AZIENDA CON SISTEMA INTEGRATO DI GESTIONE
QUALITÀ, SICUREZZA DELLE INFORMAZIONI, SERVIZI IT
CERTIFICATO DA DNV·GL
= ISO 9001 = ISO 27001 = ISO 20000-1 =

Entaksi Solutions srl

Manuale della conservazione

Informazioni sul documento

Progetto	SGC
ID documento	MAN eCON 20151222 Manuale della conservazione
ID prodotto	eCON
Tipo	Manuali
Data creazione	22/12/2015
Ultima revisione	02/03/2016
Versione	1.2
Autore	Alessandro Geri
Stato	Rilasciato
Allegati	
Classificazione	Pubblico

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

Approvazione del documento

Data	Addetto	Mansione	Firma
02/03/2016	Alessandro Geri	Amministratore Unico	Entaksi Solutions srl via la Piana 76 – Pontepetri 51028 San Marcello Pistoiese (PT) Alessandro Geri amministratore unico

Firmato digitalmente da GERI ALESSANDRO
Data: 2016.03.03 12:22:18 +01'00'

Revisioni

Data	Versione	Nome	Azione
22/12/2015	0.1	Alessandro Geri	Creazione
28/01/2016	1.0	Alessandro Geri	Rilascio
29/02/2016	1.1	Alessia Soccio	Adeguamento alle richieste AgID inviate in data 29/02/2016.
02/03/2016	1.2	Alessandro Geri	Modifiche cap. 4 per ulteriori richieste AgID inviate il 02/03/2016

Indice generale

1. Scopo e ambito del documento 4
2. Terminologia 5
2.1 Glossario 5
2.2 Acronimi 10
3. Normativa e standard di riferimento 10
3.1 Normativa di riferimento 11
3.2 Standard di riferimento 11
4. Ruoli e responsabilità 12
5. Struttura Organizzativa per il Servizio di Conservazione 16
5.1 Organigramma 16
5.2 Strutture organizzative 16
6. Oggetti sottoposti a Conservazione 21
6.1 Oggetti conservati 22
6.2 Pacchetto di Versamento (PDV) 37
6.3 Pacchetto di Archiviazione (PDA) 41
6.4 Pacchetto di Distribuzione (PDD) 45
7. Processo di Conservazione 46
7.1 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico 47
7.2 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in esso contenuti 48
7.3 Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico 49
7.4 Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie 53
7.5 Preparazione e gestione dei pacchetti di archiviazione 53
7.6 Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione 54
7.7 Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del Pubblico Ufficiale nei casi previsti 55
7.8 Scarto dei pacchetti di archiviazione 56
7.9 Predisposizione di misure a garanzia della interoperabilità e trasferibilità ad altri conservatori 56
7.10 Cessazione del servizio di conservazione 57
8. Il Sistema di Conservazione 57
8.1 Componenti logiche 58
8.2 Componenti tecnologiche 59
8.3 Componenti fisiche 59
8.4 Procedure di gestione ed evoluzione 60
9. Monitoraggio e controlli 62
9.1 Procedure di monitoraggio 62
9.2 Controlli di sicurezza 63
9.2.1 Piano dei controlli 63
9.2.2 Tipologia dei controlli 63
9.2.3 Modalità di esecuzione dei controlli 63
9.2.4 Registrazione e valutazione dell'efficacia dei controlli 64
9.3 Verifica della integrità degli archivi 64
9.4 Soluzioni adottate in caso di anomalie 64
9.5 Continuità Operativa e Disaster Recovery 65
9.5.1 Piano di disponibilità delle risorse 65
9.5.2 Modalità operativa in condizioni di emergenza 65

1. Scopo e ambito del documento

Il presente manuale descrive il sistema di conservazione digitale di **Entaksi Solutions srl**, denominata di seguito **Entaksi**.

L'azienda ha sede legale in via la Piana 76 - fraz. Pontepetri, 51028 San Marcello Pistoiese (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 3, in particolare il contenuto del Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 relativo alle Regole tecniche in materia di sistema di conservazione, il Decreto legislativo del 7 marzo 2005, n. 82 ossia il Codice dell'amministrazione digitale, e il Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013, che stabilisce le regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici che le firme digitali e le marche temporali utilizzate dal processo di conservazione dovranno rispettare.

Le normative sopra riportate sono applicate nel rispetto della disciplina rilevante in materia di tutela dei dati personali e, in particolare, del Codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196.

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

- **ISO 9001**: certificazione standard rilasciata in conformità alla norma UNI EN ISO 9001:2008 che ha lo scopo di descrivere i requisiti per la realizzazione e gestione del Sistema di Gestione della Qualità (SGQ).
- **ISO 27001**: certificazione standard rilasciata in conformità alla norma ISO/IEC 27001:2013 che ha lo scopo di descrivere i requisiti per la realizzazione e gestione del Sistema di Gestione della Sicurezza delle Informazioni (SIGSI).
- **ISO 20000**: certificazione standard rilasciata in conformità alla norma ISO 20000-1:2011 che ha lo scopo di descrivere i requisiti per la realizzazione e gestione del Sistema di Gestione dei Servizi Informatici (SGS).

Nell'ultimo Audit sostenuto per il rinnovo delle certificazioni (dicembre 2015) è stata inserita una puntuale attività di verifica del Sistema di Conservazione, basata su una specifica check-list stilata da DNV GL 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 dell'articolo 13 del Decreto Legislativo n. 196 del 30 giugno 2003;
- la **Nomina a Responsabile Esterno per il trattamento dei dati.**

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 per l'accreditamento presso l'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 semplificativo, la terminologia utilizzata nel manuale, suddivisa tra il glossario dei termini tecnici e gli acronimi.

2.1 Glossario

Termine	Definizione
accesso	operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici
accreditamento	riconoscimento, da parte dell’Agenzia per l’Italia digitale, del possesso dei requisiti del livello più elevato, in termini di qualità possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione
affidabilità	caratteristica che esprime il livello di fiducia che l’utente ripone nel documento informatico
aggregazione documentale informatica	aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all’oggetto e alla materia o in relazione alle funzioni dell’ente
allegato	documento associato a un documento archivistico, unito allo stesso da un legame di natura giuridica e/o funzionale, che diventa quindi parte integrante di quel documento archivistico
archivio	complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell’attività
archivio informatico	archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico
area organizzativa omogenea	un insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell’articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445
attestazione di conformità delle copie per immagine su supporto informatico di un documento	dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico

Termine	Definizione
analogico	
autenticità	caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico
base di dati	collezione di dati registrati e correlati tra loro
certificatore accreditato	soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
ciclo di gestione	arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo
classificazione	attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati
Codice	decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni
codice eseguibile	insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici
Condizioni Generali del Servizio	documento, allegato al Manuale, che contiene le condizione specifiche del servizio di conservazione, compresi l'elenco dei formati di documenti accettati dal sistema, le modalità di garanzia di leggibilità degli oggetti conservati, requisiti particolari e specifiche tecniche del servizio concordati tra il Produttore e il Conservatore
conservatore accreditato	soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, dall'Agenzia per l'Italia digitale
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 e descritto nel manuale di conservazione
Coordinatore della Gestione Documentale	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 D.P.R. 445/2000 nei casi di amministrazioni che abbiano istituito più Aree Organizzative Omogenee
copia	duplicato di un oggetto, risultante da un processo di riproduzione
copia analogica del documento informatico	documento analogico avente contenuto informativo identico a quello del documento informatico da cui è tratto
copia autentica	copia certificata da un ufficiale autorizzato a svolgere tale funzione, affinché essa risulti legalmente ammissibile in giudizio
copia di sicurezza	copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 delle Regole Tecniche del D.P.C.M. 3 dicembre 2013
copia informatica di documento analogico	documento informatico avente contenuto informativo identico a quello del documento analogico da cui è tratto
copia informatica di documento informatico	documento informatico avente contenuto informativo identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari
destinatario	identifica il soggetto/sistema al quale il documento informatico è indirizzato
documento o documento archivistico	testimonianza scritta su qualunque tipo di supporto di un fatto, un atto o un dato di natura giuridica, compilata con l'osservanza di determinate forme che conferiscono al documento pubblica fede e forza di prova; è formato o ricevuto nello svolgimento di un'attività pratica come strumento o prodotto di questa attività, e archiviato per ulteriori azioni o consultazione
documento analogico	un documento formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta (esempio: documenti cartacei), come le immagini su film (esempio: pellicole mediche, microfiches, microfilm), come le magnetizzazioni su nastro (esempio: cassette e nastri magnetici audio e video), e si distingue in documento originale e copia
documento analogico originale	un documento analogico che può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi

Termine	Definizione
documento informatico	la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti, la cui componente digitale o l'insieme di componenti sono trattati e gestiti come un documento archivistico
duplicato informatico	documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario
esibizione	operazione che consente di visualizzare un documento conservato e di ottenerne copia
estratto per riassunto	documento nel quale si attestano in maniera sintetica ma esaustiva fatti, stati o qualità desunti da dati o documenti in possesso di soggetti pubblici
evidenza informatica	una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica
fascicolo informatico	aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento; nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del Codice dell'Amministrazione Digitale
firma digitale	risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici
formato	modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
funzionalità aggiuntive	le ulteriori componenti del sistema di protocollo informatico necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni
funzionalità interoperative	le componenti del sistema di protocollo informatico finalizzate a rispondere almeno ai requisiti di interconnessione di cui all'articolo 60 del D.P.R. 28 dicembre 2000, n. 445
funzionalità minima	la componente del sistema di protocollo informatico che rispetta i requisiti di funzionalità minima operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445
funzione di *hash*	una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
generazione automatica di documento informatico	formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni
identificativo univoco	sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione
immodificabilità	caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso
impronta	la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di *hash*
integrità	insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato
insieme minimo di metadati del documento informatico	complesso dei metadati, la cui struttura è descritta nell'allegato 5 del D.P.C.M. del 13 novembre 2014, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta integrità insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato
interoperabilità	capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi
leggibilità	insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti
log di sistema	registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati
manuale di conservazione	strumento che descrive il sistema di conservazione dei documenti informatici ai sensi

Termine	Definizione
	dell'articolo 9 delle Regole Tecniche del D.P.C.M. 3 dicembre 2013
manuale di gestione	strumento che descrive il sistema di gestione informatica dei documenti di cui all'articolo 5 delle regole tecniche del protocollo informatico ai sensi delle Regole Tecniche per il protocollo informatico D.P.C.M. 31 ottobre 2000 e successive modificazioni e integrazioni
marca temporale	una evidenza informatica, risultato di una procedura con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi
memorizzazione	processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici
metadati	insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 del DCPM 3 dicembre 2013
pacchetto di archiviazione	pacchetto informativo composto dalla trasformazione di uno o più pacchetti di archiviazione versamento secondo le specifiche contenute nell'allegato 4 del presente decreto e secondo 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
pacchetto di versamento	pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione
pacchetto informativo	contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare
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 nell'ambito dell'organizzazione di appartenenza
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 nell'ambito dell'organizzazione di appartenenza
piano di conservazione	strumento, integrato con il sistema di classificazione per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445
piano generale della sicurezza	documento per la pianificazione delle attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza
presa in carico	accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione
processo di conservazione	insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 10 delle Regole Tecniche del D.P.C.M. 3 dicembre 2013
produttore	persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale.
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
registrazione informatica	insieme delle informazioni risultanti da transazioni informatiche o dalla presentazione in via telematica di dati attraverso moduli o formulari resi disponibili in vario modo all'utente
registro o registro di conservazione	Entità dell'archivio documentale che contiene la struttura dati che, per ciascun ente o struttura, permette la conservazione dei PDA raggruppati per anno / tipo documento / sezionale o serie archivistica
registro di protocollo	registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti
registro particolare	registro informatico di particolari tipologie di atti o documenti; nell'ambito della pubblica

Termine	Definizione
	amministrazione è previsto ai sensi dell'articolo 53, comma 5 del D.P.R. 28 dicembre 2000, n. 445
repertorio informatico	registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche con cui si formano altri atti e documenti o indici di atti e documenti secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica
responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi	dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al 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, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione.
responsabile della conservazione	soggetto responsabile dell'insieme delle attività elencate nell'articolo 7, comma 1 delle regole tecniche del sistema di conservazione
responsabile del trattamento dei dati	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali
responsabile della sicurezza	soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza
riferimento temporale	informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento
scarto	operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale
sistema di classificazione	strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata
sistema di conservazione	sistema di conservazione dei documenti informatici di cui all'articolo 44 del Codice
sistema di gestione informatica dei documenti	nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445; per i privati è il sistema che consente la tenuta di un documento informatico
staticità	caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione
Testo unico	decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni
tipologia documentale	classificazione del documento per categoria di contenuto
transazione informatica	particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche della base di dati
ufficio utente	riferito ad un area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico
unità archivistica	unità minima indivisibile di un complesso archivistico, può aggregare più documenti fisicamente contigui o essere costituita da una singola unità documentaria
unità documentaria	unità minima, concettualmente non divisibile, di cui è composto un archivio: corrisponde al documento archivistico
utente	persona, ente o sistema che interagisce con i servizi di un sistema di gestione utente informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse
versamento agli archivi di stato	operazione con cui il responsabile della conservazione di un organo giudiziario o amministrativo dello Stato effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali

Tabella 1: Glossario.

Torna all'indice.

2.2 Acronimi

Termine	Definizione
AgID	Agenzia per l'Italia Digitale
AOO	Area Organizzativa Omogenea
CA	*Certification Authority*
PDA	Pacchetto di Archiviazione
PDD	Pacchetto di Distribuzione
PDV	Pacchetto di Versamento
PEC	Posta Elettronica Certificata
RDV	Rapporto di Versamento
RdS	Richiesta di Servizio
RPO	il *Recovery Point Objective* (obiettivo temporale di recupero) indica la perdita dati tollerata, rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di un evento imprevisto
RTO	il *Recovery Time Objective* (tempo ripristino richiesto) è l'arco temporale entro il quale un processo informatico ovvero il Sistema Informativo primario deve essere ripristinato dopo un disastro o una condizione di emergenza (o interruzione), al fine di evitare conseguenze inaccettabili
SGQ	Sistema di Gestione della Qualità, definito dalla norma UNI EN ISO 9001:2008
SGS	Sistema di Gestione dei Servizi Informatici, definito dalla norma ISO 20000-1:2011
SIG	Sistema Integrato di Gestione di Entaksi, certificato conforme alle normative ISO 9001:2008, ISO/IEC 27001:2013, ISO/IEC 20000-1:2011
SIGSI	Sistema di Gestione della Sicurezza delle Informazioni, definito dalla norma ISO 27001:2013
SLA	*Service Level Agreement*
SOES	Supporto Operativo Erogazione Servizio
SOSI	Supporto Operativo Sistemi Informativi
TSA	*Time Stamping Authority*, ente terzo che emette i certificati di marcatura temporale
TSS	*Time Stamping Service*, servizio di marcatura temporale che emette marche temporali utilizzando il certificato emesso da una TSA. Questo servizio deve rispettare i requisiti del RFC 3161 e il titolo IV del D.P.C.M. 13 gennaio 2004

Tabella 2: Acronimi.

Torna all'indice.

3. Normativa e standard di riferimento

Per garantire la gestione a norma del Sistema di Conservazione, 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 30 giugno 2003, n. 196 e s.m.i.** – Codice in materia di protezione dei dati personali.
- **Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i.** – Codice dei Beni Culturali e del Paesaggio.
- **Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i.** – Codice dell'amministrazione digitale (CAD).
- **Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013** – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71.
- **Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013** – Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.
- **Circolare AGID 10 aprile 2014, n. 65** – Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.
- **Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014** – Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23- bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

Torna all'indice.

3.2 Standard di riferimento

- **ISO 14721:2012 OAIS**: (*Open Archival Information System*), un modello di sistema informativo aperto per la gestione e l'archiviazione a lungo termine di contenuti informativi.
- **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/IEC 27001:2013**: *Information technology – Security techniques – Information security management systems – Requirements,* norma che definisce i requisiti di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI o ISMS).
- **UNI 11386:2010 Standard SInCRO**: Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.
- **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.
- **ETSI TS 101 533-1 V1.3.1 (2012-04)**: *Technical Specification, Electronic Signatures and Infrastructures* (ESI); *Data Preservation Systems Security; Part 1: Requirements for Implementation and Management*, contiene i 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); *Data Preservation Systems Security; Part 2: Guidelines for Assessors*, contiene le linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.
- **ITU-T X.509 (10/2012)**: *Recommendation* (Standard identico: ISO/IEC 9594-8:2014 – *Information technology – Open Systems Interconnection – The Directory – Part 8: Public-key and attribute certificate frameworks)*.
- **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 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.

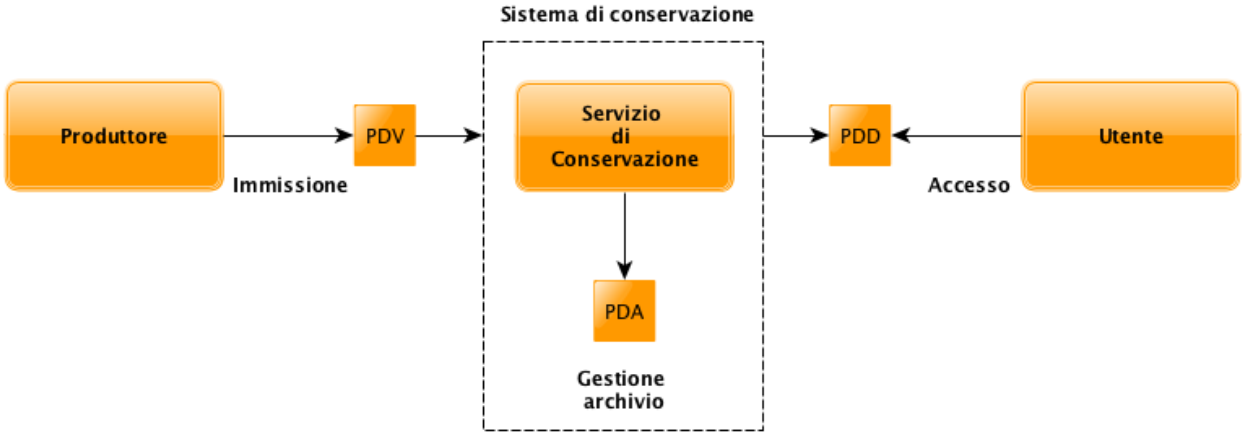

Figura 1: Ruoli e responsabilità.

Il Servizio di Conservazione erogato da Entaksi prevede i ruoli definiti in seguito, in conformità al documento “Elenco profili professionali per la conservazione” pubblicato da AgID in base alla Circolare n. 65/2014 (G.U. n. 89 del 16/04/2014). Il ruolo di Responsabile della Conservazione è altresì specificato nel D.P.C.M. 3 dicembre 2013, artt. 6-7.

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 dal D.P.C.M 3 dicembre 2013, “La conservazione può essere affidata ad un soggetto esterno, secondo i modelli organizzativi di cui all’art. 5, mediante contratto o convenzione di servizio che preveda l’obbligo del rispetto del manuale di conservazione predisposto dal responsabile della stessa.”.

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 paragrafo 5), suddivisa in aree operative, che prevede per ciascuno dei Responsabili l'assunzione degli incarichi e delle responsabilità descritti nella seguente tabella.

Ruolo e nominativo	Formazione ed esperienze minime	Attività associate al ruolo	Tipologia di rapporto contrattuale
Responsabile del servizio di conservazione - Alessandro Geri	Laureato con esperienza di almeno 5 anni nel ruolo. In assenza di laurea esperienza in ruolo analogo di almeno 8 anni.	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.	Tempo Indeterminato.
Responsabile della funzione archivistica di conservazione - Alessia Soccio	Laurea magistrale in archivistica con esperienza di almeno 2 anni nel ruolo o laurea con percorsi di formazione specialistica nel settore e con esperienza di almeno 3 anni nel ruolo o laurea con esperienza di almeno 5 anni.	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.	Tempo Indeterminato.
Responsabile del trattamento dei dati personali - Alessandro Geri	Laureato con esperienza di almeno 3 anni nel ruolo. In assenza di laurea esperienza in ruolo analogo di almeno 5 anni.	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.	Tempo Indeterminato.
Responsabile della sicurezza dei sistemi per la conservazione - Alessandro Geri	Laureato in discipline scientifiche con esperienza di almeno 3 anni nel ruolo. In assenza di laurea esperienza in ruolo analogo di almeno 5 anni.	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.	Tempo Indeterminato.
Responsabile dei sistemi informativi per la conservazione - Paola Caioli	Laureato in discipline scientifiche con esperienza nel ruolo di almeno 3 anni. In assenza di laurea esperienza in ruolo analogo di almeno 5 anni.	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.	Tempo Indeterminato.
Responsabile dello sviluppo e della manutenzione del sistema di conservazione - Stefano Travelli	Laureato in discipline scientifiche con esperienza nel ruolo di almeno 3 anni. In assenza di laurea esperienza in ruolo analogo di almeno 5 anni.	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.	Tempo Indeterminato.

Tabella 3: Responsabili.

Secondo quanto riportato nell'articolo 6 del D.P.C.M. del 3 dicembre 2013 il Responsabile del Servizio di Conservazione "può delegare lo svolgimento del processo di conservazione o di parte di esso ad uno o più soggetti di specifica competenza ed esperienza in relazione alle attività ad essi delegate". Ad oggi non sono presenti deleghe.

I ruoli sono così assegnati nel tempo:

Ruolo	Nominativo	Periodo nel ruolo
Responsabile del Servizio di Conservazione	Alessandro Geri	gennaio 2013 – oggi
Responsabile della Funzione Archivistica di Conservazione	Stefano Travelli	gennaio 2013 – giugno 2015
	Alessia Soccio	luglio 2015 – oggi
Responsabile del Trattamento dei Dati Personali	Alessandro Geri	gennaio 2013 – oggi
Responsabile della Sicurezza	Alessandro Geri	gennaio 2013 – oggi
Responsabile dei Sistemi Informativi	Paola Caioli	gennaio 2013 – oggi
Responsabile dello Sviluppo e della Manutenzione del Sistema di Conservazione	Stefano Travelli	gennaio 2013 – oggi

Tabella 4: Periodo in ruolo dei Responsabili.

Il **Responsabile del Servizio di Conservazione**, è il soggetto responsabile della creazione e del mantenimento del sistema e del processo di conservazione documentaria. Definisce e attua le politiche complessive del Sistema di Conservazione, e ne governa la gestione. In particolare:

- definisce e attua delle politiche complessive del sistema di conservazione, nonché del governo della gestione dello stesso;
- definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente;
- gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
- genera il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
- qualora venga richiesto dal manuale e nei casi previsti genera e sottoscrive i PDV, PDA, PDD con firma digitale o firma elettronica qualificata;
- effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
- si assicura con verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
- al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità, e adotta analoghe misure con riguardo all'obsolescenza dei formati;
- provvede e verifica alla duplicazione (o copia) dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
- adotta e verifica presso il Responsabile della Sicurezza l'adozione delle misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12 del D.P.C.M. 3 dicembre 2013;
- assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
- assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
- predispone il manuale di conservazione di cui all'art. 8 del D.P.C.M. 3 dicembre 2013 e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti;
- avvalendosi della struttura di gestione del Servizio (descritta nei paragrafi seguenti) assicura che tutte le componenti erogate dal Servizio vengano evase secondo i *Service Level Agreements* (SLA) concordati e i *requirements* specifici dei documenti mandati in conservazione.

Il **Responsabile della Funzione Archivistica di Conservazione** definisce, in accordo con l'ente produttore, le modalità di trasferimento dei documenti informatici verso il sistema di conservazione. Si occupa di stabilire:

- modalità di acquisizione dei documenti;
- modalità di aggregazione (se necessaria);
- il set di metadati associati ai documenti e ai fascicoli informatici.

Inoltre svolge le attività specifiche per assicurare:

- la definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente

produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferite, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato;
- il monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione;
- il versamento, per gli organi giudiziari e amministrativi dello Stato, dei documenti conservati all'Archivio Centrale dello Stato e agli Archivi di Stato secondo quanto previsto dalle norme vigenti;
- la collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali e del turismo per quanto di competenza.

Su richiesta e dietro specifica delega del Responsabile del Servizio di Conservazione, può sottoscrivere i PDV, PDA, PDD con firma digitale o firma elettronica qualificata.

Il **Responsabile del Trattamento dei Dati Personali** si occupa di garantire il rispetto della normativa vigente in materia del trattamento dei dati personali e che il trattamento dei dati affidati dal cliente avvenga nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e riservatezza.

Il **Responsabile della Sicurezza** figura interna all'azienda che ricopre al contempo anche il ruolo di Responsabile della Sicurezza dei Sistemi per la Conservazione, in conformità con lo standard internazionale ISO/IEC 27001:2013 stabilisce e manutiene le *policy* di sicurezza di Entaksi. e le condivide con il Responsabile del Servizio di Conservazione e ne verifica l'applicazione nel tempo. Inoltre vigila sul Sistema di Gestione oltre che in particolare sul Sistema di Conservazione, e nel caso individui eventuali difformità, le comunica al Responsabile del Servizio di Conservazione e pianifica le azioni correttive necessarie.

Il **Responsabile dei Sistemi Informativi** per la conservazione gestisce l'esercizio delle componenti hardware e software del sistema informativo di Entaksi, ed in particolare del sistema conservazione, garantendone nel tempo la conformità alla evoluzione delle necessità informative di Entaksi nel rispetto degli standard di riferimento. Si occupa in particolare di:
- monitoraggio dei livelli di servizio dell'infrastruttura, con segnalazione di eventuali difformità dei SLA al Responsabile del Servizio di Conservazione, pianificando eventuali azioni correttive;
- pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione;
- assicura che tutte le nuove richieste di evoluzione funzionale e/o di integrazione con altre applicazioni vengano ricevute, valutate e applicate al sistema di conservazione secondo i tempi e i requisiti concordati con il Cliente;
- si occupa di seguire il cliente in tutte le fasi del Servizio di Conservazione, dall'attivazione alla eventuale chiusura dello stesso;
- esegue test funzionali sugli applicativi del Servizio per valutarne l'efficacia e l'usabilità da parte dei clienti, e analizza eventuali possibili implementazioni prima del rilascio in produzione;
- è il responsabile della pronta segnalazione al Responsabile del Servizio di Conservazione degli incidenti con livello di gravità massimo.

Su richiesta e dietro specifica delega del Responsabile del Servizio di Conservazione, può sottoscrivere i PDV, PDA, PDD con firma digitale o firma elettronica qualificata.

Il **Responsabile dello Sviluppo e della Manutenzione del Sistema di Conservazione,** o semplicemente Responsabile dello Sviluppo e della Manutenzione, coordina lo sviluppo e la manutenzione delle componenti hardware e software del sistema di conservazione. Inoltre:
- gestisce il processo tecnico di conservazione;
- provvede alla generazione del RDV, secondo le modalità previste dal manuale di conservazione;
- monitora la corretta funzionalità tecnica del sistema di conservazione;
- pianifica e monitora i progetti di sviluppo del sistema di conservazione;
- monitora gli SLA relativi alla manutenzione del sistema di conservazione;
- si 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;
- gestisce lo sviluppo di siti web e portali connessi al Servizio di Conservazione.

Su richiesta e dietro specifica delega del Responsabile del Servizio di Conservazione, può sottoscrivere i PDV, PDA, PDD con firma digitale o firma elettronica qualificata.

Torna all'indice.

5. Struttura Organizzativa per il Servizio 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 funzionigramma:

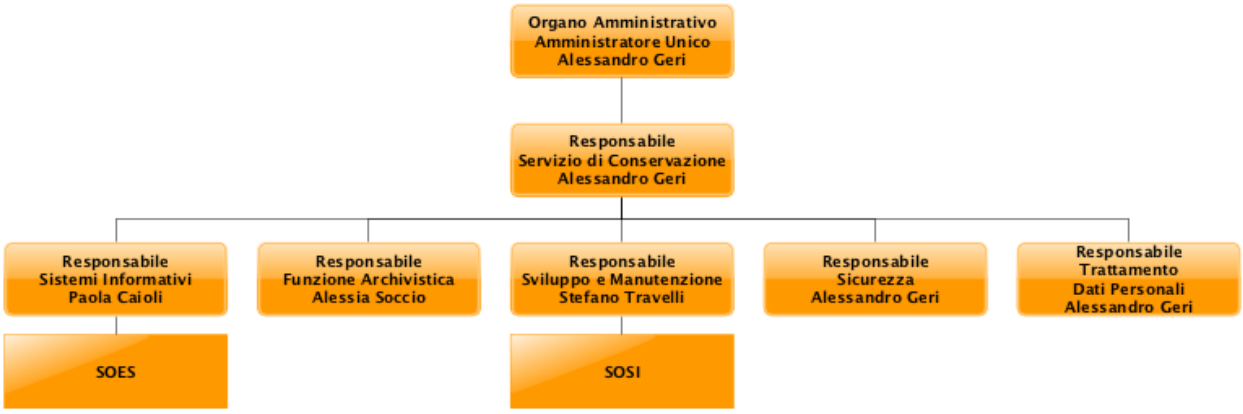

Figura 2: Funzionigramma Responsabili.

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 Sviluppo Informatico (SOSI)** è gestito dal Responsabile dello Sviluppo e della Manutenzione del Sistema di Conservazione, 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**:

	Responsabile del Servizio di Conservazione	Responsabile della Funzione Archivistica di Conservazione	Responsabile dei Sistemi Informativi	Responsabile dello Sviluppo e della Manutenzione del Sistema	Responsabile della Sicurezza	Responsabile del Trattamento dei Dati Personali
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
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

Tabella 5: Matrice delle responsabilità.

Legenda:

- R: Responsabile
- A: Agisce
- C: Collabora
- I: Informato

In base a questa descrizione, la struttura organizzativa di Entaksi si basa su un sistema di *ticketing*, attraverso il quale il cliente può richiedere, a seguito della 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., e 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 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:

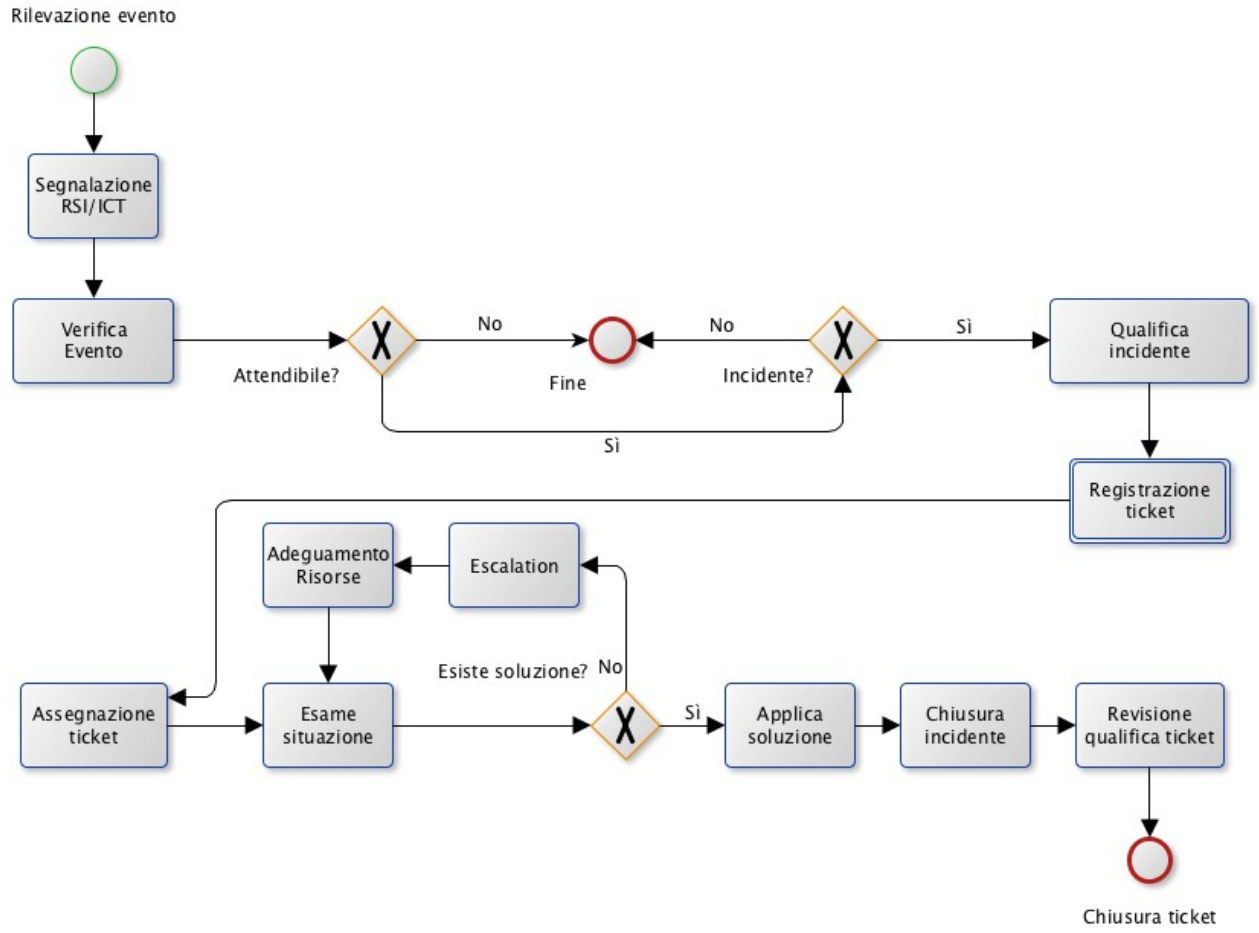

Figura 3: Workflow gestione incidenti.

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 (Procedura "PRO ISO 20130804 metodologia analisi rischi");
- requisito di sicurezza compromesso (riservatezza / integrità / disponibilità del dato);
- classificazione, riferita alle minacce censite in 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 r**ichieste 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.

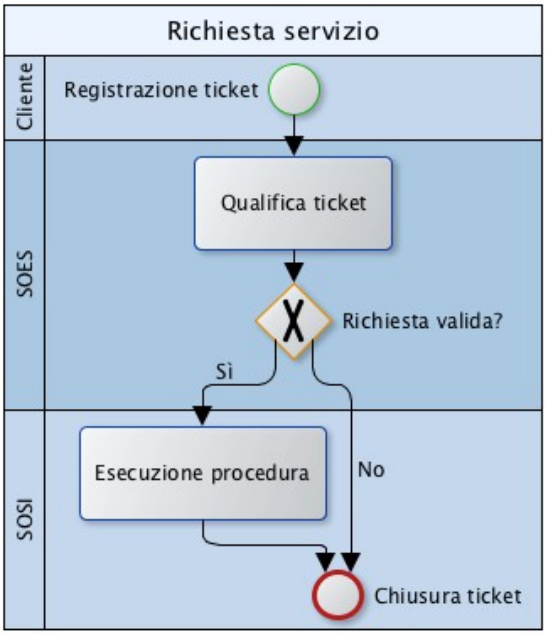

Figura 4: Workflow richiesta di servizio.

Il t**icket 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 più 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:

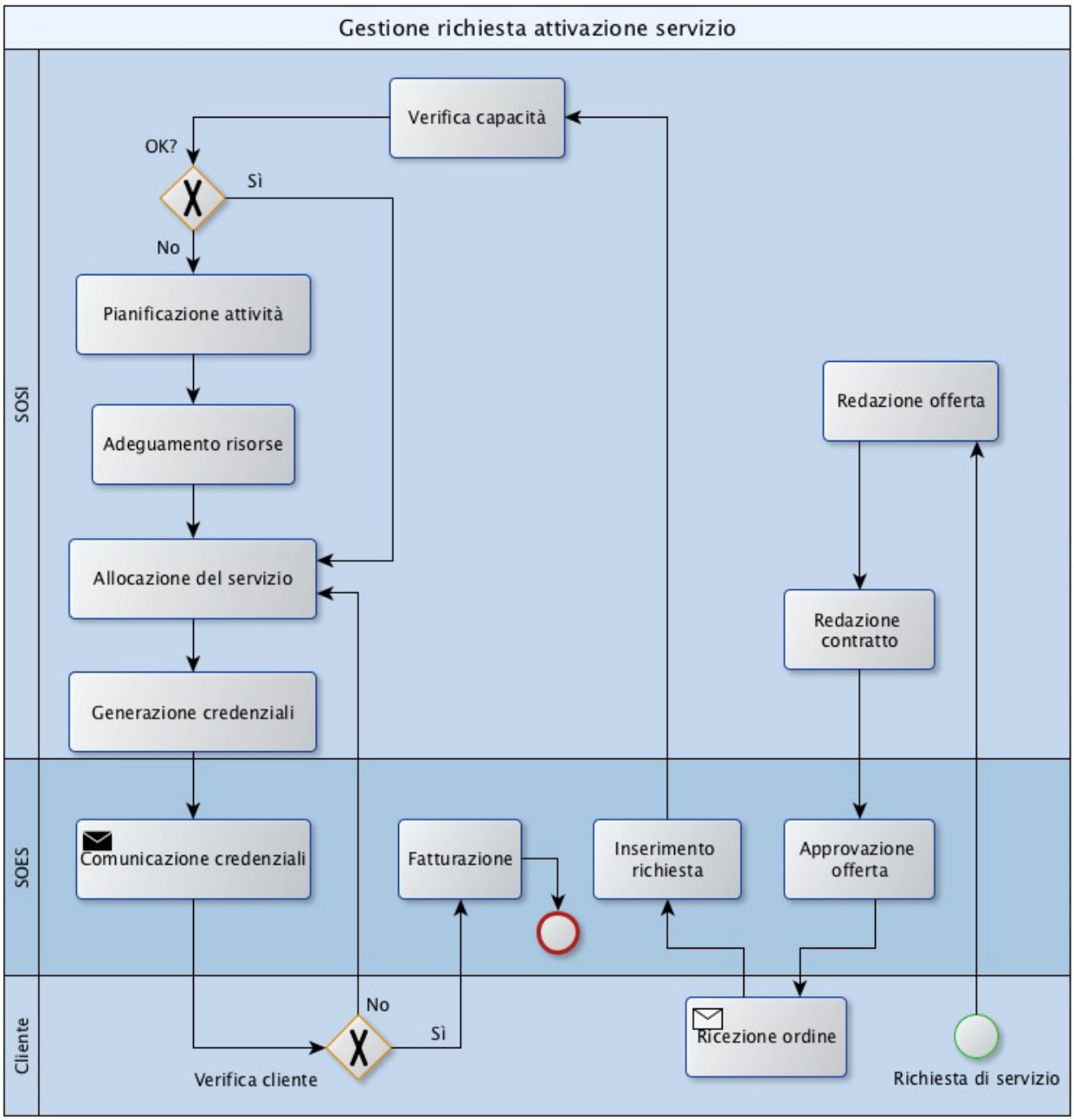

Figura 5: Workflow richiesta di attivazione del servizio.

Torna all'indice.

6. Oggetti sottoposti a Conservazione

Sono oggetti del sistema di conservazione:

a) 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 Regole Tecniche del D.P.C.M 3 dicembre 2013;
b) 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 all’art. 4 delle Regole Tecniche del D.P.C.M. 3 dicembre 2013, 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:

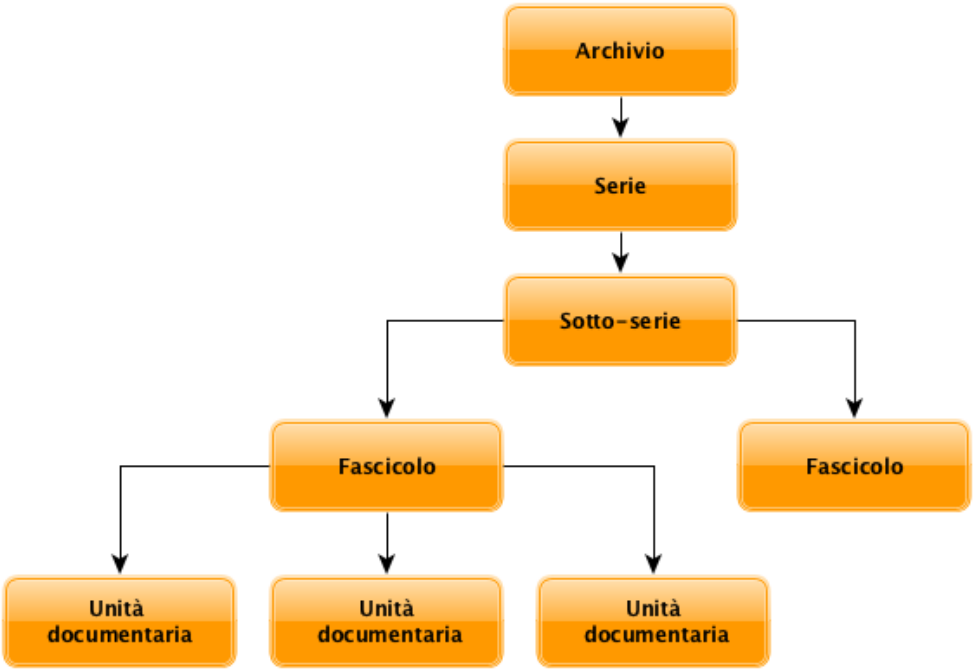

Figura 6: Struttura dell'archivio.

Dove alla voce “Archivio” corrisponde la totalità dei documenti depositati da ogni singolo Produttore, organizzati e visualizzati nel sistema in “Serie” suddivise per anno, nelle “Sotto-serie” per tipo di documento e in un'ulteriore “Sotto-serie” corrispondente al sezionale, ed infine in “Fascicoli” che contengono le singole “Unità documentarie”.

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 7.

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.

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
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

Tipo	Descrizione
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
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

Tipo	Descrizione
D77	Modello 770 semplificato
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

Tabella 6: Tipi di documento gestiti dal sistema.

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 di Conservazione e col Responsabile dello Sviluppo e della Manutenzione. Nell'evenienza, queste ulteriori tipologie sono formalizzate nell'allegato "Specificità del 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 Regole Tecniche del D.P.C.M. 3 dicembre 2013.

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.

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
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

Tipo	Estensione	Produttore	Visualizzatore	Standard	Versione	mime type
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

Tabella 7: Formati dei file accettati dal sistema.

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 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.

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.

Entità	Rappresentazione	Descrizione
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 6. Ad esempio: • `D01` Fatture attive • `D02` Fatture passive • `D03` Nota variazione aumento • … • `D84` Ricevuta presentazione modelli dichiarazione • `D85` Altri documenti
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: `AAA`. 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`.
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

Tabella 8: Definizione delle entità.

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.

Oggetto	Sintassi	Descrizione
Produttore	`<produttore> ::=` `"urn:entaksi:" <ente> ":" <struttura>`	Identifica la struttura o area organizzativa che dispone il versamento dei documenti nel sistema di conservazione. Ad esempio: `urn:entaksi:IT1234567890:ST01`

Oggetto	Sintassi	Descrizione
PDV	`<pdv> ::= <produttore> ":pdv:" <id-pdv>`	Identifica l'indice del pacchetto di versamento. Ad esempio: `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. Ad esempio: `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. Ad esempio: `urn:entaksi:IT1234567890:ST01:reg:2015:D01:S1`
PDA	`<pda> ::= <registro> ":pda:" <prog-pda>`	Identifica un pacchetto di archiviazione. Ad esempio: `urn:entaksi:IT1234567890:ST01:reg:2015:D01:S1:pda:17`
PDD	`<pdd> ::= <produttore> ":pdd:" <id-pdd>`	Identifica un pacchetto di distribuzione. Ad esempio: `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. Ad esempio: `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. Ad esempio: `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. Ad esempio: `urn:entaksi:IT1234567890:ST01:PDV:7890:fattura.pdf`

Tabella 9: Sintassi degli URN per gli oggetti rappresentati nel sistema.

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.

Oggetto	Nome file	Esempio
PDV	`<pdv.zip> ::= <pdv> ".zip"`	`urn_entaksi_IT1234567890_ST01_pdv_7890.zip`
Indice PDV	`<idpdv.xml> ::= <pdv> ".xml"`	`urn_entaksi_IT1234567890_ST01_pdv_7890.xml`
RDV	`<rdv.xml> ::= <rdv> ".xml"`	`urn_entaksi_IT1234567890_ST01_rdv_7890.xml`
PDA	`<pda.zip> ::= <pda> ".zip"`	`urn_entaksi_IT1234567890_ST01_reg_2015_D01_S1_pda_17.zip`
Indice PDA	`<idpda.xml> ::= <pda> ".xml"`	`urn_entaksi_IT1234567890_ST01_reg_2015_D01_S1_pda_17.xml`
PDD	`<pdd.zip> ::= <pdd> ".zip"`	`urn_entaksi_IT1234567890_ST01_pdd_3456.zip`
Indice PDD	`<idpdd.xml> ::= <pdd> ".xml"`	`urn_entaksi_IT1234567890_ST01_pdd_3456.xml`

Oggetto	Nome file	Esempio
Unità documentali	`<doc.zip> ::= <doc> ".zip"`	`urn_entaksi_IT1234567890_ST01_reg_2015_D01_S1_doc_123.zip`
Fascicolo	`<fascicolo.zip> ::= <fascicolo> ".zip"`	`urn_entaksi_IT1234567890_ST01_reg_2015_D01_S1_fas_123.zip`

Tabella 10: Definizione dei nomi dei file.

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 Regole tecniche del D.P.C.M. 3 dicembre 2013, 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 gruppi:

- `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
- `edoc:fattura`, che raccoglie le proprietà corrispondenti ai metadati specifici per le fatture, incluse le fatture in formato XML per la Pubblica Amministrazione

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.

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.
`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:extent`	numerico	La dimensione in byte del file
`terms:format`	alfanumerico	Il formato *mime type* del file

Termine Dublin Core	Tipo	Descrizione
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 9.
terms:isPartOf	alfanumerico (URN)	Il codice URN dell'unità documentaria che contiene il file descritto. E' 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: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.
terms:source	alfanumerico	Il codice URN del file descritto secondo la sintassi relativa al Pacchetto di Versamento di provenienza descritta nella tabella 9. 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

Tabella 11: Metadati Dublin Core.

Nella seguente tabella sono indicati i 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:matricola	alfanumerico	Matricola del destinatario (quando applicabile, ad esempio la matricola del dipendente)
destinatario:nome	alfanumerico	Nome del destinatario (in caso di persona fisica)
destinatario:ragionesociale	alfanumerico	Ragione sociale del destinatario (in caso di persona giuridica)
documento:anno	numerico	Anno di archiviazione del record come definito nella tabella 8.
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:numero	numerico	Numero progressivo del documento come definito nella tabella 8.
documento:registrazione	alfanumerico	Nei documenti ricevuti indica il protocollo di registrazione assegnato nel registro IVA.

Metadato	Tipo	Descrizione
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:sezionale	alfanumerico	Sezionale o serie archivistica come definito nella tabella 8.
documento:tipo	alfanumerico	Tipologia documentale come definito nella tabella 6.
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)
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:ragionesociale	alfanumerico	Ragione sociale del mittente (in caso di persona giuridica)
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)

Tabella 12: Metadati identificativi dell'unità documentaria.

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

Metadato		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)

Tabella 13: Metadati relativi alla verifica dell'integrità.

La seguente tabella descrive i metadati specifici dei documenti di tipo fattura, incluse le fattura XML per la Pubblica Amministrazione.

Metadato		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:scadenza`	data	La data di scadenza, se riportata nelle informazioni di pagamento

Tabella 14: Metadati specifici dei documenti fattura.

In base all'elenco definito nell'Allegato 5 delle Regole tecniche del D.P.C.M. 3 dicembre 2013, 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 nelle seguenti due tabelle, rispettivamente per quanto riguarda il *Documento informatico*, il *Documento amministrativo informatico* e il *Fascicolo informatico o aggregazione documentale informatica*. Per ciascun metadato è descritta la modalità di rappresentazione:

Metadati minimi	Descrizione
Identificativo	Identificativo univoco e persistente dell'unità documentaria. È formato da una sequenza di caratteri alfanumerici associata in modo univoco e permanente al documento informatico in modo da consentirne l'identificazione. E' rappresentato nel metadato `terms:identifier`.
Data di chiusura	Data di chiusura del documento, indica il momento dal quale è reso immodificabile. E' rappresentato nel metadato `terms:data`.
Oggetto	Riassunto breve del contenuto del documento, in modo da chiarirne la natura. E' rappresentato nel metadato `terms:subject`.
Soggetto produttore (nome, cognome, codice fiscale)	L'insieme “Soggetto produttore” contiene metadati relativi a nome, cognome e codice fiscale del soggetto che ha l'autorità e la competenza a produrre il documento informatico. E' rappresentato nei metadati `produttore:*`
Destinatario (nome, cognome, codice fiscale)	L'insieme “Destinatario” contiene i metadati relativi a nome, cognome e codice fiscale (se disponibile) del soggetto che ha l'autorità e la competenza a ricevere il documento. E' rappresentato nei metadati `destinatario:*`.
Impronta	Rappresentazione digitale del documento composta da una sequenza di simboli binari di lunghezza fissa, che garantisce l'integrità del documento. E' rappresentato nei metadati `fixity:*`.

Tabella 15: Metadati minimi del documento informatico.

Metadati minimi	Descrizione
Codice identificativo dell'amministrazione	Codice identificativo univoco e persistente dell'amministrazione che produce il documento. E' rappresentato nel codice ente definito nella tabella 8.

Metadati minimi	Descrizione
Codice identificativo dell'Area Organizzativa Omogenea (AOO)	Codice identificativo univoco e persistente dell'Area Organizzativa Omogenea (AOO) che produce il documento. E' rappresentato nel codice struttura definito nella tabella 8.
Data di protocollo	Data di protocollo del documento, indica il momento dal quale è reso immodificabile. E' rappresentato nei metadati `terms:data` e `documento:dataprotocollo`.
Progressivo di protocollo	Numero progressivo di protocollo del documento. E' rappresentato nel metadato `documento:protocollo`.
Oggetto	Riassunto breve del contenuto del documento, in modo da chiarirne la natura. E' rappresentato nel metadato `terms:subject`.
Mittente (nome, cognome, codice fiscale)	L'insieme “Mittente” contiene i metadati relativi ai dati identificativi del mittente. E' rappresentato nei metadati `mittente:*`.
Destinatario (nome, cognome, codice fiscale)	L'insieme “Destinatario” contiene i metadati relativi ai dati identificativi del destinatario. E' rappresentato nei metadati `destinatario:*`.
Impronta	Rappresentazione digitale del documento composta da una sequenza di simboli binari di lunghezza fissa, che garantisce l'integrità del documento. E' rappresentato nei metadati `fixity:*`.

Tabella 16: Metadati minimi del documento amministrativo informatico.

Metadati minimi	Descrizione
Identificativo	Identificativo univoco e persistente. È formato da una sequenza di caratteri alfanumerici associata in modo univoco e permanente al fascicolo informatico o all'aggregazione documentale informatica in modo da consentirne l'identificazione. E' rappresentato nel metadato `terms:identifier`.
Amministrazione titolare	Codice IPA dell'amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo. E' rappresentato nel metadato `terms:creator`.
Amministrazione partecipanti	Codice IPA delle amministrazioni che partecipano al procedimento. E' rappresentato in una o più occorrenze del metadato `terms:contributor`.
Responsabile del procedimento (nome, cognome, codice fiscale)	L'insieme “Responsabile del procedimento” contiene i dati identificativi del responsabile del procedimento. E' rappresentato nei metadati `mittente:*`.
Oggetto	Riassunto breve del contenuto del fascicolo, in modo da chiarirne la natura. E' rappresentato nel metadato `terms:subject`.
Documento	Elenco degli identificativi dei documenti contenuti nel fascicolo, che ne consente la reperibilità. E' rappresentato in una o più occorrenze del metadato `terms:hasPart` che indicano gli `URN` dei documenti contenuti.

Tabella 17: Metadati minimi del fascicolo informatico o dell'aggregazione documentale informatica.

Inoltre, anche se non facente parte dei metadati minimi, il sistema gestisce il metadato “identificativo” anche per i documenti amministrativi informatici.

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 6. 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.

Tipologia di documento	Metadati	Mappatura metadati
`D01` Fatture attive	Codice cessionario / committente	`fattura:codicepa`
	Descrizione cessionario / committente	`fattura:descrizionepa`
	Scadenza	`fattura:scadenza`
	Importo	`fattura:importo`
	Codice CIG	`fattura:cig`

Tipologia di documento	Metadati	Mappatura metadati
	CUP	fattura:cup
	ID SDI	fattura:idsdi
	Esito	fattura:esito
	Terzo Intermediario / Soggetto emittente	intermediario:*
	Firmatario	fattura:firmatario
D02 Fatture passive	Scadenza	fattura:scadenza
	Importo	fattura:importo
	CIG	fattura:cig
	CUP	fattura:cup
	ID SDI	fattura:idsdi
	Esito	fattura:esito
	Terzo Intermediario / Soggetto emittente	intermediario:*
	Firmatario	fattura:firmatario
	Protocollo di registrazione nel registro IVA	documento:registrazione
	Protocollo di registrazione nel registro protocollo	documento:protocollo
	Protocollo di registrazione nella prima nota	documento:primanota
	Data di registrazione nel registro protocollo	documento:dataprotocollo
	Data di registrazione nel registro IVA o nella prima nota	documento:dataregistrazione
D03 Nota variazione aumento D04 Nota variazione diminuzione	**Se emessa**	
	Codice cessionario / committente	fattura:codicepa
	Codice cessionario / committente	fattura:codicepa
	Descrizione cessionario / committente	fattura:descrizionepa
	Scadenza	fattura:scadenza
	Importo	fattura:importo
	CIG	fattura:cig
	CUP	fattura:cup
	ID SDI	fattura:idsdi
	Tipo documento (TD04 – TD05, cfr. regole tecniche SDI)	terms:type
	Esito	fattura:esito
	Terzo Intermediario / Soggetto emittente	intermediario:*
	Firmatario	fattura:firmatario
	Se ricevuta	
	Cedente / prestatore	mittente:*
	Scadenza	fattura:scadenza
	Importo	fattura:importo
	CIG	fattura:cig
	CUP	fattura:cup
	ID SDI	fattura:idsdi
	Tipo documento (TD04 – TD05, cfr. regole tecniche SDI)	terms:type
	Esito	fattura:esito
	Terzo Intermediario / Soggetto emittente	intermediario:*
	Firmatario	fattura:firmatario
	Protocollo di registrazione nel registro IVA	documento:registrazione

Tipologia di documento	Metadati	Mappatura metadati
	Protocollo di registrazione nel registro protocollo	documento:protocollo
	Protocollo di registrazione nella prima nota	documento:primanota
	Data di registrazione nel registro protocollo	documento:dataprotocollo
	Data di registrazione nel registro IVA o nella prima nota	documento:dataregistrazione
D05 Documento di trasporto D08 Bolla	Numero progressivo	terms:subject
	Data della consegna o della spedizione dei beni (non necessariamente coincide con la data del documento)	terms:dateSubmitted
	Dati del trasportatore (nome, cognome, CF, o denominazione ditta)	intermediario:*
	Sommario beni trasportati (natura, quantità, qualità)	terms:abstract
D06 Scontrino D07 Ricevuta	Numero progressivo	terms:subject
	Importo comprensivo d'IVA	fattura:importo
	Descrizione dei beni ceduti o dei servizi prestati	terms:abstract
D09 Libro giornale D10 Libro inventari D11 Libro mastro	Denominazione	terms:subject
	Data inizio	documento:datainizio
	Data termine	documento:datatermine
	Numero di pagine	terms:extent
D12 Registro cronologico	Denominazione	terms:subject
	Data inizio	documento:datainizio
	Data termine	documento:datatermine
	Descrizione incassi e pagamenti	terms:abstract
	Numero di pagine	terms:extent
D13 Libro cespiti	Denominazione	terms:subject
	Anno di validità	documento:anno
	Descrizione dei beni	terms:abstract
	Numero di pagine	terms:extent
D14 Registro Irpef D15 Registro fatture acquisto D16 Registro acquisti agenzie viaggio D17 Registro fatture emesse D18 Registro fatture in sospeso D19 Registro corrispettivi D21 Registro corrispettivi agenzie viaggio D22 Registro emergenza Iva 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	Denominazione	terms:subject
	Data inizio	documento:datainizio
	Data termine	documento:datatermine
	Numero di pagine	terms:extent
	Descrizione del contenuto	terms:abstract
	Tipologia di registro	terms:type

Tipologia di documento	Metadati	Mappatura metadati
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 D50 Registro editori		
D20 Giornale di fondo D23 Bollettario	Denominazione	terms:subject
	Data inizio	documento:datainizio
	Data termine	documento:datatermine
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	Denominazione	terms:subject
	Data inizio	documento:datainizio
	Data termine	documento:datatermine
	Numero di pagine	terms:extent
	Sommario del contenuto	terms:abstract
D59 Unico persone fisiche D60 Unico società di persone D61 Unico società di capitali D62 Unico enti non commerciali	N. Protocollo	terms:subject
	Anno di validità	documento:anno
	Tipologia modello	terms:type
D63 Irap persone fisiche D64 Irap Società persone D65 Irap Società capitale D66 Irap enti non commerciali ed equiparati	Anno di validità	documento:anno
	Tipologia modello	terms:type

Tipologia di documento	Metadati	Mappatura metadati
D67 Irap amministrazioni ed enti pubblici		
D68 Modello 730 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 D78 Modello 770 ordinario	Tipologia modello	terms:type
	Dati dell'eventuale mediatore nella consegna (nome, cognome, codice fiscale)	intermediario:*
D79 Modello certificazione CUD	Denominazione	terms:subject
	Anno di validità	documento:anno
	Tipologia modello	terms:type
	Dati del dipendente	destinatario:*
D80 Modello F23 D81 Modello F24 D82 Modelli allegati alla Dichiarazione dei Redditi Modello Unico D83 Modelli annotazione separata	Denominazione	terms:subject
	Anno di validità	documento:anno
	Tipologia modello	terms:type
D84 Ricevuta presentazione modelli dichiarazione	Numero di protocollo	terms:subject
	Tipologia documento	terms:type
	Data di invio	terms:date

Tabella 18: Metadati aggiuntivi per tipologia di documento.

Per quanto invece riguarda le due categorie "D58 Altri registri" o "D85 Altri documenti":

Tipologia di documento	Metadati	Mappatura metadati
D58 Altri registri	Da concordare con il produttore	Secondo l'accordo con il produttore definito nelle Specificità del contratto
D85 Altri documenti	Da concordare con il produttore	Secondo l'accordo con il produttore definito nelle Specificità del contratto

Tabella 19: Metadati aggiuntivi per altre tipologie di documento.

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:

Formato	Contenuto	Descrizione
`F000`	Fatture PA XML	Il formato `F000` si riferisce ad un file ZIP che contiene esclusivamente fatture elettroniche per la Pubblica Amministrazione in formato Fattura PA XML e le relative notifiche. Si suppone che il ciclo di gestione delle fatture elettroniche contenute sia stato gestito dal produttore tramite una delle modalità previste e che sia completato. 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 PA XML gestite dal sistema eIPA	Il sistema di conservazione è integrato con il sistema di gestione della fattura elettronica per la Pubblica Amministrazione di Entaksi (denominato eIPA). Il formato `F001` si riferisce ai pacchetti costituiti dalle fatture elettroniche in formato Fattura PA XML e dalle relative notifiche quando questi documenti sono gestiti direttamente dal servizio eIPA, erogato da Entaksi per l'invio al Sistema di Interscambio dei documenti Fattura PA XML e la gestione delle notifiche di ritorno.
`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.

Tabella 20: Formati di validazione dei Pacchetti di Versamento.

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:

```
<pdv xmlns="http://entaksi.eu/schemas/econ/1.0/"
     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://entaksi.eu/schemas/econ/1.0/ https://entaksi.eu/schemas/econ/1.0/econ.xsd">
    <dc> (1)
        <terms:format>F999</terms:format>
    </dc>
    <formato>F999</formato> (2)
    <fileGroup> (3)
        <dc> (4)
            <terms:type>Fattura</terms:type>
            <terms:date>2014-10-17T09:27:48Z</terms:date>
            <terms:subject>Fattura 6/8 del 2014-10-16 Destinatario: Alpha Spa</terms:subject>
            <terms:abstract>Specchio grande</terms:abstract>
        </dc>
        <metadata key="produttore:idfiscale">IT1234567890</metadata> (5)
        <metadata key="produttore:ragionesociale">Acme Srl</metadata>
        <metadata key="destinatario:ragionesociale">Alpha Spa</metadata>
        <metadata key="documento:anno">2014</metadata>
        <metadata key="documento:tipo">D01</metadata>
        <metadata key="documento:sezionale">6</metadata>
        <metadata key="documento:numero">8</metadata>
        <metadata key="documento:data">2014-10-16</metadata>
        <registro>urn:entaksi:IT1234567890:_default:reg:2014:D01:6</registro> (6)
        <file> (7)
            <dc> (8)
                <terms:title>Fattura 6.pdf</terms:title>
                <terms:format>application/pdf</terms:format>
                <terms:type>Fattura</terms:type>
            </dc>
            <hashAlgorithm canonicalXML="false">SHA256</hashAlgorithm> (9)
            <hashValue>dgI+j0ke9WrVpyVBgkf0JOlLP/bEax/TJH8Xhs+DQtA=</hashValue>
        </file>
    </fileGroup>
</pdv>
```

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

Elemento	Contenuto richiesto
(1) /pdv/dc	Questo elemento contiene i metadati *Dublin Core* del PDV.
(2) /pdv/formato	Indica il formato di validazione del PDV.
(3) /pdv/fileGroup	Dichiara una unità documentaria, può essere ripetuto più volte.
(4) /pdv/fileGroup[*]/dc	Contiene i metadati *Dublin Core* dell'unità documentaria.
(5) /pdv/fileGroup[*]/metadata	I metadati chiave/valore dell'unità documentaria.
(6) /pdv/fileGroup[*]/registro	L'URN del registro in cui deve essere archiviata l'unità documentaria, così come definito nella tabella 9.
(7) /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.

Elemento	Contenuto richiesto
(8) `/pdv/fileGroup[*]/file[*]/dc`	Metadati *Dublin Core* relativi al file
(9) `/pdv/fileGroup[*]/file[*]/hashValue`	Riporta l'impronta del file rappresentata con la codifica Base64. La tag `hashAlgorithm` definisce l'algoritmo usato per calcolare l'impronta.

Tabella 21: Elementi dell'indice del Pacchetto di Versamento.

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 9, 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 11386:2010 – 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 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.
- I**nformazioni 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 inclusa 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: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="customMetadataType">
        <xs:complexContent>
            <xs:extension base="dcAndMetadataType"/>
        </xs:complexContent>
    </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:schema>
```

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

```
<?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:IT1234567890:_default:reg:2014:D01:3:pda:1</sincro:ID>
        <sincro:CreatingApplication>
            <sincro:Name>eCon</sincro:Name>
            <sincro:Version>1.0.0</sincro:Version>
            <sincro:Producer>Entaksi Solutions Srl</sincro:Producer>
        </sincro:CreatingApplication>
        <sincro:MoreInfo sincro:XMLScheme="http://entaksi.eu/schemas/econ/1.0/econ.xsd">
            <sincro:EmbeddedMetadata> (1)
                <econ:customMetadata xmlns:econ="http://entaksi.eu/schemas/econ/1.0/"
                                     xmlns="http://entaksi.eu/schemas/econ/1.0/"
                                     xmlns:dc="http://purl.org/dc/elements/1.1/"
                                     xmlns:terms="http://purl.org/dc/terms/">
                    <dc>
                        <terms:source>urn:entaksi:IT1234567890:_default:pdv:1089</terms:source>
                    </dc>
                </econ:customMetadata>
            </sincro:EmbeddedMetadata>
        </sincro:MoreInfo>
    </sincro:SelfDescription>
    <sincro:VdC>
        <sincro:ID sincro:scheme="local">urn:entaksi:IT1234567890:_default:reg:2014:D01:3:pda:1</sincro:ID>
        <sincro:MoreInfo sincro:XMLScheme="http://entaksi.eu/schemas/econ/1.0/econ.xsd">
            <sincro:EmbeddedMetadata> (2)
                <econ:customMetadata xmlns:econ="http://entaksi.eu/schemas/econ/1.0/"
                                     xmlns="http://entaksi.eu/schemas/econ/1.0/"
                                     xmlns:dc="http://purl.org/dc/elements/1.1/"
                                     xmlns:terms="http://purl.org/dc/terms/">
                    <dc>

<terms:identifier>urn:entaksi:IT1234567890:_default:reg:2014:D01:3:pda:1</terms:identifier>
                        <terms:subject>Pacchetto di archiviazione numero 1 per il registro 2014 D01
3</terms:subject>
                    </dc>
                </econ:customMetadata>
            </sincro:EmbeddedMetadata>
        </sincro:MoreInfo>
    </sincro:VdC>
    <sincro:FileGroup>
        <sincro:Label>Fattura 3/1 del 2014-07-01 Destinatario: Alpha Spa</sincro:Label>
        <sincro:File sincro:encoding="binary" sincro:format="application/pkcs7-mime">
            <sincro:ID
```

```
sincro:scheme="local">urn:entaksi:IT1234567890:_default:pdv:1089:IT0987654321_1.xml.p7m</sincro:ID>
            <sincro:Hash sincro:canonicalXML="false"
sincro:function="SHA256">UCNxauBon4bsElQfoPyiy59k060zPQAU5mVMAzuh/qo=</sincro:Hash>
            <sincro:MoreInfo sincro:XMLScheme="http://entaksi.eu/schemas/econ/1.0/econ.xsd">
                <sincro:EmbeddedMetadata> (3)
                    <econ:customMetadata xmlns:econ="http://entaksi.eu/schemas/econ/1.0/"
                                         xmlns="http://entaksi.eu/schemas/econ/1.0/"
                                         xmlns:dc="http://purl.org/dc/elements/1.1/"
                                         xmlns:terms="http://purl.org/dc/terms/">
                        <dc>

<terms:source>urn:entaksi:IT1234567890:_default:pdv:1089:IT1234567890.xml.p7m</terms:source>
                            <terms:title>IT1234567890.xml.p7m</terms:title>
                            <terms:medium>application/pkcs7-mime</terms:medium>
                            <terms:format>text/xml</terms:format>

<terms:isPartOf>urn:entaksi:IT1234567890:_default:reg:2014:D01:3:doc:1</terms:isPartOf>
                            <terms:extent>36502</terms:extent>
                            <terms:type>Fattura</terms:type>
                            <terms:subject>Fattura 3/1 del 2014-07-01 Destinatario: Alpha Spa</terms:subject>
                            <terms:date>2014-07-08T09:51:35Z</terms:date>
                        </dc>
                    </econ:customMetadata>
                </sincro:EmbeddedMetadata>
            </sincro:MoreInfo>
        </sincro:File>
        <sincro:File sincro:encoding="binary" sincro:format="text/xml">
            <sincro:ID
sincro:scheme="local">urn:entaksi:IT1234567890:_default:pdv:1089:IT1234567890_1_RC_002.xml</sincro:ID>
            <sincro:Hash sincro:canonicalXML="false"
sincro:function="SHA256">O8X9WqSPo3wQiiQ1dSwvJe0E+ZD74U+DHOuqwYY/SI4=</sincro:Hash>
            <sincro:MoreInfo sincro:XMLScheme="http://entaksi.eu/schemas/econ/1.0/econ.xsd">
                <sincro:EmbeddedMetadata> (4)
                    <econ:customMetadata xmlns:econ="http://entaksi.eu/schemas/econ/1.0/"
                                         xmlns="http://entaksi.eu/schemas/econ/1.0/"
                                         xmlns:dc="http://purl.org/dc/elements/1.1/"
                                         xmlns:terms="http://purl.org/dc/terms/">
                        <dc>

<terms:source>urn:entaksi:IT1234567890:_default:pdv:1089:IT1234567890_1_RC_002.xml</terms:source>
                            <terms:title>IT1234567890_1_RC_002.xml</terms:title>
                            <terms:format>text/xml</terms:format>

<terms:isPartOf>urn:entaksi:IT1234567890:_default:reg:2014:D01:3:doc:1</terms:isPartOf>
                            <terms:extent>4236</terms:extent>
                            <terms:type>RICEVUTA DI CONSEGNA</terms:type>

<terms:isReferencedBy>urn:entaksi:IT1234567890:_default:pdv:1089:IT1234567890_1.xml.p7m</terms:isReferencedBy>
                            <terms:subject>RICEVUTA DI CONSEGNA</terms:subject>
                            <terms:date>2014-07-08T11:01:10Z</terms:date>
                        </dc>
                    </econ:customMetadata>
                </sincro:EmbeddedMetadata>
            </sincro:MoreInfo>
        </sincro:File>
        <sincro:File sincro:encoding="binary" sincro:format="text/xml">
            <sincro:ID
sincro:scheme="local">urn:entaksi:IT1234567890:_default:pdv:1089:IT1234567890_1_NE_003.xml</sincro:ID>
            <sincro:Hash sincro:canonicalXML="false"
sincro:function="SHA256">NqE3xow6njdG3Ul/juA4Wm/9Li7RlKIM1zo+OjWhEyk=</sincro:Hash>
            <sincro:MoreInfo sincro:XMLScheme="http://entaksi.eu/schemas/econ/1.0/econ.xsd">
                <sincro:EmbeddedMetadata> (5)
                    <econ:customMetadata xmlns:econ="http://entaksi.eu/schemas/econ/1.0/"
                                         xmlns="http://entaksi.eu/schemas/econ/1.0/"
                                         xmlns:dc="http://purl.org/dc/elements/1.1/"
                                         xmlns:terms="http://purl.org/dc/terms/">
                        <dc>
```

```
<terms:source>urn:entaksi:IT1234567890:_default:pdv:1089:IT1234567890_1_NE_003.xml</terms:source>
                            <terms:title>IT1234567890_1_NE_003.xml</terms:title>
                            <terms:format>text/xml</terms:format>

<terms:isPartOf>urn:entaksi:IT1234567890:_default:reg:2014:D01:3:doc:1</terms:isPartOf>
                            <terms:extent>4240</terms:extent>
                            <terms:type>NOTIFICA DI ESITO</terms:type>

<terms:isReferencedBy>urn:entaksi:IT1234567890:_default:pdv:1089:IT1234567890_1.xml.p7m</terms:isReferencedBy>
                            <terms:subject>NOTIFICA DI ESITO: ACCETTAZIONE</terms:subject>
                        </dc>
                    </econ:customMetadata>
                </sincro:EmbeddedMetadata>
            </sincro:MoreInfo>
        </sincro:File>
        <sincro:MoreInfo sincro:XMLScheme="http://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:dc="http://purl.org/dc/elements/1.1/"
                                     xmlns:terms="http://purl.org/dc/terms/">
                    <dc> (6)

<terms:identifier>urn:entaksi:IT1234567890:_default:reg:2014:D01:3:doc:1</terms:identifier>
                        <terms:type>Fattura</terms:type>
                        <terms:date>2014-07-08T09:51:35Z</terms:date>
                        <terms:subject>Fattura 3/1 del 2014-07-01 Destinatario: Alpha Spa</terms:subject>
                        <terms:abstract>Prodotto 1</terms:abstract>
                    </dc>
                    <metadata key="produttore:idfiscale">IT1234567890</metadata>
                    <metadata key="produttore:ragionesociale">Acme Srl</metadata>
                    <metadata key="destinatario:ragionesociale">Alpha Spa</metadata>
                    <metadata key="destinatario:idfiscale">IT0987654321</metadata>
                    <metadata key="documento:anno">2014</metadata>
                    <metadata key="documento:sezionale">3</metadata>
                    <metadata key="documento:numero">1</metadata>
                    <metadata key="documento:data">2014-06-30</metadata>
                    <metadata key="documento:posizionelotto">1</metadata>
                    <metadata key="fattura:codicepa">XXXXX</metadata>
                    <metadata key="fattura:descrizionepa">Alpha Spa</metadata>
                    <metadata key="fattura:scadenza">2014-08-30T22:00:00Z</metadata>
                    <metadata key="fattura:importo">292.76 EUR</metadata>
                    <metadata key="fattura:firmatario">Mario Rossi</metadata>
                    <metadata key="fattura:idsdi">1111111</metadata>
                    <metadata key="fattura:esito">Accettata</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">IT01621900479</sincro:Agent_ID>
        </sincro:Agent>
        <sincro:TimeReference>
            <sincro:TimeInfo>2015-10-09T10:22:47.562+02:00</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#" Id="id-
006f0fde76113146fe5d67cd75f6b743">...</ds:Signature></sincro:IdC> (7)
```

La seguente tabella illustra i punti salienti dell'indice:

Elemento	Contenuto richiesto
(1) `/IdC/SelfDescription/MoreInfo`	Informazioni sul PDA con i riferimenti ai PDV di provenienza dei documenti. In questa sezione `MoreInfo` sono riportati, tramite il termine *Dublin Core* `terms:source`, gli identificativi URN dei Pacchetti di Versamento da cui provengono i documenti contenuti nel Pacchetto di Archiviazione.
(2) `/Idc/VdC/MoreInfo`	Informazioni sul contenuto del PDA con l'identificativo assegnato. In questa sezione `MoreInfo` sono riportati, tramite i termini *Dublin Core* `terms:identifer` e `terms:subject`, l'identificativo del Pacchetto di Archiviazione e una descrizione del pacchetto leggibile dall'utente.
(3) `/IdC/FileGroup[1]/File[1]/MoreInfo`	In questa sezione `MoreInfo` sono riportati i metadati relativi al file principale dell'unità documentaria.
(4) `/IdC/FileGroup[1]/File[2]/MoreInfo`	In questa sezione `MoreInfo` sono riportati i metadati relativi al primo allegato all'unità documentaria.
(5) `/IdC/FileGroup[1]/File[2]/MoreInfo`	In questa sezione `MoreInfo` sono riportati i metadati relativi al secondo allegato all'unità documentaria.
(6) `/IdC/FileGroup[1]/MoreInfo`	In questa sezione `MoreInfo` sono riportati i metadati relativi all'unità documentaria.
(7) `/Signature`	Firma digitale e marca temporale XML in formato XaDES-T

Tabella 22: Elementi del file indice del Pacchetto di Archiviazione.

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 6.3, incluse le definizioni relative alle 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:

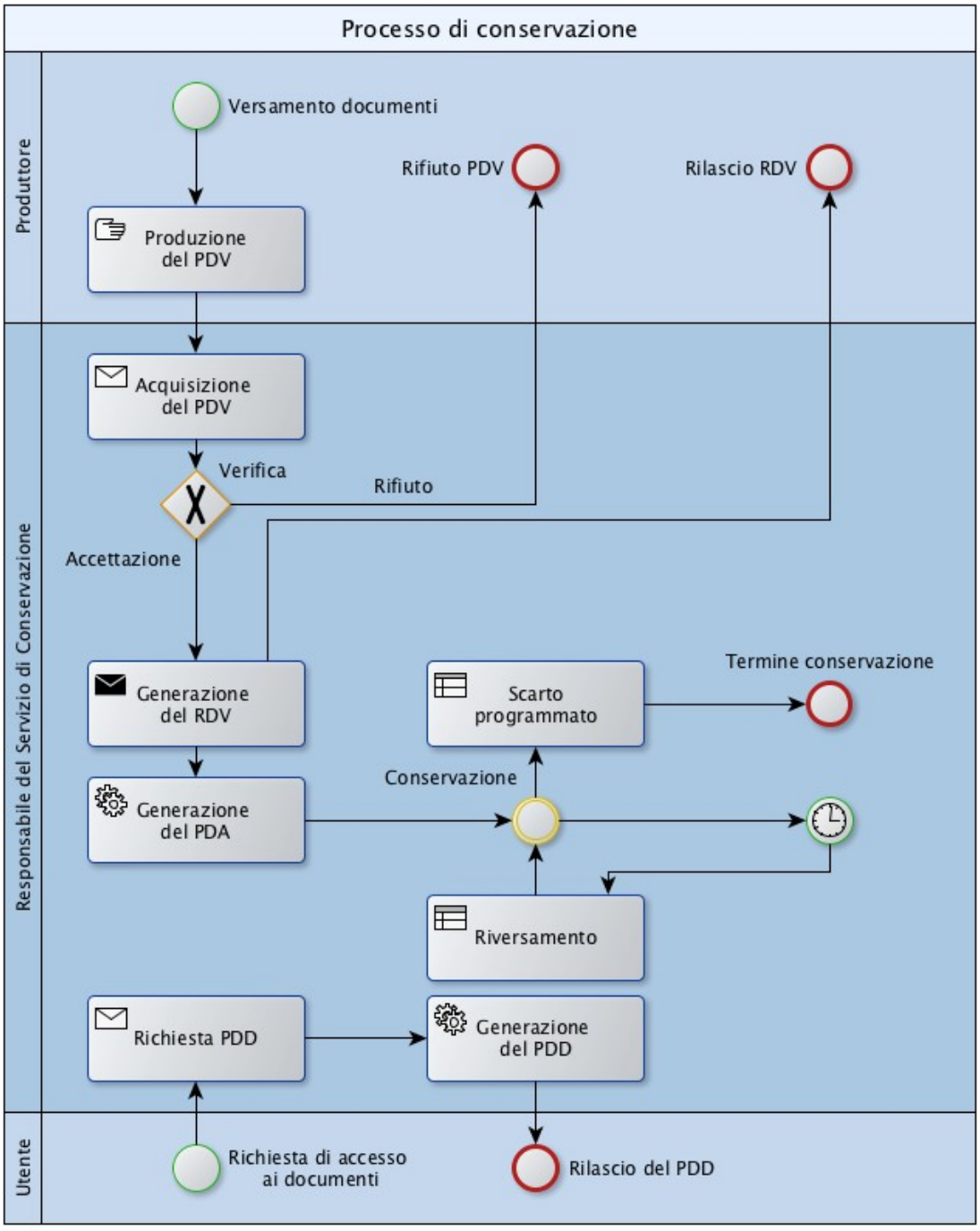

Figura 7: Workflow del processo di conservazione.

In fase di versamento dovranno essere definiti a cura del Produttore i metadati previsti nell'allegato 5 del D.P.C.M. 13 novembre 2014, in modo da consentire la ricerca del documento per uno di questi campi oppure per loro associazioni logiche, in base a quanto descritto nel paragrafo 6.2.

L'**archivio** è realizzato mediante l'utilizzo del sistema di gestione documentale Alfresco che, oltre a garantire affidabilità, robustezza e costante allineamento alla evoluzione tecnologica, permette un'efficace gestione del sistema, una elevata scalabilità, una sofisticata e granulare definizione dei diritti di accesso ai documenti e la possibilità di fruire di funzionalità avanzate, quali la ricerca a testo libero, ove il formato del documento lo consenta, sull'intero insieme dei documenti cui l'Utente ha accesso oltre che la ricerca per metadati.

Operativamente, l'archivio è costituito da una o più istanze Alfresco nelle quali è presente, per ciascun produttore (identificato come ente più struttura), una cartella in cui sono organizzati i registri di archiviazione.

In pratica, ogni Pacchetto di Archiviazione risulta essere una cartella posizionata nel sistema documentale di conservazione all'interno della seguente struttura:

```
<produttore>/Registro/<anno>/<tipo-documento>/<sezionale>/<prog-pda>
```

Gli elementi citati nel percorso della cartella hanno il significato descritto nella tabella 8.

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 ed 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 ed 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 6.2, 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 7.2, 7.3 e 7.4:

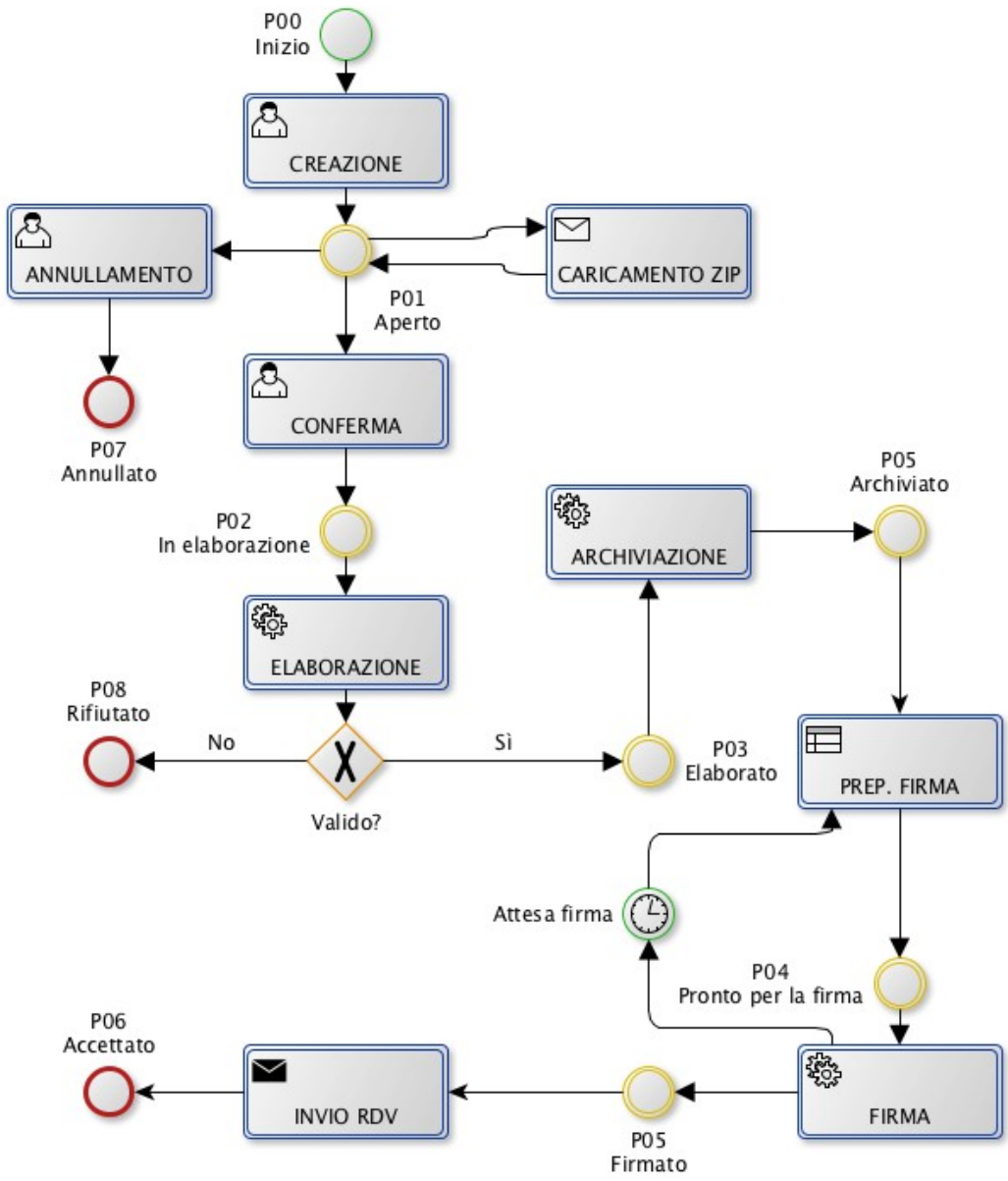

Figura 8: Creazione di un PDV.

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 6.1.
I Pacchetti di Versamento caricati sono sottoposti al backup e alle verifiche di integrità insieme al resto del database del sistema, dove i pacchetti sono memorizzati finché non vengono versati nel sistema di conservazione.

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 7.1 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 6.2 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 Srl</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:isReferencedBy>
 <terms:source>urn:entaksi:IT41141111411:_default:pdv:13777:IT01621900479_00Dm2_RC_002.xml</terms:source>
                    <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:isReferencedBy>
<terms:source>urn:entaksi:IT41141111411:_default:pdv:13777:IT01621900479_00Dm2_DT_003.xml</terms:source>
                    <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 7.2, 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 7.3, 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 chiusura del Pacchetto di Archiviazione si occupa invece 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 6.3, 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.

In seguito, prima di procedere con la formazione del PDA, viene essere eseguita una verifica dei numeratori delle unità documentarie contenute.

Le unità documentarie che hanno una numerazione all'origine conservano questa numerazione durante il versamento e il sistema di archiviazione verifica che la numerazione sia progressiva e continua, ovvero senza duplicati e interruzioni, anche in relazione al pacchetto di archiviazione precedente nello stesso registro di archiviazione.

Le unità documentarie prive di una numerazione all'origine assumono una numerazione progressiva determinata durante la fase di versamento.

La mancanza di progressività, di continuità o la presenza di duplicati nella numerazione interrompe il processo di formazione del Pacchetto di Archiviazione che viene rimandato in attesa che nuove operazioni di versamento completino la serie.

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 6.3;
  Il file indice assume il nome in base alla numerazione del pacchetto di archiviazione: `pda_1.xml`, `pda_2.xml`, … `pda_`*`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 Responsabile del Servizio di Conservazione 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 DSS sviluppato dalla Commissione Europea allo scopo di facilitare gli stati membri nell'adozione di soluzioni interoperabili nell'ambito dei 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 autorità di certificazione accreditate presso l'Agenzia per l'Italia Digitale.

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 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 emergenza definite dal Sistema Integrato di Gestione certificato ISO 27001:2013 per il ripristino dei dati dalle copie di backup.

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 (se il formato del documento consente una visualizzazione) e scaricare il documento conservato all'interno dell'archivio a norma;
- verificare ed eventualmente scaricare 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 6.4 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 6.4, 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 emergenza definite dal Sistema Integrato di Gestione certificato ISO 27001:2013 per il ripristino dei dati dalle copie di backup.

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 download su una connessione cifrata HTTPS autenticata tramite le credenziali dell'utente. 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 di Conservazione, 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:

Tipologie di scritture	Termini di conservazione
Scritture contabili (fatture, registri, libri…)	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

Tabella 23: Tempi di scarto.

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 della Conversazione e del Responsabile della Funzione Archivistica di Conservazione.

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 all'art. 9 comma L del D.P.C.M del 3 dicembre 2013.

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 23 per quei pacchetti in cui non è presente il metadato `terms:accessRight` definito nella tabella 11.

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 11386:2010 (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 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.

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

Torna all'indice.

8. Il 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, ai fini dell'archiviazione dei documenti, ha integrato la piattaforma *open source Alfresco Community Edition*.

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 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.

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 ISO 9001.

I sistema di conservazione fa parte dei servizi informatici di Entaksi Solutions la cui gestione è certificata ISO 20000.

Torna all'indice.

8.1 Componenti logiche

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

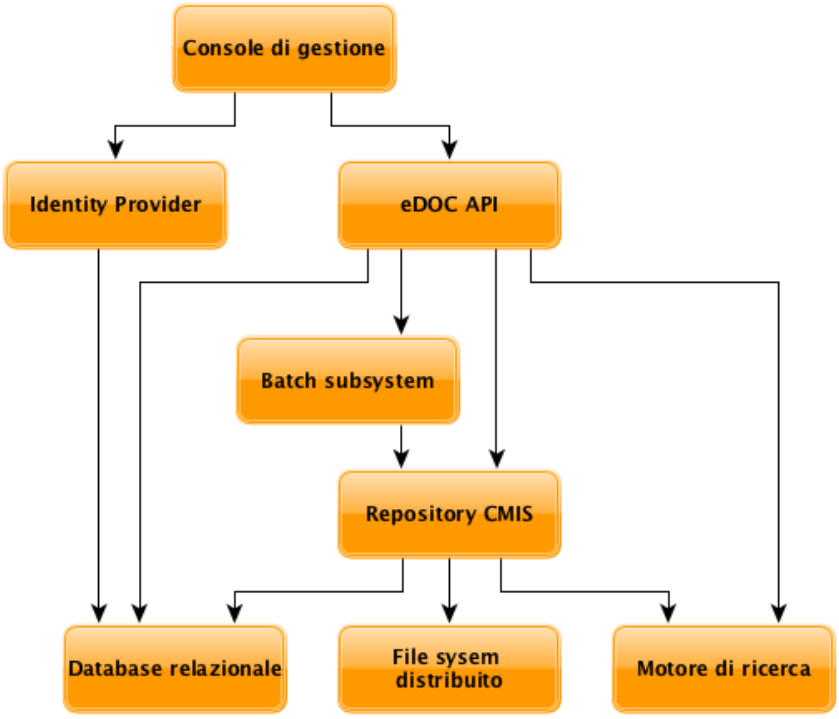

Figura 9: Componenti logiche del sistema di conservazione.

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 nel “*Repository CMIS*” il quale utilizza un “*File system* distribuito” come supporto per l'archiviazione vera e propria dei documenti. Il “Motore di ricerca” interagisce con il “*Repository CMIS*” per indicizzare i documenti e i loro metadati consentendo alla componente “eDoc API” di eseguire ricerche sulla base dati documentale.

Torna all'indice.

8.2 Componenti tecnologiche

Le componenti logiche descritte nel paragrafo 8.1 sono implementate tramite le componenti tecnologiche illustrate nel seguente diagramma.

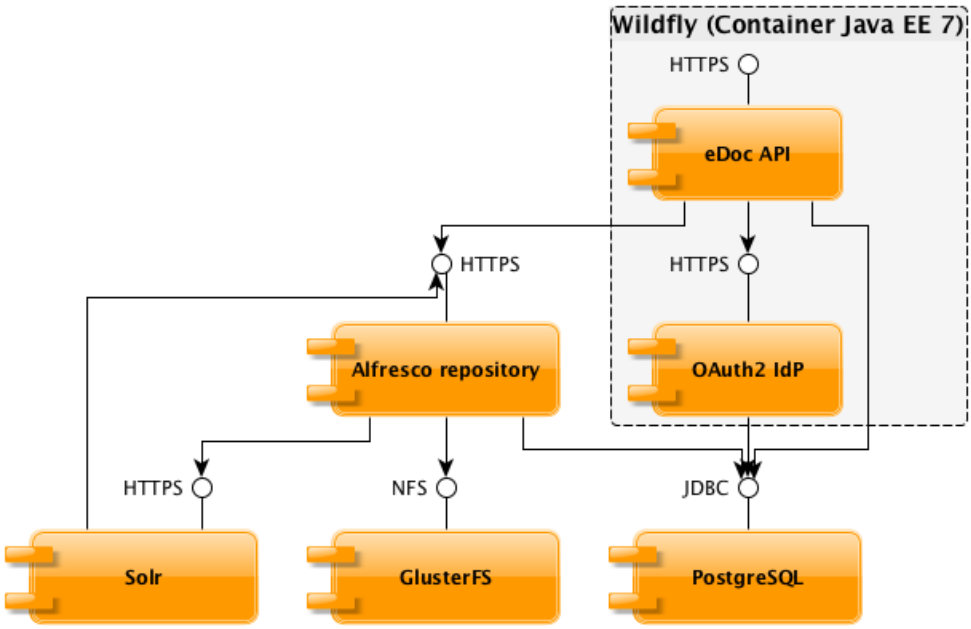

Figura 10: Componenti tecnologiche del sistema di conservazione.

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.

Le componenti logiche "*Repository CMIS*" e "Motore di ricerca" sono implementate dal software *open source Alfresco Community Edition* che dispone di un modulo "*Alfresco repository*" e da una istanza del sistema di indicizzazione "Solr" integrati tra di loro.

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 duplicata su un altro server.

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 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 eroga i servizi dalla propria infrastruttura gestita direttamente fino al livello del sistema operativo, mentre utilizza un servizio di *outsourcing* per la gestione dell'*hardware* e della connettività di rete.

Le componenti fisiche si trovano quindi distribuite in server collocati in vari *datacenter* distribuiti geograficamente e divisi in due categorie:

- *Datacenter* per istanze del servizio rivolto ad enti pubblici e privati per i quali la normativa richiede che i dati archiviati siano conservati in un paese dell'Unione Europea
- *Datacenter* per istanze del servizio rivolto a enti della Pubblica Amministrazione italiana per i quali l'Agenzia per l'Italia Digitale stabilisce il requisito dell'ubicazione nell'ambito dei confini nazionali della Repubblica Italiana

Nella prima categoria rientrano i seguenti due *datacenter*:

- Hetzner Online AG - Nuremberg Data Center Park
  Sigmundstrasse 135
  90431 Nürnberg
  Germany
- Hetzner Online AG - Falkenstein Data Center Park
  Am Datacenterpark 1
  08223 Falkenstein
  Germany

Nella seconda categoria rientrano i seguenti due *datacenter*:

- SeeWeb Srl – Frosinone
  Via A. Vona 66
  03110 Frosinone
- SeeWeb Srl – Milano
  Via Caldera 21
  20153 Milano

Sui server fisici forniti da questi *datacenter* sono installate macchine virtuali con sistema operativo GNU/Linux. I *datacenter* selezionati forniscono i più alti livelli di prestazioni in termini di affidabilità, sicurezza e connettività alla rete Internet sia con protocollo IPv4 che IPv6. I due *datacenter* italiani sono a loro volta certificati ISO 27001.

Torna all'indice.

8.4 Procedure di gestione ed evoluzione

Il sistema eCON fa parte dell'insieme di servizi Entaksi sottoposto alla certificazione ISO 20000-1:2011 e adotta quindi una serie di procedure di gestione e di evoluzione del sistema in accordo con il dettato più generale di questa norma, 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.

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 iniziativa 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:

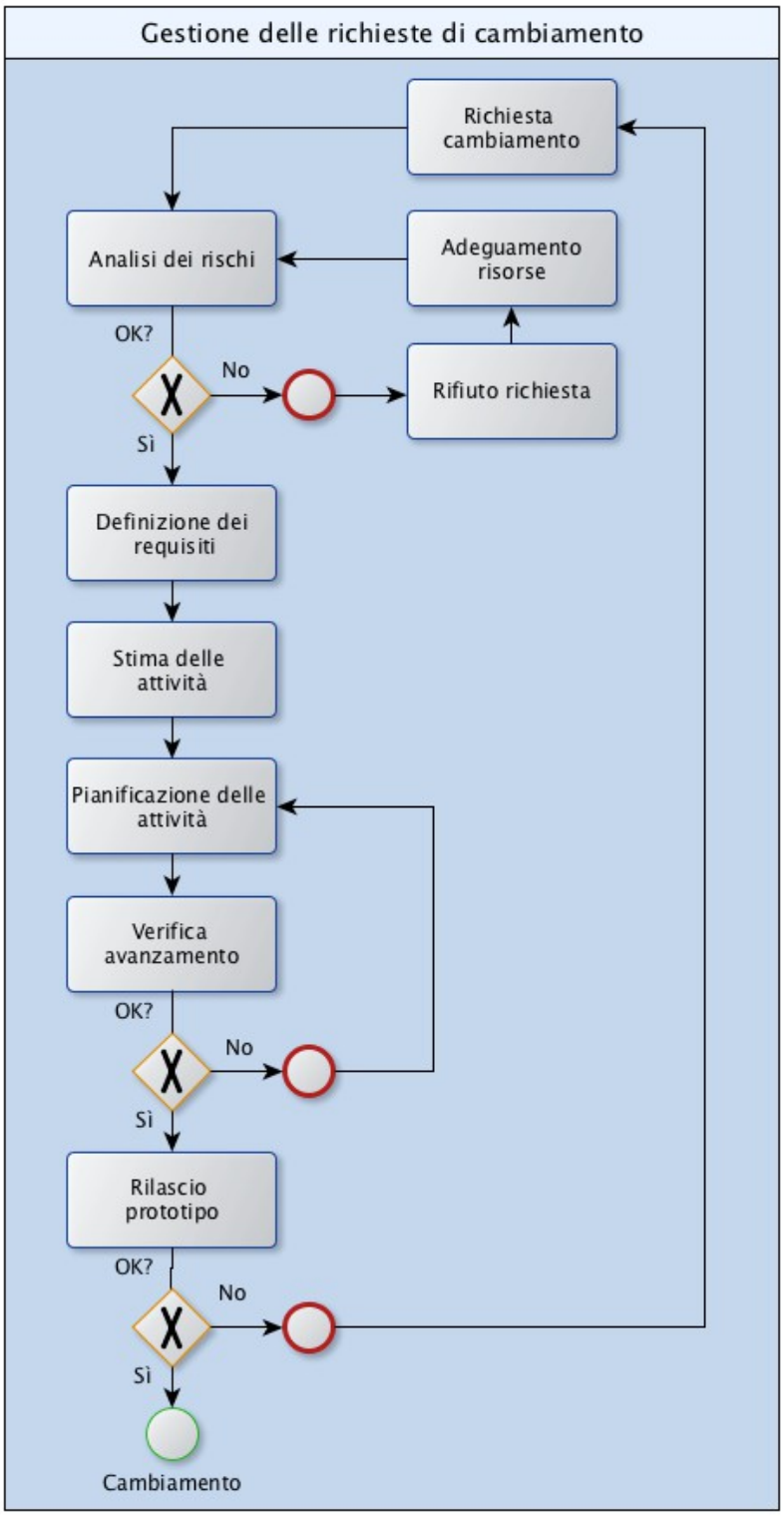

Figura 11: Gestione delle richieste di cambiamento.

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 EN ISO 9001:2008, ISO/IEC 27001:2013 e ISO 20000-1:2011, e l'evoluzione dello stesso segue gli aggiornamenti a questi standard. 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 c*hange 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 9.1, 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:

- **ISO 9001**: certificazione standard rilasciata in conformità alla norma UNI EN ISO 9001:2008 che ha lo scopo di descrivere i requisiti per la realizzazione e gestione del Sistema di Gestione della Qualità (SGQ), per la progettazione, produzione e assistenza di applicativi e servizi software.
- **ISO 27001**: certificazione standard rilasciata in conformità alla norma ISO/IEC 27001: 2013 che ha lo scopo di descrivere i requisiti per la realizzazione e gestione del Sistema di Gestione della Sicurezza delle Informazioni (SIGSI). Questa definisce: la progettazione, produzione e assistenza di applicativi software, inclusi quelli riguardanti i sistemi di firme elettroniche digitali, avanzate, qualificate e autenticazione biometrica; erogazione di servizi applicativi in modalità *SaaS* (*Software as a Service*) per la manutenzione ordinaria e straordinaria di macchine ed impianti e la gestione documentale e conservazione;
- **ISO 20000**: certificazione standard rilasciata in conformità alla norma ISO 20000-1:2011 che ha lo scopo di descrivere i requisiti per la realizzazione e gestione del Sistema di Gestione dei Servizi Informatici (SGS).

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 risorse, la disponibilità e le prestazioni dei 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 il software SensuApp.

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. L'archivio centrale dei *log* di Entaksi è realizzato tramite il software LogStash.

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 dalla norma ISO/IEC 27001:2013. 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.

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 SIG 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 SIG 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 gradi 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 della norma ISO/IEC 27001:2013. 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, “AR ISO <aaaammgg> rapporto valutazione rischi”, ed il conseguente piano di trattamento “AR ISO <aaaammgg> 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 della congruenza dell'impronta del documento, sono pianificati dal Responsabile del Servizio di Conservazione, tenendo conto dello stato e dell’importanza dei processi e delle aree oggetto di verifica, nonché dei risultati delle precedenti verifiche.

La frequenza con la quale vengono disposti i controlli di integrità è almeno annuale. Al termine delle verifiche viene predisposto il relativo verbale di verifica.

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. 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 *storage* 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 in condizioni di emergenza

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 emergenza, riportati dettagliatamente nei manuali del SIG, da utilizzare in funzione dei vari livelli di indisponibilità del Sistema.

Torna all'indice.