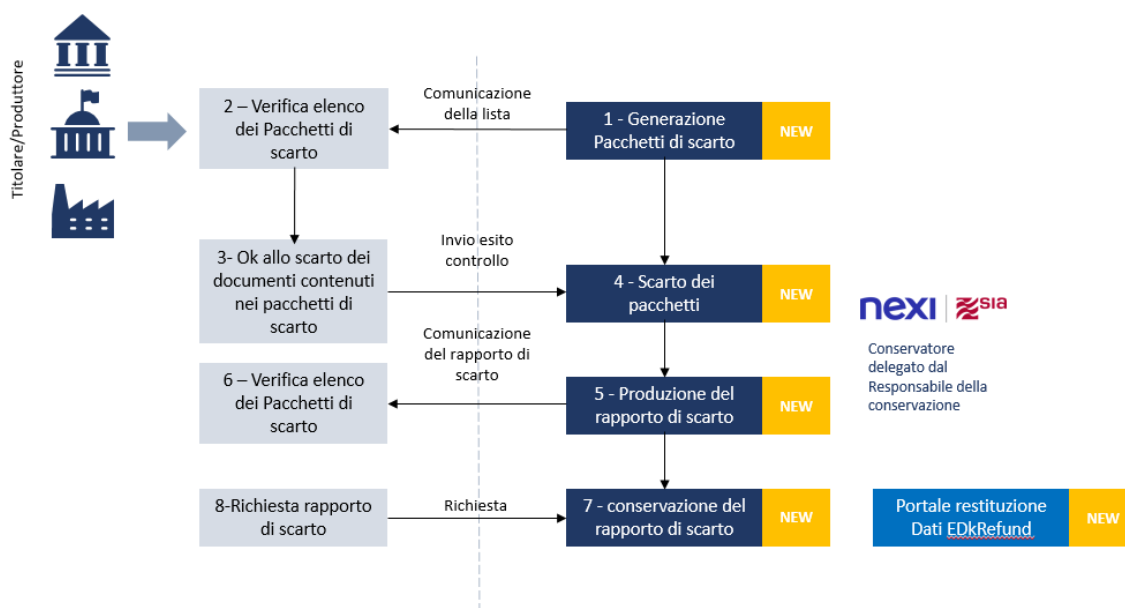


Figura 3 Processo di scarto

[Torna al sommario](#)

6.1 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti

6.1.1 Verifiche relative all'Ente soggetto Produttore

Ogni versamento da parte del Produttore deve contenere pacchetti omogenei per tipologia documentale ed Ente soggetto Produttore.

La verifica relativa all'identificazione dell'Ente soggetto Produttore è eseguita mediante il controllo delle credenziali di accesso dell'Utente (Postazione, Azienda, Utente), incrociando le stesse con le informazioni relative al codice tipologia documentale e al codice Azienda (identificativo Univoco del soggetto Titolare del dato) contenute all'interno del pacchetto di versamento e alla configurazione preventivamente eseguita in sede di avviamento del servizio. Se tali verifiche portassero a una incongruenza tra questi elementi, allora il pacchetto di versamento verrebbe rifiutato.

Nelle specifiche tecniche, documento allegato al contratto di affidamento del servizio di conservazione, vengono indicati quei soggetti abilitati dal produttore che possono accedere ai documenti richiesti dal produttore al conservatore. L'abilitazione e l'autenticazione degli Utenti abilitati avviene in base alle procedure di gestione utenze indicate nel piano della sicurezza del sistema di conservazione e nel rispetto delle misure di sicurezza vigenti.

In fase di censimento dell'Azienda sono richiesti i seguenti dati identificativi significativi:

- Ragione Sociale Cliente
- P. I.V.A.\Codice Fiscale

[Torna al sommario](#)

6.1.2 Verifiche in fase di versamento dei formati dei documenti

Il servizio prevede di gestire i formati previsti dalla normativa vigente.

All'atto del caricamento di un pacchetto di versamento viene controllato il formato di ciascun file versato. Su ogni singola tipologia documentale è possibile configurare la restrizione dei formati gestiti.

Se il formato del file non dovesse essere contemplato tra quelli previsti Allegato 2 LLGG sarà valutato insieme al Produttore la fattibilità e potrà essere gestito con apposito allegato "Specificità del contratto".

[Torna al sommario](#)

6.1.3 Verifiche in fase di versamento dei metadati minimi

Il sistema prevede che in fase di acquisizione del pacchetto di versamento venga verificata la presenza dei metadati obbligatori specifici della tipologia documentale.

[Torna al sommario](#)

6.1.4 Verifiche in fase di versamento della firma del documento

Nel caso in cui il pacchetto di versamento contenga documenti firmati digitalmente dal Produttore si prevede di verificare:

- l'integrità del documento;
- la validità del certificato;
- l'algoritmo di firma utilizzato;
- l'attendibilità della CA.

Per le verifiche della firma descritte se queste fossero negative, il pacchetto sarà rifiutato.

[Torna al sommario](#)

6.1.5 Verifiche in fase di versamento di documenti singoli

Sul singolo documento è verificata la presenza dei metadati obbligatori previsti per la tipologia documentale e la presenza o meno della firma digitale: se la firma è presente, si opera la verifica della firma.

6.1.6 Verifiche in fase di versamento dei gruppi di caricamento

Nel caso di caricamento massivo, per ogni gruppo di caricamento le operazioni di verifica svolte dal Servizio sono le seguenti:

- controllare la correttezza semantica della distinta, la conformità allo schema definito e la completezza dei documenti rispetto al numero di documenti indicato in distinta;
- verificare la firma dei documenti firmati digitalmente.

[Torna al sommario](#)

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

Nel caso in cui le verifiche di caricamento singolo o massivo siano andate a buon fine, il sistema provvede a memorizzare ed indicizzare i documenti e a produrre un Rapporto di versamento firmato digitalmente.

Il Rapporto di versamento è costituito da un identificativo univoco, dalla distinta di versamento e dal riferimento temporale del versamento e contiene le impronte (*hash*) di ciascun documento.

Il Rapporto di versamento resta a disposizione archiviato sul sistema, fino a che tutti i documenti presenti nel rapporto hanno concluso il processo di *ingest* (rif. OAIS). Il Rapporto di versamento è conservato e presente nel pacchetto di distribuzione.

La restituzione delle impronte permette la verifica da parte del Produttore della corrispondenza del documento preso in carico con quello inviato.

Il Rapporto di versamento costituisce il documento di controllo e di presa in carico da parte del Servizio verso il Produttore, in quanto viene garantita la conservazione di tutti e soli i documenti per i quali viene emesso il Rapporto di versamento.

In particolare, dal punto di vista organizzativo, laddove sia prevista un'integrazione applicativa tra il sistema documentale alimentante e il Servizio, la responsabilità di assicurarsi della corretta presa in carico di tutti i documenti da parte del Servizio è in carico al Produttore, attraverso il sistema documentale, che deve provvedere ad aggiornare sui propri archivi il buon esito del caricamento in conservazione e consentire di individuare eventuali incompletezze o anomalie nel processo di conservazione.

E' inoltre possibile, come descritto nel "Specifiche del contratto", attivare la generazione del rapporto di versamento secondo quanto previsto nelle LLGG.

[Torna al sommario](#)

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

Il rifiuto del pacchetto di versamento avviene quando il pacchetto risulta non conforme alle specifiche per:

- elenco file e distinta non coerenti;
- distinta o metadati del documento non corretti;
- oppure quando un documento contenuto nel pacchetto non supera una delle verifiche descritte nei paragrafi precedenti (verifica dell'Ente produttore, verifica del formato, verifica della firma, ecc..)

In caso di rifiuto, il Sistema restituisce al Produttore l'elenco degli errori riscontrati e le relative causali.

La modalità con cui si restituisce al Produttore il messaggio di rifiuto del pacchetto di versamento, dipende dalla modalità di caricamento dello stesso:

- In caso di caricamento del pacchetto di versamento mediante interfaccia Utente via browser, il messaggio di rifiuto contenente tutte le informazioni di cui sopra;
- in caso di caricamento mediante interfaccia applicativa con un sistema informativo alimentante, il messaggio di rifiuto viene trasmesso in risposta alla chiamata effettuate tramite interfacce applicative.

Il messaggio di rifiuto non viene sottoposto a conservazione digitale, ma tutte le informazioni di tracciatura dell'operazione sono registrate nei log di sistema, corredati dal riferimento temporale per ciascuna di esse.

Di seguito, si descrive la procedura in caso di pacchetti di versamento aventi certificato di firma digitale scaduto. Il sistema di default non accetta i documenti che hanno una firma con certificato scaduto al momento del caricamento; pertanto al verificarsi della condizione, il documento viene scartato.

Previo accordo con il Produttore è possibile però procedere all'accettazione del documento secondo due modalità distinte. Se è attiva la gestione dei documenti scaduti, il documento, invece di essere scartato, è caricato e posto in un uno stato particolare, definito "In attesa di seconda firma". L'operatività di accettazione "firma documenti scaduti" è abilitata solo su determinati profili che vengono rilasciati a chi, lato Produttore, è abilitato per tale compito, è possibile scegliere come il documento proseguirà il suo processo verso la conservazione. Le possibili scelte sono due:

- **apporre una seconda firma:** in questo caso la firma con certificato scaduto viene inglobata in una nuova busta con firma valida. Chi appone la seconda firma garantisce che la firma originaria era stata apposta quando il certificato era valido;
- **accettare che il documento sia conservato ugualmente:** in questo caso il documento prosegue nel suo percorso senza modifiche. Questo è possibile quando ci sono delle condizioni che consentono di validare la firma presente; è il caso ad esempio di un documento protocollato da una Pubblica Amministrazione, per cui la data del protocollo è riconosciuta valida al pari di una marcatura temporale.

Non è stato impostato un limite sul numero di tentativi di invio dei pacchetti di versamento.

[Torna al sommario](#)

6.3 Preparazione e gestione del pacchetto di archiviazione

Conclusa la fase della presa in carico del pacchetto di versamento viene generato il pacchetto di archiviazione.

Ogni pacchetto di archiviazione è univocamente identificato all'interno del sistema.

La cadenza con cui vengono creati i pacchetti di archiviazione è stabilita in sede contrattuale con il responsabile della conservazione. L'insieme di documenti appartenenti ad un pacchetto di archiviazione è sempre omogeneo per tipologia di documenti contenuti al suo interno.

I documenti vengono raggruppati automaticamente in base ai parametri definiti nel sistema, generando l'indice del pacchetto (PIndex), che contiene le impronte di tutti i documenti indicizzati e le altre informazioni definite nelle LLGG.

L'indice viene firmato digitalmente e marcato temporalmente dal Conservatore, ed è univocamente identificato all'interno del sistema.

Per quanto riguarda la descrizione delle procedure di ripristino in caso di corruzione o perdita dei dati si rimanda al paragrafo "Verifica dell'integrità degli archivi".

In generale il processo di conservazione standard non prevede l'utilizzo della crittografia degli oggetti conservati (la sua attivazione è possibile in relazione alle "Specificità del contratto"), in quanto:

- deve assicurare la conservazione a lungo termine del documento digitale e di conseguenza la piena disponibilità nei confronti non solo del Responsabile della conservazione, ma di tutta la comunità di riferimento (previa verifica dell'autorizzazione all'accesso ai documenti);
- non deve in alcun modo alterare il documento inviato in conservazione utilizzando tecniche crittografiche proprie.

[Torna al sommario](#)

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

I documenti sono ricercabili tramite opportune funzioni di ricerca messe a disposizione dall'applicazione di conservazione che permettono di valorizzare, quale criterio per la ricerca, ciascuno dei metadati caratteristici del documento.

L'accesso al sistema in modalità di consultazione è garantito agli Utenti abilitati opportunamente autorizzati, limitatamente agli archivi del Responsabile della conservazione di appartenenza e in base agli accordi contrattuali con esso intercorsi.

Gli Utenti abilitati all'accesso al Servizio verranno comunicati al soggetto Responsabile della conservazione, tramite modalità stabilite tra le parti nel contratto di Servizio.

Le credenziali (user e password da variare al primo accesso) verranno inviate ai diretti interessati.

È quindi disponibile al Conservatore e all'Utente la funzionalità di esportazione di pacchetti e relativi indici, attraverso la quale è possibile scaricare un file .zip contenente il file indice dei pacchetti, i documenti conservati e le evidenze della conservazione (firme e marche temporali). Inoltre sono disponibili le interfacce applicative per poter operare l'estrazione dei documenti tramite applicazione esterna (tale modalità sarà descritta nelle "Specificità del contratto").

Le segnalazioni di errore da parte dell'Utente, anche dovuti ad errori di trasmissione, sono gestite attraverso il sistema di Trouble Ticket Management (TTM) attivato nelle modalità come descritte nell'allegato "Specificità del contratto".

Nel caso di cessazione e/o recesso del contratto si può prevedere l'utilizzo, ad esempio, di supporti fisici rimovibili per la trasmissione dei pacchetti di distribuzione.

Si specifica che i supporti fisici sono prodotti con le seguenti caratteristiche concordate con il Produttore:

- non devono presentare riferimenti esterni che possano permettere l'identificazione dell'ente soggetto Produttore, dei dati contenuti, della loro tipologia, ecc.;
- modalità attivabile a richiesta: i dati trasmessi devono essere protetti con sistemi crittografici.

[Torna al sommario](#)

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

Il pubblico ufficiale, come descritto nell'allegato 3 "certificazione di processo", è coinvolto dal Responsabile del servizio della conservazione poiché "assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite". Il Servizio offre la possibilità, al soggetto Produttore, di generare i pacchetti di distribuzione che tramite l'intervento di un pubblico ufficiale posso essere validate come copie conformi per l'attestazione di conformità.

[Torna al sommario](#)

7.8 Scarto dei pacchetti di archiviazione

Così come stabilito dalle Linee Guida, il Sistema di Conservazione di Nexi consente lo scarto del Pacchetto di Archiviazione alla scadenza dei termini di conservazione previsti dalla norma, o dagli specifici accordi contrattuali, dandone preventiva informativa al Produttore.

Qualora oggetto della conservazione siano archivi pubblici o privati che rivestono interesse storico, lo scarto del pacchetto di archiviazione avviene solamente dopo l'autorizzazione del Ministero per i beni e le attività culturali secondo quanto previsto dalla normativa vigente.

Le procedure specifiche di scarto sono concordate con il soggetto Produttore e sono descritte nell'allegato "Specificità del contratto".

[Torna al sommario](#)

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

Il Servizio è in grado di accettare il versamento di pacchetti strutturati secondo lo standard UNI 11386:2020, in accordo con quanto definito nelle LLGG.

Allo stesso modo, il sistema è in grado di versare ad altri sistemi di conservazione pacchetti e indici secondo la medesima struttura, trasformando i pacchetti di archiviazione in opportuni pacchetti di distribuzione.

[Torna al sommario](#)

8. IL SISTEMA DI CONSERVAZIONE

Il Servizio è reso in modalità Software as a Service (SaaS) in conformità a quanto descritto nei documenti delle “Specificità del Contratto” e nel “Modello operativo del servizio”. Il documento “Specifiche tecniche del Servizio” descrive le specificità contrattuali in termini di:

- Tipologie di documenti trattati, dettagliando le definizioni, i parametri per la conservazione e il contesto specifico di ciascuna tipologia di documento;
- Livelli di servizio (SLA).

[Torna al sommario](#)

8.1 Componenti Logiche

Il Servizio si basa sulle seguenti tre macro componenti:

- la componente applicativa che rende disponibile l'insieme delle componenti funzionali a supporto del processo di conservazione;
- il supporto di memorizzazione, che rappresenta il sistema fisico su cui vengono conservati nel tempo i documenti sottoposti al processo di conservazione;
- il dispositivo HSM per la gestione della procedura di firma dei documenti.

Nello specifico, l'applicativo di conservazione interagisce con varie tipologie di attori esterni:

- Sistemi alimentanti/in consultazione in grado di:
 - o alimentare automaticamente il Servizio con documenti da sottoporre al processo di conservazione;
 - o consultare documenti preventivamente sottoposti a conservazione;
 - o *dispositivo HSM* per la firma dei documenti;
 - o *sistema di memorizzazione*, che rappresenta il sottosistema su cui vengono fisicamente memorizzati tutti i documenti sottoposti a processo di conservazione;
- *Responsabile del Servizio di conservazione*, per le attività di amministrazione, monitoraggio e altre funzioni di supporto
- *Utenti abilitati* che accedono al Servizio in forza di una credenziale di accesso e di un ruolo e quindi un profilo funzionale a cui sono associati, per effettuare:
 - o versamento di singoli documenti;
 - o consultazione di documenti conservati.
- Sistemi delle Certification/Time Stamp Authorities per:
 - o verifica dei certificati e delle CRL
 - o apposizione dei Time Stamp
- Time Server per l'apposizione del riferimento temporale

La schema (Figura 4) seguente evidenzia le componenti che costituiscono la soluzione.

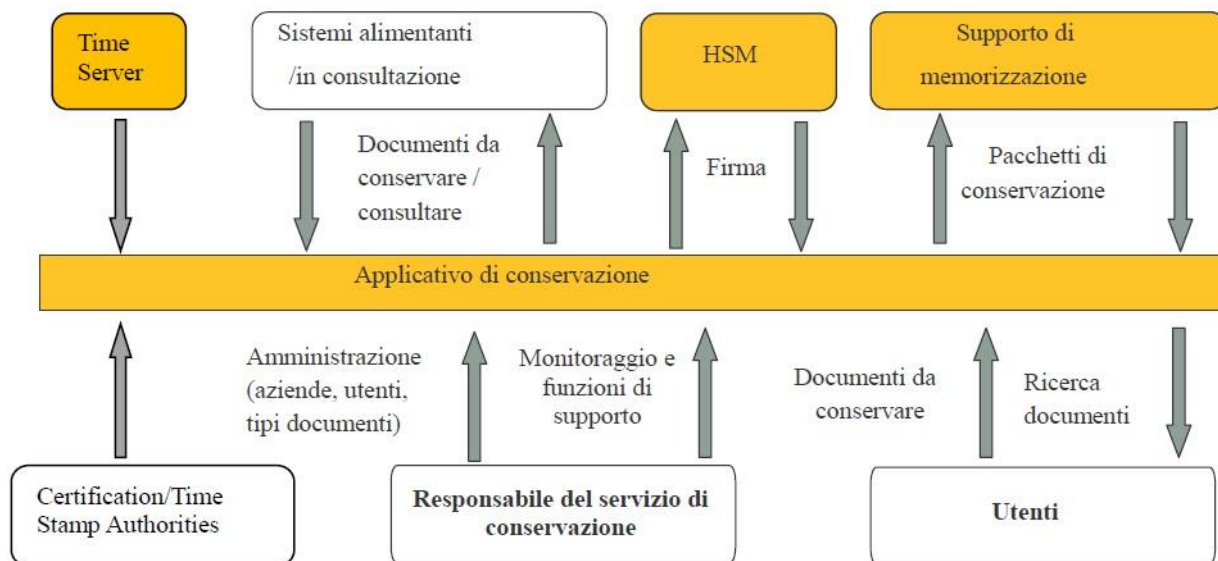


Figura 4 Componenti Logiche

L'applicazione viene erogata in logica SaaS dalle infrastrutture tecnologiche specificatamente predisposte.

Tutti i componenti del Sistema sono protetti da adeguate misure di sicurezza, descritte all'interno del Piano della sicurezza.

È mantenuta la separazione degli ambienti di sviluppo, di test e di produzione.

[Torna al sommario](#)

8.2 Componenti Fisiche

L'architettura del Sistema presenta una piattaforma con "no-single-point-of-failure" che è altamente scalabile ed implementa un servizio senza interruzioni, in quanto fondato sull'utilizzo di diversi nodi cooperanti e garantisce performance ottimali utilizzando meccanismi di load balancing tra i diversi nodi.

Inoltre la continuità del servizio è garantita dalla presenza di un sito secondario con logiche di disaster recovery.

Il Sistema presenta un'architettura a tre livelli:

1. livello di presentazione (IS-Web Server)
2. livello di logica applicativa (Application Server)
3. livello dati (Database, Storage)

Le componenti di **Web Server** e **Application Server** sono ospitate su due distinte istanze Linux virtuali all'interno dell'infrastruttura HP con prodotto di virtualizzazione che consente di gestire le istanze in alta affidabilità permettendone anche lo spostamento senza interruzione di servizio all'interno dell'infrastruttura HP.

La **componente dati** è realizzata su una istanza Linux virtuale all'interno dell'infrastruttura HP con prodotto di virtualizzazione RHEV. La gestione dei dati (database RDBMS e dati applicativi) su tutte le componenti previste per l'infrastruttura utilizza una "storage area network"- SAN- che ospita i dischi dove sono

memorizzati i dati del servizio con un sistema ridondato in fibra ottica e una SAN consolidata che permette una definizione di concetti di zoning, una connessione dei server di produzione in modalità dual path e un'alta affidabilità in condizioni di path failure. Il Sottosistema di Storage utilizzato è completamente in Fibre Channel e dual controller.

La **componente di gestione documentale**, per mezzo della quale vengono erogate tutte le funzionalità applicative inerenti la gestione dei documenti correlati ai processi di Business della piattaforma, è realizzata da un apposito strato applicativo che si appoggia a una SAN disponibile nell'infrastruttura e alla componente Storage per la memorizzazione dei documenti sottoposti a conservazione. Lo Storage viene integrato per mezzo di una specifica interfaccia che fa uso di API proprietarie del Sistema.

L'interconnessione adottata tra i sistemi applicativi e il sottosistema di Storage è realizzata attraverso la SAN con dispositivi di commutazione ottica e mezzo trasmissivo basato interamente su tratte in fibra ottica.

La **connettività** tra i dispositivi di switching ottici, lo Storage e i server è assicurata in alta affidabilità tramite doppio link .

Il **backup** è centralizzato su un'unica libreria di backup attraverso un numero opportuno di switch (dipendente dal numero di server connessi e dal numero di drives della libreria). L'infrastruttura utilizzata per effettuare i backup si appoggia su apparecchiature centralizzate e ridondate su entrambe le sedi e su un terzo sito distinto per l'archiviazione e la ritenzione storica.

[Torna al sommario](#)

8.3 Procedure di gestione e di evoluzione

Per quanto concerne la gestione operativa del servizio, nell'ambito del sistema di qualità aziendale sono definiti i processi di Realizzazione progetti di sviluppo sistemi applicativi (FR127) e il Modello Operativo del servizio, che hanno l'obiettivo di gestire tutto il ciclo del servizio, per garantire il raggiungimento degli concordati contrattualmente con i clienti. I processi di gestione coprono tutto il ciclo di vita del servizio e consentono di monitorarne e controllarne tutti gli aspetti.

Le procedure di gestione operativa del servizio e dei relativi sistemi a supporto, sono referenziati nelle Procedure Organizzative che descrivono:

- processi di incident e problem management;
- conduzione e manutenzione del Servizio;
- change & release management;
- Back-up e Disaster Recovery;
- verifica periodica di conformità a normativa e standard di riferimento.

In particolare il processo di *Incident Management* definisce tutti gli aspetti e le attività necessarie per la gestione di incidenti e/o anomalie (*incident*) rilevate dal personale interno o dai clienti nell'intero ciclo che va dalla segnalazione fino alla chiusura. Nel caso in cui la chiusura di un *incident* non risultasse definitiva ma avesse bisogno di ulteriori indagini, tramite l'apertura di un *problem* viene attivato il processo di *Problem Management*.

Il Servizio viene inoltre continuativamente monitorato e controllato al fine di verificare che sia conforme agli SLA definiti (*SLA Management*), ovvero che garantisca gli opportuni livelli di *capacity*, *continuity* ed *availability*.

Le verifiche periodiche di conformità a normativa e standard di riferimento sono effettuate in conformità al Piano della Sicurezza e al Sistema di gestione della Qualità di Nexi Payments.

Il Sistema di Gestione della sicurezza delle informazioni certificato ISO/IEC 27001 di Nexi prevede specifici controlli per la gestione e conservazione dei log, conformi ai requisiti della normativa sulla Privacy nonché ai requisiti specifici del Servizio dei documenti informatici.

Eventuali modifiche al sistema necessarie per la risoluzione di *incident* o *problem* o per rispondere a richieste di evoluzione da parte dei clienti o per rispondere a modifiche della normativa vigente, vengono gestite nell'ambito del sistema di qualità aziendale secondo quanto definito nel processo di *Change Management*, eventualmente accorpate in release e rilasciate in produzione secondo quanto descritto nel processo di *Release Management*.

Per garantire l'erogazione di servizi a valore aggiunto per i clienti Nexi, sono previsti, tra i *processi di business*:

- il *processo di fattibilità*, che viene attivato per analizzare le richieste del soggetto Produttore (del mercato di riferimento o interne), per tradurle in requisiti e proporre soluzioni di alto livello che implementino tali requisiti, per analizzare i rischi dell'iniziativa, per effettuare studi di natura tecnica ed economico/finanziaria e per fornire al processo di vendita le informazioni necessarie per la formalizzazione delle richieste dei clienti;
- il *processo di progettazione*, che ha lo scopo di effettuare l'analisi di dettaglio dei requisiti (funzionali e non funzionali) e il disegno delle soluzioni da implementare, e di realizzare quanto progettato in conformità con i requisiti iniziali, nel rispetto dei tempi e dei costi pianificati.

Nexi si impegna a trattare i dati del Cliente nel territorio dell'Unione Europea nonché dello SEE. Qualsiasi trasferimento verso Paesi al di fuori dall'Unione Europea nonché dallo SEE richiede il consenso esplicito, preventivo e in forma scritta del Titolare e può avvenire solo se le condizioni di cui agli Artt. 44 GDPR e seqq.

sono soddisfatte. Se Nexi è tenuta al trasferimento verso Paesi al di fuori dall'Unione Europea nonché dallo SEE in base a norme inderogabili di legge dell'Unione Europea o dello Stato Membro a cui è soggetti a Nexi, quest'ultima informerà il Titolare di tale obbligo legale prima che abbia inizio tale trasferimento, a meno che la legge non vieti a Nexi di fornire tale informazione al Titolare.

[Torna al sommario](#)

9. MONITORAGGIO E CONTROLLI

L'attività di monitoraggio applicativo sui pacchetti di archiviazione prevede il controllo su di un apposito cruscotto che evidenzia il numero di documenti in attesa di elaborazione. L'evidenza di una coda di documenti non ancora attribuiti a pacchetti di archiviazione innesca la verifica dell'operatore, che può analizzarli in dettaglio, arrivando ad evidenziare quali documenti, di quale tipologia e Produttore non sono stati correttamente processati. Verificato il problema, l'operatore può intervenire manualmente, sbloccando gli automatismi o ripristinandoli.

La stessa logica di intervento si applica per la firma e la marcatura temporale dei pacchetti di archiviazione.

9.1 Procedure di monitoraggio

Il monitoraggio dei servizi è interamente effettuato con agenti ITM e consente di controllare le principali risorse di sistema (CPU, Memoria, File System, Processi di Base, Traffico di Rete, Carichi Macchina) e applicative (File System Applicativi, Processi Applicativi, Log Oracle, Log Applicativi, URL).

[Torna al sommario](#)

9.2 Verifica dell'integrità degli archivi

Per quanto riguarda la verifica dell'integrità dei documenti, l'attività viene compiuta direttamente dalla componente infrastrutturale di gestione documentale (Storage), attraverso il meccanismo di mirroring e la continua verifica della disponibilità dei nodi e della integrità dei dati.

L'infrastruttura genera automaticamente una copia di sicurezza per ogni documento all'atto della conservazione, che risiede fisicamente su un nodo differente del supporto fisico primario; ambedue le copie sono costantemente monitorate attraverso meccanismi di verifica dell'impronta.

Ogni volta che il Sistema riscontra una non conformità in merito alla leggibilità o all'integrità di un documento memorizzato, traccia in opportuni file di log l'esito negativo della verifica di leggibilità e integrità.

E procede alla rigenerazione del documento a partire dalla copia ancora integra. Pertanto si ha una evidenza oggettiva di tutti gli interventi di rigenerazione eseguiti dal sistema.

Maggiori dettagli sulla gestione dell'integrità degli archivi sono riportati nel Piano della Sicurezza.

[Torna al sommario](#)

9.3 Soluzioni adottate in caso di anomalie

Le procedure interne che prevedono la messa in atto di soluzioni che vengono adottate a fronte di anomalie riscontrate a seguito del monitoraggio delle funzionalità del Servizio e delle verifiche sull'integrità degli archivi sono descritte nel documento "Modello Operativo del servizio". Accordi specifici sono concordati con il soggetto Produttore e descritti nell'allegato "Specificità del contratto".

Incident Management – Entry point info/incident

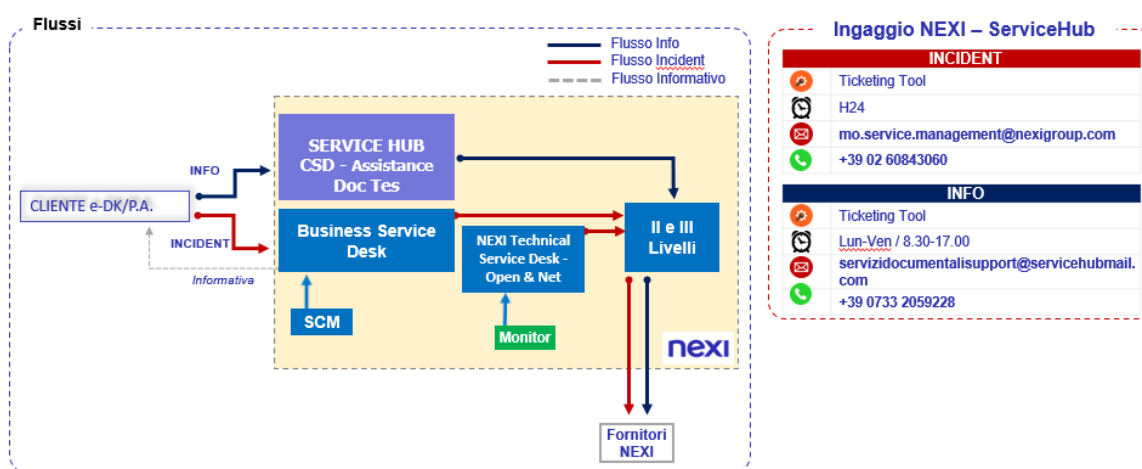


Figura 5 Processo Incident Management del servizio di conservazione

[Torna al sommario](#)

10. IMPIANTO CONTRATTUALE DEL SERVIZIO (SPECIFICITA' DEL CONTRATTO)

Lo schema contrattuale che regola l'erogazione del Servizio nei confronti del Titolare del dato che affida tale servizio in modalità outsourcing, si basa sulla documentazione contrattuale e tecnica elencata e d è resa disponibile all'atto del perfezionamento dell'accordo di servizio.

Lo schema contrattuale generale prevede i seguenti documenti (contratto diretto):

- Contratto di Servizio Conservazione Digitale (Condizioni Generali)
- Descrizione Servizio Conservazione
- Specifiche Tecniche Servizio Conservazione
- Nomina Responsabile Trattamento Dati Personali
- Nomina del Responsabile del Servizio di Conservazione
- Modulo di attivazione

[Torna al sommario](#)

INFORMAZIONI GENERALI

Versioni del documento

N°Ver/Rev/Bozza	Data emissione	Codice interno documento
1.0	24/02/2022	Prima emissione - 0000012567
2.0	16/05/2022	Seconda emissione - 0000012567
2.1	27/03/2023	Terza emissione - 0000012567
2.2	12/07/2023	Quarta emissione - 0000012567
2.3	15/11/2023	Quinta emissione - 0000012567
2.4	18/10/2024	Sesta emissione - 0000012567

Riferimenti procedure interne

- [1] FR127 Realizzazione progetti di sviluppo sistemi applicativi
- [2] FR160 Change Management
- [3] POG 025 Gestione degli incidenti ICT
- [4] POG 046 Gestione incidenti di sicurezza informatica e violazioni di dati personali – Data Breach
- [5] POG 045 Cancellazione dei dati (Data retention)
- [6] POG 039 Gestione accessi utente
- [7] PP 08 Information Security Policy
- [8] Gestione Metadati Allegato 5_e-DK
- [9] Manuale Utente – E-dk Servizio di conservazione digitale
- [10] Manuale Amministratore – E-dk Servizio di conservazione digitale
- [11] PP-040 operational risk management (orm) policy
- [12] PP -040 all. 1 framework rischi ict e di sicurezza modello di analisi e valutazione
- [13] POG-046 v.07_ita gestione incidenti di sicurezza e data breach
- [14] bcp nexi p business continuity plan nexi payments
- [15] Gestione del backup v6.0

La visione delle procedure a rilevanza interna è possibile richiederla con richiesta audit alla funzione

INDICE DELLE FIGURE

Figura 1 Struttura dati del pacchetto di archiviazione secondo standard UNI 11386:2020 Standard SInCRO	30
Figura 2 Processo conservazione	32
Figura 3 Processo di scarto	32
Figura 4 Componenti Logiche	40
Figura 5 Processo Incident Management del servizio di conservazione	44