ENTAKSISOLUTIONS

SISTEMA DI GESTIONE CERTIFICATO
ISO 9001 | ISO 20000-1 | ISO 22301
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
SERVIZIO DI CONSERVAZIONE CERTIFICATO
ETSI 319 401 | ETSI 119 511
PER LA CONSERVAZIONE A LUNGO TERMINE

Manuale

MAN eCON 20151222 Manuale della conservazione

Entaksi Solutions SpA

Indice

Informazioni sul documento

Progetto	Sistema Integrato di Gestione
Tipo	Manuale
Nome documento	MAN eCON 20151222 Manuale della conservazione
Versione	1.9.0
Data creazione	22/12/2015
Ultima revisione	11/02/2022
Autore	Alessandro Geri
Stato	Rilasciato
Classificazione	Confidenziale

Riproduzioni cartacee di questo documento sono da considerarsi copie di lavoro non censite dal SIG.

Revisioni e relative distribuzioni

Data	Versione	Nome	Mansione	Azione	Distribuzione
22/12/2015	0.1	Alessandro Geri	ReCON	Creazione bozza	Interno
28/01/2016	1.0	Alessandro Geri	ReCON	Rilascio	AgID
29/02/2016	1.1	Alessia Soccio	RARC	Adeguamento alle richieste AgID inviate in data 29/02/2016.	AgID
02/03/2016	1.2	Alessandro Geri	ReCON	Modifiche cap. 4 per ulteriori richieste AgID inviate il 02/03/2016.	AgID
01/09/2017	1.3.0	Alessia Soccio	RARC	Conversione del documento nel nuovo formato. Nuovo template. Aggiornamento al nuovo sistema di versionamento. Modifica nomenclatura norma 9001:2015. Modifica formato date in ruolo responsabili. Modifica capitolo "Cessazione del servizio di conservazione".	AgID
23/11/2018	1.4.0	Alessia Soccio	RARC	Modifiche in assegnazione ruoli e responsabilità, e nella struttura fisica del sistema.	AgID

Data	Versione	Nome	Mansione	Azione	Distribuzione
30/10/2019	1.5.0	Alessia Soccio	RARC	Aggiunte deleghe di firma PDV, PDA e PDD. Aggiornamento capitolo "Normativa e standard di riferimento". Aggiornamento paragrafo "Cessazione del servizio di conservazione".	AgID
27/11/2020	1.6.0	Alessia Soccio	RARC	Aggiornamento capitoli 6-9 per evoluzione del sistema. Aggiunta delega per Vice Responsabile del Servizio di Conservazione. Aggiornata terminologia e normativa.	AgID
01/12/2021	1.7.0	Alessia Soccio	RARC	Revisione generale del documento e adeguamento a "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici" e "Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici".	AgID
31/01/2022	1.8.0	Alessia Soccio	RARC	Correzioni formali e adeguamento a norme ETSI EN 319 401 V2.3.1 (2021-05) e ETSI TS 119 511 v1.1.1 (2019-06) per Long-Term Preservation.	AgID
11/02/2022	1.9.0	Alessia Soccio	RARC	Aggiornamento della descrizione della struttura fisica del sistema di conservazione.	AgID

Approvazione del documento

Data	Addetto	Mansione	Firma
11/02/2022	Alessandro Geri	Responsabile del Servizio di Conservazione	*Firmato digitalmente*

ENTAKSISOLUTIONS
Entaksi Solutions Spa
Sistema di gestione certificato
ISO 9001 | ISO 20000-1 | ISO 22301
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
Servizio di Conservazione certificato
ETSI 319-401 | ETSI 119-511
per la conservazione a lungo termine
Alessandro Geri
amministratore unico

Firmato digitalmente da Geri Alessandro
Data: 2022.02.11 15:01:05 +01'00'

1. Scopo e ambito del documento

Il presente manuale descrive il sistema di conservazione digitale di **Entaksi Solutions SpA**, denominata di seguito **Entaksi**. L'azienda ha sede legale in via la Piana 76, fraz. Pontepetri, 51028 San Marcello Piteglio (PT) (sito web: http://www.entaksi.eu).
Il manuale ha lo scopo di illustrare il Servizio di Conservazione **eCON** fornito da Entaksi, ed in particolare:

- il modello organizzativo, le competenze, i ruoli e le responsabilità degli attori coinvolti nel processo di gestione e archiviazione documentaria;
- come è stato sviluppato il processo di conservazione, la struttura e gli aspetti operativi del dispositivo contenente la documentazione digitale;
- le procedure di conservazione e di verifica dei documenti e la gestione delle copie di sicurezza;
- l'infrastruttura tecnologica;
- le misure di sicurezza.

Il documento recepisce le norme e gli standard indicati nel capitolo Normativa di riferimento, in particolare le "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici" e il "Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici", pubblicati dall'Agenzia per l'Italia Digitale e la normativa eIDAS.

Il servizio di conservazione eCON è un servizio fiduciario che fornisce la conservazione a lungo termine di firme digitali e dati in generale utilizzando tecniche di firma digitale, come definito dal Regolamento (UE) eIDAS n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 relativo a servizi di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.

Il documento rappresenta il principale riferimento per la descrizione e regolamentazione di ogni aspetto del Servizio, compresa la gestione della comunicazione fra Entaksi e il Cliente.

Entaksi si riserva di apportare al documento le modifiche e gli aggiornamenti che si renderanno necessari per l'adeguamento del Servizio alle evoluzioni normative ed organizzative, riportandone gli estremi nel cartiglio iniziale.

Il Servizio di Conservazione fornisce al Cliente le seguenti funzioni:

- **Conservazione a lungo termine dei documenti**: memorizzazione dei documenti informatici inviati dal Cliente su un supporto di cui sia garantita l'integrità e la leggibilità nel tempo, secondo le prescrizioni stabilite dalla normativa vigente in materia, con le modalità, nei tempi e limiti definiti contrattualmente. Il servizio comprende la verifica periodica dell'integrità dei documenti, l'eventuale riversamento diretto e le attività necessarie per le ottemperanze fiscali, ove richiesto.
- **Consultazione dei documenti conservati**: ricerca e visualizzazione dei documenti inviati al sistema di conservazione. Tale servizio ed il relativo software di visualizzazione è garantito per il tempo definito contrattualmente per la conservazione dei documenti.
- **Accesso ai documenti conservati**: il servizio consiste nella possibilità per il Cliente di richiedere, e in seguito di scaricare, dei Pacchetti di Distribuzione.

Entaksi eroga il Servizio di Conservazione utilizzando infrastrutture tecnologiche che soddisfano i requisiti di alta affidabilità richiesti dalla normativa.

Entaksi, nell'ambito dello sviluppo e del mantenimento del proprio Sistema Integrato di Gestione (SIG), ha ottenuto le seguenti certificazioni:

UNI ISO 9001:2015

Sistemi di Gestione per la Qualità – Requisiti.

ISO/IEC 20000-1:2018

Tecnologie informatiche – Erogazione di servizi informatici.

ISO/IEC 27001:2013

Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti.

ISO/IEC 27017:2015

Tecnologia delle informazioni - Tecniche di sicurezza - Codice di condotta per i controlli di sicurezza delle informazioni basato su ISO / IEC 27002 per i servizi cloud.

ISO/IEC 27018:2019

Tecnologia delle informazioni - Tecniche di sicurezza - Codice di condotta per la protezione delle informazioni di identificazione personale (PII) nei cloud pubblici che fungono da processori PII.

ISO/IEC 27035:2016

Tecnologia delle informazioni - Tecniche di sicurezza - Gestione degli incidenti di sicurezza delle informazioni.

ISO/IEC 22301:2019

Tecnologia delle informazioni - Sicurezza e resilienza - Sistemi di gestione della continuità operativa aziendale.

Sistema di conservazione dei documenti digitali

Tecnologia delle informazioni - Conservazione digitale - art. 24 Regolamento UE n° 910/2014 sull'identità digitale.

eIDAS

Regolamento (UE) n. 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.

ETSI EN 319 401 V2.3.1 (2021-05)

Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers, policy e requisiti per i fornitori di servizi fiduciari.

ETSI TS 119 511 v1.1.1 (2019-06)

Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques, policy e requisiti di sicurezza per servizi fiduciari di conservazione di firme digitali e la conservazione di dati mediante tecniche basate sulla firma digitale.

Nell'audit periodico per il rinnovo delle certificazioni è inserita una puntuale attività di verifica del Sistema di Conservazione, basata su una specifica check-list stilata dal certificatore secondo i requisiti AgID.

Il rapporto tra Entaksi e il Cliente viene concordato tramite un dispositivo contrattuale composto dai seguenti documenti:

- il presente **Manuale**, che descrive il funzionamento operativo del Servizio di Conservazione;
- le **Condizioni Generali del Servizio**, che riportano i termini contrattuali di fruizione del Servizio, ed in allegato eventuali richieste aggiuntive rispetto allo standard descritto nel manuale (es.: diversi set di metadati per i documenti, diversi termini di disdetta dal servizio, etc.);
- l'**Informativa in materia di protezione dei dati personali**, per l'autorizzazione al trattamento dei dati personali, ai sensi del Regolamento dell'Unione Europea n° 2016/679 sulla protezione dei dati;
- la **Nomina a Responsabile Esterno per il trattamento dei dati**;
- i documenti **eIDAS** che descrivono i processi di conservazione a lungo termine certificati secondo gli standard ETSI EN 319 401 V2.3.1 (2021-05), ETSI TS 119 511 v1.1.1 (2019-06) e ETSI TS 119 512 V1.1.2 (2020-10).

Il Servizio è erogato da un Cloud Privato, costituito da macchine che operano in configurazione ad alta affidabilità, posizionate, ai sensi della norma 244/2007, entro i confini dell'Unione Europea.
Per l'erogazione del servizio nei termini definiti dai requisiti espressi dall'Agenzia per l'Italia Digitale per la fornitura di servizi di conservazione alla Pubblica Amministrazione, un'istanza del servizio è disponibile con macchine operanti in configurazione ad alta affidabilità posizionate entro i confini della Repubblica Italiana.

Il presente manuale del Servizio di Conservazione rientra nel Sistema Integrato di Gestione (SIG) di Entaksi, e ne segue l'impostazione definita dall'azienda per la gestione dei propri documenti interni. Parti di questo manuale, in particolare aspetti che riguardano le definizioni, la struttura interna, il funzionigramma e l'organigramma generali dell'azienda, la politica sulla sicurezza, oltre a tutte le specifiche tecniche, sono riprese da documenti interni classificati come "confidenziali", e che dunque non vengono resi pubblici nella loro interezza, ma rimangono disponibili all'Agenzia per l'Italia Digitale per effettuare controlli sull'affidabilità del sistema.

Torna all'indice.

2. Terminologia

Viene di seguito riportata, a scopo di esempio, la terminologia utilizzata nel manuale, suddivisa tra il glossario dei termini tecnici e gli acronimi.

2.1. Glossario

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.

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.

Classificazione

Attività di organizzazione di tutti i documenti secondo uno schema costituito da un insieme di voci articolate in modo gerarchico e che individuano, in astratto, le funzioni, competenze, attività e/o materie del soggetto produttore.

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 filesystem o pacchetto.

Coordinatore della Gestione Documentale

Soggetto responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 nei casi di amministrazioni che abbiano istituito più AOO.

Destinatario

Soggetto o sistema al quale il documento informatico è indirizzato.

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: "il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario".

eSeal

Vedi sigillo elettronico.

Esibizione

Operazione che consente di visualizzare un documento conservato.

eSignature

Vedi firma elettronica.

Estratto di documento informatico

Parte del documento tratto dal documento originale.

Estratto per riassunto di documento informatico

Documento nel quale si attestano in maniera sintetica fatti, stati o qualità desunti da documenti informatici.

Estrazione statica dei dati

Estrazione di informazioni utili da grandi quantità di dati (es. database, datawarehouse ecc...), attraverso metodi automatici o semi-automatici.

Evidenza informatica

Sequenza finita di bit che può essere elaborata da una procedura informatica.

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 discrittura, nella memoria di un computer.

File container

Vedi Formato contenitore.

File wrapper

Vedi Formato contenitore.

File-manifesto

File che contiene metadati riferiti ad un file o ad un pacchetto di file.

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: "dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare".

Firma elettronica avanzata

Vedi articoli 3 e 26 del Regolamento eIDAS: "Una firma elettronica avanzata soddisfa i seguenti requisiti: a) è connessa unicamente al firmatario; b) è idonea a identificare il firmatario; c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; e d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati."

Firma elettronica qualificata

Vedi articolo 3 del Regolamento eIDAS: "una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche".

Flusso (binario)

Sequenza di bit prodotta in un intervallo temporale finito e continuativo che ha un'origine precisa ma di cui potrebbe non essere predeterminato il suo istante di interruzione.

Formato contenitore

Formato di file progettato per consentire l'inclusione ("imbustamento" o wrapping), in uno stesso file, di una o più evidenze informatiche soggette a differenti tipi di codifica e al quale possono essere associati specifici metadati.

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.

Funzioni aggiuntive del protocollo informatico

Nel sistema di protocollo informatico, componenti supplementari rispetto a quelle minime, necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni.

Funzioni minime del protocollo informatico

Componenti del sistema di protocollo informatico che rispettano i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445.

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).

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 peril corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

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 filesystem) 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.

Path

Vedi Percorso.

Pathname

Concatenazione ordinata del percorso di un file e del suo nome.

Percorso

Informazioni relative alla localizzazione virtuale del file all'interno del filesystem 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 di organizzazione delle aggregazioni documentali

Strumento integrato con il sistema di classificazione a partire dai livelli gerarchici inferiori di quest'ultimo e finalizzato a individuare le tipologie di aggregazioni documentali (tipologie di serie e tipologie di fascicoli) che devono essere prodotte e gestite in rapporto ai procedimenti e attività in cui si declinano le funzioni svolte dall'ente.

Piano generale della sicurezza

Documento che pianifica le attività volte alla realizzazione del sistema di protezione e ditutte 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.

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.

Registro di protocollo

Registro informatico ove sono memorizzate le informazioni prescritte dalla normativa per tutti i documenti ricevuti e spediti da un ente e per tutti i documenti informatici dell'ente stesso.

Registro particolare

Registro informatico individuato da una pubblica amministrazione per la memorizzazione delle informazioni relative a documenti soggetti a registrazione particolare.

Regolamento eIDAS

electronic IDentification Authentication and Signature, Regolamento (UE) Nº 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari perle transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.

Repertorio

Registro su cui vengono annotati con un numero progressivo i fascicoli secondo l'ordine cronologico in cui si costituiscono all'interno delle suddivisioni del piano di classificazione.

Responsabile dei sistemi informativi per la conservazione

Soggetto che coordina i sistemi informativi all'interno del conservatore.

Responsabile del servizio di conservazione

Soggetto che coordina il processo di conservazione all'interno del conservatore, in conformità ai requisiti definiti da AgID nel "Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici".

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, in conformità ai requisiti definiti da AgID nelle "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici".

Responsabile della funzione archivistica di conservazione

Soggetto che coordina il processo di conservazione dal punto di vista archivistico all'interno del conservatore, in conformità ai requisiti definiti da AgID nel "Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici".

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.

Responsabile dello sviluppo e della manutenzione del sistema di conservazione

Soggetto che assicura lo sviluppo e la manutenzione del sistema all'interno del conservatore.

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.

Serie

Raggruppamento di documenti con caratteristiche omogenee (vedi anche aggregazione documentale informatica).

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.

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.

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.

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.

Torna all'indice.

2.2. Acronimi

AgID

Agenzia per l'Italia Digitale.

AOO

Area Organizzativa Omogenea.

CA

Certification Authority.

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

Firma Elettronica Avanzata.

FEQ

Firma Elettronica Qualificata.

PDA (AiP)

Pacchetto di Archiviazione.

PDD (DiP)

Pacchetto di Distribuzione.

PDV (SiP)

Pacchetto di Versamento.

TUDA

Testo Unico della Documentazione Amministrativa, Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni e integrazioni.

UOR

Unità Organizzativa Responsabile

Torna all'indice.

3. Normativa e standard di riferimento

Per garantire la gestione a norma del Servizio di Conservazione eCON, Entaksi definisce i criteri e i processi del Servizio in base alla normativa italiana ed europea in materia, oltre ad implementare standard internazionali che definiscono la gestione teorica, operativa e funzionale del sistema. Vengono qui di seguito riportati le norme e gli standard di riferimento per l'azienda.

Torna all'indice.

3.1. Normativa di riferimento

Codice Civile, R. D. 16 marzo 1942 n. 262

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 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, comma3, lettera b), 35, comma 2, 36, comma 2, e 71.

Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio

Regolamento UE del 23 luglio 2014 (eIDAS), in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.

Linee Guida sulla formazione, gestione e conservazione dei documenti informatici

Linee guida ufficiali sulla creazione, gestione e conservazione dei documenti informatici, pubblicate da AgID in data 11/09/2020 alle quali vengono aggiunte le modifiche con la relativa proroga contenute nella Determinazione 371/2021 del 17/05/2021.

Determinazione AgID 25 giugno 2021 n.455

Concernente l'adozione del "Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici".

Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici

Regolamento AgID sui criteri per la fornitura dei servizi di conservazione dei documenti informatici

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio

Regolamento UE del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

Decreto Legislativo 10 agosto 2018, n. 101

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

Torna all'indice.

3.2. Standard di riferimento

UNI ISO 9001:2015

Sistemi di Gestione per la Qualità – Requisiti.

ISO/IEC 20000-1:2018

Tecnologie informatiche – Erogazione di servizi informatici.

ISO/IEC 27001:2013

Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti.

ISO/IEC 27017:2015

Tecnologia delle informazioni - Tecniche di sicurezza - Codice di condotta per i controlli di sicurezza delle informazioni basato su ISO / IEC 27002 per i servizi cloud.

ISO/IEC 27018:2019

Tecnologia delle informazioni - Tecniche di sicurezza - Codice di condotta per la protezione delle informazioni di identificazione personale (PII) nei cloud pubblici che fungono da processori PII.

ISO/IEC 27035:2016

Tecnologia delle informazioni - Tecniche di sicurezza - Gestione degli incidenti di sicurezza delle informazioni.

ISO/IEC 22301:2019

Tecnologia delle informazioni - Sicurezza e resilienza - Sistemi di gestione della continuità operativa aziendale.

Sistema di conservazione dei documenti digitali

Tecnologia delle informazioni - Conservazione digitale - art. 24 Regolamento UE n° 910/2014 sull'identità digitale.

eIDAS

Regolamento (UE) n. 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.

ETSI EN 319 401 V2.3.1 (2021-05)

Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers, policy e requisiti per i fornitori di servizi fiduciari.

ETSI TS 119 511 v1.1.1 (2019-06)

Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques, policy e requisiti di sicurezza per servizi fiduciari di conservazione di firme digitali e la conservazione di dati mediante tecniche basate sulla firma digitale.

ETSI TS 119 512 V1.1.2 (2020-10)

Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services, protocolli per fornitori di servizi fiduciari che forniscono servizi di conservazione dei dati a lungo termine.

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.

ETSI EN 319 102-1 V1.1.1 (2016-5)

Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation

UNI 11386:2020

Standard SinCRO, Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.

ISO/IEC 14721:2012

(Open Archival Information System), un modello di sistema informativo aperto per la gestione e l'archiviazione a lungo termine di contenuti informativi.

UNI ISO 15489-1:2006

Informazione e documentazione – Gestione dei documenti di archivio – Principi generali sul record management.

UNI ISO 15489-2:2007

Informazione e documentazione – Gestione dei documenti di archivio – Linee Guida sul record management.

ISO 15836:2009

Information and documentation – The Dublin Core metadata element set, la norma che contiene il sistema di metadati del Dublin Core per la descrizione dei documenti informatici.

ISO 16363:2012

Space data and information transfer systems — Audit and certification of trustworthy digital repositories.

ISO/TR 18492:2005

Long-term preservation of electronic document-based information.

ISAD(G)

General International Standard Archival Description, standard per la descrizione di archivi destinati alla registrazione di documenti prodotti da organizzazioni, persone e famiglie.

UNI EN ISO 9000:2015

Sistema di Gestione per la Qualità - Fondamenti e vocabolario.

ISO/IEC 9594-8:2014

Information technology – Open Systems Interconnection – The Directory – Part 8: Public-key and attribute certificate frameworks.

ISO/IEC 27002:2013

Tecniche di sicurezza SGSI – codice di prassi.

ISO/IEC 27013:2012

Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1.

UNI EN ISO 19011:2018

Linea Guida per gli audit di Sistemi di Gestione per la qualità e/o di Gestione ambientale.

ETSI TS 119 312 V1.4.1 (2021-08)

Electronic Signatures and Infrastructures (ESI) - Cryptographic Suites.

IETF RFC 822 (1982)

Standard for the format of ARPA internet text messages.

IETF RFC 2083 (1997)

PNG (Portable Network Graphics) Specification.

IETF RFC 2141 (1997)

URN Syntax.

IETF RFC 2306 (1998)

Tag Image File Format (TIFF) - F Profile for Facsimile.

IETF RFC 2527 (1999)

Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

IETF RFC 3161 (2001)

Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP).

IETF RFC 3949 (2005)

File Format for Internet Fax.

IETF RFC 5280 (2008)

Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

IETF RFC 5322 (2008)

Internet Message Format.

IETF RFC 6749 (2012)

The OAuth2 Authorization Framework.

Torna all'indice.

4. Ruoli e responsabilità

Viene in questo capitolo definita la comunità di riferimento del Sistema di Conservazione, così come caratterizzata nello Standard ISO/IEC 14721:2012 OAIS (Open Archival Information System). Questo standard definisce un modello di sistema informativo aperto per la gestione e l'archiviazione a lungo termine di contenuti informativi, ed è applicabile ad ogni tipo di archivio. Vengono inoltre definiti i ruoli e le attività di ogni responsabile all'interno del servizio.

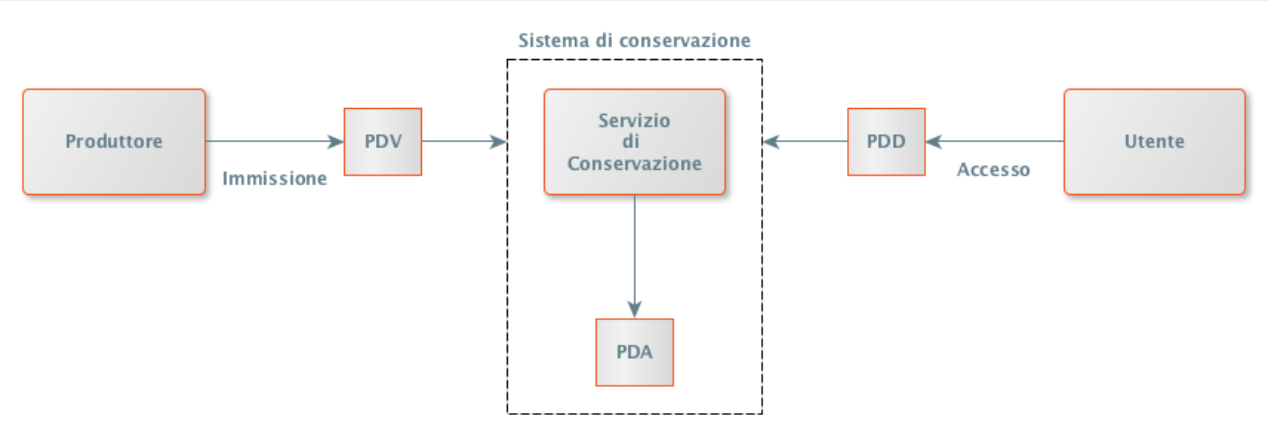

Figura 1. Ruoli e responsabilità.

Il Servizio di Conservazione erogato da Entaksi prevede i ruoli definiti in seguito, in conformità alle "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici" e al "Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici".

La normativa definisce "**Produttore**" la persona fisica o giuridica responsabile della creazione del Pacchetto di Versamento (PDV) e del suo invio verso il sistema di conservazione. Verifica l'esito della presa in carico da parte del Servizio di Conservazione tramite il controllo del Rapporto di Versamento (RDV).

La normativa definisce "**Responsabile della conservazione**" la persona fisica che definisce e attua le politiche necessarie alla conservazione documentaria, ed è responsabile della gestione dei documenti. Il Responsabile della Conservazione affida ad Entaksi il servizio di conservazione digitale a norma dei documenti informatici, così come definito nel contratto. Nelle pubbliche amministrazioni, il ruolo del responsabile della conservazione è svolto da un dirigente o da un funzionario formalmente designato.

Secondo quanto specificato nelle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, "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".

Si definisce come "**Utente**" la persona, ente o sistema in grado di richiedere al Sistema di Conservazione, nei limiti indicati nelle Condizioni Generali del Servizio e consentiti dalla legge, l'esibizione del Pacchetto di Distribuzione (PDD), ovvero di fruire delle informazioni di interesse.

Il Servizio di Conservazione di Entaksi è formato da vari "**Responsabili**", ognuno dei quali ricopre nell'azienda e in particolare nel servizio un ruolo ben preciso, al fine di garantire al meglio l'affidabilità del sistema, senza sovrapposizioni di attività e con compartimentazione dei ruoli.

Ai fini della gestione operativa, è stata costituita una specifica Struttura Organizzativa per il Servizio di Conservazione (descritta in dettaglio nel capitolo Struttura organizzativa per il Sistema di Conservazione), suddivisa in aree operative, che prevede per ciascuno dei Responsabili l'assunzione degli incarichi e delle responsabilità descritti nella seguente tabella.

Sebbene in conseguenza del passaggio al nuovo Regolamento le sole figure del Responsabile del Servizio di Conservazione e del Responsabile della Funzione Archivistica rimangano obbligatorie per AgID, Entaksi ha deciso di mantenere i ruoli definiti per il precedente istituto dell'Accreditamento, in ragione dell'efficacia nel tempo di tale impostazione.

Tabella 1. Responsabili.

Ruolo e nominativo	Attività associate al ruolo
Responsabile del Servizio di Conservazione - Alessandro Geri	Definizione e attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione; Definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente. Corretta erogazione del servizio di conservazione all'ente produttore. Gestione delle convenzioni, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.
Responsabile della Funzione Archivistica di Conservazione - Alessia Soccio	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. Definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici. Monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione. Collaborazione con 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.
Responsabile del Trattamento dei Dati Personali - Alessandro Geri	Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali. Garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.
Responsabile della Sicurezza dei Sistemi per la Conservazione - Alessandro Geri	Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza. Segnalazione delle eventuali difformità al Responsabile del Servizio di Conservazione e individuazione e pianificazione delle necessarie azioni correttive.

Ruolo e nominativo	Attività associate al ruolo
Responsabile dei Sistemi Informativi per la Conservazione - Stefano Travelli	Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione. Monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore. Segnalazione delle eventuali difformità degli SLA al Responsabile del Servizio di Conservazione e individuazione e pianificazione delle necessarie azioni correttive. Pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione. Controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del Servizio di Conservazione.
Responsabile dello Sviluppo e della Manutenzione del Sistema di Conservazione - Luigi Ruocco	Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione. Pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione. Monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione. Interfaccia con l'ente produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche. Gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.

Il Responsabile del Servizio di Conservazione ha delegato per la firma elettronica dei PDV, PDA e PDD:

- Responsabile della Funzione Archivistica, Alessia Soccio;
- Responsabile dei Sistemi Informativi, Stefano Travelli;
- Responsabile dello Sviluppo e della Manutenzione, Luigi Ruocco.

Alessia Soccio assume il ruolo di Vice Responsabile del Servizio di Conservazione, svolgendone le sue funzioni in sua assenza o sotto sua delega.

I ruoli sono così assegnati nel tempo:

Tabella 2. Periodo in ruolo dei responsabili.

Ruolo	Nominativo	Periodo nel ruolo
Responsabile del Servizio di Conservazione	Alessandro Geri	07/01/2013 – oggi
Responsabile della Funzione Archivistica di Conservazione	Stefano Travelli	07/01/2013 – 22/07/2015
	Alessia Soccio	23/07/2015 – oggi
Responsabile del Trattamento dei Dati Personali	Alessandro Geri	07/01/2013 – oggi
Responsabile della Sicurezza dei Sistemi per la Conservazione	Alessandro Geri	07/01/2013 – oggi

Ruolo	Nominativo	Periodo nel ruolo
Responsabile dei Sistemi Informativi per la Conservazione	Paola Caioli	07/01/2013 – 12/11/2018
	Stefano Travelli	13/11/2018 – oggi
Responsabile dello Sviluppo e della Manutenzione del Sistema di Conservazione	Stefano Travelli	07/01/2013 – 12/11/2018
	Luigi Ruocco	13/11/2018 - oggi

5. Struttura organizzativa per il Sistema di Conservazione

A supporto del processo di Conservazione sono state definite specifiche figure interne all'organizzazione di Entaksi in grado di garantire la corretta erogazione e adeguati supporti nei confronti del Produttore e dell'Utente.

Torna all'indice.

5.1. Organigramma

Queste strutture sono coordinate dal Responsabile del Servizio di Conservazione, secondo il seguente organigramma:

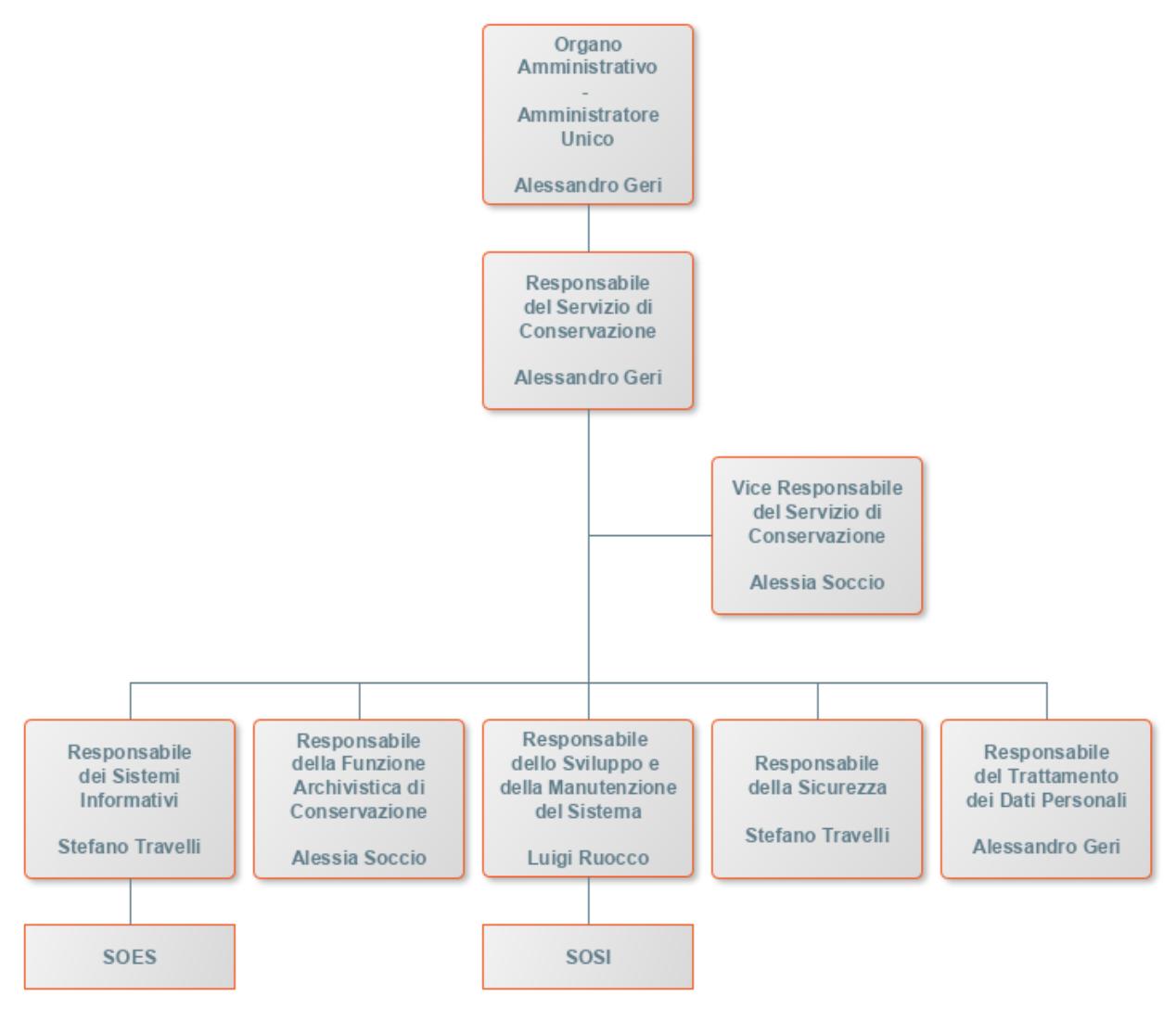

Figura 2. Organigramma responsabili.

Torna all'indice.

5.2. Strutture organizzative

L'Organo Amministrativo ha il compito di pianificare, controllare e supervisionare le attività di Entaksi, nonché di definire e sorvegliare le politiche aziendali, assegnare le responsabilità, e sorvegliare sulle attività finanziarie e sulla promozione degli indirizzi.

Il **Supporto operativo erogazione servizio (SOES)** costituisce il punto di contatto tra Entaksi e i propri clienti, è gestito dal Responsabile dei Sistemi Informativi, e si occupa principalmente della raccolta delle segnalazioni provenienti sia dai clienti stessi (Produttore e Utente) che dalle strutture interne coinvolte nell'erogazione del Servizio di Conservazione.

I clienti possono inviare segnalazioni e richieste al Servizio tramite e-mail all'indirizzo assistenza@entaksi.eu .
Il SOES prende in carico le segnalazioni e le inserisce nel sistema di ticketing di Entaksi, dal quale vengono prese in carico dai Responsabili di competenza. Si occupa inoltre di tutte le segnalazioni, sia interne che esterne, categorizzandole per tipologia in una delle seguenti classi:

- incidente;
- richiesta di servizio.

Il SOES è attivo dal lunedì al venerdì dalle ore 09:00 alle ore 18:00

Il **Supporto Operativo dei Sistemi Informativi (SOSI)** è gestito dal Responsabile dello Sviluppo e della Manutenzione, e ha lo scopo di assicurare il corretto funzionamento della infrastruttura tecnologica di Entaksi e degli applicativi su questa installati, fra i quali l'applicativo di Conservazione a Norma. Opera di concerto con il SOES per la gestione delle eventuali segnalazioni di malfunzionamento.

Il SOSI è attivo dal lunedì al venerdì dalle ore 09:00 alle ore 18:00.

Il SOSI, dietro indicazione del Responsabile del Servizio di Conservazione, mantiene aggiornata l'infrastruttura informatica e la piattaforma applicativa secondo la politica di evoluzione di Entaksi e le esigenze dei clienti, nel rispetto della normativa vigente e degli standard internazionali.

Il SOSI ha i seguenti compiti:

- monitoraggio applicativo in modalità h24;
- supporto specialistico di sviluppo funzionalità utente e assistenza applicativa;
- produzione della reportistica di competenza;
- presa in carico delle Richieste di Servizio provenienti dal SOES;
- presidio e gestione dell'infrastruttura tecnologica ed applicativa del sistema di Conservazione;
- configurazione, manutenzione e monitoraggio delle trasmissioni dei dati da e verso il sistema di Conservazione;
- installazione, configurazione e gestione dei sistemi operativi, software di base e tools propri dell'infrastruttura del sistema di Conservazione;
- risoluzione delle anomalie sistemistiche in collaborazione con il SOES;
- monitoraggio dell'utilizzo delle risorse, con particolare attenzione alle tendenze relative all'utilizzo delle stesse;
- definizione e realizzazione di un piano di adeguamento delle risorse ai consumi;
- monitoraggio e gestione degli allarmi tecnologici relativi allo stato dei sistemi provenienti dagli strumenti di controllo e automazione;
- esecuzione e adeguamento delle procedure di backup standard dei dati.

Le principali tipologie di segnalazione gestite dal SOSI sono:

- segnalazioni di malfunzionamenti generati dalla piattaforma di Conservazione;
- segnalazioni di malfunzionamenti dovuti ad un errata formattazione dei documenti ricevuti del Produttore;
- problematiche relative ad aspetti funzionali sul processo che alimenta la piattaforma di Conservazione.

In base a quanto precedentemente elencato, è qui di seguito riportata la **matrice delle responsabilità**:

Tabella 3. Matrice delle responsabilità.

	RSC	RFA	RSI	RSM	RS	RTD
attivazione del servizio di conservazione (a seguito della sottoscrizione di un contratto)	R	C	C	I	I	I
definizione formati, metadati, criteri di aggregazione e classificazione documentale	C	R	C	C	I	I
acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento	I	C	R	C	I	I
preparazione e gestione dei PDV, PDA, PDD	I	I	R	C	I	I
scarto dei PDA	C	C	R	C	I	I

	RSC	RFA	RSI	RSM	RS	RTD
chiusura del servizio di conservazione (al termine di un contratto)	R	C	C	I	I	I
conduzione e manutenzione del sistema di conservazione	R	C	A	A	I	I
monitoraggio del sistema di conservazione	R	C	A	A	I	I
gestione delle richieste di servizio	C	I	C	C	I	I
verifica periodica di conformità a normativa e standard di riferimento	R	C	C	C	I	I

RSC = Responsabile del Servizio di Conservazione

RFA = Responsabile della Funzione Archivistica di Conservazione

RSI = Responsabile dei Sistemi Informativi per la Conservazione

RSM = Responsabile dello Sviluppo e della Manutenzione del Sistema di Conservazione

RS = Responsabile della Sicurezza dei Sistemi per la Conservazione

RTD = Responsabile del Trattamento dei Dati Personali

In base a questa descrizione, la struttura organizzativa di Entaksi si basa su un sistema di ticketing, attraverso il quale il cliente può richiedere, in seguito alla sottoscrizione del contratto, l'attivazione del servizio di conservazione.

Il contratto, stipulato tramite il SOES, definisce, oltre ai termini di attivazione del servizio, il perimetro delle **attività del sistema di conservazione**, che comprende:

- acquisizione, verifica e gestione dei pacchetti di versamento presi in carico dal sistema di conservazione, e la generazione del rapporto di versamento;
- preparazione e gestione del pacchetto di archiviazione;
- preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta;
- scarto dei pacchetti di archiviazione;
- chiusura del servizio di conservazione (al termine di un contratto).

Per quanto invece riguarda le **attività proprie di gestione dello sviluppo informatico**, controllate dal SOSI, sono identificate in:

- conduzione e manutenzione del sistema di conservazione;
- monitoraggio del sistema di conservazione;
- change management;
- verifica periodica di conformità a normativa e standard di riferimento.

Il SOES e il SOSI si occupano inoltre di:

- gestione degli incidenti;
- gestione delle richieste di servizio;
- gestione delle richieste di cambiamento;
- gestione delle richieste di attivazione del servizio.

Per quanto riguarda la **gestione degli incidenti**, una volta ricevuta la segnalazione, il Responsabile della Sicurezza, il Responsabile dei Sistemi Informativi ed il Responsabile dello Sviluppo e della Manutenzione si coordineranno per eseguire le seguenti attività:

1. Verifica dell'attendibilità della segnalazione.
2. Se la segnalazione si dimostra attendibile l'incidente viene qualificato, tenendo conto del contesto in cui si è verificato, della presenza di eventuali SLA, ecc., è registrato mediante l'inserimento di un apposito ticket sul sistema di gestione dei ticket standard di Entaksi (per i dettagli della registrazione vedi paragrafo seguente).
3. Il ticket viene assegnato, tenendo conto della priorità e gravità dell'incidente, immediatamente o durante le periodiche riunioni di pianificazione o revisione della pianificazione.
4. Se è possibile individuare una soluzione, questa viene applicata (registrando sul ticket le operazioni svolte) e l'incidente chiuso. In questa fase deve essere posta particolare attenzione alla natura dell'incidente; infatti, se l'incidente riguarda sia la sicurezza delle informazioni che l'erogazione di un servizio, occorre ben bilanciare la necessità di ripristinare celermente la

normale erogazione del servizio con l'esigenza di non presentare, o reiterare, falle nel sistema di sicurezza.

5. Viene altrimenti fatta una escalation, durante la quale il Responsabile dello Sviluppo e della Manutenzione valuta se è necessario impiegare per la risoluzione dell'incidente un maggior numero di risorse o un insieme più vasto di competenze, e dispone l'allocazione delle risorse necessarie.
6. Adeguate le risorse, si torna al punto 3.
7. A seguito della risoluzione dell'incidente, il Responsabile della Sicurezza, con il contributo del Responsabile dello Sviluppo e della Manutenzione e del Responsabile dei Sistemi Informativi, effettua una revisione della qualificazione del ticket e lo chiude.
8. Se durante l'iter di gestione dell'incidente viene individuato il possibile problema che lo ha determinato, si affronta la gestione di tale problema mediante la procedura descritta nel Sistema Integrato di Gestione (SIG) certificato di Entaksi. Nel caso in cui, conseguentemente ad un incidente, il Responsabile della Sicurezza intraveda la necessità di intraprendere un'azione legale (sia civile che penale) contro una persona od organizzazione, raccoglierà tutte le prove necessarie e le gestirà in maniera conforme alla leggi vigenti.

Inoltre, nel caso in cui il Sistema di Conservazione rilevi situazioni anomale dovute alla presenza di dati errati forniti dal Produttore (metadati non coerenti, problemi sui flussi, sequenze di numerazione non rispettate, ecc.), il SOES prende in carico l'anomalia, e può contattare il Produttore tramite i canali e le modalità concordate per la notifica e per eventuali azioni da intraprendere per la chiusura del ticket.

La figura seguente riporta lo schema del workflow utilizzato per la gestione degli incidenti:

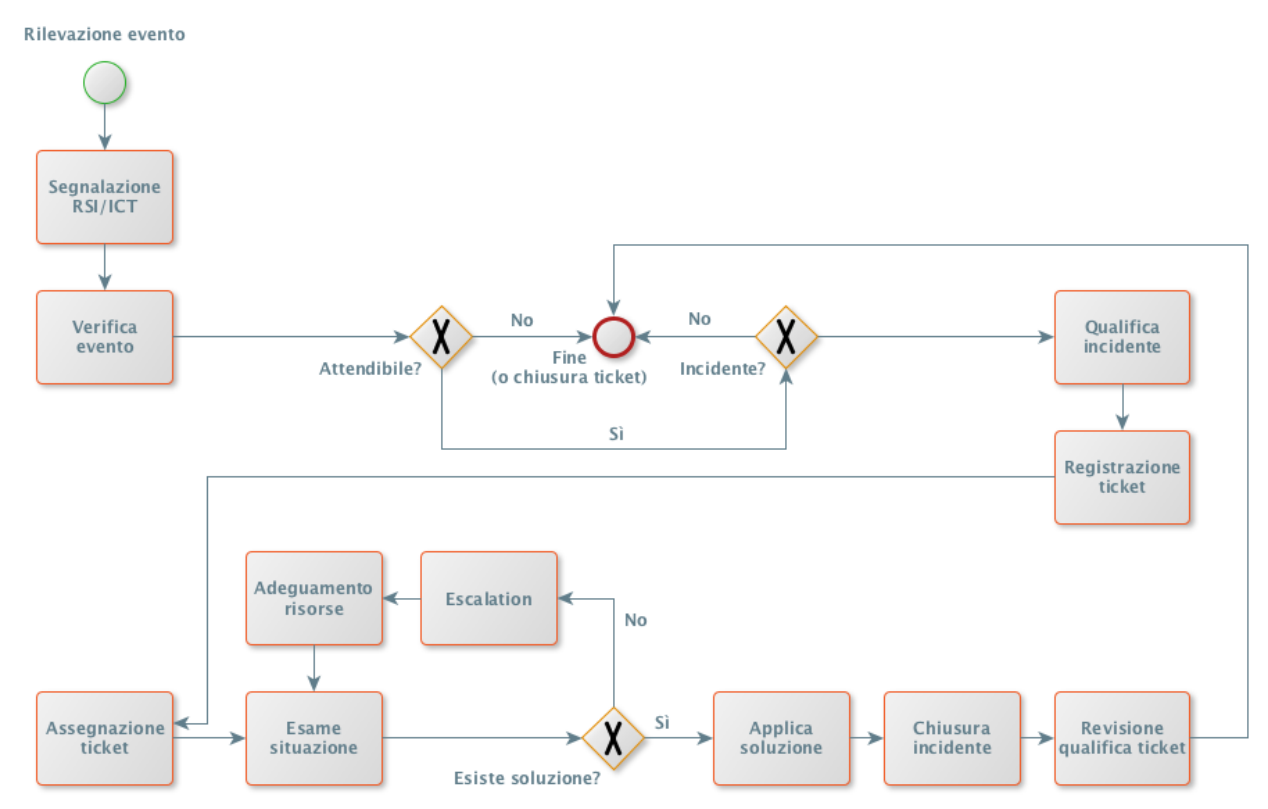

Figura 3. Workflow gestione incidenti.

Il ticket di registrazione degli incidenti dovrà contenere i seguenti dati:

- numero progressivo del ticket;
- data di registrazione;
- luogo in cui è stato rilevato l'incidente o vulnerabilità;
- sistema a cui si riferisce (sicurezza, servizi o entrambi);
- descrizione dell'evento o vulnerabilità;
- descrizione dell'eventuale danno provocato;
- eventuale impatto, con assegnazione di un valore di impatto coerente con la classificazione prevista dalla procedura di

valutazione dei rischi;
- requisito di sicurezza compromesso (riservatezza / integrità / disponibilità del dato);
- classificazione, riferita alle minacce censite nel SIG (se la minaccia non è censita, deve essere inserita nell'elenco);
- priorità (bassa, normale, alta, urgente);
- gravità (scarsa, media, grave, critica);
- indicazione della eventuale escalation necessaria;
- risoluzione: eventuali azioni intraprese per limitare il danno o per impedirne l'eventuale ulteriore accadimento;
- revisione della qualificazione del ticket;
- note e data di chiusura del ticket.

Per quanto riguarda sia la **gestione delle richieste di cambiamento** che le **richieste di servizio** vere e proprie, la descrizione dei vari step operativi che compongono il workflow è la seguente:

1. Il richiedente inserisce la RdS nel sistema di gestione dei ticket (direttamente, se la richiesta proviene da personale interno Entaksi, o attraverso l'invio di una mail ad assistenza@entaksi.eu se la richiesta proviene da un cliente).
2. La RdS viene verificata dal Responsabile dei Sistemi Informativi e dal Responsabile dello Sviluppo e della Manutenzione. Se la RdS si dimostra attendibile viene qualificata, tenendo conto del contesto in cui è pervenuta, della presenza di eventuali SLA, ecc. (per i dettagli della qualificazione vedi paragrafo seguente). Il ticket passa allo stato 'in elaborazione'.
3. La RdS viene evasa, in accordo a quanto previsto dalle procedure in essere per la natura della Richiesta (bug fixing, nuovo servizio, ecc.).
4. Al termine della corretta evasione della RdS, il ticket viene chiuso dal Responsabile dei Sistemi Informativi o dal Responsabile dello Sviluppo e della Manutenzione. La figura seguente riporta lo schema generale del workflow utilizzato per la gestione delle RdS.

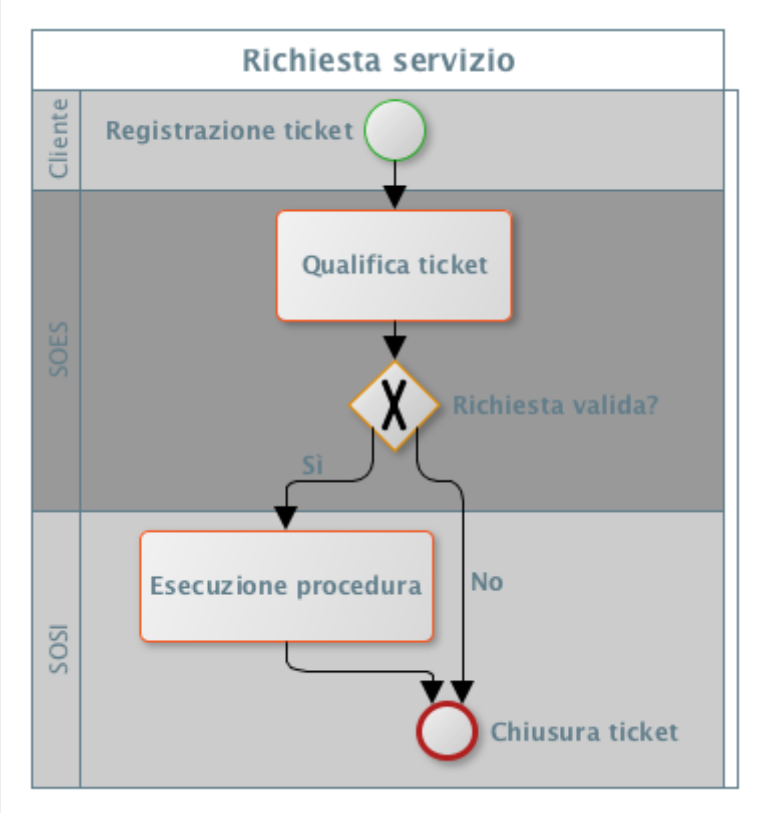

Figura 4. Workflow richiesta di servizio.

Il **ticket di registrazione delle richieste di servizio** conterrà i seguenti dati:

- numero progressivo del ticket;
- data di registrazione;
- ambiente a cui la RdS si riferisce;
- descrizione della RdS;

- classificazione (segnalazione malfunzionamento, richiesta consulenza, richiesta servizi);
- origine della richiesta (se interna o esterna);
- priorità (bassa, normale, alta, urgente);
- gravità (scarsa, media, grave, critica);
- indicazione della eventuale escalation necessaria;
- revisione della qualificazione del ticket;
- note di chiusura del ticket.

Nel caso che la Richiesta di Servizio riguardi una **Richiesta di Attivazione del Servizio**, il workflow precedente si inserisce in un flusso piu vasto, che comprende le attività commerciali e di rendicontazione e fatturazione dei servizi erogati. Lo schema di riferimento di tale workflow è riportato di seguito:

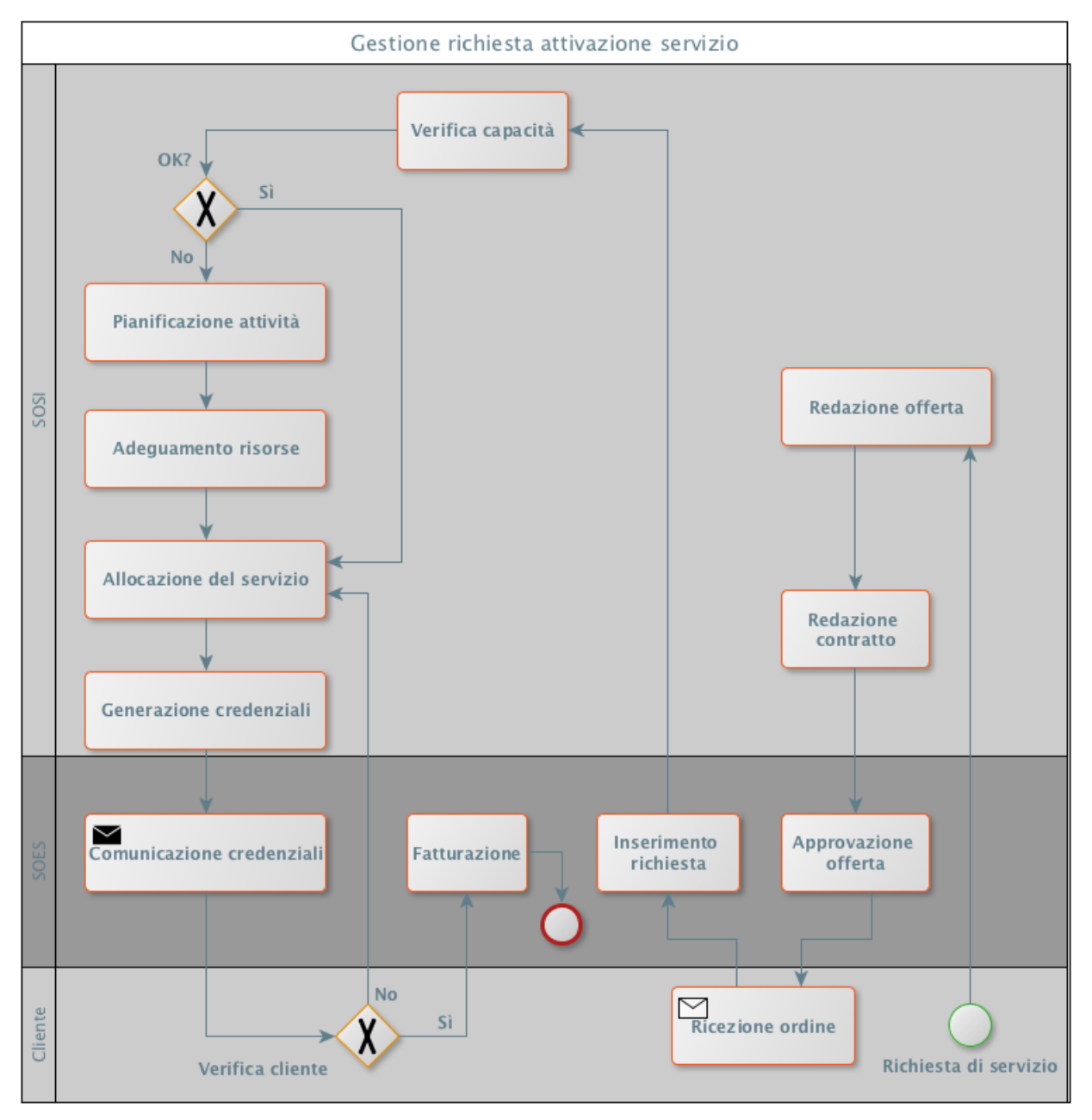

Figura 5. Workflow richiesta di attivazione del servizio.

Torna all'indice.

6. Oggetti sottoposti a conservazione

Sono oggetti del sistema di conservazione:

1. i **documenti informatici e i documenti amministrativi informatici** prodotti dal cliente e acquisiti da Entaksi, con i metadati ad essi associati di cui all'allegato 5 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici;
2. i **fascicoli informatici** ovvero le **aggregazioni documentali informatiche** con i metadati ad essi associati, contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che appartengono al fascicolo o all'aggregazione documentale.

I documenti e i fascicoli da sottoporre a conservazione vengono acquisiti dal Sistema sotto forma di aggregazione documentaria, e come tale trattati e distribuiti, congiuntamente ai metadati a loro attribuiti. Questo tipo di aggregazione, chiamata "pacchetto informativo", è conforme alle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, e si suddivide in:

- **Pacchetto di Versamento (PDV)**, aggregazione creata al momento del versamento da parte del Produttore degli oggetti da portare in conservazione;
- **Pacchetto di Archiviazione (PDA)**, aggregazione formata al momento in cui i documenti o i fascicoli vengono portati in conservazione;
- **Pacchetto di Distribuzione (PDD)**, aggregazione formata al fine della distribuzione agli Utenti degli oggetti sottoposti a conservazione.

La struttura dell'archivio rispecchia in generale quella definita dallo standard ISAD(G): *General International Standard Archival Description*, per la quale l'archivio viene così strutturato:

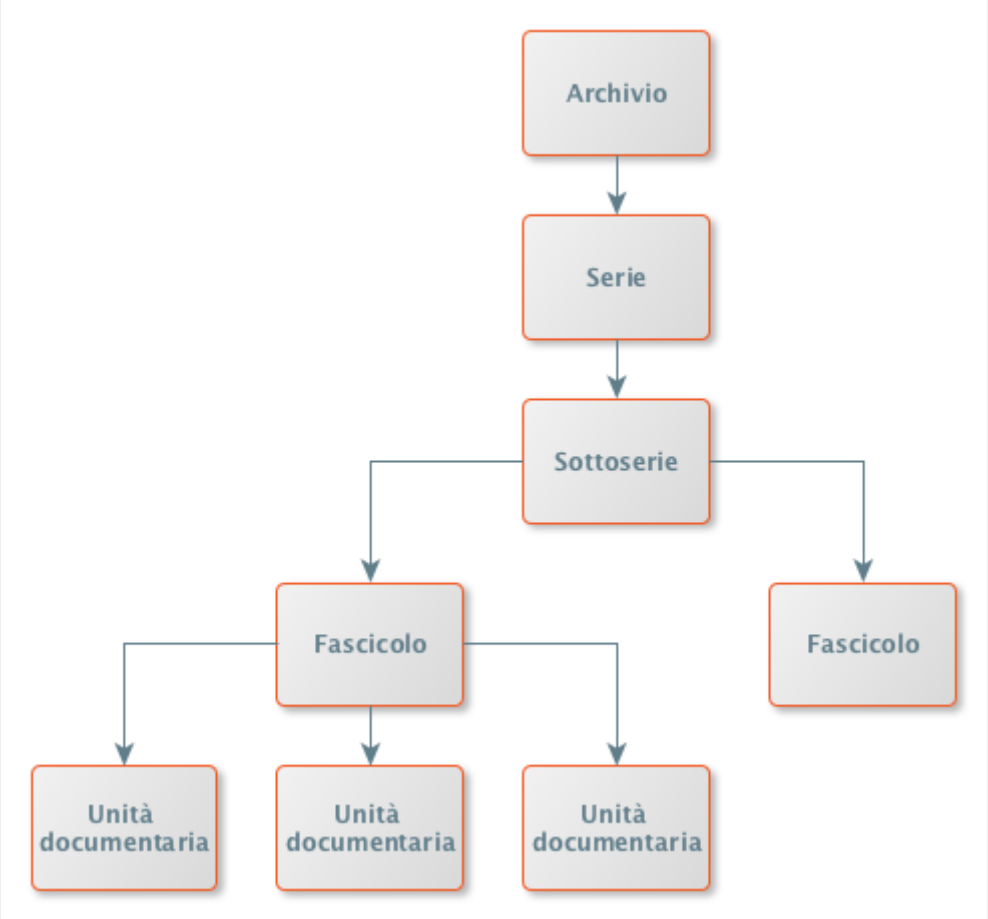

Figura 6. Struttura dell'archivio.

Dove alla voce "Archivio" corrisponde la totalità dei documenti depositati da ogni singolo Produttore, organizzati e visualizzati nel sistema in "Serie", "Sotto-serie" ed eventualmente ulteriori "Sotto-serie", per arrivare alle singole "Unità documentarie" che possono essere organizzate o meno in "Fascicoli".

I documenti e i fascicoli sono suddivisibili in categorie in base alla tipologia documentaria, così come descritte nel paragrafo successivo, e i file di appartenenza possono avere diversi formati, che vengono descritti nella tabella "Formati dei file accettati dal sistema".

Torna all'indice.

6.1. Oggetti conservati

Le tipologie documentali gestite dal sistema, afferenti agli oggetti descritti nel precedente paragrafo, sono le 85 categorie descritte nell'elenco dei tipi di documento di cui all'Allegato 1 del Provvedimento Prot. N. 2010/143663 del Direttore dell'Agenzia delle Entrate del 25 ottobre 2010: "Provvedimento attuativo della comunicazione dell'impronta relativa ai documenti informatici rilevanti ai fini tributari, ai sensi dell'articolo 5 del del Decreto 23 gennaio 2004".

La seguente tabella elenca queste tipologie indicando nella colonna "tipo" il codice utilizzato del sistema per rappresentarle.

Tabella 4. Tipi di documento gestiti dal sistema.

Tipo	Descrizione
D01	Fatture attive
D02	Fatture passive
D03	Nota variazione aumento
D04	Nota variazione diminuzione
D05	Documento di trasporto
D06	Scontrino
D07	Ricevuta
D08	Bolla
D09	Libro giornale
D10	Libro inventari
D11	Libro mastro
D12	Registro cronologico
D13	Libro cespiti
D14	Registro Irpef
D15	Registro fatture acquisto
D16	Registro acquisti agenzie viaggio
D17	Registro fatture emesse
D18	Registro fatture in sospeso
D19	Registro corrispettivi
D20	Giornale fondo
D21	Registro corrispettivi agenzie viaggio

Tipo	Descrizione
D22	Registro emergenza Iva
D23	Bollettario
D24	Registro prima nota
D25	Registro unico Iva
D26	Registro riepilogativo Iva
D27	Registro sezionale Iva acquisiti intra-UE
D28	Registro acquisti intra-UE non commerciali
D29	Registro trasferimenti intra-UE
D30	Registro dichiarazioni d'intenti emesse
D31	Registro dichiarazioni d'intenti ricevute
D32	Registro omaggi
D33	Registro memoria produzione contrassegno
D34	Registro lavorazione produzione contrassegno
D35	Registro carico produzione contrassegno
D36	Registro scarico produzione contrassegno
D37	Registro di beni in deposito
D38	Registro di beni in conto lavorazione
D39	Registro di beni in comodato
D40	Registro di beni in prova
D41	Registro sezionale Iva interno
D42	Registro carico stampati fiscali
D43	Registro società controllanti e controllate
D44	Registro carico scarico regime margine metodo analitico
D45	Registro acquisti regime margine metodo globale
D46	Registro vendite regime margine metodo globale
D47	Registro carico centri elaborazione dati
D48	Registro scarico centri elaborazione dati
D49	Registro somme ricevute in deposito

Tipo	Descrizione
D50	Registro editori
D51	Libro soci
D52	Libro obbligazioni
D53	Libro adunanze e delibere di assemblee
D54	Libro adunanze e delibere del consiglio di amministrazione
D55	Libro adunanze e delibere del collegio sindacale
D56	Libro adunanze e delibere del comitato esecutivo
D57	Libro adunanze e delibere delle assemblee azionisti
D58	Altri registri
D59	Unico persone fisiche
D60	Unico società persone
D61	Unico società capitale
D62	Unico enti non commerciali
D63	Irap persone fisiche
D64	Irap Società persone
D65	Irap Società capitale
D66	Irap enti non commerciali ed equiparati
D67	Irap amministrazioni ed enti pubblici
D68	Modello730
D69	Modello consolidato nazionale e mondiale
D70	Modello Iva
D71	Modello Iva VR richiesta rimborso credito Iva
D72	Modello Iva 26LP/2006 prospetto liquidazioni periodiche
D73	Modello Iva 74 bis
D74	Comunicazione annuale dati Iva
D75	Modello richiesta rimborso credito Iva trimestrale
D76	Modello dati contenuti dichiarazione intento ricevute
D77	Modello 770 semplificato

Tipo	Descrizione
D78	Modello 770 ordinario
D79	Modello certificazione CUD
D80	Modello F23
D81	Modello F24
D82	Modelli allegati alla Dichiarazione dei Redditi Modello Unico
D83	Modelli annotazione separata
D84	Ricevuta presentazione modelli dichiarazione
D85	Altri documenti

A fronte di specifiche esigenze, su richiesta ed in accordo con il cliente Produttore e il Responsabile della Conservazione, altre tipologie documentali possono essere individuate dal Responsabile del Servizio di Conservazione, d'intesa con il Responsabile della Funzione Archivistica e col Responsabile dello Sviluppo e della Manutenzione.
Nell'evenienza, queste ulteriori tipologie sono formalizzate nei manuali specifici per ogni servizio allegati al contratto, e rientrano in fase di conservazione, in base alla loro struttura, nelle categorie "D58 Altri registri" o "D85 Altri documenti".

Il fascicolo informatico rappresenta un collegamento logico tra documenti, che formano un insieme coerente relativo a un affare, una materia, un procedimento, una persona. Si tratta di un'aggregazione funzionale di singole unità documentarie. Nella struttura del Sistema di Conservazione il fascicolo è identificato con un elemento che contiene uno o più riferimenti alle unità documentarie che intendono essere raccolte nel fascicolo stesso.

Il fascicolo ha un identificativo proprio e le unità documentarie contenute nel fascicolo possono essere unità archivistiche già conservate nel Sistema di Conservazione, che creano una nuova unità archivistica nel fascicolo stesso, oppure unità documentarie versate nel Sistema di Conservazione contestualmente al versamento del fascicolo.

In fase di attivazione del servizio viene comunicato al cliente che sono accettati dal sistema di conservazione solo i formati dei documenti informatici idonei ad essere correttamente conservati, individuati dall'Allegato 2 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici. Tali formati rispettano i requisiti di "standard aperti" previsti nella normativa, in modo da garantire tecnicamente, anche in futuro, la possibilità di accedere ai dati conservati. A fronte di specifiche esigenze, su richiesta ed in accordo con il Cliente, possono essere eventualmente definiti altri formati idonei alla conservazione, tenendo conto delle peculiarità delle classi documentali e delle caratteristiche dei formati dei file accettabili in conservazione. Nell'evenienza, questi formati sono riportati nell'allegato "Specificità del contratto".

I formati dei file accettati dal sistema di conservazione sono riepilogati nella seguente tabella.

Tabella 5. Formati dei file accettati dal sistema.

Tipo	Estensione	Produttore	Visualizzatore	Standard	Versione	mime type
PDF	.pdf	Adobe System Inc.	Adobe Reader, Evince, Anteprima file e altri	ISO32000-1	1.7	application/pdf
PDF/A	.pdf	Adobe System Inc.	Adobe Reader, Evince, Anteprima file e altri	ISO19005-1:2005 ISO19005-2:2011	1.7	application/pdf

Tipo	Estensione	Produttore	Visualizzatore	Standard	Versione	mime type
TIFF	.tif	Aldus Corporation, ora Adobe System Inc.	Vari visualizzatori di immagini	ISO 12234-2 ISO 12639 RFC 2306 RFC 3949	6.0	image/tiff
JPEG	.jpg .jpeg	Joint Photographic Experts Group	Vari visualizzatori di immagini	ISO/IEC 10918 ITU-T T.81 ITU-T T.83 ITU-T T.84 ITU-T T.86	n/d	image/jpeg
PNG	.png	World Wide Web Consortium	Vari visualizzatori di immagini	ISO/IEC 15948 RFC 2083	1.0	image/png
OOXML	.docx .docm .xlsx .xlsm .pptx .pptm	Microsoft	Microsoft Office, LibreOffice, OpenOffice e altri	ISO/IEC 29500 ECMA-376	1.1	application/vnd.openxmlformats-officedocument.wordprocessingml.document application/vnd.openxmlformats-officedocument.spreadsheetml.sheet application/vnd.openxmlformats-officedocument.presentationml.presentation
ODF	.odt .odp .ods .odg	OASIS	Microsoft Office, LibreOffice, OpenOffice e altri	ISO/IEC 26300	1.2	application/vnd.oasis.opendocument.text application/vnd.oasis.opendocument.presentation application/vnd.oasis.opendocument.spreadsheet application/vnd.oasis.opendocument.graphics
XML	.xml .xsd	World Wide Web Consortium	Browser, visualizzatori di testo	W3C XML	1.0	application/xml text/xml
TXT	.txt	n/d	Visualizzatori di testo	ASCII ISO/IEC 8859 UTF-8	N/d	application/txt text/plain
EML	.eml	OASIS	Outlook, Mail, Thunderbird, vari client di posta elettronica	RFC 822 RFC 5322	n/d	message/rfc822

I formati così indicati acquisiscono in fase di conservazione la garanzia di immodificabilità e staticità. Il Responsabile del

Servizio di Conservazione attua tutti gli aggiornamenti necessari per renderli intelligibili nel tempo, eventualmente tramite riversamento, con un trasferimento dei dati da una piattaforma di elaborazione a un'altra, conservandone le caratteristiche informative originarie.

Nel sistema di conservazione ciascun oggetto è identificato univocamente tramite un codice delle risorsa (Uniform Resource Name, URN) per la cui definizione si rimanda a https://tools.ietf .org/html/rfc2141[RFC2141].

L' URN ha la seguente sintassi:

`<URN> ::= "urn:" <NID> ":" <NSS>`

Dove NID (Namespace Identifier) è l'identificativo dello spazio di nomi che determina il modo in cui deve essere interpretata la stringa specifica all'interno dello spazio di nomi (Namespace Specific String, NSS).
Nel Sistema di Conservazione viene utilizzato entaksi come valore del NID, mentre la stringa NSS viene interpretata come descritto nelle seguenti specifiche.

Per descrivere la sintassi della stringa NSS il sistema definisce le entità riportate nella seguente tabella.

Tabella 6. Definizione delle entità.

Entità	Rappresentazione	Descrizione
Ente	`<ente>`	È il soggetto giuridico che utilizza il sistema di conservazione. Viene rappresentato con una stringa equivalente al suo identificativo fiscale composto ad esempio dal codice paese seguito dalla partita IVA, oppure dal codice fiscale. Ad esempio: `IT1234567890`.
Struttura	`<struttura>`	È la struttura o area organizzativa che gestisce i documenti inviati al sistema di conservazione. Viene rappresentato con una stringa composta da lettere maiuscole e numeri. Ad esempio: `A000`. In alcuni casi la struttura o area organizzativa potrebbe non essere specificata. Ad esempio perché il produttore non definisce una suddivisione in aree organizzative oppure perché ci si riferisce ad un'area organizzativa principale che il produttore ritiene di non associare ad un codice. In questi casi nel sistema di archiviazione si utilizza il codice convenzionale `_default`, per indicare il codice mancante.
Anno	`<anno>`	Rappresenta l'anno di produzione dei documenti che vengono versati nel sistema di conservazione composto da 4 numeri, ad esempio: `2015`.
Tipologia documentale	`<tipo-documento>`	La tipologia documentale (o classificazione) è il primo livello di classificazione dei documenti versati nel sistema. Viene rappresentato con una stringa composta da lettere maiuscole e numeri secondo la tabella "Tipi di documento gestiti dal sistema". Ad esempio: `D01` Fatture attive, `D02` Fatture passive, ecc.
Sezionale	`<sezionale>`	Il sezionale (o serie archivistica) è un criterio di raggruppamento delle unità documentali appartenenti alla stessa tipologia documentale e costituisce una sotto classificazione dei documenti in una serie archivistica in cui i documenti assumono una numerazione progressiva. È rappresentato da una stringa composta da lettere e/o numeri. Ad esempio: `AAA123`. In alcuni casi non è specificato alcun sezionale o serie archivistica. Per raggruppare i documenti per i quali manca il codice del sezionale o serie archivistica si utilizza il valore convenzionale `_default`.

Entità	Rappresentazione	Descrizione
Numero documento	`<numero-documento>`	È il numero progressivo assegnato ad un documento che lo identifica all'interno di una serie archivistica ovvero di un sezionale. Esso può essere preesistente, per le unità documentarie che dispongono di una numerazione progressiva già definita (come le fatture attive), oppure assegnato dal sistema durante il versamento dei documenti per le unità documentarie che non definiscono una numerazione.
Numero fascicolo	`<numero-fascicolo>`	È il numero progressivo assegnato ad un fascicolo che lo identifica all'interno di una serie archivistica ovvero di un sezionale. Esso può essere preesistente, per i fascicoli che dispongono di una numerazione progressiva già definita, oppure assegnato dal sistema durante il versamento dei documenti per i fascicoli che non definiscono una numerazione.
Identificativo PDV	`<id-pdv>`	È un codice numerico assegnato dal sistema ai Pacchetti di Versamento
Progressivo PDA	`<prog-pda>`	È un numero progressivo assegnato dal sistema ai Pacchetti di Archiviazione all'interno di una serie archivistica.
Identificativo PDD	`<id-pdd>`	È un codice numerico assegnato dal sistema ai Pacchetti di Distribuzione.

Tramite la definizione delle entità è stabilita la sintassi degli URN che identificano i vari oggetti trattati. La seguente tabella riporta la sintassi in formato Backus-Naur Form degli URN di ciascun oggetto.

Tabella 7. Sintassi degli URN per gli oggetti rappresentati nel sistema.

Oggetto	Sintassi e descrizione
Produttore	`<produttore> ::= “urn:entaksi:” <ente> “:” <struttura>` Identifica la struttura o area organizzativa che dispone il versamento dei documenti nel sistema di conservazione. Es.: `urn:entaksi:IT1234567890:ST01`
PDV	`<pdv> ::= <produttore> “:pdv:” <id-pdv>` Identifica l'indice del pacchetto di versamento. Es.: `urn:entaksi:IT1234567890:ST01:pdv:7890`
RDV	`<rdv> ::= <produttore> “:rdv:” <id-pdv>` Identifica il rapporto di versamento prodotta dal sistema di conservazione dopo l'elaborazione di un pacchetto di versamento. Es.: `urn:entaksi:IT1234567890:ST01:rdv:7890`

Registro	`<registro> ::=`
	`<produttore> “:reg:“ <anno> “:” <tipo-documento> “:” <sezionale>`
	
	Identifica un registro di archiviazione in cui sono contenuti pacchetti di archiviazione. Es.:
	`urn:entaksi:IT1234567890:ST01:reg:2015:D01:S1`

Oggetto	Sintassi e descrizione
PDA	`<pda> ::= <registro> ":pda:" <prog-pda>` Identifica un pacchetto di archiviazione. Es.: `urn:entaksi:IT1234567890:ST01:reg:2015:D01:S1:pda:17`
PDD	`<pdd> ::= <produttore> ":pdd:" <id-pdd>` Identifica un pacchetto di distribuzione. Es.: `urn:entaksi:IT1234567890:ST01:pdd:3456`
Unità documentaria	`<doc> ::= <registro> ":doc:" <numero-documento>` Identifica l'unità documentaria collocata all'interno di un registro di archiviazione. Es.: `urn:entaksi:IT1234567890:ST01:reg:2015:D01:S1:doc:123`
Fascicolo	`<fascicolo> ::= <registro> ":fas:" <numero-fascicolo>` Identifica il fascicolo collocato all'interno di un registro di archiviazione. Es.: `urn:entaksi:IT1234567890:ST01:reg:2015:D01:S1:fas:456`
File	`<file> ::= <pdv> ":" <nome-file>` Identifica il singolo file che compone una unità documentaria sulla base del Pacchetto di Versamento con cui è stato introdotto nel sistema di conservazione. Es.: `urn:entaksi:IT1234567890:ST01:PDV:7890:fattura.pdf`

Alcuni degli oggetti gestiti dal sistema e identificati dai rispettivi URN corrispondono a dei file il cui nome si ricava dall'URN sostituendo il carattere ":" (due punti) con il carattere "_" (trattino basso) e aggiungendo l'estensione opportuna.

I nomi dei file così ottenuti sono esemplificati nella tabella seguente.

Tabella 8. Definizione dei nomi dei file.

Oggetto	Nome file ed esempio
PDV	`<pdv.zip> ::= <pdv> ".zip"` es.: `urn_entaksi_IT1234567890_ST01_pdv_7890.zip`
Indice PDV	`<idpdv.xml> ::= <pdv> ".xml"` es.: `urn_entaksi_IT1234567890_ST01_pdv_7890.xml`
RDV	`<rdv.xml> ::= <rdv> ".xml"` es.: `urn_entaksi_IT1234567890_ST01_rdv_7890.xml`
PDA	`<pda.zip> ::= <pda> ".zip"` es.: `urn_entaksi_IT1234567890_ST01_reg_2015_D01_S1_pda_17.zip`
Indice PDA	`<idpda.xml> ::= <pda> ".xml"` es.: `urn_entaksi_IT1234567890_ST01_reg_2015_D01_S1_pda_17.xml`

Oggetto	Nome file ed esempio
PDD	`<pdd.zip> ::= <pdd> ".zip"` es.: `urn_entaksi_IT1234567890_ST01_pdd_3456.zip`
Indice PDD	`<idpdd.xml> ::= <pdd> ".xml"` es.: `urn_entaksi_IT1234567890_ST01_pdd_3456.xml`
Unità documentali	`<doc.zip> ::= <doc> ".zip"` es.: `urn_entaksi_IT1234567890_ST01_reg_2015_D01_S1_doc_123.zip`
Fascicolo	`<fascicolo.zip> ::= <fascicolo> ".zip"` es.: `urn_entaksi_IT1234567890_ST01_reg_2015_D01_S1_fas_123.zip`

Tutti i documenti versati nel sistema di conservazione sono contraddistinti da un insieme di metadati obbligatori.

I metadati gestiti dal sistema si applicano alle varie entità gestite, alle unità documentarie e ai fascicoli archiviati, rendendo possibile la ricerca e la collocazione archivistica secondo l'insieme minimo definito nell'Allegato 5 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, che il sistema può estendere con un modello di metadati aggiuntivi in base alle diverse tipologie documentarie.

Per ogni aggregazione documentaria (PDV, PDA e PDD), vengono definiti metadati a livello di pacchetto, per la gestione, e a livello di unità documentaria, per la descrizione.

La rappresentazione dei metadati avviene con una duplice modalità:

1. Sfruttando la semantica definita dalle specifiche *Dublin Core* per quegli attributi che trovano una corrispondenza negli attributi base o negli attributi estesi di questa specifica.
2. Utilizzando una struttura generica di coppie chiave/valore per quegli attributi che non trovano questa corrispondenza, ma che è utile o necessario avere rappresentati tra i metadati del documento archiviato.

Per ciascuna tipologia documentaria è definito l'insieme dei metadati e i criteri di corrispondenza con gli attributi dell'una o dell'altra modalità. Il complesso dei metadati utilizzati per ogni tipologia di oggetto documentario mandato in conservazione viene definito al momento della stipula del contratto, in osservanza delle richieste minime descritte nel sopracitato Allegato 5, e in accordo con il Produttore nel caso di ulteriori specifiche richieste. Non tutti i metadati descritti sono obbligatori: per determinati documenti possono non essere valorizzati nei valori non considerati necessari.

I metadati sono divisi in quattro categorie:

- `edoc:dcmi`, che raccoglie le proprietà corrispondenti ai metadati *Dublin Core*;
- `edoc:record`, che raccoglie le proprietà identificative dell'unità documentaria;
- `edoc:fixity`, che raccoglie le proprietà necessarie per la verifica dell'integrità del materiale archiviato;
- metadati specifici per la tipologia documentale, ossia una categoria che raccoglie le proprietà corrispondenti ai metadati specifici per un determinato tipo di documento.

L'ultima categoria viene definita e descritta nei manuali specifici per ogni servizio, e tutti i metadati possono essere ampliati in base alle esigenze dei produttori.

Nella seguente tabella sono indicati i termini Dublin Core utilizzati per il posizionamento archivistico dei documenti. Per ciascun metadato è descritto il significato specifico nell'ambito del sistema stesso.

Tabella 9. Metadati Dublin Core.

Termine Dublin Core	Tipo	Descrizione
`terms:accessRights`	alfanumerico	Nei documenti proveniente da archivi pubblici o privati di rilevante interesse storico, indica che lo scarto del pacchetto di archiviazione può avvenire solo previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo. Contiene l'indicazione della legge di riferimento che ne regola l'accesso per lo scarto.

Termine Dublin Core	Tipo	Descrizione
`terms:abstract`	alfanumerico	Sommario del contenuto del documento, per alcuni tipi di documento in assenza di metadati specifici può contenere informazioni sul contenuto che si ritengano necessarie per la ricerca del documento.
`terms:contributor`	alfanumerico	Nei fascicoli prodotti da enti della Pubblica Amministrazione, indica (in una o più occorrenze) il codice IPA dell'amministrazione partecipante al procedimento secondo la sintassi `IPA:<codice>`.
`terms:creator`	alfanumerico	Nei fascicoli prodotti da enti della Pubblica Amministrazione, indica il codice IPA dell'amministrazione titolare del procedimento secondo la sintassi `IPA:<codice>`.
`terms:date`	data e ora	La data e ora di chiusura o finalizzazione del documento. Nei documenti firmati digitalmente è la data e ora della firma digitale.
`terms:dateAccepted`	data e ora	Nei documenti ricevuti, indica la data di registrazione del documento.
`terms:dateSubmitted`	data e ora	Nei documenti inviati, indica la data di invio del documento.
`terms:description`	alfanumerico	Descrizione estesa del documento.
`terms:extent`	numerico	La dimensione in byte del file.
`terms:format`	alfanumerico	Il formato mime type del file.
`terms:hasPart`	alfanumerico (URN)	Il codice URN dell'unità documentaria contenuta nel documento descritto in aggiunta all'unità documentaria costituita dal documento descritto stesso. Può essere ripetuto più volte. Quando applicato ad un fascicolo ciascun termine indica una delle unità documentarie contenute nel fascicolo.
`terms:identifier`	alfanumerico (URN)	Il codice URN assegnato dal sistema all'unità documentaria o al fascicolo, come definito nella tabella "Sintassi degli URN per gli oggetti rappresentati nel sistema".
`terms:isPartOf`	alfanumerico (URN)	Il codice URN dell'unità documentaria che contiene il file descritto. È applicato alla descrizione di tutti i file allegati di una certa unità documentaria. Quando applicato al file principale di una unità documentaria indica che il contenuto di quella unità documentaria è effettivamente incluso in un'altra unità documentaria (ad esempio quando viene archiviata una mail che contiene vari documenti come allegati).
`terms:isReferencedBy`	alfanumerico (URN)	Il codice URN del documento principale a cui si riferisce.
`terms:medium`	alfanumerico	Il formato *mime type* del contenitore utilizzato per il documento, ad esempio `application/pkcs7-mime` per i file inclusi in una busta PKCS#7 con la firma digitale.

Termine Dublin Core	Tipo	Descrizione
`terms:provenance`	alfanumerico (URN)	Ai documenti riversati è applicato il metadato Dublin Core `terms:provenance` contenente l'URN dell'unità documentaria in cui è archiviata la prova di archiviazione precedente.
`terms:publisher`	alfanumerico	Metadato descrittivo che contiene per i documenti riversati l'indicazione del conservatore precedente.
`terms:references`	alfanumerico	Il codice URN del documento secondario a cui si riferisce.
`terms:replaces`	alfanumerico	Identificativo del documento che viene rimpiazzato all'interno del sistema da un riversamento successivo (utilizzato per documenti che conservano un ordine).
`terms:source`	alfanumerico	Il codice URN del file descritto secondo la sintassi relativa al Pacchetto di Versamento di provenienza descritta nella tabella "Sintassi degli URN per gli oggetti rappresentati nel sistema". Nei metadati del Pacchetto di Archiviazione contiene l'URN del Pacchetto di Versamento da cui provengono i documenti, ripetuto per ogni Pacchetto di Versamento coinvolto dai documenti contenuti.
`terms:subject`	alfanumerico	Un breve testo che descrive il documento archiviato includendo un suo codice identificativo nell'ambito dei documenti del produttore (ad esempio `Fattura 3/2013 del 01/01/2015`).
`terms:title`	alfanumerico	Il nome del file del documento.
`terms:type`	alfanumerico	Il tipo di file in termini leggibili dall'utente.

Nella seguente tabella sono indicati i metadati identificativi dell'unità documentaria.

Tabella 10. Metadati identificativi dell'unità documentaria.

Metadato	Tipo	Descrizione
`destinatario:codicefiscale`	alfanumerico	Codice fiscale del destinatario (obbligatorio se non è indicato l'identificativo fiscale).
`destinatario:cognome`	alfanumerico	Cognome del destinatario (in caso di persona fisica).
`destinatario:idfiscale`	alfanumerico	Identificativo fiscale composto dal codice paese e dalla partita IVA del destinatario (obbligatorio se non è indicato il codice fiscale).
`destinatario:nome`	alfanumerico	Nome del destinatario (in caso di persona fisica).
`destinatario:pec`	alfanumerico	PEC del destinatario.
`destinatario:ragionesociale`	alfanumerico	Ragione sociale del destinatario (in caso di persona giuridica).

Metadato	Tipo	Descrizione
destinatario:tipo	alfanumerico	- PF per Persona Fisica - PG per Organizzazione - PAI per Amministrazioni Pubbliche italiane.
documento:anno	numerico	Anno di archiviazione del record.
documento:aoo	alfanumerico	Area Organizzativa Omogenea. In riferimento al produttore, individua l'area organizzativa a cui il documento appartiene, nel caso siano presenti più flussi documentari.
documento:conservazione	alfanumerico	Tempo di conservazione del documento, viene valorizzato automaticamente dal sistema in base alla tipologia di documento secondo il massimario di scarto.
documento:data	data	Data del documento.
documento:datainizio	data	Data di inizio del periodo di riferimento del documento (solo per i documenti che hanno un periodo di riferimento).
documento:dataprotocollo	data	Data della registrazione nel protocollo di ricezione.
documento:dataregistrazione	data	Data della registrazione nel registro IVA o nella prima nota.
documento:datatermine	data	Data di termine del periodo di riferimento del documento (solo per i documenti che hanno un periodo di riferimento).
documento:flusso	alfanumerico	Indica il flusso del documento, e può assumere i seguenti valori: - U = in uscita - E = in entrata - I = interno.
documento:formato	alfanumerico	Indica il formato del documento nel codice definito dall'allegato 2 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici.
documento:formazione	alfanumerico	Indica il processo di creazione del documento, e riporta una delle seguenti lettere: a) creazione tramite l'utilizzo di strumenti software che assicurino la produzione di documenti nei formati previsti nell'Allegato 2 delle Linee Guida; b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico; c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente; d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

Metadato	Tipo	Descrizione
documento:numero	numerico	Numero progressivo del documento.
documento:primanota	alfanumerico	Nei documenti ricevuti indica il protocollo di registrazione assegnato nella prima nota.
documento:posizionelotto	numerico	L'indice della posizione del documento descritto all'interno del file contenitore archiviato (solo nel caso in cui il file archiviato è un formato che può contenere più documenti).
documento:protocollo	alfanumerico	Nei documenti ricevuti indica il protocollo assegnato nel protocollo di ricezione.
documento:registrazione	alfanumerico	Nei documenti ricevuti indica il protocollo di registrazione assegnato nel registro IVA.
documento:sezionale	alfanumerico	Sezionale o serie archivistica del documento.
documento:tipo	alfanumerico	Tipologia documentale.
documento:tipoRegistro	alfanumerico	Può essere: - Nessuno - Protocollo Ordinario/Protocollo Emergenza - Repertorio/Registro.
intermediario:codicefiscale	alfanumerico	Codice fiscale del terzo intermediario (obbligatorio se non è indicato l'identificativo fiscale).
intermediario:cognome	alfanumerico	Cognome del terzo intermediario (in caso di persona fisica).
intermediario:idfiscale	alfanumerico	Identificativo fiscale composto dal codice paese e dalla partita IVA del terzo intermediario (obbligatorio se non è indicato il codice fiscale).
intermediario:nome	alfanumerico	Nome del terzo intermediario (in caso di persona fisica).
intermediario:ragionesociale	alfanumerico	Ragione sociale del terzo intermediario (in caso di persona giuridica).
intermediario:tipo	alfanumerico	- PF per Persona Fisica - PG per Organizzazione - PAI per Amministrazioni Pubbliche italiane.
mittente:codicefiscale	alfanumerico	Codice fiscale del mittente (obbligatorio se non è indicato l'identificativo fiscale).
mittente:cognome	alfanumerico	Cognome del mittente (in caso di persona fisica).
mittente:idfiscale	alfanumerico	Identificativo fiscale composto dal codice paese e dalla partita IVA del mittente (obbligatorio se non è indicato il codice fiscale).
mittente:nome	alfanumerico	Nome del mittente (in caso di persona fisica).
mittente:pec	alfanumerico	PEC del mittente.

Metadato	Tipo	Descrizione
`mittente:ragionesociale`	alfanumerico	Ragione sociale del mittente (in caso di persona giuridica).
`mittente:tipo`	alfanumerico	- PF per Persona Fisica - PG per Organizzazione - PAI per Amministrazioni Pubbliche italiane.
`modifica:autore`	alfanumerico	Corrisponde all'autore (o al produttore) della rettifica.
`modifica:data`	data	Corrisponde alla data e ora del documento modificato.
`modifica:numero`	alfanumerico	Il numero di versione del documento.
`modifica:tipo`	alfanumerico	Indica il tipo di modifica apportata al documento e può assumere i seguenti valori: - Annullamento - Rettifica - Integrazione - Annotazione.
`produttore:codicefiscale`	alfanumerico	Codice fiscale del produttore (obbligatorio se non è indicato l'identificativo fiscale).
`produttore:cognome`	alfanumerico	Cognome del produttore (in caso di persona fisica).
`produttore:idfiscale`	alfanumerico	Identificativo fiscale composto dal codice paese e dalla partita IVA del produttore (obbligatorio se non è indicato il codice fiscale).
`produttore:nome`	alfanumerico	Nome del produttore (in caso di persona fisica).
`produttore:ragionesociale`	alfanumerico	Ragione sociale del produttore (in caso di persona giuridica).
`produttore:tipo`	alfanumerico	- PF per Persona Fisica - PG per Organizzazione - PAI per Amministrazioni Pubbliche italiane.

La seguente tabella descrive i metadati relativi alla verifica dell'integrità:

Tabella 11. Metadati relativi alla verifica dell'integrità.

Metadato	Tipo	Descrizione
`fixity:canonicalXML`	alfanumerico	Valido solo per i file in formato XML, vale "true" se il file è stato ridotto in forma canonica prima di calcolare l'impronta.
`fixity:messageDigest`	alfanumerico	La rappresentazione Base64 dell'impronta del file calcolata secondo un determinato algoritmo.
`fixity:messageDigestAlgorithm`	alfanumerico	L'algoritmo con cui è stata calcolata l'impronta del file.
`fixity:messageDigestOriginator`	alfanumerico	L'applicazione che ha calcolato l'impronta del file (vale "edoc" se l'impronta è calcolata dal sistema di conservazione).
`verifica:firma`	booleano	Indica se il documento è firmato digitalmente, valore "vero" o "falso".

Metadato	Tipo	Descrizione
`verifica:sigillo`	booleano	Indica se il documento è sigillato digitalmente, valore "vero" o "falso".
`verifica:marca`	alfanumerico	Indica se il documento è marcato digitalmente, valore "vero" o "falso".
`verifica:conforme`	booleano	Indica se il documento è una copia sostitutiva conforme, valore "vero" o "falso".

La seguente tabella descrive i metadati specifici dei documenti di tipo fattura.

Tabella 12. Metadati specifici dei documenti fattura.

Metadato	Tipo	Descrizione
`fattura:cig`	alfanumerico	Valido solo se il documento è nel formato FatturaPA XML, il Codice Identificativo di Gara.
`fattura:codicepa`	alfanumerico	Valido solo se il documento è nel formato FatturaPA XML, il codice della Pubblica Amministrazione destinataria della fattura.
`fattura:cup`	alfanumerico	Valido solo se il documento è nel formato FatturaPA XML, il Codice Unico di Progetto.
`fattura:descrizionepa`	alfanumerico	Valido solo se il documento è nel formato FatturaPA XML, la descrizione della Pubblica Amministrazione destinataria della fattura.
`fattura:esito`	alfanumerico	Valido solo se il documento è nel formato FatturaPA XML, l'esito dell'invio della fattura.
`fattura:firmatario`	alfanumerico	Il nome e cognome del titolare del certificato digitale che ha firmato la fattura.
`fattura:idsdi`	numerico	Valido solo se il documento è nel formato FatturaPA XML, l'identificativo assegnato dal Sistema di Interscambio.
`fattura:importo`	alfanumerico	Il totale documento così come riportato nella fattura inclusa la valuta.
`fattura:numero`	numerico	Il numero della fattura.
`fattura:scadenza`	data	La data di scadenza, se riportata nelle informazioni di pagamento.

Tabella 13. Metadati specifici dei documenti PEC.

Metadato	Tipo	Descrizione
`pec:direzione`	alfanumerico	Direzione del messaggio. Verifica se il nome della casella si trova nel mittente o tra i destinatari R se il messaggio è ricevuto, T se il messaggio è trasmesso.
`pec:gestore`	alfanumerico	Gestore della PEC.

Metadato	Tipo	Descrizione
`pec:id`	alfanumerico	Identificativo della PEC.
`pec:msgid`	alfanumerico	msgid della PEC.

Tabella 14. Metadati specifici dei documenti LUL.

Metadato	Tipo	Descrizione
`lul:ccosto`	alfanumerico	Il centro di costo di riferimento del LUL.
`lul:livello`	alfanumerico	Il livello del dipendente.
`lul:matricola`	alfanumerico	Matricola del dipendente.
`lul:qualifica`	alfanumerico	La qualifica del dipendente.
`lul:stabilimento`	alfanumerico	Stabilimento assegnato al dipendente.
`lul:tipologia`	alfanumerico	Tipologia del LUL (Dipendente, Somministrato, Distaccato).

Tabella 15. Metadati specifici dei documenti FIR.

Metadato	Tipo	Descrizione
`fir:copia`	numerico	Numero della copia del documento (assume valore da 1 a 4).
`fir:numero`	alfanumerico	Identificativo univoco del FIR.
`fir:pec`	alfanumerico	PEC alla quale viene indirizzato il FIR.

Altri metadati per le presenti e per altri tipologie di documento possono essere definiti in accordo con il produttore.

In base all'elenco definito nell'Allegato 5 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, l'insieme minimo di metadati prevede che vengano censite dal sistema delle informazioni considerate fondamentali per la definizione dei documenti informatici, dei documenti amministrativi informatici, e dei fascicoli informatici o delle aggregazioni documentali informatiche. In base a queste indicazioni il sistema di conservazione gestisce i metadati minimi riportati nella seguente tabella. Per ciascun metadato è descritta la modalità di rappresentazione.

Tabella 16. Metadati minimi.

Metadato	Rappresentazione
Metadato `IdDoc`	
`IdDoc/ImprontaCrittograficaDelDocumento/Impronta`	Viene rappresentato dal metadato `fixity:messageDigest`.
`IdDoc/ImprontaCrittograficaDelDocumento/Algoritmo`	Viene rappresentato dal metadato `fixity:messageDigestAlgorithm`.
`IdDoc/Identificativo`	Viene rappresentato dal metadato `terms:identifier`.
Metadato `ModalitaDiFormazione`	
`ModalitaDiFormazione`	Viene rappresentato dal metadato `documento:formazione`.

Metadato	Rappresentazione
Metadato `TipologiaDocumentale`	
`TipologiaDocumentale`	Viene rappresentato dal metadato `terms:type`.
Metadato `DatiDiRegistrazione`	
`DatiDiRegistrazione/TipologiaDiFlusso`	Viene rappresentato dal metadato `documento:flusso`.
`DatiDiRegistrazione/TipoRegistro`	Viene rappresentato dal metadato `documento:tipoRegistro`.
`DataRegistrazioneDocumento` `OraRegistrazioneDocumento`	Vengono rappresentati dai metadati `documento:dataRegistrazione`, `documento:dataProtocollo`.
`NumeroRegistrazioneDocumento`	Viene rappresentato dal metadato `documento:numero`.
`CodiceRegistro`	Viene rappresentato dal metadato `documento:registrazione` solo nel caso sia presente un registro.
Metadato `Soggetti`	
`Soggetti/Ruolo`	Viene rappresentato all'interno dei metadati relativi al soggetto produttore: `produttore:codicefiscale`, `produttore:cognome`, `produttore:idfiscale`, `produttore:nome`, `produttore:ragionesociale`.
`Soggetti/TipoSoggetto`	Viene rappresentato nei metadati `:tipo` del soggetto (ad esempio `mittente:tipo`, `destinatario:tipo`, ecc).
`Soggetti/TipoSoggetto/PF`	Viene rappresentato nei metadati `:cognome`, `:nome`, `:idfiscale` del soggetto (ad esempio `mittente:nome`, `destinatario:cognome`, ecc).
`Soggetti/TipoSoggetto/PG`	Viene rappresentato nei metadati `:ragionesociale` del soggetto (ad esempio `produttore:ragionesociale`, ecc).
`Soggetti/TipoSoggetto/PAI`	Viene rappresentato nei metadati `:tipo` del soggetto (ad esempio `mittente:tipo`, `destinatario:tipo`, ecc).
`Soggetti/TipoSoggetto/PAE`	Viene rappresentato nei metadati `:tipo` del soggetto (ad esempio `mittente:tipo`, `destinatario:tipo`, ecc).
`Soggetti/TipoSoggetto/AS`	Viene rappresentato nei metadati `:tipo` del soggetto (ad esempio `mittente:tipo`, `destinatario:tipo`, ecc).
`Soggetti/TipoSoggetto/SW`	Viene rappresentato nei metadati `:tipo` del soggetto (ad esempio `mittente:tipo`, `destinatario:tipo`, ecc).
Metadato `ChiaveDescrittiva`	
`ChiaveDescrittiva/Oggetto`	Viene rappresentato dal metadato `terms:subject`.

Metadato	Rappresentazione
ChiaveDescrittiva/ParoleChiave	Viene rappresentato dal metadato terms:description (non obbligatorio).
Metadato Allegati	
Allegati/NumeroAllegati	Il sistema gestisce due modalità per allegare dei file a un documento. 1) Allegati che vengono versati insieme al documento principale, ad esempio le notifiche delle fatture che vengono emesse dal sistema di interscambio; 2) Documenti che vengono versati separatamente dopo che è stato versato il documento principale; Nel primo caso si considerano allegati i file successivi al primo nell'elemento <fileGroup> dell'indice del PDV, che sono riportati come file successivi al primo anche nell'elemento <FileGroup> dell'indice SInCRO. In questo caso il numero di allegati è implicito nel numero di elementi <file>. Nel secondo caso i documenti allegati vengono versati successivamente, sono considerati delle unità documentarie indipendenti e legate al documento principale mediante il metadato terms:isPartOf che riporta l'indentificativo del documento principale. La modalità di rappresentazione suggerita dallo schema dei metadati allegato alle Linee Guida prevede di indicare tra i metadati l'identificativo del documento allegato. Questo implica, in sostanza, che gli allegati vengono versati in conservazione prima del documento principale in modo che al momento del versamento del documento principale è possibile conoscere gli identificativi degli allegati. Questa modalità nel sistema si realizza utilizzando il metadato terms:hasPart che riporta uno o (ripetendo più volte il metadato) più identificati di documenti esistenti.
Allegati/IndiceAllegati	V. Allegati/NumeroAllegati.
Allegati/IndiceAllegati/IdDoc	V. Allegati/NumeroAllegati.
Allegati/IndiceAllegati/Descrizione	V. Allegati/NumeroAllegati.
Metadato Riservato	
Riservato	Viene rappresentato dal metadato terms:accessRights.
Metadato IdentificativoDelFormato	
IdentificativoDelFormato/Formato	Viene rappresentato dal metadato documento:formato in corrispondenza del file.
Metadato Verifica	
Verifica/FirmatoDigitalmente	Viene rappresentato dal metadato verifica:firma.
Verifica/SigillatoElettronicamente	Viene rappresentato dal metadato verifica:sigillo.
Verifica/MarcaturaTemporale	Viene rappresentato dal metadato verifica:marca.

Metadato	Rappresentazione
`Verifica/ConformitaCopieImmagineSuSupportoInformatico`	Viene rappresentato dal metadato `verifica:conforme`.
Metadato Agg (identificativo dell'aggregazione documentale)	
`Agg/IdAgg`	Viene rappresentato dal metadato `terms:isPartOf`.
Metadato `NomeDelDocumento`	
`NomeDelDocumento`	Viene rappresentato dal metadato `terms:title`.
Metadato `VersionedelDocumento`	
`VersionedelDocumento`	Viene rappresentato dal metadato `modifica:numero`.
Metadato `TracciatureModificheDocumento`	
`TracciatureModificheDocumento/TipoModifica`	Viene rappresentato dal metadato `modifica:tipo`.
`TracciatureModificheDocumento/SoggettoAutoreDellaModifica`	Viene rappresentato dal metadato `modifica:autore`.
`TracciatureModificheDocumento/DataModifica` `TracciatureModificheDocumento/OraModifica`	Viene rappresentato dal metadato `modifica:data`.
`TracciatureModificheDocumento/IdDocVersionePrecedente`	Viene rappresentato dal metadato `terms:replaces`.
Metadato `TempoDiConservazione`	
`TempoDiConservazione`	Viene rappresentato dal metadato `documento:conservazione`.

Oltre ai metadati precedenti, gestiti dal sistema per ogni documento, il sistema rende possibile la mappatura di metadati aggiuntivi per tutte le tipologie documentali riportate nella tabella "Tipi di documento gestiti dal sistema".
Questi metadati sono definiti in base alle diverse tipologie di informazioni contenute nei documenti, e mappati, ove possibile, sullo standard *Dublin Core*.
La valorizzazione di questi metadati viene definita in accordo con il Cliente in sede contrattuale, allo scopo di garantire la piena reperibilità dei dati durante la ricerca da parte di utenti terzi.

Torna all'indice.

6.2. Pacchetto di Versamento (PDV)

I Pacchetti di Versamento (PDV) sono costituiti da un file in formato ZIP contenente documenti appartenenti ad una o più unità documentarie da portare in conservazione, e da un file indice del PDV in formato XML.

Il Sistema di Conservazione definisce una serie di formati del PDV che determinano la modalità di validazione del pacchetto. Questi formati possono essere di uso generale oppure concordati con il singolo produttore per implementare specifiche esigenze relative alla dichiarazione o anche all'estrazione automatica di metadati dal materiale versato in aggiunta a quelli dichiarati nell'indice.

Il Servizio di Conservazione riceve i documenti inviati dal Produttore attraverso un insieme di servizi REST su protocollo HTTPS mediante una connessione in cui è garantita l'autenticazione dell'utente.

I documenti contenuti nel PDV confluiscono poi, nelle modalità di seguito descritte, in uno o più Pacchetti di Archiviazione.

In funzione del formato dei PDV ammessi e gestiti nel sistema, si determina la modalità con cui il pacchetto deve essere verificato e conseguentemente il modo in cui verrà elaborato dal sistema.

Le informazioni necessarie per trattare il contenuto del pacchetto sono le seguenti:

- il raggruppamento dei file in unità documentarie;
- i metadati di ciascuna unità documentaria;
- il registro di conservazione di ciascuna unità documentaria.

Tali informazioni devono essere presenti nell'indice del PDV, oppure ricavabili in altro modo (ad esempio interpretando il contenuto stesso dei documenti o utilizzando indici provenienti da sistemi di terze parti, ovvero da altri conservatori) secondo quanto stabilito nella definizione del formato di validazione del PDV.

La seguente tabella descrive i formati di validazione dei PDV gestiti dal sistema.

Tabella 17. Formati di validazione dei Pacchetti di Versamento.

Formato	Contenuto	Descrizione
F000	Fatture elettroniche emesse XML	Il formato F000 è utilizzato per le fatture elettroniche emesse e le relative notifiche, formate utilizzando il tracciato XML utilizzato dal Sistema di Interscambio.+ Questo formato non necessita di un file indice poiché il sistema è in grado di ricavare autonomamente i metadati, recuperando le informazioni necessarie dalla lettura dei documenti contenuti nel pacchetto. Durante la verifica del pacchetto il sistema raggruppa i file contenuti in unità documentarie e definisce il registro di conservazione in cui esse devono essere versate.
F001	Fatture elettroniche emesse XML gestite dal sistema eIFE	Il sistema di conservazione è integrato con il sistema di gestione delle fatture elettroniche di Entaksi (denominato eIFE). Il formato F001 si riferisce ai pacchetti costituiti dalle fatture elettroniche emesse in formato XML e dalle relative notifiche quando questi documenti sono gestiti direttamente dal servizio erogato da Entaksi per l'invio al Sistema di Interscambio dei documenti e la gestione delle notifiche di ritorno.
F002	Fatture elettroniche ricevute XML	Il formato F002 è utilizzato per le fatture elettroniche ricevute e le relative notifiche, formate utilizzando il tracciato XML utilizzato dal Sistema di Interscambio.+ Come avviene per il formato F000 non necessita di un file indice poiché il sistema è in grado di ricavare autonomamente i metadati, recuperando le informazioni necessarie dalla lettura dei documenti contenuti nel pacchetto. Durante la verifica del pacchetto il sistema raggruppa i file contenuti in unità documentarie e definisce il registro di conservazione in cui esse devono essere versate.
F003	Fatture elettroniche ricevute XML gestite dal sistema eIFE	Come avviene per il formato F003 si riferisce ai pacchetti costituiti dalle fatture elettroniche ricevute in formato XML e dalle relative notifiche quando questi documenti sono gestiti direttamente dal servizio erogato da Entaksi per l'invio al Sistema di Interscambio dei documenti e la gestione delle notifiche di ritorno.
F004	Pacchetti di versamento eDOC	Formato dismesso.
F005	PEC	Il formato F005 consente di versare in conservazione le PEC. L'indice di versamento viene creato automaticamente dal sistema, utilizzando le informazioni fornite dai metadati estratti dai documenti stessi e dal posizionamento convenzionale stabilito per costruire il file zip del PDV (una cartella per ogni casella PEC).

Formato	Contenuto	Descrizione
F006	Ordini elettronici	Formato per versare gli ordini ricevuti mediante il canale NSO. Pacchetti di questo tipo possono essere generati dal servizio eNSO, contenendo gli ordini ricevuti tramite il canale gestito da Entaksi, oppure ordini ricevuti mediante altri canali, nel caso il produttore voglia costruire autonomamente l'indice del pacchetto di versamento.
F997	Documenti analogici	Formato con il quale il produttore può versare dei documenti analogici, ovvero delle scansioni di documenti in formato PDF o PDF/A, per fare in modo che durante la validazione di questi PDV il sistema apponga la firma digitale necessaria alla validazione del documento informatico.
F998	Pacchetto precedente conservatore	Il formato F998 viene utilizzato per indicare i PDV provenienti da un altro conservatore.
F999	Pacchetto generico	Il formato F999 viene utilizzato per indicare i PDV che contengono un indice del pacchetto in cui sono indicati in maniera completa i metadati delle unità documentarie contenute nel pacchetto.

Altri formati del Pacchetto di Versamento possono essere stabiliti con il produttore nell'ambito delle Specificità del Contratto.

L'indice del Pacchetto di Versamento utilizzato nel formato F999 deve essere posizionato in un file `pdv.xml` e contenere le informazioni secondo la sintassi definita nello schema XSD seguente:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:dcterms="http://purl.org/dc/terms/"
xmlns="http://entaksi.eu/schemas/econ/1.0/" targetNamespace="http://entaksi.eu/schemas/econ/1.0/"
elementFormDefault="qualified" attributeFormDefault="unqualified">
    <xs:import namespace="http://purl.org/dc/terms/"
schemaLocation="http://dublincore.org/schemas/xmls/qdc/2008/02/11/dcterms.xsd"/>
    <xs:element name="pdv" type="pdvType"/>
    <xs:complexType name="dcAndMetadataType" abstract="true">
        <xs:sequence>
            <xs:element name="dc" type="dcterms:elementOrRefinementContainer"/>
            <xs:element name="metadata" type="metadataType" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="pdvType">
        <xs:complexContent>
            <xs:extension base="dcAndMetadataType">
                <xs:sequence>
                    <xs:element name="registro" type="registroType" minOccurs="0" maxOccurs="1"/>
                    <xs:element name="dataVersamento" type="xs:dateTime" minOccurs="1"
maxOccurs="1"/>
                    <xs:element name="formato" type="xs:string" minOccurs="1" maxOccurs="1"/>
                    <xs:element name="fileGroup" type="fileGroupType" minOccurs="1"
maxOccurs="unbounded"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="fileGroupType">
        <xs:complexContent>
            <xs:extension base="dcAndMetadataType">
                <xs:sequence>
                    <xs:element name="registro" type="registroType" minOccurs="0" maxOccurs="1"/>
```

```
                    <xs:element name="file" type="fileType" minOccurs="1" maxOccurs="unbounded"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="fileType">
        <xs:complexContent>
            <xs:extension base="dcAndMetadataType">
                <xs:sequence>
                    <xs:element name="esitoElaborazione" type="esitoElaborazioneType" minOccurs="1"
maxOccurs="1"/>
                    <xs:element name="errore" type="erroreType" minOccurs="0" maxOccurs="unbounded"
/>
                    <xs:element name="avvertenza" type="avvertenzaType" minOccurs="0"
maxOccurs="unbounded" />
                    <xs:element name="hashAlgorithm" type="hashAlgorithmType" minOccurs="1"
maxOccurs="1" />
                    <xs:element name="hashValue" type="xs:base64Binary" minOccurs="1" maxOccurs="1"
/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="hashAlgorithmType">
        <xs:simpleContent>
            <xs:extension base="xs:string">
                <xs:attribute name="canonicalXML" type="xs:boolean"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:complexType name="erroreType">
        <xs:simpleContent>
            <xs:extension base="xs:token">
                <xs:attribute name="codice" type="xs:string" use="required"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:complexType name="avvertenzaType">
        <xs:simpleContent>
            <xs:extension base="xs:token">
                <xs:attribute name="codice" type="xs:string" use="required"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:complexType name="metadataType">
        <xs:simpleContent>
            <xs:extension base="xs:token">
                <xs:attribute name="key" type="xs:string" use="required"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:simpleType name="esitoElaborazioneType">
        <xs:restriction base="xs:token">
            <xs:enumeration value="OK"/>
            <xs:enumeration value="KO"/>
        </xs:restriction>
    </xs:simpleType>
```

```
    <xs:simpleType name="registroType">
        <xs:restriction base="xs:anyURI"/>
    </xs:simpleType>
    <xs:simpleType name="TokenNonVuotoType">
        <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
        </xs:restriction>
    </xs:simpleType>
</xs:schema>
```

Quello che segue è un esempio di indice del Pacchetto di Versamento:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<pdv xmlns:terms="http://purl.org/dc/terms/" xmlns="http://entaksi.eu/schemas/econ/1.0/"
xmlns:dc="http://purl.org/dc/elements/1.1/">
    <dc>
        <terms:format>F999</terms:format>
        <terms:subject>Log del sistema</terms:subject>
    </dc>
    <dataVersamento>2022-01-09T02:00:00.402+01:00</dataVersamento>
    <formato>F999</formato>
    <fileGroup>
        <dc>
            <terms:subject>Log del sistema</terms:subject>
            <terms:type>log</terms:type>
        </dc>
        <metadata key="produttore:idfiscale">IT01621900479</metadata>
        <metadata key="produttore:ragionesociale">Entaksi Solutions SpA</metadata>
        <metadata key="documento:anno">2021</metadata>
        <metadata key="documento:tipo">meta</metadata>
        <metadata key="documento:sezionale">log</metadata>
        <metadata key="documento:data">2022-01-09</metadata>
        <metadata key="documento:datainizio">2021-12-01</metadata>
        <metadata key="documento:datatermine">2021-12-31</metadata>
        <metadata key="documento:formazione">d</metadata>
        <registro>urn:entaksi:IT01621900479:_default:reg:2021:meta:log</registro>
        <file>
            <dc>
                <terms:title>pdalog-2021-12-2022-01-09.csv</terms:title>
                <terms:format>text/csv</terms:format>
            </dc>
        </file>
    </fileGroup>
    <fileGroup>
        <dc>
            <terms:subject>Log del sistema</terms:subject>
            <terms:type>log</terms:type>
        </dc>
        <metadata key="produttore:idfiscale">IT01621900479</metadata>
        <metadata key="produttore:ragionesociale">Entaksi Solutions SpA</metadata>
        <metadata key="documento:anno">2021</metadata>
        <metadata key="documento:tipo">meta</metadata>
        <metadata key="documento:sezionale">log</metadata>
        <metadata key="documento:data">2022-01-09</metadata>
        <metadata key="documento:datainizio">2021-12-01</metadata>
        <metadata key="documento:datatermine">2021-12-31</metadata>
        <metadata key="documento:formazione">d</metadata>
        <registro>urn:entaksi:IT01621900479:_default:reg:2021:meta:log</registro>
        <file>
            <dc>
                <terms:title>pddlog-2021-12-2022-01-09.csv</terms:title>
                <terms:format>text/csv</terms:format>
            </dc>
            <hashAlgorithm canonicalXML="false">SHA256</hashAlgorithm>
            <hashValue>e7z6BsQl86e+DV8JvHAXa4W21sY8m77z5t5NazsKlbA=</hashValue>
        </file>
    </fileGroup>
</pdv>
```

La seguente tabella definisce la modalità di compilazione dei punti annotati nel listato precedente:

Tabella 18. Elementi dell'indice del Pacchetto di Versamento.

Elemento	Contenuto richiesto
/pdv/dc	Questo elemento contiene i metadati Dublin Core del PDV.
/pdv/formato	Indica il formato di validazione del PDV.
/pdv/fileGroup	Dichiara una unità documentaria, può essere ripetuto più volte.
/pdv/fileGroup/dc	Contiene i metadati Dublin Core dell'unità documentaria.
/pdv/fileGroup/metadata	I metadati chiave/valore dell'unità documentaria.
/pdv/fileGroup/registro	L'URN del registro in cui deve essere archiviata l'unità documentaria, così come definito nella tabella "Sintassi degli URN per gli oggetti rappresentati nel sistema".
/pdv/fileGroup/file	Dichiara un file dell'unità documentaria e può essere ripetuto più volte. Il primo file è considerato il file principale dell'unità, i seguenti sono considerati allegati.
/pdv/fileGroup/file/dc	Metadati Dublin Core relativi al file.
/pdv/fileGroup/file/hashValue	Riporta l'impronta del file rappresentata con la codifica Base64. Il tag hashAlgorithm definisce l'algoritmo usato per calcolare l'impronta.

Torna all'indice.

6.3. Pacchetto di Archiviazione (PDA)

Il pacchetto di archiviazione (PDA), composto dalle unità documentarie provenienti da uno o più PDV, è un'entità logica che contiene un numero variabile di unità documentarie ed un file indice che viene firmato digitalmente e marcato temporalmente dal Responsabile del Servizio di Conservazione. Questo file indice costituisce la prova di archiviazione delle unità archivistiche contenute.

L'indice del PDA è un file in formato XML che riporta, per ognuna delle unità documentarie contenute, alcune informazioni tra cui l'identificativo univoco assegnato secondo il codice URN definito nella tabella "Sintassi degli URN per gli oggetti rappresentati nel sistema", e, per ogni file, un'impronta digitale (hash) e l'algoritmo con cui è stata calcolata questa impronta digitale.

La modalità di conservazione mediante indice permette di verificare l'integrità di ogni singolo file, a prescindere da tutti gli altri file conservati nello stesso blocco. Infatti sarà sufficiente essere in possesso del file per poter eseguire l'algoritmo di hash sul suo contenuto e confrontare l'impronta ricalcolata con la stringa riportata nell'indice.

La soluzione adottata da Entaksi utilizza lo standard UNI 11386:2020 – Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali, definito anche SinCRO, per il formato dell'indice del Pacchetto di Archiviazione.

All'interno della sottocommissione DIAM/SC11 (Gestione dei documenti archivistici) dell'Ente Nazionale Italiano di Unificazione (UNI), un apposito gruppo di lavoro denominato SInCRO ha definito la struttura dell'insieme dei dati a supporto del processo di conservazione individuando gli elementi informativi necessari alla creazione di un Indice di Conservazione ("file di chiusura").

L'implementazione di tale indice, del quale SInCRO ha descritto sia la semantica sia l'articolazione, permette di utilizzare una struttura dati condivisa e raggiungere un soddisfacente grado d'interoperabilità nei processi di migrazione, mediante l'adozione di uno Schema XML appositamente elaborato.

Lo schema dell'indice del pacchetto di archiviazione definito nello standard UNI 11386:2020 comprende quattro punti di estensione, in cui la soluzione di archiviazione può inserire informazioni supplementari secondo uno schema personalizzato.

- **Informazioni supplementari sulla descrizione del pacchetto** (`SelfDescription/MoreInfo`). In questa sezione vengono riportati i riferimenti ai pacchetti di versamento da cui provengono i dati archiviati.

- **Informazioni supplementari sul contenuto del pacchetto** (`VdC/MoreInfo`). In questa sezione vengono riportati i metadati che caratterizzano il pacchetto di archiviazione.
- **Informazioni supplementari sulle singole unità archivistiche** (`FileGroup/MoreInfo`). In questa sezione vengono riportati i metadati dell'unità archivistica.
- **Informazioni supplementari sui singoli file** (`File/MoreInfo`). In questa sezione vengono riportati i metadati del singolo file dell'unità archivistica.

Il sistema utilizza la modalità embedded per rappresentare i metadati all'interno delle sezioni MoreInfo dell'indice, perciò in ciascuno degli elementi MoreInfo è incluso un tag EmbeddedMetadata (definita dallo schema SInCRO) che a sua volta include una tag customMetadata (definita dal sistema di conservazione) il cui formato aderisce al seguente schema XSD:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:dcterms="http://purl.org/dc/terms/"
xmlns="http://entaksi.eu/schemas/econ/1.0/" targetNamespace="http://entaksi.eu/schemas/econ/1.0/"
elementFormDefault="qualified" attributeFormDefault="unqualified">
    <xs:import namespace="http://purl.org/dc/terms/"
schemaLocation="http://dublincore.org/schemas/xmls/qdc/2008/02/11/dcterms.xsd"/>
    <xs:element name="pdv" type="pdvType"/>
    <xs:complexType name="dcAndMetadataType" abstract="true">
        <xs:sequence>
            <xs:element name="dc" type="dcterms:elementOrRefinementContainer"/>
            <xs:element name="metadata" type="metadataType" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="pdvType">
        <xs:complexContent>
            <xs:extension base="dcAndMetadataType">
                <xs:sequence>
                    <xs:element name="registro" type="registroType" minOccurs="0" maxOccurs="1"/>
                    <xs:element name="dataVersamento" type="xs:dateTime" minOccurs="1"
maxOccurs="1"/>
                    <xs:element name="formato" type="xs:string" minOccurs="1" maxOccurs="1"/>
                    <xs:element name="fileGroup" type="fileGroupType" minOccurs="1"
maxOccurs="unbounded"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="fileGroupType">
        <xs:complexContent>
            <xs:extension base="dcAndMetadataType">
                <xs:sequence>
                    <xs:element name="registro" type="registroType" minOccurs="0" maxOccurs="1"/>
                    <xs:element name="file" type="fileType" minOccurs="1" maxOccurs="unbounded"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="fileType">
        <xs:complexContent>
            <xs:extension base="dcAndMetadataType">
                <xs:sequence>
                    <xs:element name="esitoElaborazione" type="esitoElaborazioneType" minOccurs="1"
maxOccurs="1"/>
                    <xs:element name="errore" type="erroreType" minOccurs="0" maxOccurs="unbounded"
/>
                    <xs:element name="avvertenza" type="avvertenzaType" minOccurs="0"
```

```
maxOccurs="unbounded" />
                    <xs:element name="hashAlgorithm" type="hashAlgorithmType" minOccurs="1"
maxOccurs="1" />
                    <xs:element name="hashValue" type="xs:base64Binary" minOccurs="1" maxOccurs="1"
/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="hashAlgorithmType">
        <xs:simpleContent>
            <xs:extension base="xs:string">
                <xs:attribute name="canonicalXML" type="xs:boolean"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:complexType name="erroreType">
        <xs:simpleContent>
            <xs:extension base="xs:token">
                <xs:attribute name="codice" type="xs:string" use="required"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:complexType name="avvertenzaType">
        <xs:simpleContent>
            <xs:extension base="xs:token">
                <xs:attribute name="codice" type="xs:string" use="required"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:complexType name="metadataType">
        <xs:simpleContent>
            <xs:extension base="xs:token">
                <xs:attribute name="key" type="xs:string" use="required"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:simpleType name="esitoElaborazioneType">
        <xs:restriction base="xs:token">
            <xs:enumeration value="OK"/>
            <xs:enumeration value="KO"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="registroType">
        <xs:restriction base="xs:anyURI"/>
    </xs:simpleType>
    <xs:simpleType name="TokenNonVuotoType">
        <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
        </xs:restriction>
    </xs:simpleType>
</xs:schema>
```

Quello che segue è un esempio di indice del Pacchetto di Archiviazione utilizzato fino al 31/12/2021:

```
<?xml version="1.0" encoding="UTF-8"?>
<sincro:IdC xmlns:sincro="http://www.uni.com/U3011/sincro/"
sincro:url="http://www.uni.com/U3011/sincro/" sincro:version="1.0">
    <sincro:SelfDescription>
        <sincro:ID
sincro:scheme="local">urn:entaksi:IT01621900479:_default:reg:2015:D5802:_default:pda:1</sincro:ID>
        <sincro:CreatingApplication>
            <sincro:Name>eCon</sincro:Name>
            <sincro:Version>1.0.8</sincro:Version>
            <sincro:Producer>Entaksi Solutions Srl</sincro:Producer>
        </sincro:CreatingApplication>
        <sincro:MoreInfo sincro:XMLScheme="https://entaksi.eu/schemas/econ/1.0/econ.xsd">
            <sincro:EmbeddedMetadata>
                <econ:customMetadata xmlns:econ="http://entaksi.eu/schemas/econ/1.0/"
xmlns="http://entaksi.eu/schemas/econ/1.0/" xmlns:terms="http://purl.org/dc/terms/">
                    <dc xmlns="http://entaksi.eu/schemas/econ/1.0/"/>
                </econ:customMetadata>
            </sincro:EmbeddedMetadata>
        </sincro:MoreInfo>
    </sincro:SelfDescription>
    <sincro:VdC>
        <sincro:ID
sincro:scheme="local">urn:entaksi:IT01621900479:_default:reg:2015:D5802:_default:pda:1</sincro:ID>
        <sincro:MoreInfo sincro:XMLScheme="https://entaksi.eu/schemas/econ/1.0/econ.xsd">
            <sincro:EmbeddedMetadata>
                <econ:customMetadata xmlns:econ="http://entaksi.eu/schemas/econ/1.0/"
xmlns="http://entaksi.eu/schemas/econ/1.0/" xmlns:terms="http://purl.org/dc/terms/">
                    <dc xmlns="http://entaksi.eu/schemas/econ/1.0/">

<terms:identifier>urn:entaksi:IT01621900479:_default:reg:2015:D5802:_default:pda:1</terms:identifier
>
                        <terms:subject>Pacchetto di archiviazione numero 1 per il registro 2015
D5802 _default</terms:subject>
                    </dc>
                </econ:customMetadata>
            </sincro:EmbeddedMetadata>
        </sincro:MoreInfo>
    </sincro:VdC>
    <sincro:FileGroup>
        <sincro:Label>Documento 1</sincro:Label>
        <sincro:File sincro:encoding="binary" sincro:format="application/pdf">
            <sincro:ID sincro:scheme="local"/>
            <sincro:Path>1.0_Documento1.pdf</sincro:Path>
            <sincro:Hash sincro:canonicalXML="false"
sincro:function="SHA256">cSWcshKnIZoHH37nZAH0DjiJqUxtRrYu4q8LQHi//hE=</sincro:Hash>
            <sincro:MoreInfo sincro:XMLScheme="https://entaksi.eu/schemas/econ/1.0/econ.xsd">
                <sincro:EmbeddedMetadata>
                    <econ:customMetadata xmlns:econ="http://entaksi.eu/schemas/econ/1.0/"
xmlns="http://entaksi.eu/schemas/econ/1.0/" xmlns:terms="http://purl.org/dc/terms/">
                        <dc xmlns="http://entaksi.eu/schemas/econ/1.0/">
                            <terms:title>Documento1.pdf</terms:title>
                            <terms:format>application/pdf</terms:format>
                            <terms:extent>111989 bytes</terms:extent>
                            <terms:type>Descrizione del documento</terms:type>
                        </dc>
```

```
                    </econ:customMetadata>
                </sincro:EmbeddedMetadata>
            </sincro:MoreInfo>
        </sincro:File>
        <sincro:MoreInfo sincro:XMLScheme="https://entaksi.eu/schemas/econ/1.0/econ.xsd">
            <sincro:EmbeddedMetadata>
                <econ:customMetadata xmlns:econ="http://entaksi.eu/schemas/econ/1.0/"
xmlns="http://entaksi.eu/schemas/econ/1.0/" xmlns:terms="http://purl.org/dc/terms/">
                    <dc xmlns="http://entaksi.eu/schemas/econ/1.0/">

<terms:identifier>urn:entaksi:IT01621900479:_default:reg:2015:D5802:_default:doc:1</terms:identifier
>
                        <terms:type>Tipo di documento</terms:type>
                        <terms:subject>Descrizione del documento 1</terms:subject>
                    </dc>
                    <metadata xmlns="http://entaksi.eu/schemas/econ/1.0/"
key="produttore:idfiscale">IT01621900479</metadata>
                    <metadata xmlns="http://entaksi.eu/schemas/econ/1.0/"
key="produttore:ragionesociale">Entaksi Solutions srl</metadata>
                    <metadata xmlns="http://entaksi.eu/schemas/econ/1.0/"
key="destinatario:idfiscale">IT01621900479</metadata>
                    <metadata xmlns="http://entaksi.eu/schemas/econ/1.0/"
key="destinatario:ragionesociale">Entaksi Solutions srl</metadata>
                    <metadata xmlns="http://entaksi.eu/schemas/econ/1.0/"
key="documento:anno">2015</metadata>
                    <metadata xmlns="http://entaksi.eu/schemas/econ/1.0/"
key="documento:sezionale">_default</metadata>
                    <metadata xmlns="http://entaksi.eu/schemas/econ/1.0/"
key="documento:numero">1</metadata>
                    <metadata xmlns="http://entaksi.eu/schemas/econ/1.0/" key="documento:data">2015-
12-23</metadata>
                </econ:customMetadata>
            </sincro:EmbeddedMetadata>
        </sincro:MoreInfo>
    </sincro:FileGroup>
    <sincro:Process>
        <sincro:Agent sincro:role="PreservationManager" sincro:type="organization">
            <sincro:AgentName>
                <sincro:FormalName>Entaksi Solutions Srl</sincro:FormalName>
            </sincro:AgentName>
            <sincro:Agent_ID sincro:scheme="VATRegistrationNumber">IT:01621900479</sincro:Agent_ID>
        </sincro:Agent>
        <sincro:TimeReference>
            <sincro:TimeInfo>2016-01-07T09:40:15.208+01:00</sincro:TimeInfo>
        </sincro:TimeReference>
        <sincro:LawAndRegulations sincro:language="it">DLgs 7/03/2005 n. 82 (CAD), DPCM 3/12/2013,
DMEF 17/06/2014, DPCM 13/11/2014</sincro:LawAndRegulations>
    </sincro:Process>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">...</ds:Signature>
</sincro:IdC>
```

Qui invece viene riportato un esempio di indice del PDA in utilizzo dal 01/01/2022:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<ns1:PIndex xmlns:ns1="http://www.uni.com/U3011/sincro-v2/" ns1:sincroVersion="2.0"
ns1:uri="http://www.uni.com/U3011/sincro-v2/">
    <ns1:SelfDescription>
        <ns1:ID
ns1:scheme="entaksi">urn:entaksi:IT01621900479:_default:reg:2021:D8501:eCon:pda:1</ns1:ID>
        <ns1:CreatingApplication>
            <ns1:Name>eCon</ns1:Name>
            <ns1:Version>1.22.0</ns1:Version>
            <ns1:Producer>Entaksi Solutions SpA</ns1:Producer>
        </ns1:CreatingApplication>
        <ns1:MoreInfo ns1:xmlSchema="https://entaksi.eu/schemas/econ/1.0/econ.xsd">
            <ns1:EmbeddedMetadata>
                <econ:customMetadata xmlns="http://entaksi.eu/schemas/econ/1.0/"
xmlns:econ="http://entaksi.eu/schemas/econ/1.0/" xmlns:terms="http://purl.org/dc/terms/">
                    <dc>
                        <terms:source>urn:entaksi:IT01621900479:_default:pdv:22105</terms:source>
                    </dc>
                </econ:customMetadata>
            </ns1:EmbeddedMetadata>
        </ns1:MoreInfo>
    </ns1:SelfDescription>
    <ns1:PVolume>
        <ns1:ID
ns1:scheme="entaksi">urn:entaksi:IT01621900479:_default:reg:2021:D8501:eCon:pda:1</ns1:ID>
        <ns1:MoreInfo ns1:xmlSchema="https://entaksi.eu/schemas/econ/1.0/econ.xsd">
            <ns1:EmbeddedMetadata>
                <econ:customMetadata xmlns="http://entaksi.eu/schemas/econ/1.0/"
xmlns:econ="http://entaksi.eu/schemas/econ/1.0/" xmlns:terms="http://purl.org/dc/terms/">
                    <dc>

<terms:identifier>urn:entaksi:IT01621900479:_default:reg:2021:D8501:eCon:pda:1</terms:identifier>
                        <terms:subject>Pacchetto di archiviazione numero 1 per il registro 2021
D8501 eCon</terms:subject>

<terms:identifier>urn:entaksi:IT01621900479:_default:reg:2021:D8501:eCon:pda:1</terms:identifier>
                        <terms:subject>Pacchetto di archiviazione numero 1 per il registro 2021
D8501 eCon</terms:subject>
                    </dc>
                </econ:customMetadata>
            </ns1:EmbeddedMetadata>
        </ns1:MoreInfo>
    </ns1:PVolume>
    <ns1:FileGroup>
        <ns1:Label>Contratto cliente 1</ns1:Label>
        <ns1:File ns1:encoding="binary" ns1:format="application/pdf">
            <ns1:ID ns1:scheme="entaksi">00O3FJ255J0000006009</ns1:ID>
            <ns1:Path>1.0_documento1.pdf</ns1:Path>
            <ns1:Hash ns1:canonicalXML="false"
ns1:hashFunction="SHA256">K2Pd79uX6bnklJ9u8OxZwsx20gj1brAqYMpjnaXQxFs=</ns1:Hash>
            <ns1:MoreInfo ns1:xmlSchema="https://entaksi.eu/schemas/econ/1.0/econ.xsd">
                <ns1:EmbeddedMetadata>
                    <econ:customMetadata xmlns="http://entaksi.eu/schemas/econ/1.0/"
xmlns:econ="http://entaksi.eu/schemas/econ/1.0/" xmlns:terms="http://purl.org/dc/terms/">
                        <dc>
```

```
                        <terms:title>documento1.pdf</terms:title>

<terms:source>urn:entaksi:IT01621900479:_default:pdv:22105:documento1.pdf</terms:source>
                        <terms:extent>39047 bytes</terms:extent>
                        <terms:isPartOf>00O3FJ255J000000606R</terms:isPartOf>
                    </dc>
                </econ:customMetadata>
            </ns1:EmbeddedMetadata>
        </ns1:MoreInfo>
    </ns1:File>
    <ns1:MoreInfo ns1:xmlSchema="https://entaksi.eu/schemas/econ/1.0/econ.xsd">
        <ns1:EmbeddedMetadata>
            <econ:customMetadata xmlns="http://entaksi.eu/schemas/econ/1.0/"
xmlns:econ="http://entaksi.eu/schemas/econ/1.0/" xmlns:terms="http://purl.org/dc/terms/">
                <dc>
                    <terms:type>Contratto</terms:type>
                    <terms:accessRights>riservato</terms:accessRights>
                    <terms:identifier>00O3FJ255J000000606R</terms:identifier>
                </dc>
                <metadata key="documento:anno">2021</metadata>
                <metadata key="documento:tipo">D8501</metadata>
                <metadata key="documento:sezionale">eCon</metadata>
                <metadata key="documento:data">2021-11-25</metadata>
                <metadata key="documento:conservazione">20</metadata>
                <metadata key="documento:flusso">interno</metadata>
                <metadata key="documento:tiporegistro">nessuno</metadata>
                <metadata key="documento:numero">1</metadata>
                <metadata key="produttore:idfiscale">IT01621900479</metadata>
                <metadata key="produttore:ragionesociale">Entaksi Solutions SpA</metadata>
                <metadata key="produttore:tipo">PG</metadata>
                <metadata key="destinatario:idfiscale">IT01621900479</metadata>
                <metadata key="destinatario:ragionesociale">Entaksi Solutions SpA</metadata>
                <metadata key="destinatario:tipo">PG</metadata>
                <metadata key="modifica:numero">1</metadata>
            </econ:customMetadata>
        </ns1:EmbeddedMetadata>
    </ns1:MoreInfo>
</ns1:FileGroup>
<ns1:FileGroup>
    <ns1:Label>Contratto cliente 2</ns1:Label>
    <ns1:File ns1:encoding="binary" ns1:format="application/pdf">
        <ns1:ID ns1:scheme="entaksi">00O3FJ255J000000C007</ns1:ID>
        <ns1:Path>2.0_documento2.pdf</ns1:Path>
        <ns1:Hash ns1:canonicalXML="false"
ns1:hashFunction="SHA256">xKPPvdT2TjZzS04Rn2Psvyel1rv4ecrMnZsDcBBbpA8=</ns1:Hash>
        <ns1:MoreInfo ns1:xmlSchema="https://entaksi.eu/schemas/econ/1.0/econ.xsd">
            <ns1:EmbeddedMetadata>
                <econ:customMetadata xmlns="http://entaksi.eu/schemas/econ/1.0/"
xmlns:econ="http://entaksi.eu/schemas/econ/1.0/" xmlns:terms="http://purl.org/dc/terms/">
                    <dc>
                        <terms:title>documento2.pdf</terms:title>

<terms:source>urn:entaksi:IT01621900479:_default:pdv:22105:documento2.pdf</terms:source>
                        <terms:extent>39067 bytes</terms:extent>
                        <terms:isPartOf>00O3FJ255J000000C06P</terms:isPartOf>
                    </dc>
                </econ:customMetadata>
```

```
                </ns1:EmbeddedMetadata>
            </ns1:MoreInfo>
        </ns1:File>
        <ns1:MoreInfo ns1:xmlSchema="https://entaksi.eu/schemas/econ/1.0/econ.xsd">
            <ns1:EmbeddedMetadata>
                <econ:customMetadata xmlns="http://entaksi.eu/schemas/econ/1.0/"
xmlns:econ="http://entaksi.eu/schemas/econ/1.0/" xmlns:terms="http://purl.org/dc/terms/">
                    <dc>
                        <terms:type>Contratto</terms:type>
                        <terms:accessRights>riservato</terms:accessRights>
                        <terms:identifier>00O3FJ255J000000C06P</terms:identifier>
                    </dc>
                    <metadata key="documento:anno">2021</metadata>
                    <metadata key="documento:tipo">D8501</metadata>
                    <metadata key="documento:sezionale">eCon</metadata>
                    <metadata key="documento:data">2021-12-04</metadata>
                    <metadata key="documento:conservazione">20</metadata>
                    <metadata key="documento:flusso">interno</metadata>
                    <metadata key="documento:tiporegistro">nessuno</metadata>
                    <metadata key="documento:numero">2</metadata>
                    <metadata key="produttore:idfiscale">IT01621900479</metadata>
                    <metadata key="produttore:ragionesociale">Entaksi Solutions SpA</metadata>
                    <metadata key="produttore:tipo">PG</metadata>
                    <metadata key="destinatario:idfiscale">IT01621900479</metadata>
                    <metadata key="destinatario:ragionesociale">Entaksi Solutions SpA</metadata>
                    <metadata key="destinatario:tipo">PG</metadata>
                    <metadata key="modifica:numero">1</metadata>
                </econ:customMetadata>
            </ns1:EmbeddedMetadata>
        </ns1:MoreInfo>
    </ns1:FileGroup>
    <ns1:FileGroup>
        <ns1:Label>Contratto cliente 3</ns1:Label>
        <ns1:File ns1:encoding="binary" ns1:format="application/pdf">
            <ns1:ID ns1:scheme="entaksi">00O3FJ255J000000I008</ns1:ID>
            <ns1:Path>3.0_documento3.pdf</ns1:Path>
            <ns1:Hash ns1:canonicalXML="false"
ns1:hashFunction="SHA256">fqYsZ/buJAiYFCcp6NXWDoNW4vX0+oLUVW2YI15T2D8=</ns1:Hash>
            <ns1:MoreInfo ns1:xmlSchema="https://entaksi.eu/schemas/econ/1.0/econ.xsd">
                <ns1:EmbeddedMetadata>
                    <econ:customMetadata xmlns="http://entaksi.eu/schemas/econ/1.0/"
xmlns:econ="http://entaksi.eu/schemas/econ/1.0/" xmlns:terms="http://purl.org/dc/terms/">
                        <dc>
                            <terms:title>documento3.pdf</terms:title>

<terms:source>urn:entaksi:IT01621900479:_default:pdv:22105:documento3.pdf</terms:source>
                            <terms:extent>39167 bytes</terms:extent>
                            <terms:isPartOf>00O3FJ255J000000I06Q</terms:isPartOf>
                        </dc>
                    </econ:customMetadata>
                </ns1:EmbeddedMetadata>
            </ns1:MoreInfo>
        </ns1:File>
        <ns1:MoreInfo ns1:xmlSchema="https://entaksi.eu/schemas/econ/1.0/econ.xsd">
            <ns1:EmbeddedMetadata>
                <econ:customMetadata xmlns="http://entaksi.eu/schemas/econ/1.0/"
xmlns:econ="http://entaksi.eu/schemas/econ/1.0/" xmlns:terms="http://purl.org/dc/terms/">
```

```
                    <dc>
                        <terms:type>Contratto</terms:type>
                        <terms:accessRights>riservato</terms:accessRights>
                        <terms:identifier>00O3FJ255J000000I06Q</terms:identifier>
                    </dc>
                    <metadata key="documento:anno">2021</metadata>
                    <metadata key="documento:tipo">D8501</metadata>
                    <metadata key="documento:sezionale">eCon</metadata>
                    <metadata key="documento:data">2021-12-04</metadata>
                    <metadata key="documento:conservazione">20</metadata>
                    <metadata key="documento:flusso">interno</metadata>
                    <metadata key="documento:tiporegistro">nessuno</metadata>
                    <metadata key="documento:numero">3</metadata>
                    <metadata key="produttore:idfiscale">IT01621900479</metadata>
                    <metadata key="produttore:ragionesociale">Entaksi Solutions SpA</metadata>
                    <metadata key="produttore:tipo">PG</metadata>
                    <metadata key="destinatario:idfiscale">IT01621900479</metadata>
                    <metadata key="destinatario:ragionesociale">Entaksi Solutions SpA</metadata>
                    <metadata key="destinatario:tipo">PG</metadata>
                    <metadata key="modifica:numero">1</metadata>
                </econ:customMetadata>
            </ns1:EmbeddedMetadata>
        </ns1:MoreInfo>
    </ns1:FileGroup>
    <ns1:Process>
        <ns1:Submitter ns1:agentType="legal person">
            <ns1:AgentID ns1:nameRegistrationAuthority="Agenzia delle Entrate">VATIT-
01621900479</ns1:AgentID>
            <ns1:AgentName>
                <ns1:FormalName>ENTAKSI SOLUTIONS SPA</ns1:FormalName>
            </ns1:AgentName>
        </ns1:Submitter>
        <ns1:Holder ns1:agentType="legal person">
            <ns1:AgentID ns1:nameRegistrationAuthority="Agenzia delle Entrate">VATIT-
01621900479</ns1:AgentID>
            <ns1:AgentName>
                <ns1:FormalName>ENTAKSI SOLUTIONS SPA</ns1:FormalName>
            </ns1:AgentName>
        </ns1:Holder>
        <ns1:AuthorizedSigner ns1:agentType="natural person">
            <ns1:AgentID ns1:nameRegistrationAuthority="Agenzia delle Entrate">TINIT-
GRELSN54M15H980H</ns1:AgentID>
            <ns1:AgentName>
                <ns1:NameAndSurname>
                    <ns1:FirstName>Alessandro</ns1:FirstName>
                    <ns1:LastName>Geri</ns1:LastName>
                </ns1:NameAndSurname>
            </ns1:AgentName>
        </ns1:AuthorizedSigner>
        <ns1:AuthorizedSigner ns1:agentType="natural person">
            <ns1:AgentID ns1:nameRegistrationAuthority="Agenzia delle Entrate">TINIT-
TRVSFN67H13D612A</ns1:AgentID>
            <ns1:AgentName>
                <ns1:NameAndSurname>
                    <ns1:FirstName>Stefano</ns1:FirstName>
                    <ns1:LastName>Travelli</ns1:LastName>
                </ns1:NameAndSurname>
```

```
            </ns1:AgentName>
        </ns1:AuthorizedSigner>
        <ns1:AuthorizedSigner ns1:agentType="natural person">
            <ns1:AgentID ns1:nameRegistrationAuthority="Agenzia delle Entrate">TINIT-
SCCLSS87L70L113N</ns1:AgentID>
            <ns1:AgentName>
                <ns1:NameAndSurname>
                    <ns1:FirstName>Alessia</ns1:FirstName>
                    <ns1:LastName>Soccio</ns1:LastName>
                </ns1:NameAndSurname>
            </ns1:AgentName>
        </ns1:AuthorizedSigner>
        <ns1:AuthorizedSigner ns1:agentType="natural person">
            <ns1:AgentID ns1:nameRegistrationAuthority="Agenzia delle Entrate">TINIT-
RCCLGU85S19I483V</ns1:AgentID>
            <ns1:AgentName>
                <ns1:NameAndSurname>
                    <ns1:FirstName>Luigi</ns1:FirstName>
                    <ns1:LastName>Ruocco</ns1:LastName>
                </ns1:NameAndSurname>
            </ns1:AgentName>
        </ns1:AuthorizedSigner>
        <ns1:TimeReference>
            <ns1:TimeInfo ns1:attachedTimeStamp="false">2021-12-05T12:48:56.728+01:00</ns1:TimeInfo>
        </ns1:TimeReference>
        <ns1:LawsAndRegulations>Linee Guida sulla formazione, gestione e conservazione dei documenti
informatici, DL 07/03/2005 n.82, DMEF 17/06/2014, GDPR 2016/679</ns1:LawsAndRegulations>
    </ns1:Process>
</ns1:PIndex>
```

Il file indice del Pacchetto di Archiviazione è firmato con firma digitale e marca temporale dal Responsabile del Servizio di Conservazione utilizzando lo standard XaDES-T.

Torna all'indice.

6.4. Pacchetto di Distribuzione (PDD)

Il sistema permette all'utente la ricerca e l'estrazione degli oggetti conservati al fine della visualizzazione o della distribuzione degli stessi tramite Pacchetti di Distribuzione (PDD).

In base ai criteri di selezione dei documenti il Pacchetto di Distribuzione viene assemblato dal sistema di conservazione includendo:

- le unità documentarie all'interno dell'archivio corrispondenti ai criteri di selezione;
- l'insieme delle prove di conservazione delle unità documentarie selezionate (cioè gli indici firmati dei PDA in cui sono contenute).

Il Pacchetto di Distribuzione viene reso disponibile sotto forma di un file ZIP contenente:

- un indice di distribuzione firmato digitalmente dal Responsabile del Servizio di Conservazione, che costituisce anche il rapporto di distribuzione;
- le unità documentarie corrispondenti ai criteri di selezione;
- l'insieme delle prove di conservazione.

L'Utente può effettuare sul sistema una ricerca massiva, con produzione di uno o più PDD che vengono messi a disposizione per il download esclusivamente da parte dell'utente che li ha richiesti o eventualmente veicolati tramite le modalità definite tra l'utente e il Responsabile del Servizio di Conservazione.

Il Pacchetto di Distribuzione rimane disponibile per il download per un periodo di tempo concordato tra l'utente e il Responsabile del Servizio di Conservazione, prima di essere scartati.

L'indice del pacchetto di distribuzione utilizza lo stesso formato SinCRO utilizzato per l'indice del pacchetto di archiviazione descritto nel paragrafo Pacchetto di Archiviazione (PDA), incluse le definizioni relative ai tag `MoreInfo` presenti nel formato.

Torna all'indice.

7. Processo di conservazione

Il **processo di conservazione** dei documenti informatici è costituito da diverse fasi, che coinvolgono il Produttore, l'azienda e gli eventuali Utenti terzi. Di seguito viene riportato lo schema generale del processo di conservazione, con la descrizione delle varie fasi che attraversano i documenti, dal versamento alla conservazione permanente. Il sistema viene definito, qui e nei capitoli successivi, sia dal punto di vista logico, corredato da spiegazioni generali del processo, sia dal punto di vista fisico, per esplicare come viene garantita l'originalità dei documenti e la loro conservazione a lungo termine.

Il *workflow* dell'intero processo gestionale che sfocia nella conservazione è riportato nello schema seguente:

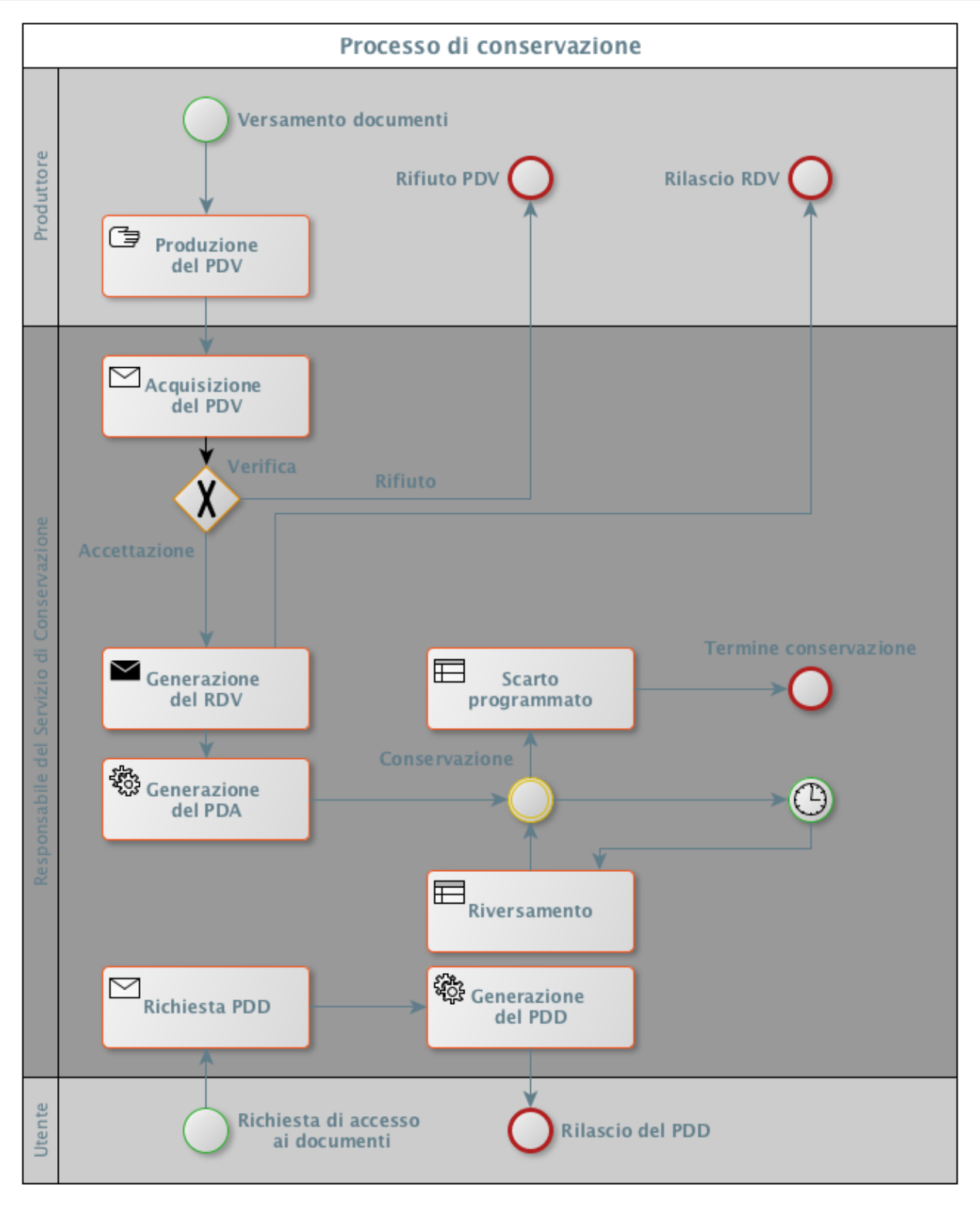

Figura 7. Workflow del processo di conservazione.

In fase di versamento dovranno essere definiti a cura del Produttore i metadati previsti nell'allegato 5 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, in modo da consentire la ricerca del documento per uno di questi campi oppure per loro associazioni logiche.

L'archivio è realizzato mediante un sistema di cartelle ben definito in cui vengono registrate tutte le informazioni che lo compongono inclusi i file dei metadati, gli indici e i documenti informatici conservati, organizzati secondo lo schema OAIS (pacchetti di versamento, di archiviazione e di distribuzione). L'insieme di questi dati risiede in un file system distribuito e

ridondato che garantisce la scalabilità e la durabilità dei dati.

Su questo archivio opera il software di gestione del sistema che, sulla base dei dati e della loro organizzazione, gestisce gli indici e la catalogazione dei documenti, garantisce l'accesso con la possibilità di fruire delle funzionalità avanzate di ricerca e sovrintende all'esecuzione di tutte le procedure di elaborazione previste, a partire da quelle di immissione dei documenti e di formazione dei pacchetti di archiviazione.

Operativamente, l'archivio è costituito da più istanze in cluster del software di gestione che agiscono sui dati contenuti nella struttura di cartelle.

L'attivazione del Servizio di Conservazione per ogni Produttore viene finalizzata al termine di un processo di configurazione che segue questi fasi fondamentali:

1. Condivisione delle informazioni tecniche di richiesta configurazione dei PDV: questa fase comprende la definizione di dettaglio dei PDV che il Produttore invierà al sistema e i controlli che verranno attivati.
2. Consolidamento delle informazioni tecniche propedeutiche all'attivazione del Servizio (tipologie documentali da gestire, metadati, modalità di trasmissione dei dati) in accordo con il Produttore.
3. Validazione delle configurazioni da parte del Responsabile del Servizio di Conservazione, del Responsabile dei Sistemi Informativi e del Responsabile dello Sviluppo e della Manutenzione.
4. Configurazione dell'ambiente di test.
5. Ricezione ed elaborazione dei PDV da conservare in ambiente di test.
6. Configurazione ambiente di produzione e start-up del servizio.
7. Definizione dei canali di comunicazione per la ricezione dei PDV e l'invio dei rapporti di versamento.

Ognuna delle fasi sopra indicate viene eseguita per ogni tipologia di configurazione e tipologia documentale richiesta.

Nella fase di attivazione del servizio vengono definiti i canali utilizzati per lo scambio informativo tra Produttore e Conservatore. Tali canali avranno opportune caratteristiche di sicurezza e identificazione dell'utente che sta operando sul sistema.

Torna all'indice.

7.1. Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico

I Pacchetti di Versamento, formati come descritto nel paragrafo Pacchetto di Versamento (PDV), vengono sottoposti ad un processo di validazione che ne verifica l'integrità e la corrispondenza ai requisiti concordati tra il Cliente, il Responsabile del Servizio di Conservazione e il Responsabile dei Sistemi Informativi.

I Pacchetti di Versamento sono caricati nel sistema di conservazione tramite una connessione HTTPS protetta da un certificato rilasciato da una autorità di certificazione verificabile con le versioni più recenti dei moderni browser.

L'operazione di caricamento avviene previa autenticazione delle credenziali dell'utente che deve essere riconducibile al produttore del Pacchetto di Versamento.

Il seguente diagramma sintetizza il flusso di lavoro di un Pacchetto di Versamento dove alcune delle fasi sono meglio descritte nei successivi paragrafi:

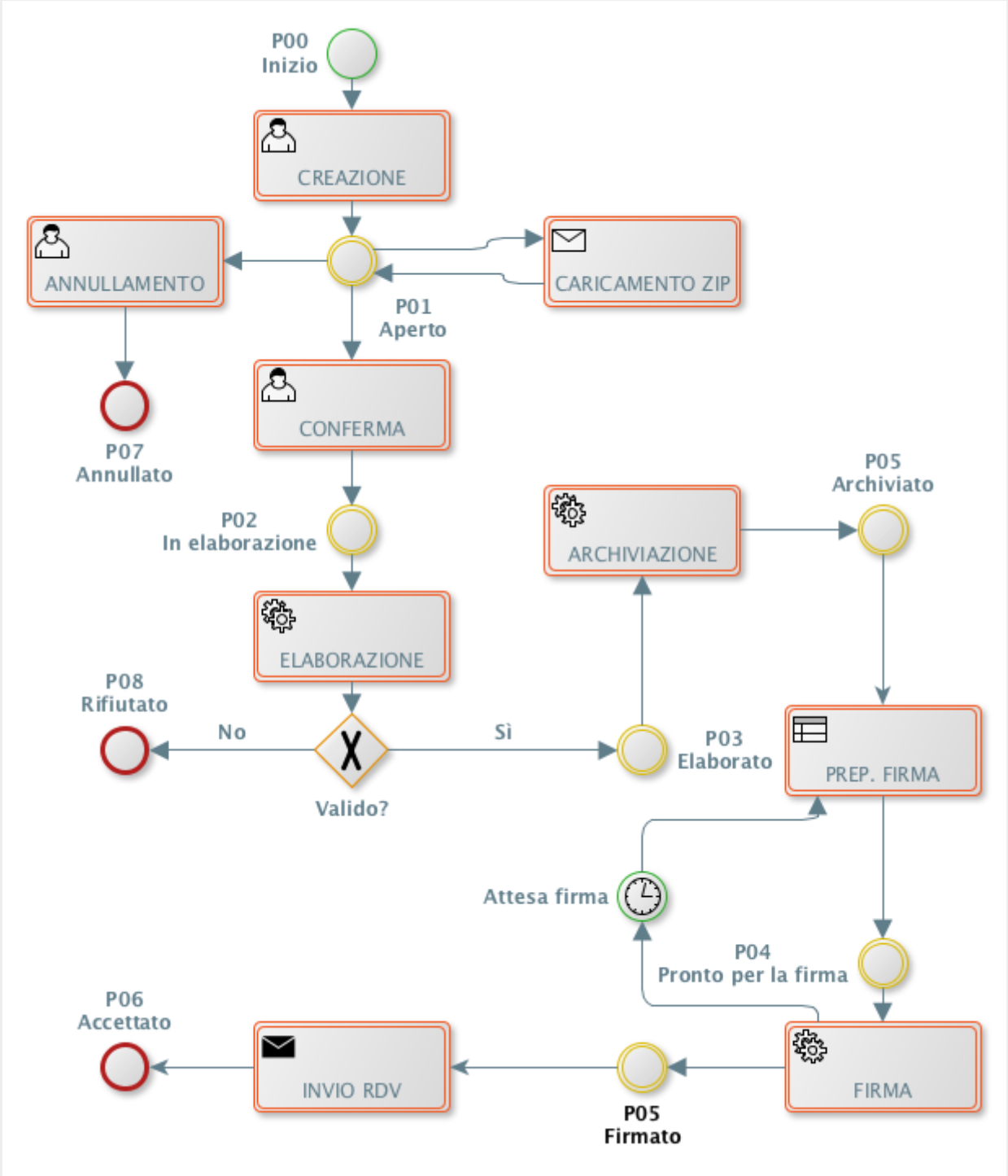

Figura 8. Creazione di un PDV.

Il sistema conserva un log delle operazioni relative all'acquisizione dei Pacchetti di Versamento dove viene registrato l'utente, la data e l'ora delle operazioni indicate nel diagramma come Creazione, Caricamento, Conferma e Annullamento.

Al Pacchetto di Versamento è assegnato un identificativo URN così come definito nel paragrafo Oggetti conservati.

I Pacchetti di Versamento caricati sono sottoposti al backup e alle verifiche di integrità insieme al resto della base dati del sistema, dove i pacchetti sono memorizzati finché i documenti non vengono inseriti in un pacchetto di archiviazione.

Torna all'indice.

7.2. Verifiche effettuate sui pacchetti di versamento e sugli oggetti in esso contenuti

La corretta ricezione dei PDV provenienti dal Produttore è monitorata dal SOSI tramite presidio del canale di comunicazione concordato.

In caso di anomalie il SOES prende in carico la segnalazione contattando i riferimenti tecnici del cliente.

Il processo di conservazione dei documenti prevede il mantenimento nel tempo di un insieme di evidenze informatiche (documenti e metadati) contenute nel PDV.

Queste evidenze comprovano l'integrità dei dati e l'autenticità dei documenti firmati digitalmente dal Produttore.

All'atto della ricezione dei documenti contenuti all'interno del PDV, il sistema esegue le seguenti operazioni:

- Controlli pregiudiziali:
  - verifica presenza dei metadati minimi e di quelli concordati;
  - verifica della correttezza dell'impronta del documento ricevuto;
  - verifica che il formato dichiarato dal Produttore sia corrispondente a quanto concordato;
  - verifica della firma digitale su ogni documento, se presente;
  - verifica che il produttore dei documenti corrisponda al produttore da cui proviene il PDV.
- Altri controlli:
  - controlli specifici relativi alla tipologia di documento da inviare in conservazione;
  - controlli supplementari concordati con il Cliente in sede contrattuale e definiti nella fase di attivazione del servizio.

Nel caso che uno di questi controlli abbia un esito negativo si genera un'eccezione che può essere gestita come:

- avvertenza: si segnala una difformità non bloccante rispetto a quanto atteso; il processo di acquisizione può proseguire fino alla conservazione;
- errore: si segnala una difformità bloccante del processo sul pacchetto di versamento nel suo complesso o in una delle unità documentarie contenute; il processo di acquisizione non può proseguire, il pacchetto verrà rifiutato e dovrà essere riproposto dopo una correzione con l'eventuale intervento da parte del Supporto Operativo.

Un controllo pregiudiziale genera sempre un errore bloccante.

L'esecuzione delle operazioni di verifica viene tracciata nel log delle operazioni relative all'acquisizione del PDV mentre l'esito delle verifiche, inclusi i messaggi di avvertenza e di errore alimentano il Rapporto di Versamento che verrà reso disponibile al Produttore al termine dell'acquisizione.

Il log delle operazioni viene mantenuto per tutto il periodo di conservazione dei documenti contenuti nel PDV, considerando il documento destinato ad essere conservato più a lungo.

Torna all'indice.

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

Qualora i controlli precedentemente descritti sui documenti ricevuti abbiano dato esito positivo, il processo descritto nel paragrafo Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico è seguito dal riversamento delle unità documentarie nell'area temporanea per la formazione dei Pacchetti di Archiviazione.

Al termine di questa operazione, il Sistema predispone i dati per la produzione dell'esito di avvenuta presa in carico del documento (ossia per la generazione di un Rapporto di Versamento).

Il rapporto di versamento (RDV) è generato in modo automatico ed è relativo ad uno specifico PDV, univocamente identificato dal Sistema di Conservazione.

Il RDV è un file XML che contiene al suo interno l'indice del PDV definito nel paragrafo Pacchetto di Versamento (PDV) a cui si riferisce, al quale sono aggiunte le informazioni elaborate durante la validazione, le informazioni che determinano l'immodificabilità delle unità archivistiche contenute, ovvero l'impronta di ciascuno dei file contenuti nel PDV.

Il formato del Rapporto di Versamento ha il seguente schema XSD:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:dcterms="http://purl.org/dc/terms/"
           xmlns="http://entaksi.eu/schemas/econ/1.0/"
targetNamespace="http://entaksi.eu/schemas/econ/1.0/"
           elementFormDefault="qualified" attributeFormDefault="unqualified">
    <xs:import namespace="http://purl.org/dc/terms/"
               schemaLocation="http://dublincore.org/schemas/xmls/qdc/2008/02/11/dcterms.xsd"/>
    <xs:element name="rdv" type="rdvType"/>
    <xs:element name="pdv" type="pdvType"/>
    <xs:complexType name="dcAndMetadataType" abstract="true">
        <xs:sequence>
            <xs:element name="dc" type="dcterms:elementOrRefinementContainer"/>
            <xs:element name="metadata" type="metadataType" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="rdvType">
        <xs:complexContent>
            <xs:extension base="dcAndMetadataType">
                <xs:sequence>
                    <xs:element name="dataElaborazione" type="xs:dateTime" minOccurs="1"
maxOccurs="1"/>
                    <xs:element name="esitoElaborazione" type="esitoElaborazioneType" minOccurs="1"
maxOccurs="1"/>
                    <xs:element name="errore" type="erroreType" minOccurs="0"
maxOccurs="unbounded"/>
                    <xs:element name="avvertenza" type="avvertenzaType" minOccurs="0"
maxOccurs="unbounded"/>
                    <xs:element name="pdv" type="pdvType" minOccurs="1" maxOccurs="1"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="pdvType">
        <xs:complexContent>
            <xs:extension base="dcAndMetadataType">
                <xs:sequence>
                    <xs:element name="registro" type="registroType" minOccurs="0" maxOccurs="1"/>
                    <xs:element name="dataVersamento" type="xs:dateTime" minOccurs="1"
maxOccurs="1"/>
                    <xs:element name="formato" type="xs:string" minOccurs="1" maxOccurs="1"/>
                    <xs:element name="fileGroup" type="fileGroupType" minOccurs="1"
maxOccurs="unbounded"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="fileGroupType">
        <xs:complexContent>
            <xs:extension base="dcAndMetadataType">
                <xs:sequence>
                    <xs:element name="registro" type="registroType" minOccurs="0" maxOccurs="1"/>
                    <xs:element name="file" type="fileType" minOccurs="1" maxOccurs="unbounded"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
```

```
    </xs:complexType>
    <xs:complexType name="fileType">
        <xs:complexContent>
            <xs:extension base="dcAndMetadataType">
                <xs:sequence>
                    <xs:element name="esitoElaborazione" type="esitoElaborazioneType" minOccurs="1"
maxOccurs="1"/>
                    <xs:element name="errore" type="erroreType" minOccurs="0"
maxOccurs="unbounded"/>
                    <xs:element name="avvertenza" type="avvertenzaType" minOccurs="0"
maxOccurs="unbounded"/>
                    <xs:element name="hashAlgorithm" type="hashAlgorithmType" minOccurs="1"
maxOccurs="1"/>
                    <xs:element name="hashValue" type="xs:base64Binary" minOccurs="1"
maxOccurs="1"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="hashAlgorithmType">
        <xs:simpleContent>
            <xs:extension base="xs:string">
                <xs:attribute name="canonicalXML" type="xs:boolean"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:complexType name="erroreType">
        <xs:simpleContent>
            <xs:extension base="xs:token">
                <xs:attribute name="codice" type="xs:string" use="required"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:complexType name="avvertenzaType">
        <xs:simpleContent>
            <xs:extension base="xs:token">
                <xs:attribute name="codice" type="xs:string" use="required"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:complexType name="metadataType">
        <xs:simpleContent>
            <xs:extension base="xs:token">
                <xs:attribute name="key" type="xs:string" use="required"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:simpleType name="esitoElaborazioneType">
        <xs:restriction base="xs:token">
            <xs:enumeration value="OK"/>
            <xs:enumeration value="KO"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="registroType">
        <xs:restriction base="xs:anyURI"/>
    </xs:simpleType>
</xs:schema>
```

Il seguente esempio illustra un Rapporto di Versamento:

```
<?xml version="1.0" encoding="UTF-8"?>
<rdv xmlns="http://entaksi.eu/schemas/econ/1.0/" xmlns:dc="http://purl.org/dc/elements/1.1/"
     xmlns:terms="http://purl.org/dc/terms/"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:schemaLocation="http://purl.org/dc/terms/
http://dublincore.org/schemas/xmls/qdc/2008/02/11/dcterms.xsd"
     xsi:schemaLocation="http://purl.org/dc/elements/1.1/
http://dublincore.org/schemas/xmls/qdc/2008/02/11/dc.xsd">
    <dataElaborazione>2015-12-01T03:56:47.910+01:00</dataElaborazione>
    <esitoElaborazione>OK</esitoElaborazione>
    <pdv>
        <dc>
            <terms:identifier>urn:entaksi:IT41141111411:_default:pdv:13777</terms:identifier>
            <terms:title>Pacchetto di versamento 13777</terms:title>
            <terms:description>Pacchetto di versamento 13777</terms:description>
            <terms:format>F001</terms:format>
        </dc>
        <dataVersamento>2015-11-11T00:00:00.000+01:00</dataVersamento>
        <formato>F001</formato>
        <fileGroup>
            <dc>

<terms:identifier>urn:entaksi:IT41141111411:_default:reg:2015:D01:2:doc:3</terms:identifier>
                <terms:type>Parcella</terms:type>
                <terms:date>2015-10-23T18:34:35+02:00</terms:date>
                <terms:subject>Parcella 2/3 del 19-10-2015 Destinatario: XXXXX COMUNE DI PORTO
CORSA</terms:subject>
                <terms:abstract>COMPENSO PER PRESTAZIONI PROFESSIONALI</terms:abstract>
            </dc>
            <metadata key="produttore:idfiscale">IT41141111411</metadata>
            <metadata key="produttore:codicefiscale">CRRSLY76H49Z404C</metadata>
            <metadata key="produttore:nome">SALLY</metadata>
            <metadata key="produttore:cognome">CARRERA</metadata>
            <metadata key="destinatario:idfiscale">IT00000000000</metadata>
            <metadata key="destinatario:codicefiscale">000000000</metadata>
            <metadata key="destinatario:ragionesociale">COMUNE DI PORTO CORSA</metadata>
            <metadata key="intermediario:idfiscale">IT01621900479</metadata>
            <metadata key="intermediario:ragionesociale">Entaksi Solutions SpA</metadata>
            <metadata key="documento:anno">2015</metadata>
            <metadata key="documento:tipo">D01</metadata>
            <metadata key="documento:sezionale">2</metadata>
            <metadata key="documento:numero">3</metadata>
            <metadata key="documento:data">2015-10-19</metadata>
            <metadata key="documento:posizionelotto">1</metadata>
            <metadata key="fattura:codicepa">UF7CB0</metadata>
            <metadata key="fattura:descrizionepa">COMUNE DI PORTO CORSA</metadata>
            <metadata key="fattura:scadenza">2015-10-19</metadata>
            <metadata key="fattura:importo">3701.17 EUR</metadata>
            <metadata key="fattura:firmatario">Alessandro Geri</metadata>
            <metadata key="fattura:idsdi">21151753</metadata>
            <metadata key="fattura:esito">Decorrenza termini</metadata>
            <registro>urn:entaksi:IT41141111411:_default:reg:2015:D01:2</registro>
            <file>
                <dc>
```

```
<terms:source>urn:entaksi:IT41141111411:_default:pdv:13777:IT01621900479_00Dm2.xml</terms:source>

<terms:isPartOf>urn:entaksi:IT41141111411:_default:reg:2015:D01:2:doc:3</terms:isPartOf>
                    <terms:title>IT01621900479_00Dm2.xml</terms:title>
                    <terms:extent>11891 bytes</terms:extent>
                    <terms:format>text/xml</terms:format>
                    <terms:type>Parcella</terms:type>
                </dc>
                <esitoElaborazione>OK</esitoElaborazione>
                <hashAlgorithm canonicalXML="false">SHA256</hashAlgorithm>
                <hashValue>UK8aiI+ijCwmVHFkHFUHL/r2PRBxEo+cr9WP+0qjwDY=</hashValue>
            </file>
            <file>
                <dc>
 <terms:isReferencedBy>urn:entaksi:IT41141111411:_default:pdv:13777:IT01621900479_00Dm2.xml</terms:i
sReferencedBy>
 <terms:source>urn:entaksi:IT41141111411:_default:pdv:13777:IT01621900479_00Dm2_RC_002.xml</terms:so
urce>

<terms:isPartOf>urn:entaksi:IT41141111411:_default:reg:2015:D01:2:doc:3</terms:isPartOf>
                    <terms:title>IT01621900479_00Dm2_RC_002.xml</terms:title>
                    <terms:extent>4230 bytes</terms:extent>
                    <terms:format>text/xml</terms:format>
                    <terms:subject>RICEVUTA DI CONSEGNA</terms:subject>
                    <terms:date>2015-10-23T18:35:01.000+02:00</terms:date>
                    <terms:type>RICEVUTA DI CONSEGNA</terms:type>
                </dc>
                <esitoElaborazione>OK</esitoElaborazione>
                <hashAlgorithm canonicalXML="false">SHA256</hashAlgorithm>
                <hashValue>w3TehtyIGlLDjhWD8ee0H8K225rG1BMboNhqdzqfqiU=</hashValue>
            </file>
            <file>
                <dc>
<terms:isReferencedBy>urn:entaksi:IT41141111411:_default:pdv:13777:IT01621900479_00Dm2.xml</terms:is
ReferencedBy>
<terms:source>urn:entaksi:IT41141111411:_default:pdv:13777:IT01621900479_00Dm2_DT_003.xml</terms:sou
rce>

<terms:isPartOf>urn:entaksi:IT41141111411:_default:reg:2015:D01:2:doc:3</terms:isPartOf>
                    <terms:title>IT01621900479_00Dm2_DT_003.xml</terms:title>
                    <terms:extent>4207 bytes</terms:extent>
                    <terms:format>text/xml</terms:format>
                    <terms:subject>NOTIFICA DI DECORRENZA TERMINI</terms:subject>
                    <terms:type>NOTIFICA DI DECORRENZA TERMINI</terms:type>
                </dc>
                <esitoElaborazione>OK</esitoElaborazione>
                <hashAlgorithm canonicalXML="false">SHA256</hashAlgorithm>
                <hashValue>wXNZV8yhdjFLdhxed3v+/OawODh6WC2dy6WXAo4Pp+Y=</hashValue>
            </file>
        </fileGroup>
    </pdv>
    <ds:Signature>...</ds:Signature>
</rdv>
```

Il riferimento temporale contenente la data di accettazione del Pacchetto di Versamento si trova rappresentata con il formato ISO 8601 nell'elemento `/rdv/dataElaborazione`.

Il rapporto di versamento è firmato digitalmente dal Responsabile del Servizio di Conservazione utilizzando il formato XaDES-BES.

L'esecuzione delle operazioni di elaborazione e firma digitale del Rapporto di Versamento e le operazioni di archiviazione dei documenti vengono tracciate nel log delle operazioni relative all'acquisizione del PDV.

Il Rapporto di Versamento viene mantenuto per tutto il periodo di conservazione dei documenti contenuti nel PDV, considerando il documento destinato ad essere conservato più a lungo.

Torna all'indice.

7.4. Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie

Nel caso in cui venga rilevato almeno un esito negativo in uno dei controlli definiti nel paragrafo Verifiche effettuate sui pacchetti di versamento e sugli oggetti in esso contenuti, il sistema produce un Rapporto di Versamento con esisto negativo, che si intende come rifiuto del pacchetto di versamento.
Il Rapporto di Versamento con esito negativo, o rapporto di rifiuto, viene generato automaticamente dalla procedura di validazione e contiene il dettaglio degli errori che sono stati incontrati durante la verifica.

Il rifiuto dei pacchetti di versamento viene comunicato al produttore rendendo disponibile il Rapporto di Versamento con esito negativo.

Il supporto operativo può contattare il Cliente secondo il canale prestabilito e concordato con esso per cercare di ovviare all'anomalia verificata.

Il formato del Rapporto di Versamento con esito negativo è lo stesso del Rapporto di Versamento descritto nel paragrafo Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico, ma l'elemento `/rdv/esitoElaborazione` contiene la stringa KO anziché OK. Inoltre nel rapporto si trova uno o più elementi `/rdv/errore` con la descrizione delle anomalie rilevate.

Il seguente esempio illustra un Rapporto di Versamento con esito negativo:

```
<?xml version="1.0" encoding="UTF-8"?>
<rdv xmlns="http://entaksi.eu/schemas/econ/1.0/" xmlns:dc="http://purl.org/dc/elements/1.1/"
     xmlns:terms="http://purl.org/dc/terms/"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:schemaLocation="http://purl.org/dc/terms/
http://dublincore.org/schemas/xmls/qdc/2008/02/11/dcterms.xsd"
     xsi:schemaLocation="http://purl.org/dc/elements/1.1/
http://dublincore.org/schemas/xmls/qdc/2008/02/11/dc.xsd">
<dataElaborazione>2015-10-08T17:55:12.525+02:00</dataElaborazione>
    <esitoElaborazione>KO</esitoElaborazione>
    <errore codice="E006">Il file IT00000000000_7B_RC_002-1.xml non ha un nome valido.</errore>
    <errore codice="E006">Il file IT00000000000_8U_RC_002-1.xml non ha un nome valido.</errore>
    <errore codice="E006">Il file IT00000000000_8T_RC_002-1.xml non ha un nome valido.</errore>
    <errore codice="E005">Il file contiene fatture non conformi.</errore>
    <pdv>
        <dc>
            <terms:identifier>urn:entaksi:IT00000000000:_default:pdv:9990</terms:identifier>
            <terms:title>Pacchetto di versamento 9990</terms:title>
            <terms:description>Pacchetto di versamento 9990</terms:description>
            <terms:format>F000</terms:format>
            <terms:source>pacchetto_001abc2w1gg.zip</terms:source>
        </dc>
        <dataVersamento>2015-10-08T17:51:58.452+02:00</dataVersamento>
        <formato>F000</formato>
        <fileGroup>
  ....
        </fileGroup>
    </pdv>
</rdv>
```

L'esecuzione delle operazioni di elaborazione del Rapporto di Versamento con esito negativo vengono tracciate nel log delle operazioni relative all'acquisizione del PDV.

I pacchetti di versamento rifiutati vengono scartati dopo un determinato periodo di tempo concordato con il Produttore e in nessun caso vengono riversati nel sistema di archiviazione.

Torna all'indice.

7.5. Preparazione e gestione dei pacchetti di archiviazione

Le unità documentarie di un PDV verificato con esito positivo, ovvero destinato all'accettazione nel sistema di archiviazione, vengono posizionate nel registro di archiviazione identificato durante la validazione in un'area temporanea dedicata alla formazione di un nuovo PDA.

Al termine del posizionamento delle unità documentarie il sistema produce il Rapporto di Versamento che, firmato digitalmente dal Responsabile del Servizio di Conservazione, viene reso disponibile al Produttore.

La procedura di formazione del Pacchetto di Archiviazione si occup di trasformare periodicamente il contenuto dell'area temporanea in un pacchetto di archiviazione creandone l'indice.

La formazione del pacchetto di archiviazione consiste nel prendere in esame il contenuto delle aree temporanee di ciascun registro di archiviazione assemblando l'indice del pacchetto di archiviazione come definito nel paragrafo Pacchetto di Archiviazione (PDA), sottoporlo alla firma digitale del Responsabile del Servizio di Conservazione e alla marcatura temporale e inserirlo nel PDA. Le varie fasi comprendono:

- identificazione del pacchetto di archiviazione precedente;
- verifica preliminare per la formazione dei pacchetti di archiviazione;
- chiusura del pacchetto di archiviazione.

L'identificazione del PDA precedente consiste nell'individuare l'ultimo pacchetto chiuso all'interno dello stesso registro di

archiviazione.

Se non ci sono PDA nel registro, il nuovo pacchetto sarà il numero 1, altrimenti si incrementa di uno il numero del pacchetto precedente.

Infine, la procedura di chiusura del PDA procede con i seguenti tre passi:

- Creazione dell'indice del PDA: il sistema recupera i metadati delle unità documentarie e le inserisce nel file indice così come definito nel paragrafo "Pacchetto di Archiviazione (PDA); Il file indice assume il nome in base alla numerazione del pacchetto di archiviazione: PIndex.1.xml, PIndex.2.xml,... PIndex.n.xml.
- Applicazione della Firma Digitale e della Marca Temporale all'indice.
- Chiusura del pacchetto: L'area temporanea per la formazione del pacchetto di archiviazione viene chiusa e diventa un pacchetto di archiviazione a tutti gli effetti.

Il file indice del Pacchetto di Archiviazione è firmato con firma digitale e marca temporale dal ile} utilizzando lo standard XaDES-T definito dalle specifiche ETSI TS 101 903 versione 1.4.1.

Per il calcolo della firma digitale e della marca temporale il sistema utilizza il software open source eSIG-DSS sviluppato nell'ambito del progetto Connecting Europe Facilities della Commissione Europea allo scopo di facilitare gli stati membri nell'adozione di soluzioni interoperabili nei processi di creazione e verifica delle firme digitali definiti dalla decisione della Commissione 2009/767/EC. Il software supporta i requisiti sui formati della firma digitale stabiliti nella decisione della Commissione 2011/130/EU.

I Certificati crittografici utilizzati nel processo di firma e le marche temporali sono emessi da una certification authority che fa parte della European Union Trusted List (EUTL) eIDAS.

L'esecuzione delle operazioni di identificazione del pacchetto di archiviazione precedente, verifica preliminare, creazione dell'indice, applicazione della firma digitale e della marca temporale e chiusura del PDA nel log applicativo prodotto dal software.
Interventi manuali sui Pacchetti di Archiviazione non sono previsti nella normale operatività del sistema. Nel caso in cui risultino necessari per risolvere situazioni anomale, essi vengono tracciati come incidenti con la procedura definita dal Sistema Integrato di Gestione certificato ISO/IEC 27001:2013. In caso di corruzione o perdita dei dati relativi agli indici o al contenuto dei Pacchetti di Archiviazione si attivano le procedure di continuità operativa definite dal Sistema Integrato di Gestione (SIG) per il ripristino dei dati.

7.5.1. Conservazione ed estensione della validità delle firme elettroniche

I documenti versati in conservazione dal 2022 in poi beneficiano anche del processo di conservazione ed estensione della validità delle firme elettroniche secondo le specifiche tecniche ETSI TS 119 511 v1.1.1 (2019-06) e il servizio è erogato come servizio fiduciario eIDAS secondo i requisiti definiti in ETSI EN 319 401 V2.3.1 (2021-05).

Il processo di conservazione delle firme elettroniche si basa sulla produzione di un report di validazione delle firme eseguito al momento del versamento dei documenti. Questo report viene quindi conservato in un registro di conservazione dedicato e contiene tutti i materiali necessari per ripetere la validazione nel tempo.

Il report di validazione rimane associato al documento firmato digitalmente e viene incluso nei Pacchetti di Distribuzione che contengono documenti firmati.

L'estensione della validità delle firme elettroniche sui documenti è ottenuta mediante l'estensione della validità della firma elettronica sull'indice SInCRO dei Pacchetti di Archiviazione che, a sua volta, è ottenuta mediante apposizione periodica di una nuova marca temporale che garantisce l'integrità e la validità della firma in caso di obsolescenza degli algoritmi utilizzati ovvero in caso di scadenza o di compromissione delle autorità che hanno emesso i certificati impiegati.

La conformità del processo di conservazione ai requisiti ETSI EN 319 401 V2.3.1 (2021-05) e alle specifiche tecniche ETSI TS 119 511 v1.1.1 (2019-06) è certificata da un ente accreditato secondo il Regolamento UE n° 910/2014 - eIDAS.

Il servizio di conservazione a lungo termine di documenti, firme elettroniche e sigilli è identificato dal seguente OID: 1.3.6.1.4.1.57823.3.1.

La policy del servizio di conservazione (Preservation Service Policy) correntemente in uso è identificata dal seguente OID: 1.3.6.1.4.1.57823.2.4.1.

Questa policy è descritta nel documento "Policy del servizio di conservazione eCON 2022-01" identificato dall'OID 1.3.6.1.4.1.57823.1.1 che è disponibile all'indirizzo https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.1.

La dichiarazione di pratica del servizio di conservazione (Preservation Service Practice Statement) è identificata dal seguente OID 1.3.6.1.4.1.57823.1.2 ed è disponibile all'indirizzo https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.2.

Torna all'indice.

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

L'Utente autorizzato dal Produttore può richiedere al Sistema di Conservazione l'accesso ai documenti conservati per acquisire le informazioni di interesse nei limiti previsti dalla legge. Tali informazioni vengono fornite ai soggetti autorizzati tramite l'accesso diretto, anche da remoto, al documento informatico conservato, attraverso la produzione di un pacchetto di distribuzione selettivo ottenuto tramite specifica ricerca nel sistema di Conservazione.

Per quanto riguarda l'attività di ricerca e l'esibizione a norma dei documenti conservati (anche a fronte di una verifica ispettiva da parte delle Autorità competenti) lo strumento di accesso dell'Utente all'archivio documentale è costituito da una apposita interfaccia utente che tramite un filtro di ricerca interagisce con il sistema di archiviazione.

Tramite questa interfaccia, e compatibilmente con i diritti di accesso al sistema, l'Utente può pertanto verificare la presenza dei documenti conservati al fine di:

- visionare i metadati del documento conservato all'interno dell'archivio a norma;
- verificare le prove di conservazione (indici dei PDA).

In base ai criteri di selezione specificati nel filtro può essere effettuata una ricerca massiva con produzione di specifico Pacchetto di Distribuzione, come definito nel paragrafo Pacchetto di Distribuzione (PDD) che viene messo a disposizione dell'utente.

La funzione di preparazione del Pacchetto di Distribuzione colleziona le unità documentarie corrispondenti ai criteri di selezione e le relative prove di conservazione, predispone un indice del Pacchetto di Distribuzione conforme al formato SinCRO come definito nel paragrafo Pacchetto di Distribuzione (PDD), sottopone l'indice alla firma del Responsabile del Servizio di Conservazione e assembla in formato ZIP l'insieme costituito dai documenti, dalle prove di conservazione e dall'indice firmato del pacchetto.

L'indice del Pacchetto di Distribuzione viene firmato in formato XaDES-BES.

Contestualmente alla produzione del Pacchetto di Distribuzione il sistema verifica l'integrità dei documenti confrontando l'impronta dei file con il valore memorizzato nell'indice del Pacchetto di Archiviazione. La mancata corrispondenza di questi valori indica che il documento è corrotto. In queste condizioni si attivano le procedure di continuità operativa definite dal Sistema Integrato di Gestione (SIG) per il ripristino dei dati.

L'esecuzione delle operazioni di selezione, verifica dell'integrità dei documenti, generazione e firma digitale dell'indice del Pacchetto di Archiviazione sono registrate nel log applicativo prodotto dal software.
Il Pacchetto di Distribuzione viene resto disponibile all'utente tramite una connessione cifrata HTTPS autenticata mediante le credenziali dell'utente. Con questa connessione l'utente può scaricare il Pacchetto di Distribuzione sul proprio dispositivo. L'accesso dell'utente al Pacchetto di Distribuzione tramite questo mezzo viene tracciato nel log applicativo prodotto dal software.

Non è previsto l'utilizzo di supporti fisici rimovibili per la trasmissione dei Pacchetti di Distribuzione.

Non è previsto l'utilizzo l'utilizzo della email per la trasmissione dei Pacchetti di Distribuzione.

Diverse modalità di selezione e distribuzione dei Pacchetti di Distribuzione possono essere previste nelle specificità del contratto con il produttore.

Torna all'indice.

7.7. Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del Pubblico Ufficiale nei casi previsti

Durante l'esercizio, può rendersi necessario effettuare il riversamento degli oggetti forniti dal produttore o gestiti dal sistema, per mantenerne la leggibilità a fronte di adeguamenti delle piattaforme tecnologiche e dei formati.

Se tale riversamento non altera il contenuto degli oggetti (e quindi non richiede l'apposizione di una nuova firma digitale, come per esempio l'esecuzione di una copia di backup), viene definito riversamento conservativo, e può essere eseguito senza ricorrere a procedure specifiche.

Se viceversa il processo di riversamento comporta una necessaria o inevitabile alterazione delle unità documentarie o, in

generale, degli oggetti gestiti dal sistema, viene definito riversamento sostitutivo, e deve essere eseguito dietro esplicita autorizzazione e supervisione del Responsabile del Servizio di Conservazione.

Questa attività, prevista dalla normativa nel caso in cui si voglia ad esempio aggiornare tecnologicamente il sistema di gestione dell'archivio documentale, è finalizzata a garantire la continuità del processo generale di conservazione a fronte di innovazioni tecnologiche.

In questo caso potrebbe essere necessaria l'apposizione di una ulteriore firma digitale, o l'attestazione di conformità all'archivio esistente da parte di Pubblico Ufficiale, il cui intervento viene valutato ed eventualmente richiesto dal Responsabile del Servizio di Conservazione.

Il coinvolgimento di un Pubblico Ufficiale esperto in processi di conservazione può essere richiesto al fine di:

1. validare il piano di acquisizione o cessione;
2. verificare che il processo di trasformazione del formato dei documenti non alteri il contenuto e la forma dei documenti stessi;
3. validare il processo di apposizione delle firme digitali sui documenti acquisiti in conformità con le normative vigenti.

Torna all'indice.

7.8. Scarto dei pacchetti di archiviazione

Alla scadenza dei termini di conservazione relativi alla specifica tipologia documentale e comunque definiti in sede contrattuale con il Produttore, avviene lo scarto del PDA dal sistema di conservazione a norma. Lo scarto porta alla cancellazione permanente dal Sistema delle unità documentarie contenute nel PDA, e avviene allo scadere definito dei termini di legge per ogni specifico documento.

Il Sistema di Conservazione si basa in questo caso sulla normativa sulla prescrizione definita dall'art. 2963 del Codice Civile, per cui la prescrizione viene conteggiata in base al calendario comune, con esclusione del giorno iniziale e considerando invece quello finale. Il computo basato sugli anni si basa sulla scadenza determinata dalla data più recente contenuta nelle unità documentarie contenute nel PDA.

È possibile, in fase di versamento, adottare i massimari di scarto dell'azienda o dell'istituzione di provenienza, con un accordo tra il Cliente e il Responsabile della Funzione Archivistica, purché detti massimari non contrastino con gli obblighi di legge.

In ambito fiscale, la conservazione di scritture e documenti contabili è disciplinata dall'art. 22 del DPR n. 600 del 29 settembre 1973, per la quale le scritture contabili obbligatorie devono essere conservate fino alla conclusione di eventuali accertamenti relativi al corrispondente periodo di imposta. Per questo motivo allo scadere dei termini di conservazione, nel caso fosse in corso un accertamento fiscale, non si potrà procedere allo scarto. Per dare la possibilità di poter prolungare i termini di conservazione verrà data informativa al Produttore con congruo anticipo (almeno 6 mesi) al fine di confermare la cancellazione.

In via generale i termini di conservazione si suddividono in:

Tabella 19. Tempi di scarto.

Tipologie di scritture	**Termini di conservazione**
Scritture contabili (fatture, registri, libri...), PEC	10 anni
Moduli (modelli)	La conservazione termina allo scadere del quarto anno solare dall'anno di riferimento del modello.
Contratti	20 anni
Altre scritture	Definiti con il Cliente

La cancellazione avverrà nei tempi e nei modi definiti dalla legge, con regole di cancellazione definite nel Sistema dopo approvazione esplicita da parte del Responsabile del Servizio di Conservazione e del Responsabile della Funzione Archivistica.

Nel caso di archivi pubblici o privati, che rivestono un interesse storico particolarmente importante, lo scarto avviene solo previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo, rilasciata al produttore secondo la normativa vigente, in ottemperanza alle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici.

La funzione di scarto dei pacchetti di archiviazione rileva periodicamente i pacchetti di archiviazione che sono prossimi allo

scadenza dei tempi di conservazione e programma l'esecuzione dello scarto per il giorno stabilito in base ai tempi definiti nella tabella precedenti per quei pacchetti in cui non è presente il metadato `terms:accessRight` definito nel paragrafo Oggetti conservati.

I pacchetti di archiviazione che hanno valorizzato tale metadato contengono documenti provenienti da archivi pubblici o privati di rilevante interesse storico, per cui lo scarto del pacchetto di archiviazione può avvenire solo previa autorizzazione del Ministero dei Beni e delle Attività Culturali e del Turismo. Il sistema consente di rilevare la presenza di questi pacchetti di archiviazione in modo che il Responsabile del Servizio di Conservazione possa richiedere l'intervento delle autorità competenti per autorizzare lo scarto.

Torna all'indice.

7.9. Predisposizione di misure a garanzia della interoperabilità e trasferibilità ad altri conservatori

Per interoperabilità si intende la capacità di cedere o acquisire copie o duplicati dei documenti conservati, migrandoli da un supporto ad un altro senza che ciò comporti una alterazione del contenuto informativo digitale e del valore degli stessi.

Tale procedimento verrà eseguito sotto la responsabilità del Responsabile del Servizio di Conservazione, e verrà concordato con il Produttore dei documenti oggetto di cessione o acquisizione.

Viene eseguita normalmente su richiesta del cliente e si effettua mediante generazione di Pacchetto di Distribuzione o l'acquisizione di un Pacchetto di Versamento.

Per procedere all'acquisizione o alla cessione di documenti, sarà necessario definire una mappatura dei dati o metadati forniti dal conservatore cedente ed acquisiti dal nuovo conservatore.

La procedura di acquisizione o cessione prevede:

- la costruzione di nuovi PDA a partire dai PDD forniti dal cedente che dovranno risultare coincidenti con gli stessi;
- il popolamento della base dati dei metadati a partire dai dati del cedente.

La procedura prevede una fase di quadratura pre e post migrazione, sotto la supervisione del Responsabile del Servizio di Conservazione.

Per garantire l'interoperabilità con altri sistemi, il sistema di conservazione adotta lo standard UNI 11386:2020 (SinCRO) per l'indice dei Pacchetti di Archiviazione e dei Pacchetti di Distribuzione.

Per garantire ulteriormente la possibilità per altri sistemi di interpretare la struttura dei metadati, il sistema adotta lo standard internazionale Dublin Core per definire la semantica di gran parte dei metadati e fornisce nel presente manuale la documentazione relativa ai metadati che non rientrano in questo standard.

Le strutture XML personalizzate presenti nel formato SinCRO (le tag MoreInfo) sono inoltre documentate tramite la pubblicazione degli schemi XSD, disponibili pubblicamente all'indirizzo https://entaksi.eu/schemas/econ/1.0/econ.xsd e utilizzabili anche per fini commerciali previa attribuzione secondo la licenza CC-BY-SA 4.0 i cui termini sono definiti all'indirizzo http://creativecommons.org/licenses/by-sa/4.0/.

Torna all'indice.

7.10. Cessazione del servizio di conservazione

Il processo di cessazione del Servizio di Conservazione per ogni Cliente/Produttore segue queste fasi principali:

1. condivisione delle informazioni tecniche di richiesta cessazione;
2. consolidamento delle informazioni tecniche propedeutiche alla cessazione del servizio, con la definizione della data formale di cessazione;
3. notifica della chiusura e delle sue modalità al Responsabile del Servizio di Conservazione;
4. cessazione del processo di acquisizione;
5. mantenimento dell'accesso al sistema per il Cliente/Produttore per i tempi contrattualmente stabiliti, al fine di permettere la autonoma esportazione dei documenti ospitati mediante la formazione di PDD o, in alternativa e ove previsto dalla condizioni contrattuali, attivazione su richiesta del cliente di un piano di riversamento;
6. scarto, entro i termini contrattuali, dei documenti non più soggetti al servizio di conservazione.

Per quanto riguarda invece la cessazione dell'erogazione del Servizio di Conservazione da parte di Entaksi Solutions SpA il processo attraversa queste fasi principali:

1. comunicazione della cessazione del servizio ai canali interessati (AgID, clienti);
2. condivisione informazioni tecniche di cessazione (piano di cessazione) alle parti interessate;
3. individuazione di un conservatore per la documentazione Entaksi relativa alla gestione del servizio (documentazione tecnica, manuali di servizio, log di sistema, contratti di servizio);
4. trasferimento dati a nuovo conservatore;
5. notifica della chiusura e delle sue modalità da parte del Responsabile del Servizio di Conservazione;
6. mantenimento dell'accesso al sistema per il Cliente/Produttore per i tempi contrattualmente stabiliti, al fine di permettere la autonoma esportazione dei documenti ospitati mediante la formazione di PDD o, in alternativa e ove previsto dalla condizioni contrattuali, attivazione su richiesta del cliente di un piano di riversamento;
7. scarto, entro i termini contrattuali, dei documenti non più soggetti al servizio di conservazione.

Per l'eventuale cessazione del Servizio di Conservazione, in quanto considerato un servizio fiduciario da AgID, verranno comunque seguite le disposizioni previste dall'art. 37 del CAD (Codice Amministrazione Digitale).

In caso di piano di riversamento o trasferimento ad altro sistema di conservazione, le modalità previste sono le stesse riportate negli specifici paragrafi 7.7 e 7.9.

Torna all'indice.

8. Sistema di conservazione

Il sistema software utilizzato per la gestione del processo di conservazione a norma dei documenti digitali è costituito dal prodotto applicativo Entaksi eCON che utilizza un file system distribuito e replicato per memorizzare i documenti, gli indici e tutte le altre informazioni che compongono l'archivio.

Il sistema eCON sviluppato da Entaksi è un sistema integrato e completo per la conservazione a norma, nel tempo, dei documenti informatici.

Esso presenta le seguenti caratteristiche generali:

- **Completezza** - presenza e disponibilità di qualsiasi documento caricato.
- **Robustezza** - garanzia di consistenza dei dati inseriti.
- **Scalabilità** – capacità di gestire un numero crescente di utenti e documenti
- **Sicurezza** - protezione dall'accesso e la manipolazione non autorizzata dei dati.
- **Affidabilità** - indipendenza dai guasti dell'hardware.
- **Chiarezza** - facilità di consultazione secondo diversi criteri di ricerca.

Il sistema di conservazione è in grado di gestire tutte le tipologie di documenti ammesse dalla normativa corrente alla conservazione, caratterizzando i file con specifici metadati che consentono di gestire insiemi di documenti omogenei.

Il sistema è progettato per segregare in maniera opportuna i dati gestiti al fine di garantire la separazione per contesto organizzativo e la consistenza dei dati. La segregazione opera tra i dati di Enti diversi o di diversi dipartimenti o strutture o uffici afferenti ad uno stesso Ente (es. le Aree Organizzative Omogenee della Pubblica Amministrazione).

Tutti le operazioni sul sistema, incluso l'accesso ai documenti, sono disponibili tramite una console di gestione accessibile via web il cui accesso è protetto dalla cifratura della connessione con protocollo HTTPS e da un meccanismo di autentifica delle credenziali degli utenti che comprende anche l'impiego di sistemi di autenticazione a due fattori.

Entaksi garantisce la protezione delle credenziali attraverso l'utilizzo del protocollo OAuth 2.0 e gestisce le credenziali single sign-on attraverso il software Open Source Keycloak. Per la gestione delle credenziali di accesso Entaksi utilizza un sistema di gestione delle identità compatibile con gli standard OAuth2 (RFC-6749, RFC-6750, RFC-6819, RFC-7662, RFC-7009, RFC-7519), SAMLv2 e con il protocollo OpenID Connect.

Il sistema è implementato dal software open source *Keycloak*.

L'architettura del prodotto consente di definire diversi livelli operativi e garantisce che ciascuna Ente/Struttura o Area Organizzativa Omogenea, possa accedere solo ed esclusivamente ai suoi documenti, in base alle credenziali e alle politiche di accesso attivate.

Le componenti software del sistema di conservazione sono sviluppate da Entaksi Solutions utilizzando librerie e tecnologie *open source* e un processo produttivo con certificazione di qualità UNI ISO 9001:2015.

I sistema di conservazione fa parte dei servizi informatici di Entaksi Solutions la cui gestione è certificata ISO/IEC 20000-1:2018.

Torna all'indice.

8.1. Componenti logiche

Le componenti logiche del sistema di conservazione sono illustrate nel seguente diagramma:

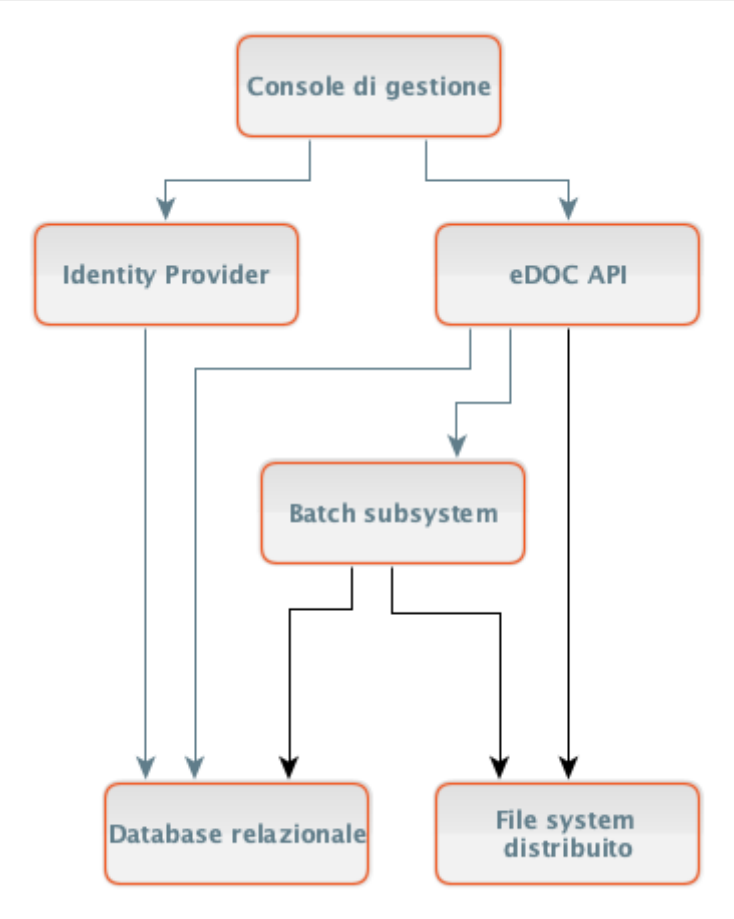

Figura 9. Componenti logiche del sistema di conservazione.

La “Console di gestione” è una applicazione HTML5 compatibile con le versioni aggiornate di un browser web sulle principali piattaforme desktop e mobili. L’applicazione è accessibile collegandosi con protocollo HTTPS e utilizza un “Identity Provider” OAuth2 per autenticare le credenziali dell’utente e consentire l’accesso alle API REST fornite dalla componente “eDoc API”.

Le API fornite dalla componente “eDoc API” consentono di gestire tutti i processi compresi nel sistema. Nel “Database relazionale” sono memorizzate le informazioni gestionali, mentre il “Batch subsystem” sovrintende l’esecuzione delle procedure batch. L’archiviazione dei documenti avviene utilizzando un “File system distribuito” come supporto per l’archiviazione vera e propria dei documenti. Il “Motore di ricerca” consente di eseguire ricerche sulla base dati documentale mediante l’indicizzazione dei metadati.

Torna all’indice.

8.2. Componenti tecnologiche

Le componenti logiche descritte nel paragrafo Componenti logiche sono implementate tramite le componenti tecnologiche illustrate nel seguente diagramma.

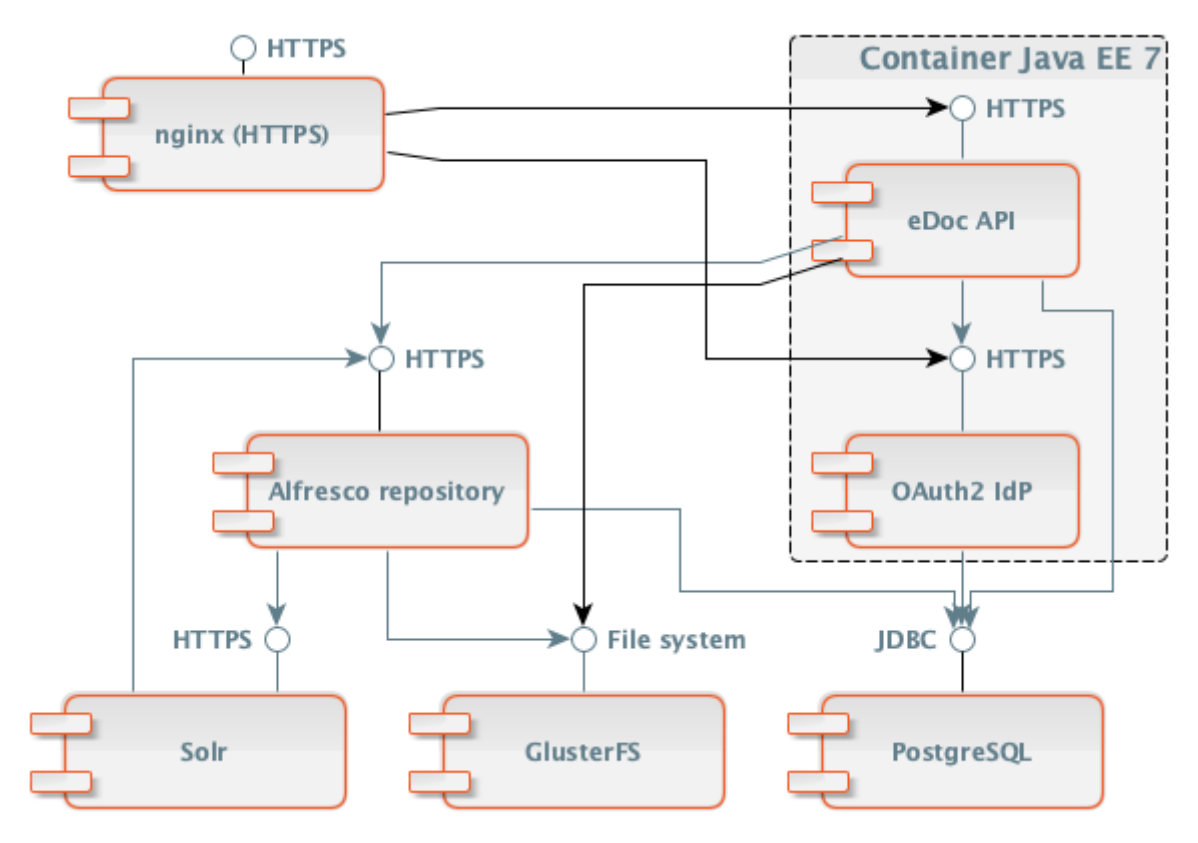

Figura 10. Componenti tecnologiche del sistema di conservazione.

Il container Java EE 7 costituito dal sistema *open source* Wildfly, prodotto da Red Hat, ospita i moduli eDoc API e il modulo Identity Provider OAuth2, costituito dal software *open source* Keycloak.

L'applicazione HTML5 che costituisce la console di amministrazione è servita come sito web statico da un server non rappresentato nella figura.

La componente "Database relazionale" è implementata dal software *open source* PostgreSQL.

La componente "File system distribuito" è implementata dal software *open source* GlusterFS che consente di disporre di un unico spazio di archiviazione virtuale distribuito fisicamente in più partizioni residenti su più server in modo tale da sommare lo spazio fornito da ciascuna partizione mantenendo un livello di replica dei dati così che una copia di ciascun oggetto sia sempre replicata su altri server secondo un predefinito livello di replica, anche utilizzando istanze geograficamente distanti.
Ciascuna delle componenti tecnologiche è configurata per funzionare in cluster in modo da assicurare la scalabilità orizzontale e verticale dell'intero sistema, nonché la continuità operativa in caso di guasto di un singolo componente.

Le componenti sono configurate come servizi dell'infrastruttura più ampia di Entaksi Solutions sottoposta a certificazione ISO/IEC 27001:2013 e in quanto tali sono conformi ai criteri di riservatezza, disponibilità, integrità e non ripudiabilità delle informazioni derivanti dall'applicazione delle norme di questa certificazione.

Torna all'indice.

8.3. Componenti fisiche

Entaksi Solutions ha deciso di:

- Posizionare in housing / hosting tutta la sua infrastrutture server. I server che ospitano ed erogano i vari servizi di cui la Società necessita per lo svolgimento delle sue attività, nonché quelli che vengono erogati ai propri clienti, sono collocati

presso datacenter gestiti da fornitori specializzati allo scopo. La scelta dei datacenter viene rivista periodicamente in funzione della dinamica del mercato, scegliendo di volta in volta le strutture che offrono il rapporto prestazioni/prezzo ritenuto più conveniente. Lo stesso criterio viene adottato per la fruizione di servizi generali di rete (quali ad esempio la risoluzione dei nomi a dominio e il relativo DNS), anch'essi affidati a servizi esterni.

- Inquadrare in un rapporto di telelavoro tutti i dipendenti e collaboratori.

Il risultato dell'adozione di questa impostazione è che la società opera totalmente in rete, senza dipendere da una sede operativa fisica centrale.

Perciò nell'organizzazione di Entaksi Solutions SpA, centrata come detto sopra sul telelavoro e sul ricorso strutturale all'outsourcing delle risorse hardware e software condivise, il controllo dell'accesso fisico da parte di personale non autorizzato alle infrastrutture non è regolato dalle procedure interne di Entaksi bensì dalle verifiche di qualità che vengono eseguita in fase di qualifica dei fornitori e durante il monitoraggio dei servizi esterni utilizzati.

È necessario d'altra parte sottolineare che, dal punto di vista della sicurezza fisica delle infrastrutture centrali, quella che per Entaksi è stata una scelta di avanguardia in uno scenario dominato dalla gestione in proprio dei server, oggi è una tendenza ampiamente assodata che con sempre maggiore frequenza vede la migrazione in cloud come il modo più sicuro per gestire i servizi.

Entaksi garantisce il rispetto di requisiti minimi nella gestione della sicurezza fisica della infrastruttura centrale mediante i processo di qualifica e quello di monitoraggio dei fornitori che sono selezionati sia sulla base della convenienza di mercato che sulle garanzie di qualità offerte in tema di sicurezza, quali ad esempio la certificazione ISO/IEC 27001:2013 e, se necessario, la disponibilità ad essere sottoposti ad audit e ispezioni per riscontrare eventuali elementi non sufficientemente coperti dalle condizioni contrattuali o dalle certificazioni stesse. Entaksi eroga servizi dalla sua infrastruttura: tutto il sistema software è interamente sotto il controllo dell'azienda, mentre invece l'hardware e la connettività di rete sono gestiti direttamente dai fornitori dei datacenter.

I componenti fisici del servizio di conservazione eCON sono collocati in server situati in vari datacenter, distribuiti geograficamente allo scopo di garantire l'alta disponibilità del servizio.

Il sistema di conservazione è situato nei seguenti tre datacenter:

- *Aruba S.p.A.*
  Via Sergio Ramelli 8
  52100 Arezzo (AR)
- *Aruba S.p.A.*
  Via Piero Gobetti 96
  52100 Arezzo (AR)
- *Aruba S.p.A.*
  Via San Clemente 53
  24036 Ponte San Pietro (BG)

La replica del sistema rafforza la continuità operativa e permette al sistema di rimanere disponibile in caso di guasto in uno qualsiasi dei tre poli.

Alcune componenti del sistema, come l'elaborazione, la verifica, l'indicizzazione e le procedure di presentazione dei dati, possono determinare il transito temporaneo dei dati nei seguenti due datacenter situati all'interno dell'Unione Europea:

- *Hetzner Online AG*
  Am Datacenterpark 1
  08223 Falkenstein
  Germany
- *Hetzner Finland Oy*
  Huurrekuja 10
  04360 Tuusul
  Finland

Entaksi utilizza sistemi operativi GNU/Linux sui suoi server. La configurazione e l'accesso sono interamente sotto il controllo esclusivo di Entaksi Solutions. Il sistemi software operano su macchine virtuali configurate all'interno di un'area dati criptata.

I datacenter garantiscono i più alti livelli di performance in termini di affidabilità, sicurezza e connettività, utilizzano i protocolli IPv4 e IPv6 e sono certificati ISO/IEC 27001:2013.

Le Time-Stamping Authorities (TSA) qualificate che forniscono le marche temporali per il servizio di conservazione eCON sono:

- *Aruba PEC S.p.A. - P.IVA IT01879020517 - REA N. BG445886.*
- *Namirial S.p.A. - P.IVA IT02046570426 - REA N. AN157295.*

Torna all'indice.

8.4. Procedure di gestione ed evoluzione

Il sistema eCON fa parte dell'insieme di servizi Entaksi sottoposto alle certificazioni ISO/IEC 20000-1:2018 e ISO/IEC 22301:2019, e adotta quindi una serie di procedure di gestione e di evoluzione del sistema in accordo con il dettato più generale di queste norme, fra le quali quelle riportate nei paragrafi seguenti. Le procedure hanno l'obiettivo di garantire la conformità del sistema alle evoluzioni normative e tecnologiche, senza intaccare l'integrità dello stesso e la continuità operativa.

Ogni procedura prevede che per il Sistema di Conservazione siano inoltre garantite, in ogni fase di gestione ed evoluzione, l'integrità, la disponibilità e la riservatezza dei documenti conservati, indipendentemente dai cambiamenti apportati.

Il sistema è sottoposto alle procedure di Change Management descritte nei manuali del Sistema Integrato di Gestione; in particolare, adotta la gestione centralizzata delle configurazioni mantenendo aggiornato il database delle configurazioni (CMDB) e traccia le modifiche a queste configurazioni mediante un sistema di ticketing interno.

Il database delle configurazioni dei sistemi di Entaksi e i suoi cambiamenti sono registrati tramite il sistema di controllo versione GIT e gestiti (cioè applicati concretamente ai sistemi) tramite il software Ansible.

Le istanze di cambiamento (che possono provenire dai Clienti o da iniziative di Entaksi, nel caso di richieste di natura normativa o tecnologica, e che sono formalizzate in appositi ticket / documenti) vengono valutate nel merito dal Responsabile del Servizio di Conservazione, tenendo conto degli impatti funzionali, sul servizio, economici, sulle risorse e sulla prospettiva commerciale, e delle modalità di installazione in produzione.

I cambiamenti con potenziale impatto critico, la cui adozione / installazione può modificare in modo sostanziale la modalità di uso del prodotto o del servizio o produrre interruzioni o degradamento dei livelli di servizio oltre quelli previsti dai Service Level Agreement, devono essere concordati con il Cliente e comunicati con ragionevole anticipo.

Se le istanze di cambiamento sono ritenute:

- opportune dal punto di vista funzionale, economico o di facilità di gestione;
- percorribili tecnicamente;
- sostenibili economicamente;

la loro implementazione (così come richiesta oppure opportunamente generalizzata) viene inserita nella backlog list e al momento opportuno pianificata.

Le variazioni delle risorse attraversano le seguenti fasi:

- analisi dei rischi;
- definizione dei requisiti (funzionali, tecnici, di sicurezza, di prestazioni, di scalabilità, ecc..);
- stima delle attività e pianificazione delle stesse;
- verifica avanzamento e ripianificazione, effettuata su base (circa) settimanale;
- rilascio del prototipo al Cliente;
- uso del prototipo da parte del Cliente rilevazione nuovi requisiti / errori.

Il workflow è così strutturato:

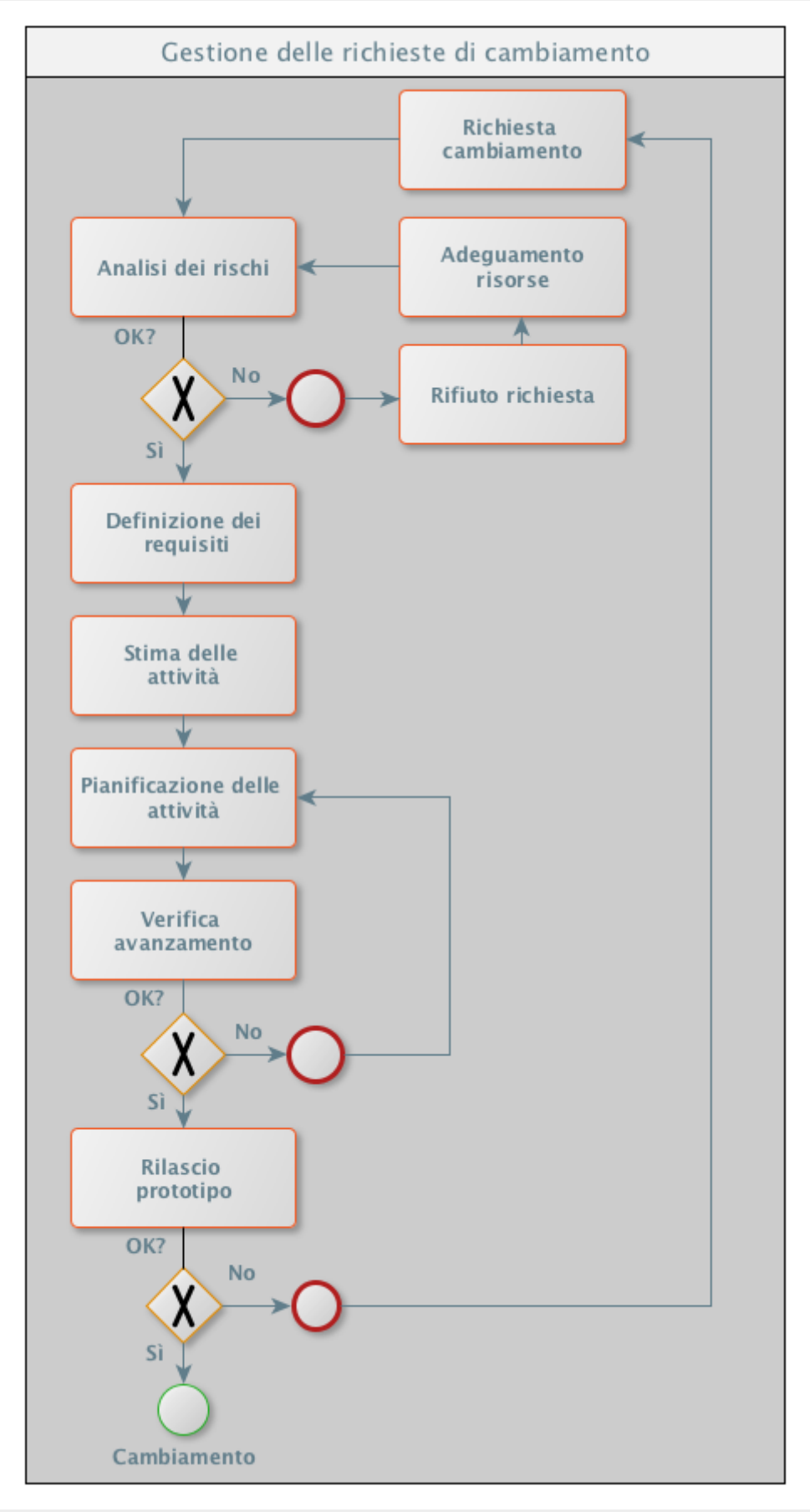

Figura 11. Gestione delle richieste di cambiamento.

Entaksi adotta una procedura di conduzione e manutenzione del sistema che ha lo scopo di descrivere tutte le attività necessarie a monitorare lo stato del software e delle apparecchiature hardware dei Sistemi Informativi. L'esercizio del Sistema risponde agli standard UNI ISO 9001:2015, ISO/IEC 27001:2013, ISO/IEC 27017:2015, ISO/IEC 27018:2019, ISO/IEC 27035:2016, ISO/IEC 20000-1:2018 e ISO/IEC 22301:2019 e l'evoluzione dello stesso segue gli aggiornamenti a questi standard. Oltre a questi standard viene fatto riferimento alle norme nazionali e internazionali in materia di conservazione, quali le norme ETSI previste per la conservazione a lungo termine di firme, sigilli o certificati elettronici relativi a tali servizi. Inoltre risponde a esigenze normative, tecnologiche e di sicurezza, che ne determinano il cambiamento nell'ottica del miglioramento continuo.

L'ambito nel quale si inserisce la conduzione e la manutenzione del sistema, e che riguarda nel particolare il Sistema di Conservazione, è quello della gestione delle richieste di implementazioni di:

- nuovi prodotti software;
- nuove funzionalità nei prodotti software già in esercizio;
- nuovo hardware.

Obiettivo della procedura è quindi descrivere i passi operativi relativi alla gestione del software e dell'hardware intendendo con ciò le attività che portano alla introduzione nel sistema di:

- rilasci dovuti alla richiesta di implementazione di nuove funzionalità;
- patch correttive;
- nuovo hardware;
- software di sistema.

In generale la procedura segue il workflow di change management precedentemente descritto. Come per il software, anche le modifiche all'hardware richiedono una formalizzazione della richiesta, la successiva analisi rischi e la valutazione dell'impatto del cambiamento, la progettazione con realizzazione di test e la valutazione finale. Solo una volta superato con successo il collaudo si procederà al passaggio in produzione della modifica.

La procedura specifica è descritta all'interno del Sistema Integrato di Gestione di Entaksi.

Entaksi verifica periodicamente la conformità alla normativa e agli standard di riferimento mediante audit interni e mediante un audit esterno annuale sostenuto da parte di un ente terzo certificato che ne stabilisce l'aderenza alle norme di qualità e sicurezza corrispondenti. I dettagli operativi di tale procedura sono descritti nei relativi documenti interni del SIG riguardante gli audit interni e i riesami della Direzione.
Entaksi conserva in modo centralizzato i log applicativi, i log degli accessi e i log dei sistemi conservando queste informazioni secondo le rispettive politiche di gestione.
Il sistema di monitoraggio, descritto anche nel capitolo Monitoraggio e controlli, consente di tenere sotto controllo le prestazioni e lo stato di funzionamento di tutte le componenti tecnologiche del sistema di conservazione.

Torna all'indice.

9. Monitoraggio e controlli

Le procedure di monitoraggio e controllo sul Sistema e sull'integrità dei documenti conservati sono necessarie a garantire la stabilità nel tempo dell'apparato. In questo capitolo viene descritto come avvengono i processi di monitoraggio, i controlli di sicurezza e le verifiche sull'integrità degli archivi, in ottemperanza alle norme e agli standard seguiti da Entaksi.

Il Sistema Integrato di Gestione di Entaksi ha ottenuto le seguenti certificazioni:

- **UNI ISO 9001:2015 – Sistema di Gestione Qualità (SGQ)**
- **ISO/IEC 20000-1:2018 – Sistema di Gestione della erogazione dei servizi IT (SGS)**
- **ISO/IEC 27001:2013 – Sistema di Gestione della Sicurezza delle Informazioni (SiGSI)**
- **ISO/IEC 27017:2015 - Estensione del Sistema di Gestione della Sicurezza delle Informazioni (SiGSI)**
- **ISO/IEC 27018:2019 - Estensione del Sistema di Gestione della Sicurezza delle Informazioni (SiGSI)**
- **ISO/IEC 27035:2016 - Sistema di Gestione degli Incidenti di Sicurezza delle Informazioni (SiGI)**
- **ISO/IEC 22301:2019 - Sistema di Gestione della Continuità Operativa Aziendale (BCMS)**
- **Sistema di conservazione dei documenti digitali - Sistema di conservazione digitale a norma art. 24 Regolamento UE n° 910/2014 - eIDAS**
- **Long-Term Preservation (LTP) - Sistema di Gestione della Conservazione (SGC)**

Entaksi ha definito sulla base di questi standard delle procedure operative per la gestione delle anomalie riscontrate a seguito del monitoraggio delle funzionalità del Sistema di Conservazione e delle verifiche sull'integrità degli archivi, che sono illustrate dettagliatamente nel Sistema Integrato di Gestione, e qui di seguito riportate.

Torna all'indice.

9.1. Procedure di monitoraggio

Il Sistema di Conservazione fa parte dei servizi certificati erogati da Entaksi, ed è quindi sottoposto a un monitoraggio continuo al fine di garantire la riservatezza, l'integrità e la disponibilità dei dati ed il rispetto dei livelli di servizio definiti nel contratto con il cliente.

La struttura di monitoraggio prevede due tipologie di controlli:

- Sistemistici, che esaminano l'utilizzo di risorse, la disponibilità e le prestazioni delle componenti del sistema.
- Applicativi che riguardano sonde sui servizi, quadrature, monitoraggio dei picchi elaborativi.

Le grandezze sono misurate con continuità, secondo adeguate frequenze di campionamento, e vengono raccolte in un sistema centrale di monitoraggio che consente di visualizzare sia l'andamento storico che quello in tempo reale dei vari componenti. Il sistema di monitoraggio di Entaksi è realizzato tramite vari strumenti di raccolta, memorizzazione, presentazione che consentono anche la definizione di soglie e allarmi che vengono notificati ad un Incident Response Team (IRT) quando vengono rilevate delle anomalie in determinate misure o nei loro andamenti.

Allo stesso modo, i log dei sistemi convergono in un sistema centrale di log dove possono essere visualizzati in maniera coordinata per intervallo temporale. I dati di monitoraggio ed i log sono conservati per 6 mesi.

Torna all'indice.

9.2. Controlli di sicurezza

La sicurezza dei dati è conseguita implementando, in modo organico e coerente, una serie di controlli di diversa origine, natura e contenuto, resi tra loro congruenti dalla metodologia adottata, quali quelli effettuati su politiche, procedure, procedimenti, organizzazione e funzioni software. In questo modo viene garantita l'indipendenza tra i controlli sul Sistema, ma al contempo la loro affidabilità su tutti gli aspetti dello stesso.

Torna all'indice.

9.2.1. Piano dei controlli

La scelta e l'attuazione dei controlli da effettuare discende da una metodica pianificazione, attenta sia al quadro generale di funzionamento che al particolare.

Nella pianificazione dei controlli non è trascurato il coinvolgimento di tutte le parti interessate, cioè, oltre agli operatori della sicurezza delle informazioni, anche utenti, fornitori, clienti ed esperti di organizzazioni esterne.

Il risultato di questa pianificazione è il piano dei controlli di Entaksi, che è comprensivo di tutti le verifiche previste per gli standard di certificazione. In particolare, per quanto riguarda gli asset critici, il piano si basa sulle considerazioni emerse dall'analisi dei rischi, mentre per gli altri asset vengono eseguiti con frequenza definita, e comunque non superiore ad un anno, i controlli atti a soddisfare i requisiti di sicurezza espressi nell'allegato A della norma ISO/IEC 27001:2013 e ricavati dagli altri standard.

Torna all'indice.

9.2.2. Tipologia dei controlli

Nell'ambito dei controlli previsti e formalizzati, sono definite due categorie:

- controlli ricorrenti del Sistema Integrato di Gestione;
- controlli specifici.

I controlli ricorrenti del Sistema Integrato di Gestione sono quei controlli che si riferiscono all'adozione delle modalità organizzative, delle procedure formali e delle impostazioni del sistema informativo atte a rendere conforme alla norma il sistema di gestione della sicurezza delle informazioni. Questo tipo di controlli viene eseguito sistematicamente con cadenza temporale non superiore ad un anno solare, e non entra a far parte di quelli eseguiti nella fase di analisi dei rischi.

I controlli specifici, invece, sono quei controlli che, in maniera dinamica, devono essere eseguiti durante l'esercizio quotidiano del Sistema, per garantire l'aderenza dello stesso all'evoluzione tecnologica, applicativa o delle condizioni d'uso. I controlli specifici vengono di norma eseguiti in un contesto di analisi del rischio.

Torna all'indice.

9.2.3. Modalità di esecuzione dei controlli

Durante l'esercizio del Sistema i controlli vengono eseguiti secondo due diverse dinamiche, corrispondenti alle due tipologie definite sopra:

- I controlli ricorrenti del Sistema Integrato di Gestione vengono eseguiti in maniera pianificata durante le attività di audit della sicurezza, con la frequenza stabilita per ciascun controllo;
- I controlli specifici possono essere eseguiti a seguito di:
  - audit;
  - variazioni dell'architettura o configurazione del sistema informativo;
  - incidenti di sicurezza;
  - altri eventi che possono determinare il mutamento del grado di sicurezza del Sistema (ad esempio la pubblicazione di nuove vulnerabilità nel software o la rilevazione di tentativi di attacco informatico mirato al sistema o genericamente presente in rete).

I controlli sul Sistema di Conservazione vengono effettuati dal Responsabile della Sicurezza che si occupa della manutenzione del Sistema e della sua conformità alle richieste degli standard di riferimento. I controlli vengono effettuati attraverso apposite schede di controllo pianificate, che riportano il riferimento alle procedure di sicurezza, e la descrizione del controllo e la periodicità con il quale deve essere eseguito. Attraverso queste schede guida i controlli eseguiti per ogni argomento riportato vengono puntualmente registrati.

Torna all'indice.

9.2.4. Registrazione e valutazione dell'efficacia dei controlli

Ad ogni attività di controllo eseguita, che consiste di norma nell'esecuzione di un insieme più o meno vasto di controlli tra loro coordinati, segue la redazione dei documenti di valutazione rischi, denominati "Rapporto valutazione rischi", ed il conseguente piano di trattamento, denominato "Piano trattamento rischi".

Nel documento di valutazione rischi sono riportate le registrazioni puntuali dei controlli eseguiti, la metodologia di verifica dell'efficacia del controllo, le considerazioni generali sulla sicurezza del sistema che emergono dalle attività condotte ed eventuali suggerimenti o proposte per l'evoluzione del sistema.

Nel piano di trattamento è riportata la pianificazione delle attività di mitigazione dei rischi emersi dall'analisi formalizzata nel documento di valutazione.

Torna all'indice.

9.3. Verifica della integrità degli archivi

I controlli periodici di integrità dei documenti conservati, eseguiti tramite il controllo dell'integrità degli indici, della leggibilità dei contenuti e della congruenza dell'impronta dei documenti, sono eseguiti da una procedura che attraversa l'intero archivio a ciclo continuo operando a bassa priorità. Impiegando mediamente alcune settimane per completare l'attraversamento, la procedura consente di eseguire la verifica più volte all'anno. I tempi di esecuzione vengono monitorati almeno trimestralmente per verificare che le prestazioni consentano di non scendere al di sotto della frequenza annuale di esecuzione del controllo.

La procedura registra sul log del sistema le deviazioni rilevate e le notifica all'Incident Response Team (IRT) che prende in esame l'anomalia operando eventualmente le operazioni necessarie per il ripristino dei dati.

Di seguito le tipologie di verifiche attuate nel processo di controllo di integrità:

- verifiche periodiche sui documenti conservati, tendenti a verificare periodicamente, con cadenza non superiore a cinque anni, l'effettiva integrità dei documenti stessi, provvedendo, se necessario, al loro riversamento. La procedura che gestisce il processo di conservazione presenta delle funzionalità di controllo massivo dei dati conservati: questi controlli consistono nell'impostare a livello informatico la periodicità dei controlli da effettuare. L'applicazione che gestisce il processo di conservazione, effettua un check automatico registrando per ogni PDA o documento conservato la data e ora in cui è stata eseguita l'ultima verifica di integrità. Nel caso siano verificate delle anomalie viene aperto un ticket per l'incidente, al fine di recuperare il dato dalle copie di sicurezza.
- verifiche periodiche sullo stato di conservazione dei supporti di memorizzazione, tendenti a verificare con l'ausilio di software appropriati lo stato di conservazione dei supporti di memorizzazione, e a ricercare eventuali difetti, provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti.

A fronte di anomalie riscontrate il documento viene recuperato in copie di backup, in conformità alle procedure definite dalle certificazioni specificate nel paragrafo successivo.

Torna all'indice.

9.4. Soluzioni adottate in caso di anomalie

Nell'eventualità vengano riscontrate anomalie nel Sistema di Conservazione che portino ad una non conformità delle impronte dei file conservati, il Responsabile della Sicurezza apre un ticket d'incidente al fine di trovare una soluzione al problema che ha portato all'anomalia, e contestualmente viene apportata, se necessario, una correzione al Sistema. Una volta accertato che il PDA o il documento conservato risulta corrotto, viene recuperata la copia originale dello stesso attraverso il backup del Sistema. I backup vengono eseguiti su tutto il sistema informativo oltre che sui file conservati, per garantire la continuità dello stesso. Le copie di backup vengono anch'esse regolarmente testate e controllate, così come i software di riferimento. Il backup viene eseguito regolarmente ogni 24 ore e trasferito in un datacenter geograficamente distante da quello in cui si trovano i dati.

Torna all'indice.

9.5. Continuità Operativa e Disaster Recovery

Entaksi mette in atto una serie di accorgimenti di sicurezza e prevenzione al fine di garantire la continuità dei principali processi per assicurare l'erogazione dei propri servizi nei confronti degli utenti finali, conformemente allo standard ISO/IEC 22301:2019. Sono attuate misure orientate a garantire la continuità e la disponibilità dei sistemi informativi rispetto al normale esaurimento del ciclo di vita dei componenti e al loro danneggiamento causato da eventi accidentali o dolosi.

Nel Sistema Integrato di Gestione di Entaksi è presente una procedura di gestione della continuità operativa che descrive nel dettaglio le attività da eseguire e le responsabilità qualora si verifichi un evento che comporti l'indisponibilità del Sistema.

Torna all'indice.

9.5.1. Piano di disponibilità delle risorse

Nell'ambito degli audit periodici sulla sicurezza del sistema, Entaksi aggiorna il Sistema di Conservazione con le modalità descritte nel documento interno del SIG relativo al piano di gestione delle capacità. Questo documento espone un piano generale di disponibilità delle risorse, sia risorse umane, definite in termini di profili professionali necessari, sia risorse infrastrutturali, definite in termini di capacità di elaborazione e di memorizzazione necessarie per il funzionamento del sistema.

Dal punto di vista dei server fisici, il sistema Entaksi è costituito da un insieme di server equipotenti in termini di capacità di

elaborazione, sui quali è configurato un sistema software distribuito e scalabile progettato per non risentire degli eventuali malfunzionamenti dei singoli componenti. Essendo i server fisici gestiti in outsourcing presso un fornitore specializzato, la sostituzione o l'aggiunta di un nuovo server o di parti di esso sono ottenute in tempi molto ridotti (di norma nell'ordine di poche ore) e con costi certi, senza richiedere investimenti o trattative di acquisto.

Torna all'indice.

9.5.2. Modalità operativa per la continuità operativa

Nel caso si verifichino eventi tali da compromettere la disponibilità dei sistemi, Entaksi applica un processo di continuità operativa basato sui seguenti criteri:

- definizione della capacità minima di elaborazione e delle comunicazioni;
- definizione dei dati fondamentali e individuazione del livello di priorità da assegnare ad ogni attività associata al loro trattamento.

Conseguentemente ai processi definiti sono stati sviluppati e sottoposti a test periodici i piani operativi di continuità operativa, riportati dettagliatamente nei manuali del SIG, da utilizzare in funzione dei vari livelli di indisponibilità del Sistema.

Torna all'indice.