MANUALE DELLA CONSERVAZIONE

V 1.0.1

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	18/19/2016	Carlo Lentini	*Incaricato della realizzazione del Sistema di Conservazione*
Verifica	02/12/2016	Carlo Lentini	*Incaricato della realizzazione del Sistema di Conservazione*
Approvazione	04/06/2019	Carlo Lentini	*Responsabile della conservazione*

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
V 1.0	02/12/2016	Prima versione	
V 1.0.1	04/06/2019	Versione finale	

INDICE

Contents

1.1. PREMESSA

Secondo quanto stabilito dal legislatore italiano nel Codice dell'Amministrazione Digitale (CAD), le pubbliche amministrazioni sono tenute a formare gli originali dei propri documenti con mezzi informatici, consentire la comunicazione con le imprese esclusivamente utilizzando le tecnologie dell'informazione e della comunicazione e ridisegnare la propria struttura organizzativa, incentivando la razionalizzazione e semplificazione dei procedimenti amministrativi, le attività gestionali, i documenti, la modulistica, le modalità di accesso e di presentazione delle istanze da parte dei cittadini e delle imprese, consentendo un migliore e più esteso utilizzo delle tecnologie[1].

L'avvento del digitale ha determinato l'utilizzo di differenti strumenti di organizzazione, memorizzazione e fruizione delle informazioni prodotte, imponendo una totale revisione della tradizionale prassi archivistica; i tempi e le procedure basate sulla distinzione classica delle tre fasi di archiviazione (corrente, di deposito e storica) si modificano profondamente e si rende necessaria una riprogrammazione delle attività di tutela e la definizione di requisiti descrittivi fin dalla fase di produzione ("concezione") dell'archivio. Di conseguenza, l'efficacia delle attività di custodia dei contenuti informativi digitali è messa in crisi dalla continua evoluzione delle tecnologie informatiche, dalla fragilità dei supporti e dall'obsolescenza dei formati elettronici.

I sistemi di riferimento attinenti alle diverse fasi del ciclo vitale dei documenti, che dovranno essere logicamente distinti ma dialogare, sono due: il sistema di gestione documentale - nel cui contesto i documenti si formano, danno avvio ai diversi procedimenti amministrativi e vengono archiviati attraverso l'ausilio di specifici strumenti descrittivi - e il sistema di conservazione.

Nell'ottica della tradizionale considerazione dell'archivio come un *unicum,* caratterizzato quindi da procedure atte a preservare e restituire nel tempo i nessi logici tra la documentazione - la quale è però soggetta a trasferimenti secondo tempistiche predefinite, basate sull'occorrenza per l'espletamento delle pratiche quotidiane - si prevede un'organizzazione capillare della documentazione, basata sugli strumenti archivistici di riferimento[2], con interventi di versamento periodico dall'archivio corrente, all'eventuale archivio di deposito, al sistema di conservazione, fino alla conservazione permanente nell'archivio storico.

Il Codice dell'Amministrazione Digitale impone per tutti i soggetti, siano essi pubblici oppure privati, l'obbligo di conservare i propri documenti informatici; inoltre secondo le regole tecniche in materia è possibile costruire sistemi di

[1] D. Lgs. 82/2005 e s.m.i., *Codice dell'Amministrazione Digitale*, artt. 5 *bis*, 15 e 40

[2] Titolario di classificazione, piano per la fascicolatura, manuale di gestione, piano di conservazione (o massimario di scarto)

conservazione che siano interni alla struttura del soggetto produttore (conservazione *in house*) oppure affidare all'esterno tutto o parte del processo (conservazione *in outsourcing*). Nel caso in cui sia una pubblica amministrazione ad affidare in outsourcing il servizio, il conservatore pubblico o privato con il quale viene stipulato il contratto deve dimostrare un'elevata affidabilità organizzativa, economica e tecnologica e dunque risultare obbligatoriamente presente nell'elenco dei conservatori accreditati dall'Agenzia per l'Italia Digitale.

Come disposto dalla normativa un sistema di conservazione ha il compito di assicurare l'autenticità, l'integrità, l'affidabilità, la leggibilità e la reperibilità dei documenti informatici, con i metadati descrittivi e di contesto ad essi associati, dei fascicoli informatici ovvero delle aggregazioni documentali informatiche e dei relativi metadati, dalla presa in carico dal produttore fino all'eventuale scarto. Tale procedura si esplica attraverso la predisposizione di pacchetti informativi (di versamento, archiviazione e distribuzione) - in linea con quanto contenuto in particolare nel modello di riferimento OAIS, "Open archive Information System" (ISO 14721:2012), e lo standard SInCRO, "Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali" (UNI 11386:2010) - la redazione del manuale di conservazione, la compilazione dei piani di continuità operativa e di disaster recovery e il monitoraggio continuo delle infrastrutture e dei sistemi hardware e software.

1.2. IL MODELLO CONSERVATIVO DELL'INAIL

INAIL ha deciso di optare per la soluzione conservativa *in house* e di gestire, dunque, all'interno della propria struttura organizzativa le attività del processo conservativo della documentazione informatica prodotta e ricevuta dall'Istituto; l'Ente ha definito i requisiti specifici del sistema per le diverse tipologie documentarie e implementato le funzionalità del software *CDeS,* sviluppato da Land Srl, adottato dall'Istituto.

Nell'ambito del Modello, Produttore è il titolare delle unità documentarie informatiche poste in conservazione e, attraverso il proprio Responsabile della conservazione, definisce e attua le politiche complessive del Sistema di conservazione governandone la gestione con piena responsabilità ed autonomia.

Il sistema garantisce la gestione e il monitoraggio del processo da parte del Responsabile della conservazione, in maniera automatizzata e il recupero nel tempo della documentazione informatica prodotta, in modo affidabile e conforme alle disposizioni della normativa vigente.

1.3. SCOPO E AMBITO DEL DOCUMENTO

Il presente documento costituisce il Manuale di Conservazione adottato da INAIL per il processo di conservazione della documentazione digitale ai sensi della vigente normativa in materia (elencata nell'apposito capitolo 3 del presente documento) e delle Linee Guida emanate dall'Agenzia per l'Italia Digitale.

Il documento illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, il processo, le architetture e infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo del sistema di conservazione.

Il Manuale descrive in particolare le procedure di trasferimento nel sistema di conservazione di serie e fascicoli relativi alla documentazione nativa digitale prodotta dall'INAIL, secondo il modello conservativo *in house* adottato, il quale prevede una gestione delle procedure di conservazione all'interno della struttura organizzativa dell'Ente.

La stesura del manuale di conservazione rispetta quanto indicato nell'art. 8 DPCM del 3 dicembre 2013 recante Regole tecniche in materia di sistema conservazione, garantendo omogeneità di struttura e completezza delle informazioni necessarie per la gestione del sistema di conservazione e per la definizione dei ruoli e delle interazioni con i soggetti esterni con i quali interagisce.

Tale documento comprende:

- i dati dei soggetti che nel tempo hanno assunto la responsabilità del sistema di conservazione, descrivendo in modo puntuale, in caso di delega, i soggetti, le funzioni e gli ambiti oggetto della delega stessa;
- la struttura organizzativa comprensiva delle funzioni, delle responsabilità e degli obblighi dei diversi soggetti che intervengono nel processo di conservazione;
- la descrizione delle tipologie degli oggetti sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di documenti e delle eventuali eccezioni;
- la descrizione delle modalità di presa in carico di uno o più pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento;
- la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione;
- la modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;
- la descrizione del sistema di conservazione, comprensivo di tutte le componenti tecnologiche, fisiche e logiche, opportunamente documentate e delle procedure di gestione e di evoluzione delle medesime;
- la descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie;

- la descrizione delle procedure per la produzione di duplicati o copie;
- i tempi entro i quali le diverse tipologie di documenti devono essere scartate ovvero trasferite in conservazione, ove, nel caso delle pubbliche amministrazioni, non già presenti nel manuale di gestione;
- le modalità con cui viene richiesta la presenza di un pubblico ufficiale, indicando anche quali sono i casi per i quali è previsto il suo intervento;
- le normative in vigore nei luoghi dove sono conservati i documenti.

Il Manuale di conservazione può essere aggiornato e sarà distribuito nella nuova versione, oltre ad essere inviato all'Agenzia dell'Italia Digitale.

Le diverse versioni del Manuale sono oggetto di conservazione nel sistema di conservazione.

Il Manuale è stato predisposto dal Responsabile della conservazione dell'Istituto, in accordo con il Coordinatore della gestione documentale ed è rivolto ai dirigenti, ai funzionari, agli operatori di protocollo ed agli istruttori delle pratiche quale strumento di riferimento per la conservazione dei documenti da parte dell'Istituto.

Per ogni tipologia documentaria sono illustrati i tempi di trasferimento e il set di metadati associato, definito per tipologia di documento trasferito nel sistema di conservazione (ALLEGATO B).

1.4. TERMINOLOGIA (GLOSSARIO E ACRONIMI)

Glossario dei termini e degli cronimi	
AgID	Agenzia per l'Italia Digitale
AOO	Area Organizzativa Omogenea
CA	Certification Authority
DCOD	**Direzione Centrale Organizzazione Digitale (INAIL)**
FTP server	Programma che permette di accettare connessioni in entrata e di comunicare con un Client attraverso il protocollo FTP
IdP	Strumento per rilasciare le informazioni di identificazione di tutti i soggetti che cercano di interagire con un Sistema; ciò si ottiene tramite un modulo di autenticazione che verifica un token di sicurezza come alternativa all'autenticazione esplicita di un utente all'interno di un ambito di sicurezza.
IPdA	Indice del Pacchetto di archiviazione
OAIS	ISO 14721:2012; Space Data information transfer system……
PdA	***Pacchetto di archiviazione***
PdD	***Pacchetto di distribuzione***
PdV	***Pacchetto di versamento***

1.5. NORMATIVA E STANDARD DI RIFERIMENTO

1.5.1. Normativa

Vengono elencati di seguito i principali riferimenti normativi italiani in materia:

- Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in

materia di documentazione amministrativa;

- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, 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;
- Decreto del Ministero dell'Economia e delle Finanze n. 55/2013 - Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'articolo 1, commi da 209 a 213, della legge 24 dicembre 2007, n. 244;
- 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 Ministero dell'Economia e delle Finanze del 17 giugno 2014 - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto – articolo 21, comma 5, del decreto legislativo n. 82/2005
- Decreto Presidente Consiglio dei Ministri 13-11-2014 -Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici
- Regolamento Europeo n. 910/2014 eIDAS (electronic IDentification Authentication and Signature)
- Regolamento (UE) n. 2016/679 in materia di protezione dei dati personali

1.5.2. Standard di riferimento

Di seguito sono riportati gli standard ai quali si fa riferimento per il Manuale di Conservazione:

- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la Conservazione elettronica delle informazioni;
- ETSI TR 101 533-2 V1.3.1 (2012-04)Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la Conservazione elettronica delle informazioni;
- UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

2. RUOLI E RESPONSABILITA'

Le figure previste sono declinate nell'Allegato 1 con il dettaglio dei nominativi delle figure responsabili per ciascun ruolo.

2.1. Responsabile della conservazione

Il Responsabile della conservazione è la persona legalmente responsabile dell'integrità e della conservazione dei documenti ed è designato dai vertici dell'organizzazione. In base a quanto stabilito dalla norma (DPCM 3 dicembre 2013, art. 7), il Responsabile della conservazione, in collaborazione con la DCOD, svolge personalmente o delega, i seguenti compiti:

- 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;
- genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
- effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
- assicura la 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; adotta analoghe misure con riguardo all'obsolescenza dei formati;
- provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
- adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12;
- assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
- provvede, per gli organi giudiziari e amministrativi dello Stato, al versamento dei documenti conservati all'archivio centrale dello Stato e agli archivi di Stato secondo quanto previsto dalle norme vigenti;
- predispone il manuale di conservazione di cui all'art. 8 e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

2.2. Responsabile della gestione documentale e suo vicario

Il responsabile della gestione documentale è individuato in ogni Area organizzativa omogenea dell'Istituto; è chiamato a conoscere tutte le funzionalità del sistema e le regole organizzative della AOO, garantendo il buon funzionamento del servizio UTP e il rispetto delle disposizioni normative e delle procedure concernenti le attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali e le attività di gestione degli archivi.

Autorizza l'apertura, l'uso e la chiusura del registro di protocollazione di emergenza, la corretta gestione del documento da trattare, la corretta registrazione e classificazione dei documenti in entrata ed in uscita della AOO.

Controlla il buon funzionamento degli strumenti e dell'organizzazione delle attività di protocollazione e le funzionalità di accesso.

Sollecita le procedure di ripristino delle funzionalità del sistema in caso di guasti o anomalie.

Esegue, periodicamente, dei controlli a campione nell'ambito della AOO per verificare l'utilizzo regolare dell'unico registro ufficiale di protocollo e la validità dei criteri di classificazione e fascicolazione utilizzati.

Autorizza le eventuali operazioni di annullamento della registrazione di protocollo.

Visualizza e verifica il contenuto del registro di protocollo giornaliero prima della chiusura e assicura il suo versamento al sistema di conservazione.

2.3. Coordinatore della gestione documentale e suo vicario

Il Coordinatore della gestione documentale, ai sensi della vigente normativa:

- predispone lo schema del manuale di gestione dei documenti, provvedendo alla sua comunicazione e diffusione;
- assicura i tempi, le modalità e le misure organizzative e tecniche finalizzate all'eliminazione dei protocolli di settore e, in generale, dei protocolli non autorizzati diversi dal protocollo informatico previsto dal testo unico;
- predispone, d'intesa con il Responsabile della conservazione ed il Responsabile dei sistemi informativi, il piano per la sicurezza informatica previsto dalle regole tecniche per il protocollo informatico;
- definisce e assicura criteri uniformi di trattamento del documento informatico e, in particolare, di classificazione e archiviazione, nonché di comunicazione interna tra le AOO, così come previsto dal TUDA;
- garantisce, di concerto con le strutture interne competenti in materia informatica, il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei

flussi documentali, incluse le funzionalità di accesso e le attività di gestione dell'archivio;

- cura, con l'ausilio del Responsabile dei sistemi informativi, che le funzionalità del sistema di gestione documentale, in caso di guasti o anomalie, siano ripristinate nel più breve tempo possibile.

Inoltre il Coordinatore:

- aggiorna periodicamente il Manuale e lo sottopone all'approvazione;
- aggiorna, quando necessario, il Piano di Classificazione (Titolario) e lo sottopone all'approvazione;
- aggiorna, quando necessario, l'elenco dei formati dei documenti elettronici.

Il Coordinatore della gestione documentale individua un vicario per i casi di vacanza, assenza o impedimento.

2.4. Responsabile Sicurezza informatica

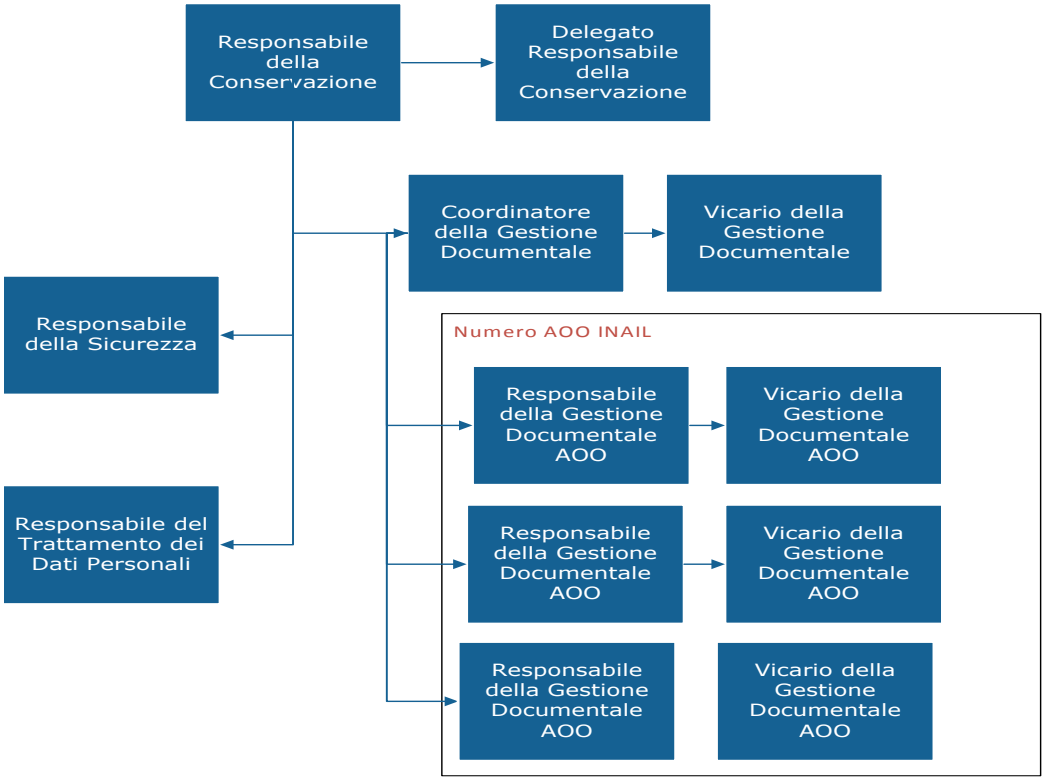
È responsabile della definizione delle policy, delle regole e delle procedure di sicurezza che devono essere implementate dalle strutture di competenza per la corretta gestione e conservazione dei documenti e delle informazioni trattate.

2.5. Responsabile del trattamento dei dati personali

Il Responsabile del trattamento dei dati, nominato ai sensi dell'art.29 del 196/03, dovrà essere informato delle attività svolte sui dati in modo che possa verificare l'attuazione e l'applicazione del regolamento dell'Istituto sul trattamento dei dati e delle altre disposizioni dell'Unione Europea relative alla protezione dei dati nonché fornire eventuali pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare i relativi adempimenti.

3. STRUTTURA ORGANIZZATIVA PER LA CONSERVAZIONE DOCUMENTALE

L'assegnazione dei ruoli in funzione della struttura organizzativa dell'INAIL è illustrata come di seguito:



:

Figura 1. Struttura organizzativa

4. OGGETTI SOTTOPOSTI A CONSERVAZIONE

Come previsto dallo standard di riferimento **ISO 14721:2012, OAIS - "Open Archive Information System",** la procedura di trasferimento della documentazione dal sistema di gestione documentale al sistema di conservazione dell'Ente, deve avvenire attraverso la creazione di pacchetti di versamento (PdV), contenenti uno o più documenti, con i metadati descrittivi e di contesto ad essi associati; l'archiviazione della documentazione versata nel sistema di conservazione, avviene sotto forma di Pacchetto di Archiviazione, cui viene è associato un Indice del Pacchetto di Archiviazione - un file XML, strutturato in maniera conforme allo standard UNI 11386 SInCRO che descrive la struttura e gli eventuali legami logici con gli altri pacchetti archiviati.

In linea con quanto definito nel modello OAIS, attraverso una specifica funzione dell'applicativo viene consentita la ricerca secondo parametri predefiniti e la documentazione è acquisibile sotto forma di Pacchetti di Distribuzione, aventi le stesse caratteristiche (documento e set di metadati associato) del Pacchetto di Archiviazione dai quali derivano.

Nei paragrafi seguenti vengono illustrate le tipologie di pacchetti informativi e il set minimo di metadati che la normativa prevede di associare alla documentazione e al fascicolo informatico.

4.1. Oggetti conservati

Il sistema di conservazione, secondo quanto previsto dall'art. 3 del DPCM 3 dicembre 2013, deve assicurare la conservazione, "garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità", delle due tipologie di unità archivistiche:

a) documenti informatici con i metadati associati;

b) fascicoli informatici o aggregazioni documentali informatiche con i relativi metadati e i riferimenti che identificano univocamente i singoli oggetti documentali appartenenti ai fascicoli o alle aggregazioni documentali.

Il sistema di conservazione accetta solo determinati formati documentali scelti tra quelli che per le loro caratteristiche sono, al momento attuale, da ritenersi coerenti con le regole tecniche del documento informatico e del sistema di conservazione.

Ai fini della formazione, gestione e conservazione, nell'ambito dei diversi sistemi produttori si scelgono formati che possano garantire la leggibilità e la reperibilità del documento informatico nel suo ciclo di vita.

La leggibilità di un documento informatico dipende dalla possibilità e dalla capacità di interpretare ed elaborare correttamente i dati binari che costituiscono il documento, secondo le regole stabilite dal formato con cui

esso è stato rappresentato.

Pertanto, prima di avviare il processo di conservazione (ovvero durate la fase di preacquisizione) vengono svolte specifiche verifiche di aderenza del formato dei documenti agli standard adottati e ne viene controllata l'integrità.

Sono principalmente accettati, per la Conservazione, i documenti nei seguenti formati:

- PDF/A;
- EML;
- XML.

I documenti sottoscritti sono accettati nei formati:

- P7M (CAdES);
- PDF (PAdES);
- XML (XAdES).

I documenti marcati temporalmente sono accettati nei seguenti formati:

- TSR;
- TST.

E' possibile prevedere di estendere la conservazione anche ad altri formati purché siano disponibili librerie di validazione per la realizzazione dei necessari controlli di conformità. Per tali aspetti, il Responsabile della conservazione collabora con il Coordinatore della gestione documentale, che rappresenta l'osservatorio tecnologico per l'evoluzione dei formati ammessi per la conservazione.

4.2. **Pacchetto di versamento**

Il Pacchetto di versamento (PdV)è il l'elemento informativo che identifica l'insieme di dati che vengono inviati al sistema di conservazione dal soggetto produttore, ed è composto dai file da conservare e da un tracciato record chiamato anche Indice del pacchetto di versamento (IPdV), nello standard XML contenente le informazioni identificative e descrittive dei file.

Il Pacchetto di Versamento per Documenti Singoli è composto da una Cartella principale contenente una serie di Cartelle Secondarie ed un file XML di indice chiamato input_XXXX.xml (XXXX è un codice numerico generato dal sistema).

Il File input_XXXX.xml contiene gli indici dei file del pacchetto di versamento.

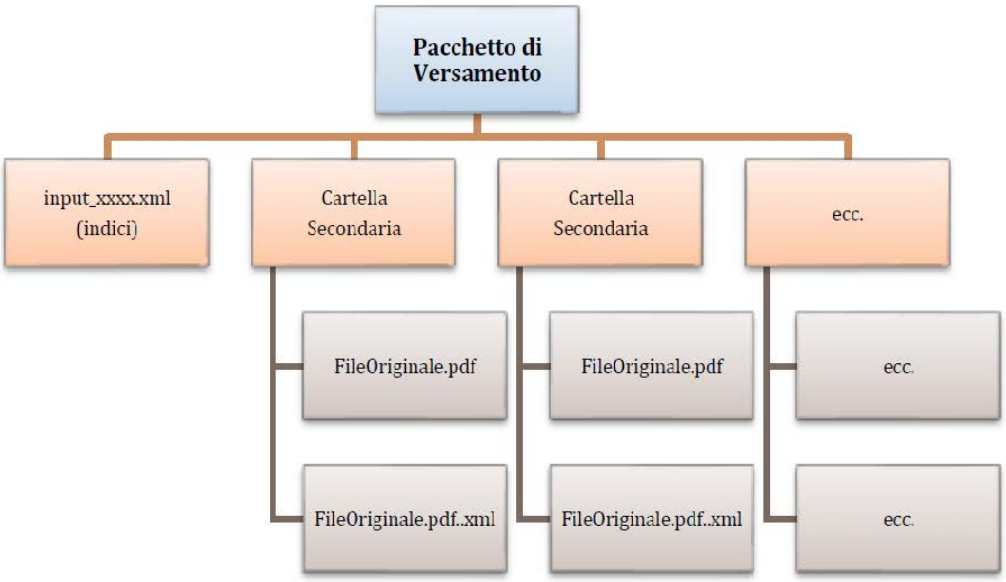


Figura 2. Struttura del pacchetto di versamento per il documento informatico

Ogni singola directory è dedicata ad un documento del pacchetto e ne replica anche il nome comprensivo di estensione.

E' possibile gestire anche gruppi di documenti, ad esempio una fattura e relativo allegato (fig. 2), che non devono essere confusi con il Fascicolo che è invece gestito in modalità diversa.

La posizione su disco del pacchetto è mappata all'interno della struttura del file input_XXXX.xml.

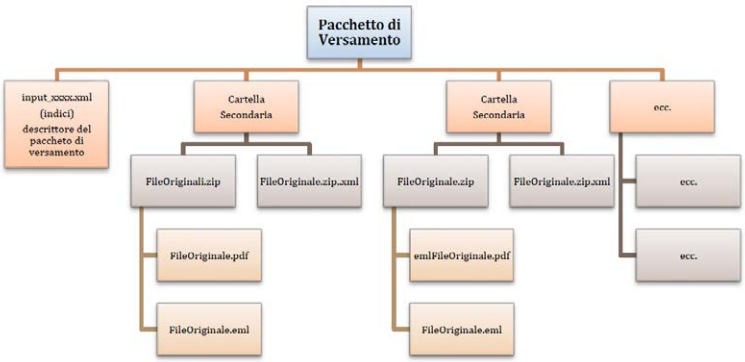


Figura 3. Struttura di dettaglio del pacchetto di versamento per gruppi di documenti

Il Pacchetto di Versamento può gestire anche Fascicoli Informatici, in questo caso la struttura è composta da una Cartella principale (Figura 3), che include una serie di cartelle secondarie ed il file XML di indice chiamato input_XXXX.xml (codice numerico generato dal sistema).

Ogni Cartella Secondaria contiene, a sua volta, il file zip con tutti i documenti relativi al Fascicolo Informatico ed il relativo file XML di indice; tale file è

denominato con lo stesso nome del file originale ma con l'aggiunta dell'estensione .xml.

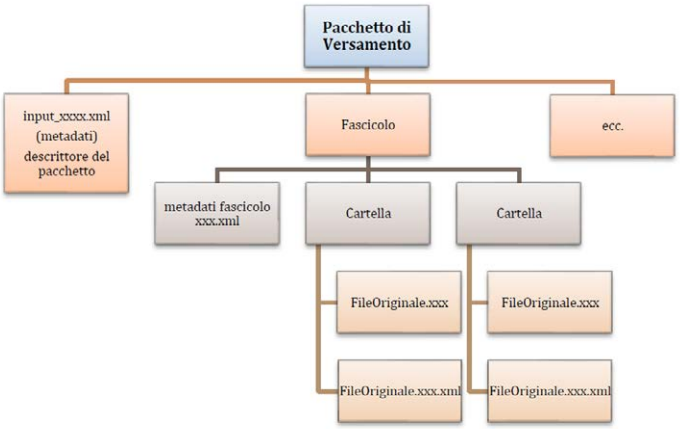


Figura 4. Struttura del pacchetto di versamento per il fascicolo elettronico

I metadati minimi del **pacchetto di versamento** possono essere così sintetizzati:

- Identificativo univoco e persistente del pacchetto di versamento;
- Riferimento temporale valido, attestante la data e l'ora di creazione del pacchetto;
- Denominazione del Responsabile della produzione del pacchetto;
- Impronta del pacchetto di versamento;
- Numero dei documenti compresi nel pacchetto.

I metadati del fascicolo informatico, dei documenti informatici e amministrativi informatici riportano le indicazioni già fornite nella fase di formazione e gestione del documento, oltre alle informazioni utili ai fini della verifica dell'autenticità, dell'integrità e dell'immodificabilità dei *file*:

I metadati minimi associati **al fascicolo informatico** sono i seguenti:

- Denominazione dell'amministrazione titolare del procedimento e delle amministrazioni partecipanti
- Estremi cronologici
- Oggetto dell'affare o del procedimento amministrativo
- Identificativo del fascicolo
- Formato dei *file*
- Lista dei documenti
- Impronta dei documenti.

Inoltre, sono specificati dalla normativa, i metadati minimi previsti per ciascuna tipologia di documento conservato.

Per il **documento informatico** sono previsti i seguenti metadati minimi:

- identificativo univoco e persistente

- data di chiusura
- oggetto (sintesi del contenuto di un documento)
- soggetto che ha formato il documento
- impronta

Per il **documento amministrativo** informatico, specifico per le pubbliche amministrazioni sono previsti i seguenti metadati minimi:

- codice identificativo dell'amministrazione
- codice identificativo dell'area organizzativa omogenea
- codice identificativo del registro
- data di protocollo
- progressivo di protocollo
- oggetto
- mittente
- destinatario o i destinatari
- impronta

Per il **fascicolo amministrativo** sono previsti i seguenti metadati minimi:

- codice identificativo dell'Amministrazione titolare del procedimento
- elenco codici identificativi delle Amministrazioni che partecipano all'iter del procedimento
- responsabile del procedimento
- oggetto del fascicolo
- elenco dei codici identificativi dei documenti contenuti nel fascicolo
- codice identificativo del fascicolo

Il Decreto Ministero Economia e Finanze del 17 giugno 2014 (art.3 comma b) definisce, per i **documenti rilevanti ai fini tributari** (di cui all'Allegato 1 del Provvedimento Attuativo Agenzia delle Entrate del 25 ottobre 2010, n. 2010/143663) l'insieme minimo dei metadati di seguito riportato:

- cognome
- nome
- denominazione
- codice fiscale
- partita Iva
- data documento
- periodo d'imposta

- tipo documento (vedi Allegato 1 del Provvedimento Agenzia delle Entrate n.2010/143663)

Questi metadati vanno ad integrarsi a quelli previsti per il documento generico previsti dall'Allegato 5 del D.P.C.M. 3 dicembre del 2013.

Nell'allegato 2 si riporta l'elenco completo dei metadati previsti per ciascuna tipologia documentale accettata dal sistema di conservazione.

4.3. **Pacchetto di archiviazione**

Il pacchetto di archiviazione rappresenta l'insieme degli oggetti conservati dal sistema di conservazione. Può essere derivato da uno o più pacchetti di versamento. Viene prodotto dal Conservatore nelle modalità e nello standard definito da AgID. In particolare il pacchetto di archiviazione si compone dei file e di un'evidenza Informatica, chiamata Indice del Pacchetto di Archiviazione (IPdA).

Il Pacchetto di Archiviazione è composto da un PDF/A a cui e allegato (attachment PDF) un Indice di Conservazione (xml) generato in formato **UNI 11386:2010** (Standard SInCRO). Nel file xml sono presenti:

- la lista completa dei documenti del pacchetto
- Il file indice IPdA firmato con firma digitale dal Responsabile della conservazione e marcato temporalmente
- I riferimenti ai file xml esterni contenenti i metadati di ogni singolo documento.

Alla chiusura del pacchetto di archiviazione (automatica o manuale), oltre alla Firma Elettronica Qualificata del RSC appone il riferimento temporale nell'Indice di Conservazione (xml UNI 11386:2010) e, se richiesto, applica la Marca Temporale al PDF.

L'indice del Pacchetto di Archiviazione viene realizzato in conformità all'Allegato 4 delle Regole tecniche in materia di sistema di conservazione contenute nel DPCM 3 dicembre 2013 e allo standard Uni SinCRO 11386:2010 che prevedono l'utilizzo dello schema XML di seguito riportato:

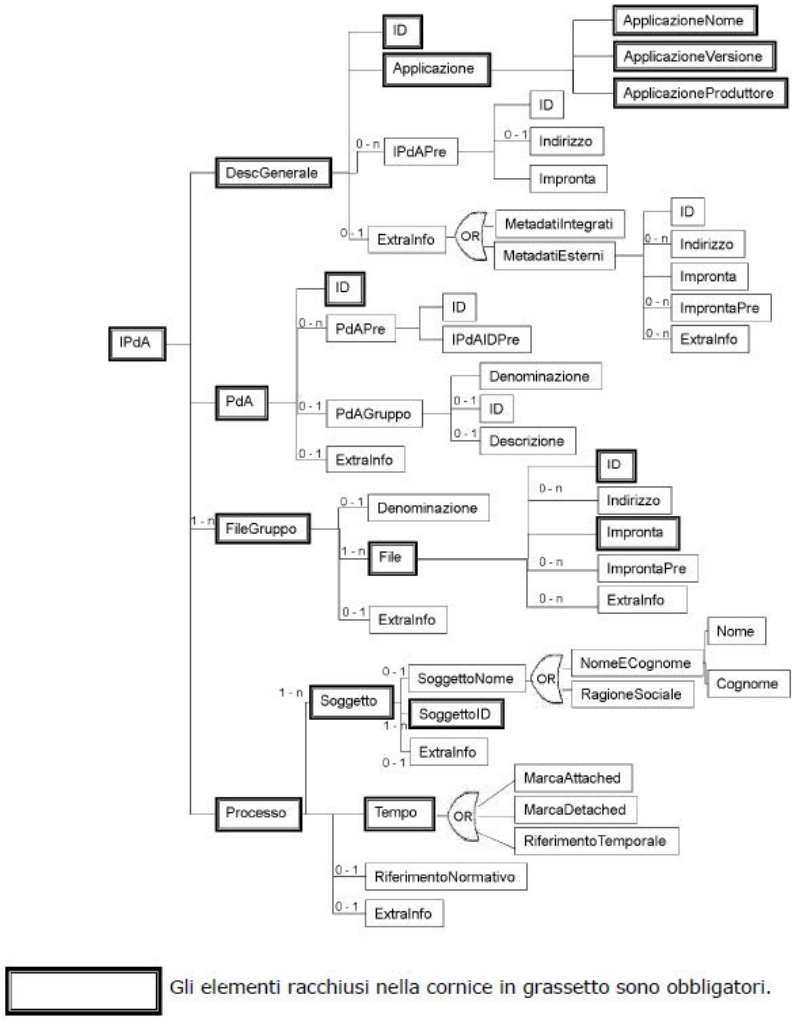


Figura 5. Indice del pacchetto di archiviazione

L'IPdA rappresenta l'evidenza informatica associata ad ogni PdA. Esso contiene le seguenti informazioni:

- informazioni inerenti il Pacchetto di Archiviazione, in particolare: un identificatore del PdA, eventuali riferimenti ad altri PdA da cui deriva il presente, informazioni relative ad una eventuale tipologia/aggregazione (di natura logica o fisica) cui il PdA appartiene ed infine un eventuale elemento "ExtraInfo" che consente di introdurre metadati soggettivi relativi al PdA;
- indicazione di uno o più raggruppamenti di uno o più file che sono contenuti nel PdA. È possibile raggruppare file sulla base di criteri di ordine logico o tipologico ed assegnare ad ogni raggruppamento/singolo file le informazioni di base ed un eventuale elemento "ExtraInfo" che consente di introdurre metadati definiti del Produttore. Ogni elemento "file" contiene l'impronta attuale dello stesso, ottenuta con l'applicazione di un algoritmo di hash e un'eventuale impronta precedentemente associata ad esso: in questo modo è possibile ad esempio gestire il passaggio da un algoritmo di hash diventato non più sicuro ad uno più robusto;

- informazioni relative al processo di produzione del PdA, come: l'indicazione del nome e del ruolo dei soggetti che intervengono nel processo di produzione del PdA (es. responsabile della conservazione, delegato, pubblico ufficiale ecc.), il riferimento temporale adottato (generico riferimento temporale o marca temporale), l'indicazione delle norme tecniche e giuridiche applicate per l'implementazione del processo di produzione del PdA ed, infine, anche per il processo, un elemento "ExtraInfo" che consente di aggiungere dati soggettivi relativi al processo.

4.4. Pacchetto di distribuzione

Il Pacchetto di Distribuzione consiste in una cartella contenente al suo interno il file o i file ricercati e il relativo Indice del Pacchetto di Archiviazione.

Il Pacchetto di Distribuzione può comprendere una ulteriore Cartella di Servizio contente gli *installer* dei programmi necessari per la visualizzazione e la verifica dei file in esso contenuto.

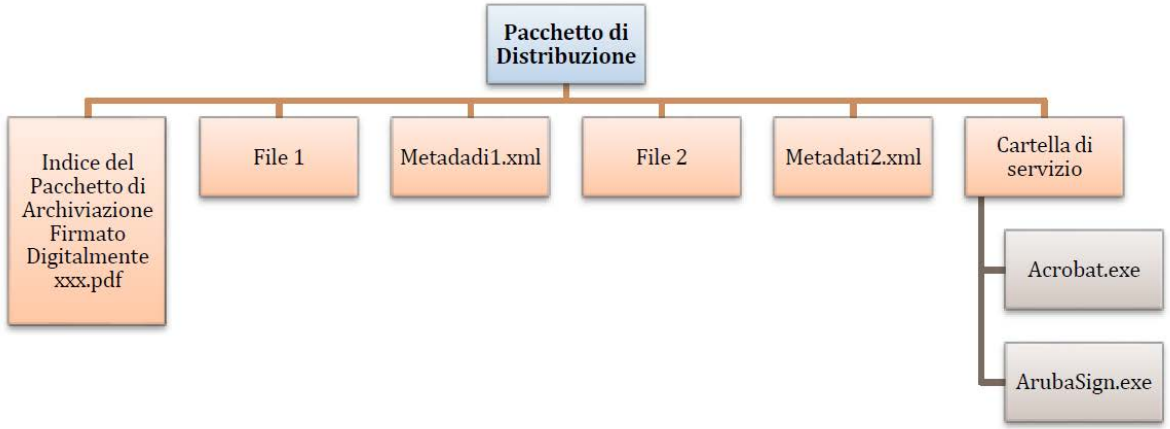


Figura 6. Struttura del pacchetto di distribuzione

5.IL PROCESSO DI CONSERVAZIONE

Il modello di conservazione *in house* adottato dall'INAIL prevede l'adozione del software CDeS, sviluppato da LAND Srl., il quale consente l'espletamento delle seguenti attività:

- acquisizione documento (caricamento automatico di file)
- creazione dei pacchetti di versamento
- verifica della conformità
- rifiuto o accettazione (comunicazione di anomalie e/o errori; produzione del Rapporto di versamento)
- passaggio in archiviazione
- chiusura dei pacchetti di archiviazione
- ricerca
- estrazione del pacchetto di distribuzione

Sono illustrate di seguito le procedure gestite dal sistema nelle diverse fasi del processo:

- **Versamento**

La prima fase consiste nell'associare ad ogni file i suoi metadati. Questa fase è denominata "versamento". Tra i dati associati vengono indicati l'organizzazione di riferimento e l'archivio di destinazione.

- **Archiviazione**

La seconda fase prevede di aggregare più file tra di loro creando un pacchetto di archiviazione che viene poi caricato sul sistema. In questa fase vengono calcolate le hash dei documenti che vengono inserite all'interno del file indice del pacchetto.

Dal momento che un file è incluso all'interno di un pacchetto che viene importato, diventa ricercabile sul sistema.

- **Chiusura**

La fase di chiusura prevede la firma e marcatura temporale del rapporto di chiusura, e fa sì che il pacchetto passi dallo stato di aperto a chiuso. Questa procedura "congela" i file contenuti all'interno del singolo pacchetto.

- **Ricerca**

Tutti i file all'interno dei pacchetti, siano essi aperti o chiusi, sono ricercabili all'interno del sistema. E' possibile ricercare i file grazie ai metadati associati.

- **Estrazione**

L'insieme dei file restituiti da una ricerca può essere esportata sotto forma di file ZIP. Il file ZIP conterrà i file oggetto della ricerca e i relativi rapporti di

chiusura

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

L'acquisizione dei Pacchetti di versamento avviene mediante i tre canali messi a disposizione tramite Interfaccia web su HTTPS, FTPS e/o Web Service, sempre tramite HTTPS.

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

Una volta creato, il PDV viene trasmesso al sistema di conservazione e il software procede con le seguenti verifiche della conformità:

- formato scelto per la creazione del file
- completezza dei metadati associati al documento
- validità del certificato di firma, in caso di documento sottoscritto
- validità della marca temporale, se apposta
- verifica dell'impronta

5.3. Accettazione dei pacchetti di versamento e generazione del rapporto di versamento

In caso di esito positivo il sistema di conservazione produce e restituisce un "Rapporto di versamento", confermando la presa in carico del pacchetto di versamento.

Il Rapporto di Versamento è conservato illimitatamente nell'ambito del sistema di conservazione dell'Ente.

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

Qualora vengano riscontrate anomalie in merito a formato prescelto, al set di metadati associato alla tipologia di documento e alla validità del certificato di firma digitale, si procede con la segnalazione degli errori, comunicando e motivando l'esito negativo della trasmissione del Pacchetto.

5.5. Preparazione e gestione del pacchetto di archiviazione

In caso di esito positivo della trasmissione del Pacchetto di Versamento, il sistema procede a generare l'"Indice del pacchetto di archiviazione", che illustra i contenuti del pacchetto di archiviazione e del relativo processo di creazione.

Al fine di garantire l'integrità del Pacchetto di Archiviazione e consentire quindi ad uno o più documenti in esso contenuti (insieme ai metadati descrittivi e di contesto), di poter essere fruiti a distanza di tempo preservando la propria efficacia probatoria, il Responsabile della conservazione sottoscrive il Pacchetto, apponendola la propria firma digitale.

Al pacchetto "chiuso", viene associato un Indice e si procede con la sottoscrizione dell'IPdA: il software consente di produrre, marcare temporalmente e firmare massivamente (con firma del Responsabile della conservazione) e in maniera automatica tramite web service (secondo tempistiche predefinite), il file in .pdf/a, attestante data e ora di produzione dell'Indice; al documento è allegato il tracciato XML dell'Indice stesso, conforme allo standard UNI 11386 SInCRO.
Il software produce inoltre un "Rapporto di chiusura", attestante data e ora dell'operazione di chiusura del PdA.

La chiusura dei pacchetti di archiviazione è al più mensile.

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

Il software adottato per la conservazione consente la funzione di ricerca (per singola tipologia documentale e trasversale tra le diverse classi), consultazione e restituzione della documentazione, esclusivamente al personale autorizzato, tramite la creazione di un Pacchetto di Distribuzione (PDD), contenente i documenti richiesti e i metadati descrittivi, coincidenti con il Pacchetto di Archiviazione.

5.7. Produzione di duplicati e copie informatiche e intervento del pubblico ufficiale nei casi previsti

Il Responsabile della conservazione può procedere con l'interrogazione del sistema per il recupero della documentazione della quale si richiede la consultazione, utilizzando la maschera di ricerca "semplice" ed "avanzata"; l'applicativo darà modo di generare il Pacchetto di Distribuzione, per visualizzare il pacchetto nel quale il documento è conservato e di consultare la documentazione contenuta.

Il download del file è consentito esclusivamente al Responsabile della conservazione per la produzione di copie e duplicati informatici conformi agli originali, per fini amministrativi, di monitoraggio dell'obsolescenza e di controllo e verifica da parte delle autorità competenti.

5.8. Scarto dei pacchetti di archiviazione

Attraverso una specifica funzionalità di monitoraggio, il software provvede a segnalare il maturamento dei tempi per lo scarto, secondo le previsioni imposte ex lege e le tempistiche definite nel Piano di conservazione (o Massimario di selezione) dell'Ente.

Viene successivamente prodotto un elenco di scarto (contente almeno una descrizione della documentazione, i relativi estremi cronologici e le motivazioni della proposta di scarto), che deve essere autorizzato dalla Soprintendenza archivistica competente.

Una volta ricevuto il nulla osta da parte della Soprintendenza si può procedere all'eliminazione della documentazione dal sistema di conservazione.

L'elenco dei documenti sottoposti allo scarto, firmato e marcato temporalmente, viene conservato illimitatamente nell'ambito del sistema.

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

Sono previste apposite procedure software che facilitano l'interoperabilità dei pacchetti di archiviazione ad eventuali altri Conservatori. In particolare, vengono fornite le strutture dei Pacchetti di Archiviazione che sono principalmente composti da una cartella (con il nome parlante) contenente un file PDF Firmato con Firma Elettronica Qualificata del Responsabile della conservazione con i dati del "Pacchetto di Archiviazione" che avrà in allegato, un file xml con struttura SInCRO (UNI ISO 11386:2010) contenenti le impronte di tutti i file contenuti nel pacchetto e, naturalmente, tutti i file conservati (nella forma di documenti, di fascicoli, o di aggregazioni documentali informatiche).

6. IL SISTEMA DI CONSERVAZIONE

Il sistema di conservazione gestisce il flusso documentale, dalla presa in carico del documento fino all'eventuale scarto (distruzione del documento/fascicolo informatico).

Il software tramite l'adozione di regole, procedure e tecnologie garantisce le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità nel tempo dei:

- documenti informatici e dei documenti amministrativi informatici con i metadati ad essi associati;
- 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.

Gli oggetti della conservazione sono trattati dal sistema di conservazione in pacchetti informativi che si distinguono in:

- pacchetti di versamento;
- pacchetti di archiviazione;
- pacchetti di distribuzione.

Ai fini dell'interoperabilità tra i sistemi di conservazione è stato adottato, come previsto dalle Regole Tecniche in materia di sistema di conservazione (pubblicate nella Gazzetta Ufficiale n. 59 del 12 marzo 2014), una struttura che fa riferimento allo standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI ISO 11386:2010), che è lo standard riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione.

Tutte le componenti funzionali della soluzione di conservazione, assicurano il trattamento dell'intero ciclo di gestione dell'oggetto conservato nell'ambito del processo di conservazione.

Il sistema di conservazione garantisce l'accesso all'oggetto conservato, per il periodo prescritto dalla norma, indipendentemente dall'evolversi del contesto tecnologico.

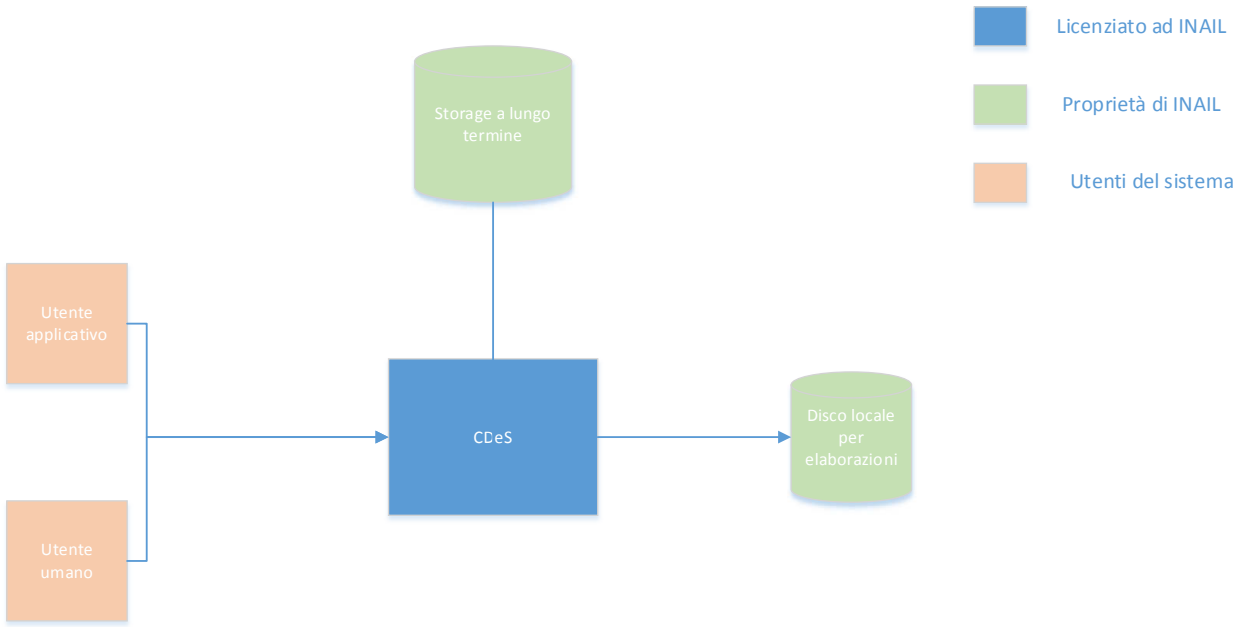


Figura 7. Struttura del sistema di conservazione

6.1. Componenti Logiche

Lo schema seguente illustra le componenti principali del sistema:

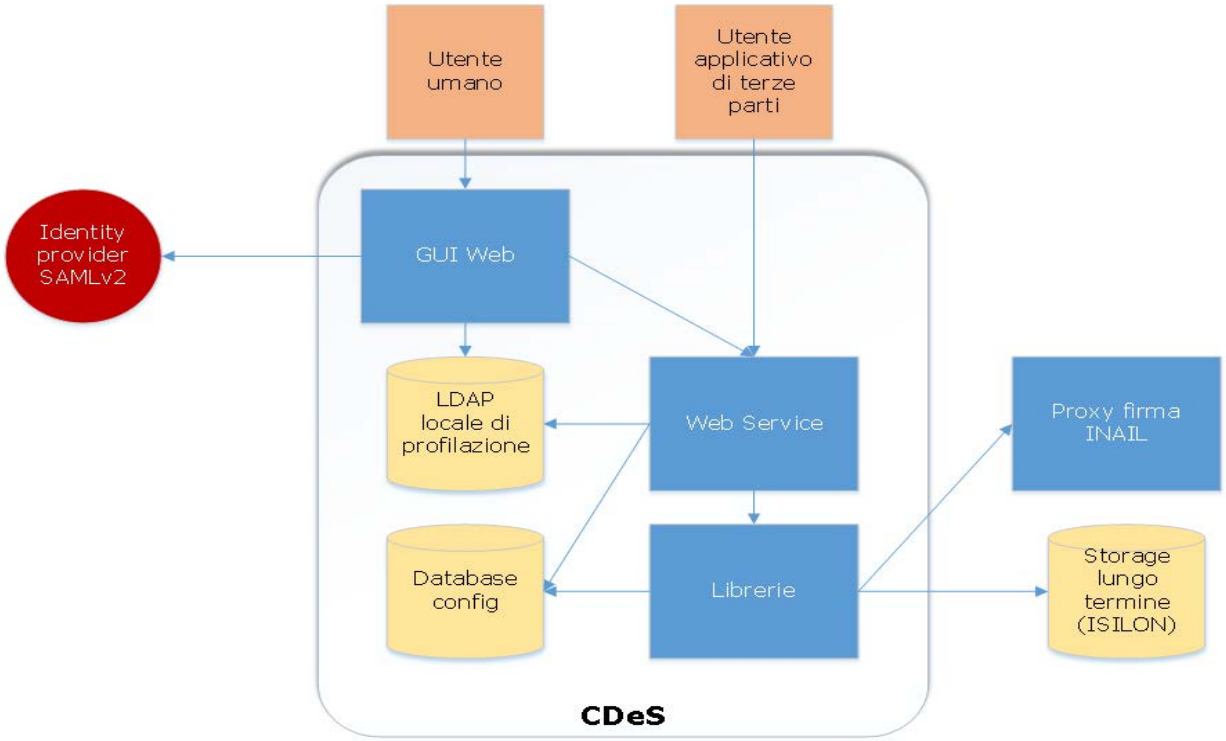


Figura 8 - Architettura logica

6.2. Elementi interni

Nello schema sono evidenziati i seguenti elementi interni:

- GUI Web

Si tratta della GUI web mediante la quale il conservatore o uno dei delegati può accedere per effettuare le operazioni di chiusura dei pacchetti oppure di consultazione dei pacchetti già archiviati o conservati. E' inoltre possibile utilizzare la pagina di caricamento dei file laddove fosse necessario un intervento manuale da parte del conservatore.

Il sistema presenta anche un'interfaccia di configurazione del sistema e di gestione dei profili utente.

La GUI web è sviluppata nel linguaggio PHP con l'utilizzo laddove necessario di parti di codice Javascript.

L'accesso alla GUI web è consentito unicamente a seguito di un'autenticazione SSO via SAMLv2 per i soli utenti profilati. La GUI web è esposta mediante protocollo HTTPS.

Il server web che espone la GUI web è Apache 2.4.

- Web Service

  I Web Service esposti dal sistema CDeS consentono, in base al profilo utente utilizzato per la connessione, di effettuare operazioni di:

  - caricamento di file
  - creazione dei pacchetti di versamento
  - passaggio in archiviazione
  - ricerca
  - estrazione del pacchetto di distribuzione
  - chiusura dei pacchetti

  L'autenticazione al web service avviene mediante connessione HTTPS con certificato client. Il CN del certificato client viene utilizzato per identificare l'utenza locale e relativa profilazione.

  I Web Service sono erogati su Tomcat8 e sono esposti mediante Apache 2.4. Apache comunica con Tomcat mediante connettore mod_jk.

- Librerie

  Le librerie rappresentano la parte core del sistema di conservazione e si occupano di gestire i pacchetti, creare gli indici necessari in formato SinCRO, indicizzare i dati, ecc.

  Le librerie sono scritte in Java.

- LDAP locale di profilazione

  Sul sistema è presente un server LDAP locale dove vengono definiti i profili utente utilizzati sul sistema. Esistono due macro tipologie di utenti per CDeS: utenti locali e utenti autenticati mediante sistema esterno. In entrambi i casi i dati dell'utente, la profilazione e quindi i livelli di accesso sono mantenuti sul sistema LDAP interno. Per le utenze locali viene anche gestita localmente la password, mentre per le utenze autenticate esternamente non vi sono password locali.

Oltre alle utenze legate ad una persona fisica possono esistere delle utenze per i sistemi client. In tal caso non vi è comunque nessuna password, ma l'autenticazione viene demandata alla presentazione di un certificato HTTPS client contenente come CN una stringa riconducibile all'utenza. I certificati possono essere auto-emessi oppure possono essere utilizzati certificati di terze parti. In quest'ultimo caso sarà necessario avere copia del certificato pubblico della CA emittente sul sistema.

L'LDAP interno è basato sul OpenLDAP 2.4. Non vi sono collegamenti dall'esterno all'appliance CDeS verso LDAP.

- Database di configurazione

  Sul sistema è infine presente un database su cui vengono salvati i dati di configurazione, i dati relativi agli indici e i log

  Il DBMS utilizzato da CDeS è PostegreSQL 9.5. Non vi sono collegamenti dall'esterno all' appliance CDeS verso il DBMS.

6.3. **Elementi esterni**

E i seguenti elementi esterni:

- Identity provider SAMLv2

  Per le utenze legate a persone fisiche, il sistema consente di demandare l'autenticazione ad un sistema esterno. Attualmente vengono gestite le modalità NTLMv2, SiteMinder (mediante reverse proxy) e SAMLv2. Nell'installazione INAIL è stata prediletta quest'ultima modalità.

- Proxy firma INAIL

  Il sistema di conservazione necessita, in alcuni passaggi, di poter firmare digitalmente alcuni documenti. In particolare è necessario che il conservatore o un suo delegato possano firmare i pacchetti messi in archiviazione per "chiuderli" e renderli di fatto "conservati". Tale operazione già per i primi archivi prevede diverse decine di firme al giorno. Onde evitare di tediare il conservatore con tale operazione è stato deciso di fare uso della firma digitale automatica. Il sistema di firma che dovrà essere contattato è quello esposto dal proxy di firma INAIL FDS.

- Storage lungo termine (ISILON)

  I dati che vengono messi in conservazione devono essere messi su uno spazio disco di grandi dimensioni, che possa essere facilmente espanso nel tempo visto che le tipologie documentali dovranno aumentare negli anni, e i dati dovranno essere manutenuti per diversi anni. La soluzione che è stata già utilizzata in passato è il sistema NFS EMC^2 ISILON già in essere all'Istituto. Tale sistema ha dei tempi di risposta adeguati ad un sistema di conservazione sia per la parte di scrittura che per quella di lettura dei dati. È anche possibile valutare il sistema ECS di EMC^2.

6.4. **Utenze**

Sono infine indicate le due tipologie di utilizzatori del sistema:

- Utenti umani

  Come già indicato nella descrizione della componente della GUI web, il sistema può essere acceduto da alcuni utenti per mezzo del loro browser. I soli utenti profilati sul sistema potranno accedere limitatamente ai propri privilegi.

  Ogni utente può essere assegnato per ruoli diversi a archivi diversi del sistema, in base al proprio ruolo istituzionale. I due ruoli principali sono: Conservatore (uno ed unico per l'intera organizzazione INAIL) e Delegato. Possono esistere più delegati, ognuno confinato al proprio archivio di riferimento, così come possono essere assegnati più delegati ad un archivio.

  Gli utenti possono essere autenticati mediante password locale oppure mediante SSO con autenticazione centralizzata. Le due modalità sono mutuamente esclusive tra di loro, ma possono essere adottate individualmente per ogni utente.

- Utenti applicativi di terze parti

  Per quanto concerne l'accesso ai web service il sistema utilizza ulteriori profili utente legati a certificati SSL utilizzati per identificare l'utente chiamante. Questi utenti non prevedono password e possono essere utilizzati unicamente per l'accesso ai web service, in base al profilo scelto (possibilità di caricare dati e creare pacchetti di versamento, di archiviare, di ricercare, ecc). Si fa uso di una politica di least privilege nella definizione di queste categorie di utenti.

6.5. **Componenti Fisiche**

Il sistema di conservazione CDeS deve garantire sia l'alta affidabilità del servizio sia la possibilità di continuare l'erogazione del servizio a seguito di eventi gravi.

È stato quindi pensato di installare più istanze di CDeS:

- L'istanza primaria presso il sito di Santuario
- L'istanza secondaria presso il sito di Tiburtino
- L'istanza di Disaster Recovery presso l'SPC Cloud

Lo schema seguente illustra le tre installazioni.

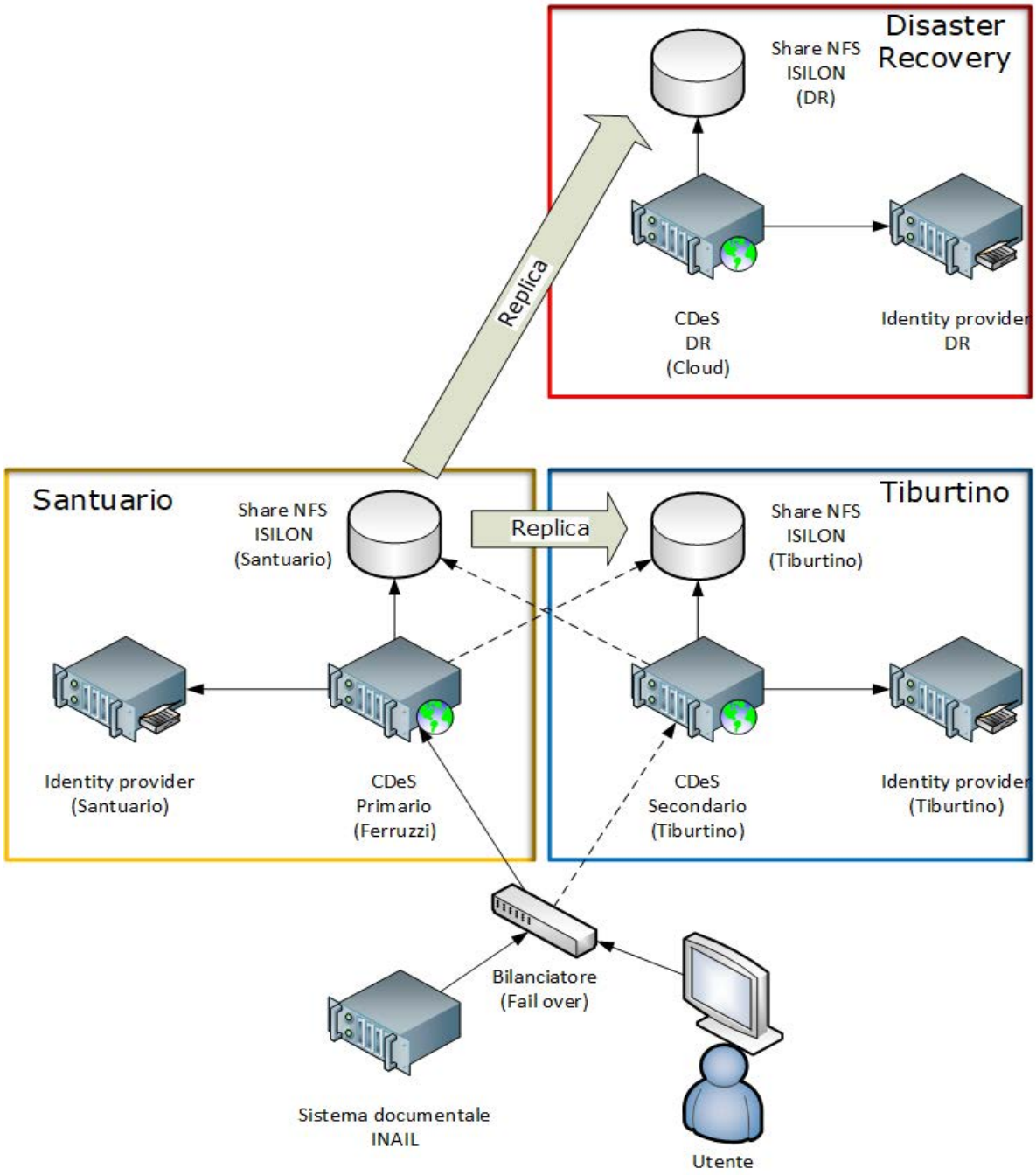


Figura 9 - Architettura fisica

I siti primario e secondario vengono gestiti in modalità Active-Passive, dove l'istanza primaria è quella attiva. Nel caso il sistema primario non fosse in grado di erogare il servizio, un bilanciatore messo a monte dovrà ridirigere il traffico verso l'istanza secondaria che nel frattempo avrà passato il proprio stato da Passivo ad Attivo.

I due siti replicano i propri dati seguendo il seguente schema:

- File archiviati: si demanda la replica ad ISILON
- File indice: si effettua una replica mediante rsync
- Database: si effettua una replica mediante file di log delle transazioni
- LDAP: si effettua una replica mediante file di log delle transazioni

Il sito di Disaster Recovery viene allineato con le stesse modalità. Può essere deciso di ridurre la frequenza di aggiornamento rispetto a quella del sito secondario per limitare il traffico di rete.

6.6. Procedure di gestione e di evoluzione

L'operatività del servizio viene assicurata attraverso l'attivazione di specifiche procedure:

- **Back-up e Disaster Recovery**

Le procedure di Back-up e Disaster Recovery sono dettagliate nell'allegato 3 al presente manuale.

- **Gestione e conservazione dei log**

I log di sistema sono memorizzati in un apposito spazio presso il CED.

In particolare i Log tracciano le attività principali del processo di versamento, conservazione ed esibizione. I LOG sono prodotti nel formato TXT e tracciano l'esecuzione delle funzioni e le eventuali eccezioni.

- **Gestione della continuità del servizio**

La continuità del servizio è garantita dalla replica del sito primario sull'istanza secondaria presso il sito di Tiburtino.

7. MONITORAGGIO E CONTROLLI

Il processo di conservazione è monitorato costantemente con l'obiettivo di fornire, per mezzo di statistiche predefinite, dati quantitativi sui documenti che giacciono nei diversi stati del processo di conservazione.

Nello specifico, sono monitorate le quattro fasi che mettono in evidenza i tempi di giacenza e il numero dei documenti nei vari stati del processo (inviato, acquisito, firmato, conservato); a queste quattro fasi si aggiunge anche un riepilogo dell'intero processo che evidenzia il numero di documenti per i quali il processo di conservazione non è andato a buon fine.

Il servizio, inoltre, è strutturato per fornire servizi continuativi con operatività H24 presidiata, garantendo:

- Implementazione dei sistemi di monitoraggio e relativo aggiornamento;
- Rilevazione degli eventi di allarme;
- Tracciamento su Sistema di Ticketing;
- Applicazione dell'opportuna procedura di fixing o innesco della Procedura di Escalation Operativa/Informativa;
- Follow-up del problema in caso di escalation.

7.1. Procedure di monitoraggio

Vengono prodotti dal Responsabile dell'Infrastruttura e resi disponibili periodicamente report di monitoraggio tecnico, su tutte le aree infrastrutturali (rete, server, storage, database, backup). Si tratta di report tra loro eterogenei, prodotti dal software di base dei sistemi e dal software di monitoraggio tecnico installato sui medesimi.

In Service Control Room è predisposto il monitoraggio del sistema di conservazione. In particolare, vengono espletate le seguenti attività:

- **Monitoraggio Infrastrutturale**

  La Service Control Room riceve in input l'architettura del sistema di conservazione da monitorare. Eventuali altri elementi da monitorare (file system, up/down processi) sono comunicati dal gruppo coinvolto per predisporne il monitoraggio.

- **Monitoraggio applicativo**

  Il sistema si presenta sotto forma di macchina virtuale basata su sistema operativo Linux Ubuntu 16.04 LTS. Su tale sistema è possibile implementare il monitoraggio applicativo e la verifica circa la compatibilità dell'agent CA per tecnologia Tomcat su macchine Linux Ubuntu. Questa attività è trattata in SCR ad alta priorità.

- **Monitoraggio EUE**

  Sul sistema di conservazione è implementato il monitoraggio del traffico simulato che avrà l'obiettivo di testare il corretto funzionamento

dell’applicazione circa la conservazione delle varie tipologie di documenti.

7.2. Verifica dell’integrità degli archivi

Sono previste procedure periodiche di controllo dell’integrità dei documenti conservati nei diversi siti e della loro congruenza, sia manuali che automatizzate; la produzione di reportistica è consentita con cadenza almeno semestrale e documenta l’oggetto, la data e l’esito dei controlli sulla leggibilità e riproducibilità della documentazione.

7.3. Allegato 1: Figure responsabili

ruoli	nominativo	data nomina	deleghe
Responsabile della conservazione	Ing. Carlo Lentini		
Vicario del responsabile della conservazione			
Coordinatore della gestione documentale	Dr. Francesco Colasuonno		
Responsabile Sicurezza informatica	Dr. Stefano Tomasini		
Responsabile trattamento dati personali	Dr. Stefano Tomasini		

7.4. Allegato 2: Elenco tipologie documentarie e set di metadati associato

Registro giornaliero di protocollo

Il set di metadati del Registro giornaliero di protocollo è definito in conformità a quanto disposto dall'allegato n. 5 alle Regole tecniche in materia di formazione, gestione e conservazione dei documenti informatici, emanate ai sensi dell'articolo 71 del Codice dell'Amministrazione Digitale e secondo quanto suggerito nel documento pubblicato dall'AgID, contenente le istruzioni per la "Produzione e conservazione del Registro giornaliero di protocollo".

Il Pacchetto "è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto"[3] e la sua conservazione è illimitata.

Il formato adottato è il pdf/a; il registro non è sottoscritto con firma digitale.

Viene schematizzata di seguito la struttura del set di metadati, in maniera normalizzata, da associare al documento, al fine di consentire la creazione del Pacchetto di Versamento, per la corretta conservazione del Registro, in conformità allo standard ISO 14721:2012 - Open Archival Information System (OAIS):

INDICE	Descrizione	Tipo	Len	Obbl
ID_Documento	Identificativo univoco e persistente è una sequenza di caratteri alfanumerici associata in modo univoco e permanente al documento informatico in modo da consentirne l'identificazione. Dublin Core raccomanda di identificare il documento per mezzo di una sequenza di caratteri alfabetici o numerici secondo un sistema di identificazione formalmente definito. Esempi di tali sistemi di identificazione includono l'Uniform Resource Identifier (URI), il Digital Object Identifier (DOI) e l'International Standard Book Number (ISBN)	STRINGA	35	SI

[3] DPCM 3 dicembre 2013 in materia di protocollo informatico, art. 7, c. 5

	Segnatura di protocollo			
Data_Chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immodificabile: data di produzione del Pacchetto di Versamento	DATE		SI
Ente_Denominazione	Denominazione del soggetto produttore	STRINGA		SI
Struttura_Denominazione	AOO (codice identificativo dell'AOO)	STRINGA		SI
Produttore_Nome	Il soggetto che ha la l'autorità e la competenza di produrre il PDV (es: Responsabile della gestione documentale)	STRINGA		SI
Produttore_Cognome		STRINGA		SI
Produttore_CF_codice_matricola	Dato che identifica legalmente il Produttore	STRINGA		SI
Tipologia_Documento	Tipo di documento (es: Registro Giornaliero di Protocollo)	STRINGA		SI
Oggetto_Documento	Descrizione del registro (es: registro giornaliero di protocollo dal num […] al num […] del […])	STRINGA	100	SI
Numero_Registro	Numero progressivo attribuito al registro	STRINGA		SI
Codice_Identificativo_Registro	Codice che identifica il registro	STRINGA		SI
Anno_Registro	Anno cui la registrazione si riferisce (AAAA)	STRINGA		SI
Numero_Prima_Registrazione	Numero della prima registrazione effettuata sul registro	STRINGA		SI
Numero_Ultima_Registrazione	Numero dell'ultima registrazione effettuata sul registro	STRINGA		SI
Data_Prima_Registrazione	Data della prima registrazione effettuata sul registro	DATE		SI
Data_Ultima_Registrazione	Data dell'ultima registrazione effettuata sul registro	DATE		SI
Classifica	Codice di classificazione	STRINGA		SI
ID_Fascicolo	Codice identificativo del fascicolo cui il documento	STRINGA		SI

	appartiene			
Tempo_Conservazione	Tempo di conservazione dell'unità documentaria, secondo il Piano di conservazione dell'Ente	STRINGA		SI
Impronta_Documento	Impronta del documento informatico	STRINGA		SI
Chiave_ gestionale	Codice che consente l'associazione logica della documentazione afferente alla stessa pratica	STRINGA		NO

Fattura PA

Le fatture attive e passive sono prelevate dal Sistema di Interscambio (SDI) e sottoposte a registrazione di protocollo; gli estremi della fattura passiva sono registrati anche nel Registro Unico delle Fatture (RUF).

Il sistema provvede a generare pacchetti informativi contenenti una o più fatture, in formato .xml.

Viene schematizzata di seguito la struttura del set di metadati, in maniera normalizzata, da associare al documento, al fine di consentire la creazione del Pacchetto di Versamento, per la corretta conservazione delle fatture in conformità allo standard ISO 14721:2012 - Open Archival Information System (OAIS) e secondo le previsioni del DMEF 17 giugno 2014, in materia di conservazione dei documenti fiscalmente rilevanti, e dal D. Lgs. 66/2014, per quanto attiene alle modalità di registrazione delle fatture passive da parte delle amministrazioni pubbliche:

INDICE	Descrizione	Tipo	Len	Obbl
ID_Documento	Identificativo univoco e persistente è una sequenza di caratteri alfanumerici associata in modo univoco e permanente al documento informatico in modo da consentirne l'identificazione. Dublin Core raccomanda di identificare il documento per mezzo di una sequenza di caratteri alfabetici o numerici secondo un sistema d' identificazione formalmente definito. Esempi di tali sistemi di identificazione includono l'Uniform Resource Identifier (URI), il Digital Object Identifier (DOI) e l'International Standard Book Number (ISBN)	STRINGA	20	SI
Data_Chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immodificabile: data di produzione del Pacchetto di Versamento	DATE		SI
Ente_Denominazione	Denominazione del soggetto produttore	STRINGA		SI
Struttura_Denominazione	AOO (codice identificativo dell'AOO)	STRINGA		SI

Produttore_Nome	Il soggetto che ha l'autorità e la competenza di produrre il PDV (Responsabile della gestione documentale)	STRINGA		SI
Produttore_Cognome		STRINGA		SI
Produttore_CF_codice matricola	Dato che identifica legalmente il Produttore	STRINGA		SI
Mittente_Nome	Dati soggetto trasmittente/creditore (D. Lgs. 66/2014, art. 42)	STRINGA		SI
Mittente_Cognome		STRINGA		SI
Mittente_CF_Piva		STRINGA		SI
Destinatario_Nome	Dati destinatario della fattura	STRINGA		SI
Destinatario_Cognome		STRINGA		SI
Destinatario_CF_Piva		STRINGA		SI
Documento_Tipologia	Tipologia del documento oggetto della trasmissione (es: *Fattura passiva*)	STRINGA		SI
Oggetto_Documento	Es. *Fattura passiva PA, n. [num. emissione], del [data emissione] – destinatario [denominazione destinatario].*	STRINGA	100	SI
Data_Documento	Data fattura	DATE		SI
Numero_Fattura	Numero progressivo della fattura	STRINGA		SI
Numero_Invio_SDI	Numero associato all'invio al Sistema di Interscambio	STRINGA		NO
Importo_Fattura	Importo fattura	STRINGA		NO
Codice CIG (Codice Identificativo di Gara)	Codice da non inserire in caso di esclusione dall'obbligo di tracciabilità di cui alla legge 13 Agosto 2010, n. 136	STRINGA		NO
Codice CUP (Codice Unico di Progetto)	Codice da inserire in caso di fatture relative a opere pubbliche, interventi di manutenzione straordinaria, interventi finanziati da contributi comunitari e ove previsto ai sensi dell'art. 11 della Legge 16 gennaio 2003, n. 3	STRINGA		NO
Allegati_Numero	Quantità di documenti allegati alla fattura	STRINGA		SI
Allegati_Tipologia_Documento	Tipologia di documento allegato	STRINGA		SI
Classifica	Codice di classificazione	STRINGA		SI
ID_Fascicolo	Codice identificativo del fascicolo	STRINGA		SI

	cui il documento appartiene			
Id_Registro	Identificativo del registro: RUF/sezionale/bollato IVA in cui è registrata la fattura	STRINGA		NO
Anno_Registro	Anno del RUF/sezionale/bollato IVA in cui è registrata la fattura (AAAA)	STRINGA		NO
Protocollo_Numero	Estremi della registrazione di protocollo	STRINGA		SI
Tempo_Conservazione	Tempo di conservazione dell'unità documentaria, secondo il Piano di conservazione dell'Ente	STRINGA		SI
Impronta_Documento	Impronta del documento informatico	STRINGA		SI
Chiave_ gestionale	Codice che consente l'associazione logica della documentazione afferente alla stessa pratica	STRINGA		NO

Contratti informatici

Il set di metadati del contratto informatico è definito in conformità a quanto disposto dall'allegato n. 5 alle regole tecniche in materia di formazione, gestione e conservazione dei documenti informatici, emanate ai sensi dell'articolo 71 del Codice dell'Amministrazione Digitale.

Il set tiene conto delle procedure di archiviazione e delle modalità di sedimentazione della documentazione nei relativi fascicoli informatici, gestiti nell'ambito del sistema documentale dell'Ente.

E' schematizzata di seguito la struttura del set di metadati, in maniera normalizzata, da associare al documento, al fine di consentire la creazione del Pacchetto di Versamento:

INDICE	Descrizione	Tipo	Len	Obbl
ID_Documento	Identificativo univoco e persistente è una sequenza di caratteri alfanumerici associata in modo univoco e permanente al documento informatico in modo da consentirne l'identificazione. Dublin Core raccomanda di identificare il documento per mezzo di una sequenza di caratteri alfabetici o numerici secondo un sistema d'identificazione formalmente definito. Esempi di tali sistemi di identificazione includono l'Uniform Resource Identifier (URI), il Digital Object Identifier (DOI) e l'International Standard Book Number (ISBN)	STRINGA	20	SI
Data_Chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immodificabile: data di produzione del Pacchetto di Versamento	DATE		SI
Ente_Denominazione	Denominazione del soggetto produttore	STRINGA		SI
Struttura_Denominazione	AOO (codice identificativo dell'AOO)	STRINGA		SI
Produttore_Nome	Il soggetto che ha l'autorità e la competenza di produrre il PDV (Responsabile della gestione documentale)	STRINGA		SI
Produttore_Cognome		STRINGA		SI

Produttore_CF_codice_matricola	Dato che identifica legalmente il Produttore	STRINGA		SI
Tipologia_Documento	Tipologia del documento (contratto)	STRINGA		SI
Oggetto_Documento	Sintesi del contenuto del contratto	STRINGA	100	SI
Data_ Decorrenza_Contratto	Data di decorrenza del contratto	DATE		NO
Data_ Scadenza_Contratto	Data di scadenza del contratto	DATE		NO
Luogo_stipula_Contratto	Luogo di stipula del contratto	STRINGA		SI
Contraente_Nominativo/ Ragione sociale	Nome e cognome del contraente/ragione sociale del contraente	STRINGA		SI
Contraente_CF/PIVA	Codice fiscale/Partita IVA del contraente	STRINGA		SI
Importo_Contratto	Importo previsto nel contratto	STRINGA		NO
Codice CIG (Codice Identificativo di Gara)	Codice da non inserire in caso di esclusione dall'obbligo di tracciabilità di cui alla legge 13 Agosto 2010, n. 136	STRINGA		NO
Codice CUP (Codice Unico di Progetto)	Codice da inserire in caso di fatture relative a opere pubbliche, interventi di manutenzione straordinaria, interventi finanziati da contributi comunitari e ove previsto ai sensi dell'art. 11 della Legge 16 gennaio 2003, n. 3	STRINGA		NO
Allegati_Numero	Quantità di documenti allegati	STRINGA		SI
Allegati_Tipologia_Documento	Tipologia di documento allegato	STRINGA		SI
Classifica	Codice di classificazione	STRINGA		SI
Fascicolo_ID	Codice identificativo del fascicolo cui il documento appartiene	STRINGA		NO
Fascicolo_titolo	Pratica/affare cui si riferisce	STRINGA		NO
Data_Registrazione_Documento	Data registrazione del contratto nel repertorio	DATE		SI
Numero_Registrazione	Numero (progressivo) di registrazione nel repertorio	STRINGA		SI
ID_ Repertorio	Identificativo del repertorio	STRINGA		NO
Anno_ Repertorio	Anno del repertorio (AAAA)	STRINGA		SI
Protocollo_Numero	Estremi della registrazione di	STRINGA		SI

	protocollo			
Protocollo_Data	Data di registrazione di protocollo	DATE		SI
Tempo_Conservazione	Tempo di conservazione dell'unità documentaria, secondo il Piano di conservazione dell'Ente (es: 10 anni)	STRINGA		SI
Impronta_Documento	Impronta del documento informatico	STRINGA		SI
Chiave_Gestionale	Codice che consente l'associazione logica della documentazione afferente alla stessa pratica	STRINGA		NO

7.5. Allegato 3: Back-up e Disaster Recovery

Back-up

La politica di backup prevede di salvaguardare mediante backup periodico tutti i file indispensabili al ripristino di un sistema. In questa definizione rientrano i file di configurazione individuali dei singoli sistemi e ovviamente i file dati.

In INAIL è stato predisposto un apposito sistema dedicato alla gestione di backup di tutti i sistemi dell'Istituto. Questo sistema gestisce il back-up del Sistema di Conservazione

Il back-up viene eseguito in automatico mediante un sistema centralizzato. I job di backup sono stati schedulati nella seguente modalità:

Schedulazione	Directory	Data retention
Incrementale giornaliero dal lunedì al sabato orario 4:30	/etc	30 gg
	/opt	30 gg
	/BACKUP	30 gg
Full settimanale domenica orario 4:30	/etc	30 gg
	/opt	30 gg
	/BACKUP	30 gg
Incrementale giornaliero dal lunedì al sabato orario 06.00	/data/larchive	90 gg
	/disk01/magazzini/M1	90 gg
Full settimanale domenica orario 06.00	/data/larchive	365 gg
	/disk01/magazzini/M1	365 gg

Per ogni sistema verranno messi sotto backup i dati ritenuti essenziali, come le configurazioni, i dati legati ai servizi e i dati relativi alla sicurezza.

La procedura del backup viene controllata dal gruppo dei sistemisti dell'Area Infrastruttura della DCOD.

Eventuali anomalie che emergono durante le fasi di monitoraggio e verifica avviano la procedura di "Incident Management".

Disaster Recovery

Lo scopo della procedura di Disaster Recovery (DR) è quello di definire la procedura operativa da attuare in caso sia necessario attivare il sito di Disaster Recovery contrattualizzato dall'Istituto e garantire quindi la continuità dell'accesso ai dati conservati.

La procedura di Disaster Recovery viene attivata quando eventi bloccanti impediscono la normale erogazione dei servizi sia dal sito primario INAIL che dal sito secondario dove si trova la replica dei sistemi per la continuità dell'operatività. Eventi che possono richiedere l'attivazione del processo di

DR possono essere:

- Eventi naturali (terremoto, alluvione, eruzione vulcanica, ecc.);
- Incendio nella struttura o nei locali deputati all'erogazione;
- Effrazione nei locali deputati all'erogazione dei servizi con danneggiamento delle apparecchiature;
- Attacco terroristico ad entrambi i siti operativi
- Intrusione informatica;

L'elenco non è esaustivo, e sarà facoltà dell'Istituto valutare se situazioni non contemplate nel presente elenco possano richiedere comunque l'attivazione della procedura.

Il sito di Disaster Recovery si trova c/o Telecom Italia, via Toscana 3/5, Rozzano (Mi).

Sul sito di Disaster Recovery il sistema sarà operativo per il recupero di documenti conservati.