PRODEO S.P.A.

Manuale di Conservazione

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Prima emissione	15/02/2016	PRODEO S.P.A.	
Seconda emissione	11/05/2018	PRODEO S.P.A.	

REGISTRO DELLE VERSIONI

N° Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
1.0	15/02/2016		
2.0	10/05/2016	Ruoli e Responsabilità	
3.0	27/05/2016	Struttura organizzativa	
4.0	15/07/2016	Integrazioni e modifiche per AGID	
5.0	26/09/2016	Integrazioni e modifiche per AGID	
6.0	11/05/2018	Aggiornamento processo di conservazione	

SOMMARIO

1. Scopo e ambito del documento

Il presente documento costituisce il manuale di conservazione di Pròdeo S.p.A. e ha lo scopo di descrivere il sistema di conservazione dei documenti informatici adottato dall'azienda. In particolare il presente manuale descrive il modello organizzativo della conservazione adottato, illustra nel dettaglio l'organizzazione della struttura che realizza il processo di conservazione, definendo i soggetti coinvolti e i ruoli svolti dagli stessi nel modello organizzativo di funzionamento dell'attività di conservazione e descrive inoltre il processo, le architetture e le 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 software utilizzato per la gestione del processo di conservazione dei documenti informatici è JSDC®. Il sistema di conservazione ha come oggetto la realizzazione di un insieme di funzionalità atte a consentire la conservazione dei documenti informatici e a fornire un supporto alle figure coinvolte nel processo di conservazione.

Il presente manuale è così localizzato:

- una copia del manuale della conservazione è archiviata presso il soggetto produttore;
- una copia del manuale della conservazione sarà inviata, se necessario, in occasione dell'acquisizione delle commesse al soggetto conservatore;
- una copia del manuale della conservazione sarà inviata in occasione dell'acquisizione delle commesse al titolare.

Dati identificativi del soggetto conservatore:

Denominazione	Pròdeo S.p.A.
Indirizzo	Viale Francesco De Blasio, 23
Legale Rappresentante	Dott. Domenico Marzocca
Referente tecnico (nome e cognome) cui rivolgersi in caso di problemi tecnico-operativi	Sig. Arcangelo Rana
E-mail del referente tecnico	a.rana@prodeo.it
N° telefono/fax	080/5870011
Sito web istituzionale	**www.prodeo.it**
E-mail istituzionale	prodeo@prodeo.it

Contesto di riferimento
Con il DPCM del 3 dicembre 2013 (G.U. n. 59 del 12 marzo 2014 – S.O. 20) sono state emanate le regole tecniche in materia di sistema di conservazione dei documenti informatici, ai sensi degli artt. 20, commi 3 e 5 bis, 23 ter, comma 4, 43, commi 1 e 3, 44, 44 bis e 71, comma 1 del CAD, in vigore dall'11 aprile 2014 (art. 14 comma 1).
Il manuale di conservazione secondo l'art. 8 DPCM 3 dicembre 2013 ha lo scopo di descrivere:

- l'organizzazione della struttura che realizza il processo di conservazione, definendo i soggetti coinvolti e i ruoli svolti dagli stessi;
- il modello di funzionamento, la descrizione delle architetture e delle infrastrutture utilizzate;
- le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.

In merito alle tipologie degli oggetti digitali sottoposti a conservazione e i rapporti con i soggetti titolari, il presente manuale dev'essere integrato sulla base delle specifiche tecniche definite dal Titolare e dal Produttore; tale documento sarà parte integrante del contratto di affidamento del servizio di conservazione, redatto per ogni soggetto titolare, in cui si definiscono le specifiche operative e le modalità di versamento nel sistema di conservazione digitale delle tipologie documentarie e delle aggregazioni documentali informatiche oggetto di conservazione.

Il presente manuale di conservazione è un documento informatico.

Torna al sommario

2. Terminologia (Glossario, Acronimi)

Le definizioni afferenti al processo di conservazione sono presenti nell'allegato 1 delle regole tecniche (DPCM 3 Dicembre 2013).

Indichiamo di seguito il *glossario* dei termini utilizzati nel presente documento:

Glossario dei termini	
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 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 che compone l'unità documentaria per integrare le informazioni contenute nel documento principale. È redatto contestualmente o precedentemente al documento principale. La sua presenza è facoltativa.
Annesso	Documento che compone l'unità documentaria, generalmente prodotto e inserito nell' unità documentaria in un momento successivo a quello di creazione dell'unità documentaria, per fornire ulteriori notizie e informazioni a corredo del documento principale.
Application server	Tipologia di server che fornisce l'infrastruttura e le funzionalità di supporto, sviluppo ed esecuzione di applicazioni nonché altri componenti server in un contesto distribuito. Si tratta di un complesso di servizi orientati alla realizzazione di applicazioni ad architettura multilivello ed *enterprise*, con alto grado di complessità, spesso orientate per il web (applicazioni web).
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 da aggregazioni documentali informatiche gestiti e conservati in ambiente informatico.
Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.
Autenticità	Caratteristica 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.
Cluster	Insieme di dispositivi di elaborazione connessi in maniera più o meno stretta, che operano insieme in modo tale da poter essere considerati un unico sistema.
Codice	Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni.
Codice eseguibile	Insieme di istruzione o comandi software direttamente elaborabili da sistemi informatici
Comunità di riferimento	Un gruppo ben individuato di potenziali utenti che dovrebbero essere in grado di comprendere un particolare insieme di informazioni. La comunità di riferimento può essere composta da più comunità di Utenti. [da OAIS]
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
Contenuto informativo	Insieme delle informazioni che costituisce l'obiettivo originario della conservazione. È composto dall'oggetto-dati e dalle informazioni di rappresentazione. [da OAIS]
Coordinatore della gestione documentale	Responsabile della definizione di criteri uniformi di classificazione d archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall' art. 50 c.4 DPR 445/00 nei casi di amministrazioni che abbiano istituito più aree organizzative omogenee.
Copia analogica di documento informatico	Documento analogico avente contenuto identico a quello del documento informatico da cui è tratto.
Copia di sicurezza	Copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell' art.12 del DPCM 3 dicembre 2013 riguardo il sistema di conservazione
Destinatario	Identifica il soggetto/sistema al quale il documento informatico è indirizzato
Duplicazione dei documenti informatici	Produzione di duplicati informatici
Data center	Struttura utilizzata per ospitare computer e componenti associati quali dispositivi di telecomunicazioni e di *storage*, in generale con adeguati livelli di

	prestazioni e di sicurezza.
Disaster recovery	Insieme delle misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi di business per imprese, associazioni o enti, a fronte di gravi emergenze che ne intacchino la regolare attività.
Esibizione	Operazione che consente di visualizzare un documento conservato e di ottenerne copia.
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.
File di indice	Indice dell'AIP, file XML che contiene tutti gli elementi del pacchetto di archiviazione, derivati sia dalle informazioni contenute nel SIP (o nei SIP) trasmessi dal produttore, sia da quelle generate dal sistema di conservazione nel corso del processo di conservazione.
Formato	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
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 un documento informatico	Formazione di documenti informatici effettuata direttamente del 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.
Insieme minimo di metadati del documento informatico	Complesso dei metadati, la cui struttura è descritta nell'allegato 5 del presente decreto, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta
Informazioni descrittive	Descrivono il pacchetto informativo e consentono di ricercarlo nel sistema di conservazione. In base alle caratteristiche della tipologia di oggetto contenuto nel pacchetto, tali informazioni possono essere un sottoinsieme di quelle presenti nel pacchetto informativo, possono coincidere o possono anche essere diverse.
Informazioni sulla conservazione (PDI)	Informazioni necessarie a conservare il contenuto informativo e garantiscono che lo stesso sia chiaramente identificato e che sia chiarito il contesto in cui è stato creato. Sono costituite da metadati che definiscono la provenienza, il contesto, l'identificazione e l'integrità del contenuto informativo oggetto della conservazione. [da OAIS]

Informazioni sulla rappresentazione	Informazioni che associano un oggetto-dati a concetti più significativi.
Informazioni sull' impacchettamento	Informazioni che consentono di mettere in relazione nel sistema di conservazione, in modo stabile e persistente, il contenuto informativo con le relative informazioni sulla conservazione.
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 dell'articolo 9 delle regole tecniche riguardo il sistema di conservazione.
Manuale della gestione	Strumento che descrive il Sistema di Gestione Informatica dei documenti di cui all'art. 5 delle Regole Tecniche del Protocollo Informatico ai sensi del DPCM 31 ottobre 2000 e successive modificazioni e integrazioni.
Marca temporale	Sequenza di caratteri che rappresentano una data e/o un orario per accertare l'effettivo avvenimento di un certo evento. La data è di solito presentata in un formato compatibile, in modo che sia facile da comparare con un'altra per stabilirne l'ordine temporale. La pratica dell'applicazione di tale marca temporale è detto timestamping.
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 DPCM 3 dicembre 2013.
Pacchetto di archiviazione	Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di 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 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.
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 sistema di conservazione.
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.
Registro di protocollo	Registro informatico di atti o 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 Amministrazione è previsto ai sensi dell'art. 53, comma 5, del DPR 28 dicembre 2000, n° 445.
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 8, 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.
Serie	Unità archivistiche o unità documentarie ordinate secondo un sistema di classificazione o conservati insieme perché: - sono il risultato di un medesimo processo di sedimentazione o archiviazione o di una medesima attività; - appartengono ad una specifica tipologia documentaria; - a ragione di qualche altra relazione derivante dalle modalità della loro produzione, acquisizione o uso. (fonte: ISAD)
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.
Soggetto produttore	La persona fisica o giuridica, la Pubblica Amministrazione o l'Ente, titolare dei documenti informatici da conservare
Testo unico	Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni.
Unità di descrizione	Insieme organizzato di unità documentarie o documenti raggruppati dal produttore per le esigenze della sua attività corrente in base al comune riferimento allo stesso oggetto, attività o fatto giuridico. Può rappresentare un'unità elementare di una serie. Un documento o un insieme di documenti, a prescindere dai loro caratteri fisici, considerati come un tutto unico e, come tali, costituenti l'oggetto di una singola descrizione [da ISAD]
Unità documentaria	Unità minima, concettualmente non divisibile, di cui è composto un archivio, per esempio, una lettera, un memorandum, un rapporto, una fotografia, una registrazione sonora. (ISAD (G)
Versamento	Azione di trasferimento di SIP dal produttore al sistema di conservazione.
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.
Utente	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.

Torna al sommario

Indichiamo di seguito gli *acronimi* dei termini utilizzati nel presente documento:

- **AgID**: Agenzia per l'Italia Digitale.
- **AIP**: Archival Information package (Pacchetto di archiviazione).
- **CA**: Certification Autorithy.
- **CAD**: Codice dell'amministrazione digitale.
- **CRL**: Certificate Revocation List, è la lista dei certificati revocati o sospesi, ovvero lista di certificati che sono stati resi non validi prima della loro naturale scadenza.
- **DIP**: Dissemination Information Package (Pacchetto di distribuzione).
- **HSM**: Hardware Security Module, è l'insieme di hardware e software che realizza dispositivi sicuri per la generazione delle firme in grado di gestire in modo sicuro una o più coppie di chiavi crittografiche.
- **IdC**: Indice di conservazione realizzato secondo le specifiche dello standard UNI SinCRO.
- **IR**: Informazioni sulla rappresentazione.
- **IRse**: Informazioni sulla rappresentazione semantiche.
- **IRsi**: Informazioni sulla rappresentazione sintattiche.
- **ISO**: International Organization for Standardization.
- **OAIS**: Open archival information system.
- **PDA**: Pacchetto di archiviazione
- **PDD**: Pacchetto di Distribuzione

- **PDI**: Preservation description information (informazioni sulla conservazione).
- **PDV**: Pacchetto di Versamento
- **PEC**: Posta Elettronica Certificata.
- **SIP**: Submission Information Package (Pacchetto di versamento).
- **SMTP**: Simple Mail Transfer Protocol (SMTP) è il protocollo standard per la trasmissione via internet di e-mail.
- **SNMP**: Simple Network Management Protocol.
- **SP**: Soggetto produttore.
- **TSA**: Time Stamping Autorithy, è il soggetto che eroga la marca temporale.
- **UNI SinCRO**: UNI 11386:2010 - Supporto all'Interoperabilità nella conservazione e nel Recupero degli oggetti digitali.
- **VdC**: Volume di conservazione.

Torna al sommario

3. Normativa e standard di riferimento

3.1. Normativa di riferimento

Il presente elenco riporta la normativa nazionale italiana di riferimento in ambito di conservazione dei documenti informatici.

- **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, art. 2215 bis) -** Documentazione informatica;
- **Legge n. 241 del 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 legislativo 30 giugno 2003, n. 196**
  "Codice in materia di protezione dei dati personali";
- **Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445**
  "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa";
- **Decreto Ministero Economia e Finanze 17.06.2014**
  "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 Ministero Economia e Finanze del 3 aprile 2013, n. 55**
  "Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'art. 1, commi da 209 a 213, della legge 24 dicembre 2007. Pubblicato in G.U. n. 118 del 22 maggio 2013";
- **Decreto legislativo 22 gennaio 2004, n. 42, e successive modificazioni**
  "Codice dei beni culturali e del paesaggio";
- **D. Lgs. 7 marzo 2005, n. 82, e s.m.i.**
  "Codice dell'Amministrazione digitale (CAD)";
- **Deliberazione Cnipa 21 Maggio 2009, n. 45**
  "Regole per il riconoscimento e la verifica del documento informatico";
- **DPCM 22 Febbraio 2013**
  "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali";
- **Circolare AGID del 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";
- **DPCM 3 dicembre 2013**
  "Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, comma 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".

Torna al sommario

3.2. Standard di riferimento

Così come richiesto dal DPCM 3 dicembre 2013 e, nello specifico dall'allegato 3, di seguito si riportano gli standard per la conservazione dei documenti informatici:

- **ISO 14721:2012 OAIS** (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- **ISO/IEC 27001:2014**, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- **ETSI TS 101 533-1 V1.3.1 (2012-04)** Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- **ETSI TR 101 533-2 V1.3.1 (2012-04)**Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- **UNI 11386:2010 Standard SInCRO** - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- **ISO 15836:2009** Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

Torna al sommario

4. Ruoli e responsabilità

Si elencano in questo capitolo le figure professionali che compongono il gruppo di lavoro del servizio di conservazione dei documenti del conservatore, al fine di garantire la corretta esecuzione del servizio.
Le procedure organizzative si basano su standard mandatori ISO 27001 e ISO 9001.

Responsabile del servizio di conservazione (RSC):
Il responsabile del servizio di conservazione è Caterina Bitetti

Cronologia dei responsabili del servizio di conservazione: **non ci sono precedenti responsabile del servizio di conservazione**

Responsabile della funzione archivistica di conservazione (RFA):
Il responsabile della funzione archivistica di conservazione è Caterina Bitetti. La nomina è stata formalizzata in data 21/03/2016 e decorre dallo stesso giorno. La nomina è stata firmata per accettazione dal responsabile designato.

Responsabile della sicurezza dei sistemi per la conservazione (RSS):
Il responsabile della sicurezza dei sistemi per la conservazione è Arcangelo Rana. La nomina è stata formalizzata in data 21/03/2016 e decorre dallo stesso giorno. La nomina è stata firmata per accettazione dal responsabile designato.

Responsabile dei sistemi informativi per la conservazione (RSI):
Il responsabile dei sistemi informativi per la conservazione è Luigi Cangellario. La nomina è stata formalizzata in data 21/03/2016 e decorre dallo stesso giorno. La nomina è stata firmata per accettazione dal responsabile designato.

Responsabile dello sviluppo e della manutenzione del sistema di conservazione (RSM):
Il responsabile dello sviluppo e della manutenzione del sistema di conservazione è Luigi Cangellario. La nomina è stata formalizzata in data 21/03/2016 e decorre dallo stesso giorno. La nomina è stata firmata per accettazione dal responsabile designato.

Responsabile e incaricati al trattamento dei dati
Il conservatore quando eroga servizi di conservazione, così come stabilito all'art. 6 comma 8 del DPCM 3 dicembre 2013, assume il ruolo di responsabile del trattamento dei dati. Ogni collaboratore del conservatore, incaricato al trattamento è nominato per iscritto. Il responsabile per il trattamento dei dati è individuato in Luigi Angelo Marzocca. La nomina è stata formalizzata in data 14/03/2016 e decorre dallo stesso giorno.

La nomina è stata firmata per accettazione dal responsabile designato.

Torna al sommario

5. Struttura organizzativa per il servizio di conservazione

Nella seguente tabella sono indicati i ruoli e le diverse attività svolte dai diversi soggetti incaricati nell'ambito del servizio di conservazione dei documenti informatici.

Responsabile del servizio di conservazione	**Responsabile dello sviluppo e della manutenzione del sistema di conservazione**	**Responsabile della sicurezza dei sistemi per la conservazione**	**Responsabile dei sistemi informativi**	**Responsabile del trattamento dei dati personali**	**Responsabile della funzione archivistica di conservazione**
Definizione e attuazione delle politiche complessive e del Sistema di conservazione, nonché del governo della gestione del sistema di conservazione.	Monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione.	Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza.	Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione.	Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali.	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 delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente.	Pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione.	Segnalazione delle eventuali difformità al responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.	Monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore.	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 riservatezza.	Definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici.
Corretta erogazione del servizio di conservazione all'ente produttore.	Coordinamento dello sviluppo e manutenzione delle componenti software del sistema di conservazione.		Segnalazione delle eventuali difformità degli SLA al responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.		Monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione.
Gestione delle convenzioni, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti e le modalità di erogazione dei servizi di conservazione.	Interfaccia con l'ente produttore relativamente alle modalità di trasferimento dei documenti e dei fascicoli informatici in merito ai formati elettronici da usare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche.		Pianificazione dello sviluppo delle infrastrutture tecnologiche 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.
	Gestione dello		Controllo e verifica		Monitoraggio del

	sviluppo di siti web e portali connessi al servizio di conservazione.		dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al responsabile del servizio di conservazione.		processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione.
					Redazione e supervisione del Manuale di conservazione con i responsabili del servizio.

Torna al sommario

5.1. Organigramma

Si riporta di seguito l'organigramma della struttura coinvolta nel servizio di conservazione della Pròdeo S.p.A.

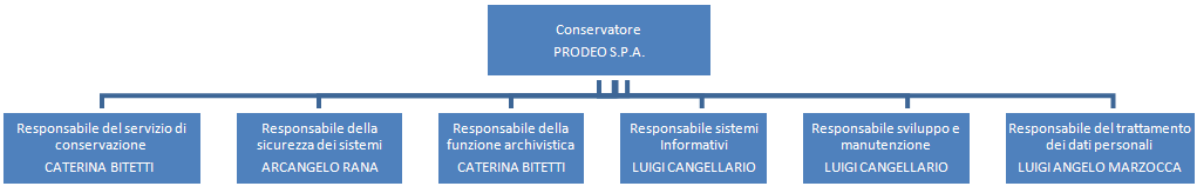


Figura 1 - Organigramma Pròdeo S.p.A.

Torna al sommario

5.2. Strutture organizzative

Pròdeo S.p.A. eroga servizi di conservazione utilizzando soluzioni tecnologiche che soddisfano i requisiti di alta affidabilità, richiesti dalla normativa. Il modello organizzativo adottato dal soggetto conservatore è idoneo a gestire il servizio di conservazione in base a quanto stabilito dalle vigenti regole tecniche, DPCM 3 Dicembre 2013 all'art. 5 comma 2 lettera b). Il sistema di conservazione opera secondo modelli organizzativi esplicitamente definiti che garantiscano la sua distinzione logica dal sistema di gestione documentale, se esistente. Il modello organizzativo del soggetto conservatore è stato realizzato tenendo conto del modello di riferimento OAIS (Open Archival Information System certificato standard ISO 14721 nel 2003 e recentemente aggiornato in ISO 14721:2012), ovvero una struttura organizzata di persone e sistemi, che accetti la responsabilità di conservare l'informazione e di renderla disponibile per una comunità di riferimento.

Seguendo quanto indicato dalle regole tecniche vigenti e, sulla base dello stesso modello di riferimento OAIS, il sistema identifica i seguenti ruoli fondamentali: produttore, utente, responsabile della conservazione.

Produttore: è la 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 il responsabile della gestione documentale.
Il produttore si impegna a depositare i documenti informatici e le loro aggregazioni documentali informatiche nei modi e nelle forme definite, garantendone l'autenticità e l'integrità nelle fasi di formazione e di archiviazione, effettuata nel rispetto delle norme sulla formazione e sui sistemi di gestione dei documenti informatici. In particolare, garantisce che il trasferimento dei documenti informatici venga

realizzato utilizzando formati compatibili con la funzione di conservazione e rispondenti a quanto previsto dalla normativa vigente. Si impegna, inoltre, a depositare e mantenere aggiornati gli strumenti di ricerca e gestione archivistica elaborati a supporto della formazione dei documenti informatici e della tenuta degli archivi digitali. Il Titolare mantiene la proprietà dei documenti depositati.
I rapporti con il Titolare sono concordati mediante un accordo formale (**specifiche tecniche** allegate al **contratto di affidamento**) che stabilisca le **tipologie documentarie**, i **metadati** oggetto di conservazione, i **formati** e le **modalità** operative **di versamento**.
Nelle pubbliche amministrazioni, il ruolo di responsabile della conservazione può essere svolto dal responsabile della gestione documentale ovvero dal coordinatore della gestione documentale, ove nominato. Il produttore è responsabile del contenuto del pacchetto di versamento (d'ora in poi SIP) ed è tenuto a trasmetterlo al soggetto conservatore, secondo quanto indicato nelle specifiche tecniche allegate al contratto di affidamento.
Il produttore e il titolare hanno accesso al sistema di conservazione direttamente dalla propria sede, tramite accesso anche da remoto. Il produttore, secondo quanto previsto nel contratto di affidamento del servizio di conservazione, si impegna a depositare i documenti informatici e le loro aggregazioni nei modi e nelle forme definite nelle specifiche tecniche, garantendone l'autenticità e l'integrità nelle fasi di produzione e di archiviazione. In particolare, garantisce che il trasferimento dei documenti informatici venga realizzato utilizzando formati compatibili con la funzione di conservazione e rispondenti a quanto previsto dalla normativa vigente. Il Titolare mantiene la proprietà dei documenti depositati.

Utente: è una persona, ente o sistema che interagisce con i servizi di un sistema per la conservazione di documenti informatici, come indicato nelle vigenti regole tecniche (DPCM 3 dicembre 2013, allegato 1, Glossario).
L'utente richiede al sistema di conservazione l'accesso ai documenti informatici per acquisire le informazioni di interesse nei limiti previsti dalla legge. Il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, ai documenti informatici conservati e consente la produzione di un pacchetto di distribuzione direttamente acquisibile dai soggetti autorizzati. In termini del modello di riferimento OAIS la comunità degli utenti può essere definita come comunità di riferimento.
Nelle specifiche tecniche, documento allegato al contratto di affidamento del servizio di conservazione, vengono indicati quei soggetti abilitati dal soggetto produttore che possono accedere ai documenti versati dal produttore al conservatore. L'abilitazione e l'autenticazione degli utenti avviene in base alle procedure di gestione utenze indicate nel piano della sicurezza del sistema di conservazione e nel rispetto delle misure di sicurezza previste negli articoli da 31 a 36 del Dlgs 30 giugno 2003, n. 196, in particolare di quelle indicate all'art. 34 comma 1 e dal disciplinare tecnico di cui all'allegato B del medesimo decreto.

Responsabile del servizio di conservazione: è la persona fisica nell'organizzazione del conservatore che svolge le attività di conservazione, tramite il servizio di conservazione, così come stabilito nel contratto di affidamento del servizio. Le responsabilità del responsabile del servizio di conservazione sono definite all'art. 7 del DPCM 3 dicembre 2013. Nel contratto di affidamento del servizio di conservazione, sottoscritto tra il soggetto produttore e il soggetto conservatore vengono definite le attività e le responsabilità affidate al conservatore e quelle che rimangono a carico del produttore.

Organismo di tutela e vigilanza (in riferimento alle amministrazioni pubbliche): è il Ministero per i beni e le attività culturali e del turismo (MiBACT) che esercita funzioni di tutela e vigilanza dei sistemi di conservazione degli archivi di enti pubblici o di enti privati dichiarati di interesse storico particolarmente importante e autorizza le operazioni di scarto e trasferimento della documentazione conservata ai sensi del Dlgs. 42/2004.
La tutela e vigilanza sugli archivi di enti pubblici non statali è esercitata dal MiBACT, tramite le soprintendenze archivistiche competenti per territorio.
"Lo spostamento, anche temporaneo dei beni culturali mobili" compresi gli archivi storici e di deposito è soggetto ad autorizzazione della soprintendenza archivistica (Dlgs. 22 gen. 2004, n. 42, art. 21, c. 1, lettera b).
Anche "il trasferimento ad altre persone giuridiche di complessi organici di documentazione di archivi pubblici, nonché di archivi di privati per i quali sia intervenuta la dichiarazione ai sensi dell'articolo 13", sia

che comporti o non comporti uno spostamento, rientra tra gli interventi soggetti ad autorizzazione della Soprintendenza archivistica (Dlgs. 22 gen. 2004, n. 42, art.21, c. 1, lettera e).
La disposizione si applica anche:

- all'affidamento a terzi dell'archivio (outsourcing), ai sensi del Dlgs. 22 gen. 2004, n. 42, art.21, c. 1, lettera e)
- al trasferimento di archivi informatici ad altri soggetti giuridici, nell'ottica della conservazione permanente sia del documento sia del contesto archivistico.

La soprintendenza può, in seguito a preavviso, effettuare ispezioni per accertare lo stato di conservazione e custodia degli Archivi e può emettere prescrizioni per la tutela degli Archivi.
In base alle regole tecniche i sistemi di conservazione delle amministrazioni pubbliche e i sistemi di conservazione dei conservatori accreditati sono soggetti anche alla vigilanza di AgID.

Torna al sommario

6. Oggetti digitali sottoposti a conservazione

La rappresentazione degli oggetti sottoposti conservazione è parte integrante delle specifiche tecniche (allegato al contratto di affidamento del servizio di conservazione).

Torna al sommario

6.1. Oggetti conservati

Il SdC acquisisce pacchetti informativi trasformandoli in PdA e conservandoli in linea con i requisiti della normativa.
Un pacchetto informativo può contenere qualsiasi tipologia di documento informatico, nonché una o più aggregazioni documentali informatiche. Di seguito si descrivono le principali aggregazioni gestite:

Tipologia documentale	Descrizione
Fatture elettroniche (in formato XML FatturaPA)	Fatture commerciali emesse e/o ricevute dalle Amministrazioni Pubbliche in formato FatturaPA.
Fatture clienti	Fatture commerciali attive (elettroniche ed analogiche) emesse da organizzazioni private e pubbliche fruitrici del servizio di conservazione.
Fatture fornitori	Fatture commerciali passive (elettroniche ed analogiche) ricevute da organizzazioni private e pubbliche fruitrici del servizio di conservazione.
Documenti di trasporto	Documenti emessi per giustificare il trasferimento di un materiale da cedente a cessionario attraverso il trasporto dello stesso, in base a quanto sancito dal Testo del D.P.R. 14 agosto 1996 n. 472. ("Regolamento di attuazione delle disposizioni contenute nell'art. 3, comma 147, lettera d), della legge 28 dicembre 1995, n. 549, relativamente alla soppressione dell'obbligo della bolla di accompagnamento delle merci viaggianti").
Libri contabili	Libri, registri, documenti e altre scritture contabili obbligatorie e/o richieste dalla natura e dalle dimensioni dell'impresa, quali (a titolo esemplificativo): libro giornale, libro inventari, piano dei conti, libro mastro, libro magazzino, registri iva, ecc.
Documenti di protocollo	Documenti afferenti al sistema di gestione del protocollo informatico nella Pubblica Amministrazione quali (a titolo esemplificativo): mail PEC, registro di protocollo.
Atti amministrativi	Documenti formati dalla Pubblica Amministrazione nella gestione ordinaria della sua attività istituzionale, quali (a titolo esemplificativo): delibere di giunta, delibere di consiglio, determine, ordinanze, albo pretorio, contratti, ecc.
Mandati di pagamento e reversali informatici	Documenti di interscambio tra la Pubblica Amministrazione e l'Istituto Bancario gestore del Servizio di Tesoreria.

I metadati di ogni tipologia documentale sono definiti in modo parametrico attraverso il SdC per ogni singolo produttore e formalizzati nel Contratto di Servizio. Nella definizione dei metadati dei documenti aventi rilevanza fiscale si fa riferimento all'art. 3 del DMEF 17 giugno 2014.
Il set di metadati minimi associati ai documenti informatici è allineato con quanto definito dall'allegato 5 del DPCM.

Il SdC, in linea con quanto indicato nell'allegato 2 del DPCM, gestisce i documenti informatici mediante diversi formati di file tra i quali si indicano, di seguito, i principali:

Formato del file	Visualizzatore	Standard	Versione del formato	Sistema Operativo
PDF - PDF/A	Adobe Reader	ISO 32000-1 ISO 19005-1:2005 ISO 19005-1:2011	1.4 -1.7	Qualsiasi
XML	Browser internet o text editor	ISO 26300:2006	ND	Qualsiasi
EML	MS Outlook o Mozilla Thunderbird	RFC 5322	ND	Qualsiasi
Documento con firma digitale	Dike, ArubaSign.	CADES, XADES, PADES	ND	Qualsiasi

Torna al sommario

6.2. Pacchetto di Versamento (PdV)

Il PdV è il pacchetto informativo, inviato dal produttore al SdC, il cui formato e contenuto sono concordati con il soggetto produttore.

I PdV contengono insiemi informativi da sottoporre a conservazione e sono generati tramite:

- appositi web service che consentono l'inserimento nel SdC;
- trasmissione telematica tramite canale sicuro;
- interfaccia web-based e mediante una azione di "upload" dei documenti informatici;
- altri software sviluppati da partner.

Il PdV, eventualmente integrato da ulteriori informazioni concordate con il produttore, viene trasferito dal produttore al soggetto conservatore tramite una apposita procedura informatica automatizzata che consente l'identificazione certa del soggetto, dell'ente o dell'amministrazione che ha formato e trasmesso il documento.

Le informazioni relative alle diverse tipologie di pacchetti di versamento trattati, sono descritte nel contratto di servizio e sono concordate specificamente con ciascun soggetto produttore.
A titolo di esempio riportiamo, di seguito, un tracciato XML di un PdV.

```
<?xml version="1.0" encoding="utf-8"?>
<IdC xmlns:xsi=”http://www.w3.org/2001/XMLSchema-instance”
xmlns:xsd=”http://www.w3.org/2001/XMLSchema”  p3:version=”-“ p3:url=”“ p3:schemaLocation="-"
xmlns:p3=”http://www.uni.com/U3011/sincro/” xmlns="http://www.uni.com/U3011/sincro/">
    <p3:SelfDescription>
        <p3:ID p3:scheme="local">d170cb44-62b3-4084-87b2-d63642202588</p3:ID>
        <p3:CreatingApplication>
            <p3:Name>JDoc</p3:Name>
            <p3:Version>6.0.0.0</p3:Version>
            <p3:Producer>prodeo s.r.l.</p3:Producer>
        </p3:CreatingApplication>
    </p3:SelfDescription>
    <p3:VdC>
        <p3:ID p3:scheme="local">36cfc425-d08e-4fc9-8bdc-5b3811c3de71</p3:ID>
    </p3:VdC>
    <p3:FileGroup>
        <p3:File p3:encoding="binary" p3:extension="p7m" p3:format="application/p7m">
            <p3:ID p3:scheme="local">210b033f-e467-4289-8055-77f94a7c29a2</p3:ID>
            <p3:Path>./File/210b033f-e467-4289-8055-77f94a7c29a2.p7m</p3:Path>
            <p3:Hash p3:function="SHA256">
                4826a0a7634c2b96b4cfb1d6e1fc1aef21394791f46338d16d356aa1a9b410a
            </p3:Hash>
            <p3:MoreInfo p3:XMLScheme="">
                <p3:ExternalMetadata p3:format="application/xml" p3:encoding="binary">
                    <p3:ID p3:scheme="local">0d3c702d-9e25-4b87-a7ce-b87f413b29d4</p3:ID>
                    <p3:Path>./Meta/0d3c702d-9e25-4b87-a7ce-b87f413b29d4.xml</p3:Path>
                    <p3:Hash p3:function="SHA256">
                        48b849509eb8994cee42a233bf19063ecfec6a88b11c91517ff8d86663ba3809
                    </p3:Hash>
                </p3:ExternalMetadata>
            </p3:MoreInfo>
        </p3:File>
        <p3:File p3:encoding="binary" p3:extension="p7m" p3:format="application/p7m">
            <p3:ID p3:scheme="local">d001c351-b862-440e-a5dc-490574244c98</p3:ID>
            <p3:Path>./File/d001c351-b862-440e-a5dc-490574244c98.p7m</p3:Path>
            <p3:Hash p3:function="SHA-256">
                69eb58664b83234a804d231a117629673bbeb0b3f767e9b03897d1459e7fc758
            </p3:Hash>
            <p3:MoreInfo p3:XMLScheme="">
                <p3:ExternalMetadata p3:format="application/xml" p3:encoding="binary">
                    <p3:ID p3:scheme="local">a477ebf5-df4f-4df9-adbc-f85fc1b5e114</p3:ID>
                    <p3:Path>./Meta/a477ebf5-df4f-4df9-adbc-f85fc1b5e114.xml</p3:Path>
                    <p3:Hash p3:function="SHA-256">
                        e3ee0413622956a9ccdeb9ef3e8edfc90808a4d2cae1d09e4a4de66f503c0a7d
                    </p3:Hash>
                </p3:ExternalMetadata>
            </p3:MoreInfo>
        </p3:File>
        <p3:File p3:encoding="binary" p3:extension="p7m" p3:format="application/p7m">
```

```
            <p3:ID p3:scheme="local">a50e8671-fa15-47b6-b1d1-97a34a8a8316</p3:ID>
            <p3:Path>./File/a50e8671-fa15-47b6-b1d1-97a34a8a8316.p7m</p3:Path>
            <p3:Hash p3:function="SHA-256">
                c2b1e05b9f7999fb00060cfe5adb371ec8844b65b923253834fbb040418f4203
            </p3:Hash>
            <p3:MoreInfo p3:XMLScheme="">
                <p3:ExternalMetadata p3:format="application/xml" p3:encoding="binary">
                    <p3:ID p3:scheme="local">1b32e85b-58e2-432d-bd06-5cda0b64e0a7</p3:ID>
                    <p3:Path>./Meta/1b32e85b-58e2-432d-bd06-5cda0b64e0a7.xml</p3:Path>
                    <p3:Hash p3:function="SHA-256">
                        b16495efe3ad36832146bd18179d036d6129830c2988e78367e035c50ed26863
                    </p3:Hash>
                </p3:ExternalMetadata>
            </p3:MoreInfo>
        </p3:File>
    </p3:FileGroup>
    <p3:Process>
        <p3:Agent p3:type="organization" p3:role="OtherRole" p3:otherRole="Producer">
            <p3:AgentName>
                <p3:FormalName>ESEMPIO S.p.A.</p3:FormalName>
            </p3:AgentName>
            <p3:Agent_ID p3:scheme="VATRegistrationNumber">12345678910</p3:Agent_ID>
        </p3:Agent>
        <p3:TimeReference>
            <p3:AttachedTimeStamp>2015-06-03T14:04:01.444+02:00</p3:AttachedTimeStamp>
        </p3:TimeReference>
    </p3:Process>
</IdC>
```

Torna al sommario

6.3. Pacchetto di Archiviazione (PdA)

Il PdA viene formato secondo le regole tecniche definite nella norma UNI 11386:2010 Standard SInCRO (Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti Digitali).
Le informazioni più rilevanti che il sistema di conservazione gestisce, in relazione ad ogni PdA prodotto, sono:

- Informazioni relative al soggetto produttore (Codice anagrafico, Ragione Sociale, Codice Fiscale, Partita IVA, ...);
- Identificativo univoco dell'IPdA generato automaticamente dal SdC;
- Informazioni sull'applicazione che ha generato il PdA (produttore del software, nome e versione);
- Informazioni sui PdA contenuti nell'indice;
- Informazioni sui documenti (ID, Impronta di hash, formato, percorso);
- Informazioni relative al processo di conservazione (elementi identificativi del RSC);
- Informazioni relative alla data di produzione del pacchetto stesso (marca temporale);
- Informazioni relative alla firma digitale.
- Informazioni relative ai metadati dei documenti previste negli accordi specifici del Contratto del Servizio;
- Informazioni necessarie per il controllo ed il log delle operazioni relative al pacchetto stesso.

La norma definisce il contenuto del PdA in base alla tassonomia specificamente determinata dal DPCM e schematizzata come segue:

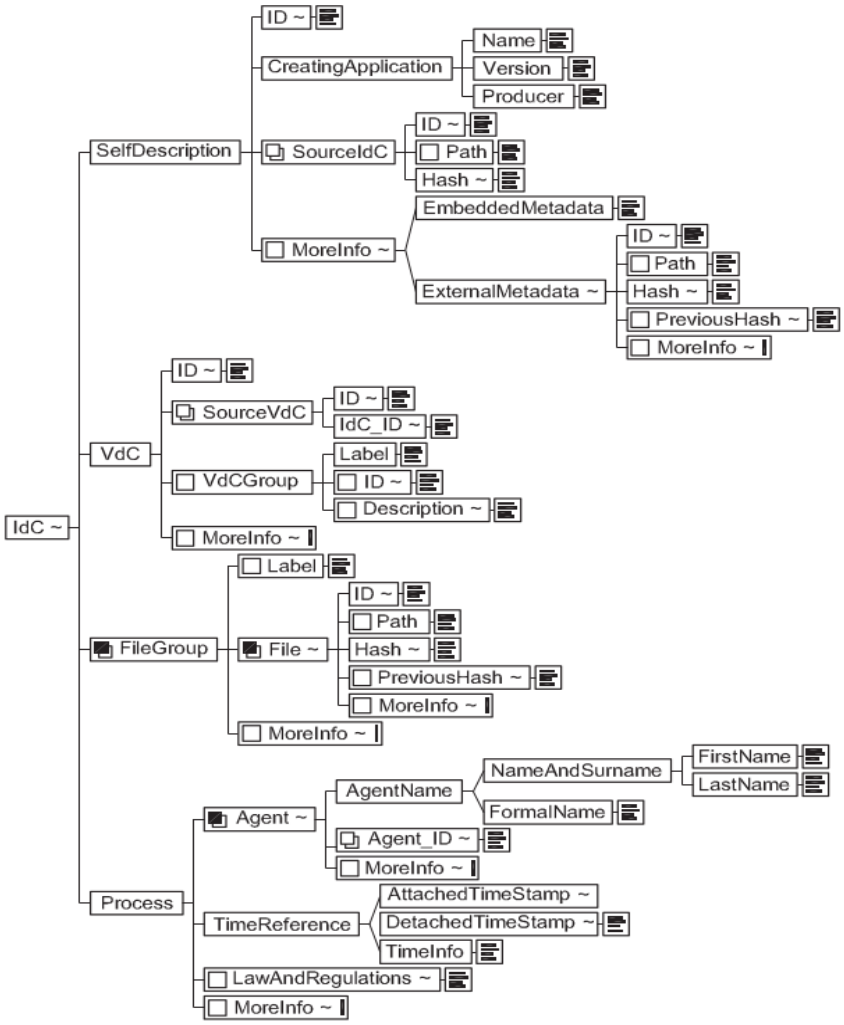


Figura 2 - Struttura dell'indice del pacchetto di archiviazione

A titolo esemplificativo riportiamo, di seguito, un tracciato XML di un PdA.

```
<?xml version="1.0" encoding="utf-8"?>
<IdC xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" p3:version="-" p3:url="" p3:schemaLocation="-"
xmlns:p3="http://www.uni.com/U3011/sincro/" xmlns="http://www.uni.com/U3011/sincro/">
    <p3:SelfDescription>
        <p3:ID p3:scheme="local">d170cb44-62b3-4084-87b2-d63642202588</p3:ID>
        <p3:CreatingApplication>
            <p3:Name>JDoc</p3:Name>
            <p3:Version>6.0.0.0</p3:Version>
            <p3:Producer>prodeo s.r.l.</p3:Producer>
        </p3:CreatingApplication>
    </p3:SelfDescription>
    <p3:VdC>
        <p3:ID p3:scheme="local">36cfc425-d08e-4fc9-8bdc-5b3811c3de71</p3:ID>
    </p3:VdC>
    <p3:FileGroup>
        <p3:File p3:encoding="binary" p3:extension="p7m" p3:format="application/p7m">
            <p3:ID p3:scheme="local">210b033f-e467-4289-8055-77f94a7c29a2</p3:ID>
            <p3:Path>./File/210b033f-e467-4289-8055-77f94a7c29a2.p7m</p3:Path>
            <p3:Hash p3:function="SHA-256">
                4826a0a7634c2b96b4cfb1d6e1fc1aef21394791f46338d16d356aa1a9b2410a
            </p3:Hash>
            <p3:MoreInfo p3:XMLScheme="">
                <p3:ExternalMetadata p3:format="application/xml" p3:encoding="binary">
                    <p3:ID p3:scheme="local">0d3c702d-9e25-4b87-a7ce-b87f413b29d4</p3:ID>
                    <p3:Path>./Meta/0d3c702d-9e25-4b87-a7ce-b87f413b29d4.xml</p3:Path>
                    <p3:Hash p3:function="SHA-256">
                        48b849509eb8994cee42a233bf19063ecfec6a88b11c91517ff8d86663ba3809
```

```
                    </p3:Hash>
                </p3:ExternalMetadata>
            </p3:MoreInfo>
        </p3:File>
        <p3:File p3:encoding="binary" p3:extension="p7m" p3:format="application/p7m">

            <p3:ID p3:scheme="local">d001c351-b862-440e-a5dc-490574244c98</p3:ID>
            <p3:Path>./File/d001c351-b862-440e-a5dc-490574244c98.p7m</p3:Path>
            <p3:Hash p3:function="SHA-256">
                69eb58664b83234a804d231a117629673bbeb0b3f767e9b03897d1459e7fc758
            </p3:Hash>
            <p3:MoreInfo p3:XMLScheme="">
                <p3:ExternalMetadata p3:format="application/xml" p3:encoding="binary">
                    <p3:ID p3:scheme="local">a477ebf5-df4f-4df9-adbc-f85fc1b5e114</p3:ID>
                    <p3:Path>./Meta/a477ebf5-df4f-4df9-adbc-f85fc1b5e114.xml</p3:Path>
                    <p3:Hash p3:function="SHA-256">
                        e3ee0413622956a9ccdeb9ef3e8edfc90808a4d2cae1d09e4a4de66f503c0a7d
                    </p3:Hash>
                </p3:ExternalMetadata>
            </p3:MoreInfo>
        </p3:File>
        <p3:File p3:encoding="binary" p3:extension="p7m" p3:format="application/p7m">
            <p3:ID p3:scheme="local">a50e8671-fa15-47b6-b1d1-97a34a8a8316</p3:ID>
            <p3:Path>./File/a50e8671-fa15-47b6-b1d1-97a34a8a8316.p7m</p3:Path>
            <p3:Hash p3:function="SHA-256">
                c2b1e05b9f7999fb00060cfe5adb371ec8844b65b923253834fbb040418f4203
            </p3:Hash>
            <p3:MoreInfo p3:XMLScheme="">
                <p3:ExternalMetadata p3:format="application/xml" p3:encoding="binary">
                    <p3:ID p3:scheme="local">1b32e85b-58e2-432d-bd06-5cda0b64e0a7</p3:ID>
                    <p3:Path>./Meta/1b32e85b-58e2-432d-bd06-5cda0b64e0a7.xml</p3:Path>
                    <p3:Hash p3:function="SHA-256">
                        b16495efe3ad36832146bd18179d036d6129830c2988e78367e035c50ed26863
                    </p3:Hash>
                </p3:ExternalMetadata>
            </p3:MoreInfo>
        </p3:File>
    </p3:FileGroup>
    <p3:Process>
        <p3:Agent p3:type="organization" p3:role="PreservationManager">
            <p3:AgentName>
                <p3:FormalName>prodeo s.r.l.</p3:FormalName>
            </p3:AgentName>
            <p3:Agent_ID p3:scheme="VATRegistrationNumber">03466010232</p3:Agent_ID>
        </p3:Agent>
        <p3:Agent p3:type="organization" p3:role="Delegate">
            <p3:AgentName>
                <p3:FormalName>prodeo s.r.l.</p3:FormalName>
            </p3:AgentName>
            <p3:Agent_ID p3:scheme="VATRegistrationNumber">03466010232</p3:Agent_ID>
        </p3:Agent>
        <p3:Agent p3:type="organization" p3:role="OtherRole" p3:otherRole="Producer">
            <p3:AgentName>
                <p3:FormalName>ESEMPIO S.p.A.</p3:FormalName>
            </p3:AgentName>
            <p3:Agent_ID p3:scheme="VATRegistrationNumber">12345678910</p3:Agent_ID>
        </p3:Agent>
        <p3:TimeReference>
            <p3:AttachedTimeStamp>2015-06-03T14:04:01.444+02:00</p3:AttachedTimeStamp>
        </p3:TimeReference>
    </p3:Process>
</IdC>
```

Alla struttura del PdA citata in precedenza sono collegate ulteriori strutture, in formato XML, contenenti i metadati del documento, tramite i diversi elementi “MoreInfo” previsti nello standard SInCRO. Di seguito riportiamo un esempio di una struttura implementata per la conservazione delle fatture elettroniche alla PA.

```
<?xml version="1.0" encoding="utf-8"?>
<documento IDDocumento="210b033f-e467-4289-8055-77f94a7c29a2">
    <datachiusura>2015-01-13</datachiusura>
    <oggettodocumento>esempio</oggettodocumento>
    <soggettoproduttore>
        <nome>Mario</nome>
        <cognome>Rossi</cognome>
```

```
        <codicefiscale>esempioesempioes</codicefiscale>
    </soggettoproduttore>
    <destinatario>
        <nome>Nome responsabile PA destinataria</nome>
        <cognome>Cognome responsabile PA destinataria</cognome>
        <codicefiscale>esempioesempioes</codicefiscale>
    </destinatario>
    <ProgressivoInvio>0000069284</ProgressivoInvio>
    <NomeFile>IT03466010232_00I1U.xml</NomeFile>
    <DatiGeneraliDocumento>
        <TipoDocumento>TD01</TipoDocumento>
        <Data>2015-09-02</Data>
        <Numero>2015110727</Numero>
    </DatiGeneraliDocumento>
    <CessionarioCommittente>
        <CodiceFiscale>xxxxxx00988</CodiceFiscale>
        <PartitaIVA>ITxxxxxx00988</PartitaIVA>
        <Denominazione>Nome Pubblica Amministrazione</Denominazione>
    </CessionarioCommittente>
</documento>
```

Torna al sommario

6.4. Pacchetto di Distribuzione (PdD)

La richiesta di esibizione dei documenti conservati da parte dell'utente viene soddisfatta attraverso la generazione di un PdD.

Il PdD viene formato secondo le regole tecniche definite nello Standard SInCRO. Il PdD ha una struttura analoga a quella del PdA ed include i riferimenti univoci ai PdA che sono stati estratti dal SdC.

Il PdD è corredato da ulteriori informazioni quali:

- Informazioni relative al soggetto produttore (Codice anagrafico, Ragione Sociale, Codice Fiscale, Partita IVA, ...);
- Identificativo univoco dell'PdD generato automaticamente dal SdC;
- Informazioni sull'applicazione che ha generato il PdD (produttore del software, nome e versione);
- Informazioni sui PdA contenuti nel PdD;
- Informazioni sui documenti (ID, Impronta di hash, formato, percorso);
- le immagini in formato originale estratte dai PdA;
- Informazioni relative al processo di conservazione (elementi identificativi del RSC);
- Informazioni relative alla data di produzione del pacchetto stesso (marca temporale);
- Informazioni relative alla firma digitale.
- eventuali informazioni relative ai metadati dei documenti previste negli accordi specifici del Contratto del Servizio;
- Informazioni necessarie per il controllo ed il log delle operazioni relative al pacchetto stesso.

Le richieste di esibizione dei PdD sono accettate solamente se provenienti dai soggetti autorizzati dal produttore.

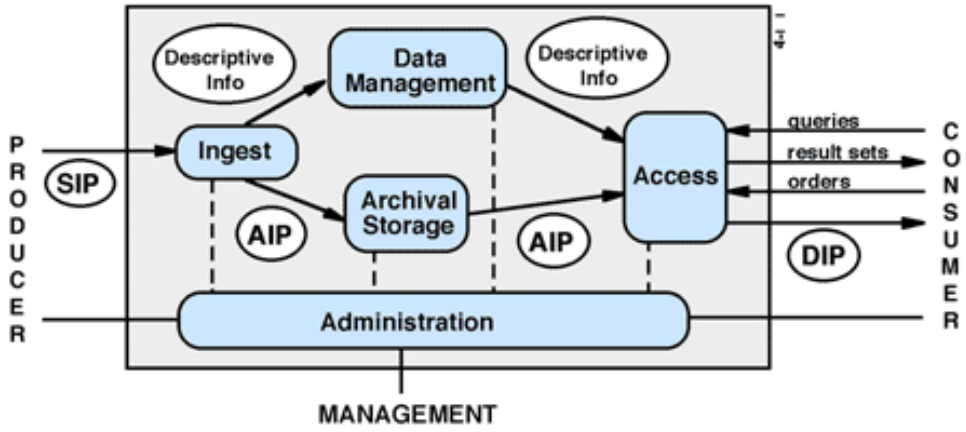
Torna al sommario

7. Processo di conservazione

Il processo di conservazione si esegue sulla base delle modalità previste dall' art. 9 del DPCM, e delle specifiche contenute nella Procedura di gestione della Conservazione Digitale (PCD) afferente al ISMS e dalle peculiarità presenti nei Contratti di Servizio.

Il processo di conservazione è realizzato sulla base del modello funzionale OAIS (Open Archival Information System) normato dallo standard ISO 14721:2003 a cui si è fatto riferimento. Il modello OAIS ha introdotto nella gestione degli archivi informatici i concetti fondamentali relativi alle modalità di transazione dei pacchetti informativi (PdV, PdA, PdD) contemplati e descritti nel presente manuale.

Nello schema che segue si evidenziano le modalità che regolano il flusso informativo di pacchetti informativi generati da un soggetto produttore (nello schema: Producer) sotto forma di PdV (nello schema: SIP) ad un SdC (nello schema: management) che lo trasforma in PdA (nello schema: AIP) e ne cura la conservazione ed il mantenimento nel tempo. Il SdC provvede anche a mettere a disposizione dell'utente (nello schema: consumer) il contenuto del PdA tramite opportune modalità di accesso (nello schema: Access) e sotto forma di PdD (nello schema DIP).



Schema 1 - Modello funzionale OAIS

Torna al sommario

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

Le principali modalità di trasmissione del pacchetto di versamento sono:

- appositi web service che consentono l'inserimento nel SdC;
- trasmissione telematica tramite canale sicuro;
- interfaccia web-based e mediante una azione di "upload" dei documenti informatici,
- altri software sviluppati da partner

Tutti i canali FTP/HTTP di comunicazione instaurati con i Clienti sono cifrati per la protezione dei dati oggetto di transazione con il produttore. Il ripristino delle funzionalità del sistema in caso di corruzione o perdita dei dati è implementato e descritto nel PRBCDR Business Continuity e disaster recovery Plan (Procedura SGSI). Per l'intero processo di acquisizione dei PdV, il SdC produce i log di sistema necessari alla

tracciatura delle attività e delle operazioni svolte, così come descritto nella sezione dedicata al Log Management del Manuale della Sicurezza del Sistema Informativo (MSI).

Torna al sommario

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

Il SdC, opera uno o più controlli sul contenuto del pacchetto di versamento ricevuto dal soggetto produttore, per determinare la correttezza delle caratteristiche formali e dei documenti informatici e/o delle aggregazioni documentali informatiche afferenti al pacchetto stesso. Nelle sezioni successive, detti controlli sono ulteriormente approfonditi dal punto di vista procedurale.

Di seguito sono riportati alcuni tra gli automatismi più consueti implementati per il controllo e la verifica delle caratteristiche dei documenti relativi alle diverse aggregazioni documentali informatiche successivamente sottoposti al processo di conservazione.

- Identificazione certa del produttore: il sistema verifica l'identità del produttore attraverso diverse modalità in relazione alla disponibilità tecnica e tecnologica dello stesso.
- Vengono verificate: le credenziali fornite ad esso, lo specifico canale sicuro di comunicazione messo a disposizione, il filtro sugli indirizzi internet, la codifica specifica del codice cliente attribuita ai dati che il produttore invia in fase di versamento.
- Controlli di corretto trasferimento via rete internet: dove previsto dalla parametrizzazione del SdC il trasferimento via rete internet il SdC verificata l'integrità dei documenti contenuti nei pacchetti di versamento, attraverso il confronto delle impronte di hash.
- Controlli di formato: il SdC verifica se i formati inviati dal produttore sono censiti e contrattualizzati nel periodo di competenza del servizio. I formati vengono verificati attraverso librerie e procedure software automatiche che effettuano un log completo delle operazioni effettuate. Per alcuni formati, dove possibile, viene anche controllata la correttezza dei dati.
- Automatismi per la verifica della consistenza dei documenti presenti nel flusso: il sistema verifica la presenza di tutti i dati e/o dei metadati dei documenti informatici che compongono l'archivio da sottoporre al procedimento di conservazione. L'utente del servizio ha a disposizione un insieme completo di informazioni e di riscontri utilizzabili in relazione ai dati di origine del flusso (sistema gestionali contabile, ERP, CRM, ecc.).
- Verifica dell'omogeneità dei documenti: dove previsto viene verificata la coerenza nella progressione numerica e temporale dei protocolli nonché la progressività dei protocolli rispetto all'ultima operazione di conservazione.
- Verifica dei metadati minimi obbligatori: il sistema verifica la presenza dei metadati minimi obbligatori per ogni documento e specifici per ogni produttore e per ogni tipologia documentale, così come definito negli accordi specifici del contratto di servizio.

Ulteriori automatismi possono essere implementati su richiesta del soggetto produttore ed in base alle esigenze dello stesso e sulla base degli accordi specifici del contratto di servizio.

Torna al sommario

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

L'accettazione del PdV dà luogo alla generazione automatica del rapporto di versamento relativo ad uno o più pacchetti di versamento.

Il rapporto di versamento è strutturato secondo quanto previsto dalle regole tecniche (Art. 9, comma 1, lettere d ed e del DPCM) ed è comprensivo dell'elenco dei pacchetti di versamento accettati.
Il SdC attribuisce un identificatore univoco a ciascun rapporto di versamento generato e lo riferisce temporalmente (coordinato con il sistema di gestione del Tempo Universale Coordinato - UTC -).

Il rapporto di versamento include, a titolo non esaustivo, le seguenti informazioni:

- dati del produttore
- dati dell'utente richiedente il versamento
- tipologie dei documenti
- formati dei documenti
- impronte dei documenti
- esiti dei controlli
- metadati del PdV
- riferimenti temporali

L'accettazione del PdV è subordinata ai controlli previsti dal SdC per il produttore, le tipologie di documento oggetto di conservazione, i formati e quanto previsto al paragrafo 7.2. Tali controlli sono parametrizzati nel SdC stesso e sono parte integrante del contratto di servizio.
Nel rapporto di versamento sono elaborate e specificate le impronte, una o più, calcolate sull'intero contenuto del pacchetto di versamento, mediante procedura automatizzata.

Il SdC inoltra i rapporti di versamento al produttore secondo diverse modalità in base a quanto espresso nel contratto di servizio. Le modalità utilizzate sono:

- trasmissione a mezzo mail,
- trasmissione a mezzo PEC,
- messa a disposizione tramite interfaccia web.

L'interfaccia web consente al produttore di monitorare lo stato di tutti i PdV inviati al SdC e pertanto gestire anche eventuali errori risultanti dai controlli (si veda paragrafo 7.4).
Tutti le informazioni inerenti alle operazioni eseguite dagli utenti e dai processi informatici relative ai PdV accettati dal produttore al SdC vengono storicizzate su appositi log. Tra queste, a titolo non esaustivo, citiamo: data e ora di ogni singola operazione, utente, processo informatico, codice cliente, tipo di operazione, metadati completi, identificativo univoco del PdV, informazioni di sicurezza.

Torna al sommario

7.4. Rifiuto del pacchetto di versamento

In caso di esito negativo dei controlli e delle verifiche applicati sul PdV, il SdC genera una comunicazione di rifiuto, che viene riferita temporalmente e trasmessa al produttore.

Nella comunicazione sono indicate le anomalie presenti nel PdV che ne determinano il rifiuto, quali (a titolo esemplificativo e non esaustivo):

- Presenza di documenti informatici non integri o corrotti in fase di trasmissione;
- Incongruenze relative a errata numerazione di protocollo;
- Incongruenze relative alla consecutività temporale dei documenti informatici;
- Assenza dal PdV dei dati essenziali specificati nel contratto di servizio;
- Anomalie relative alla sicurezza dei dati.

La comunicazione viene inoltrata al produttore secondo diverse modalità in base a quanto espresso nel contratto di servizio. Le modalità utilizzate sono:

- trasmissione a mezzo mail,
- trasmissione a mezzo PEC,
- messa a disposizione tramite interfaccia web.

Tutti le informazioni inerenti le operazioni eseguite dagli utenti e dai processi informatici relative ai PdV rifiutati dal SdC vengono storicizzate su appositi log. Tra queste, a titolo non esaustivo, citiamo: data e ora di ogni singola operazione, utente, processo informatico, codice cliente, tipo di operazione, metadati completi, identificativo univoco del PdV, informazioni di sicurezza.

Torna al sommario

7.5. Preparazione e gestione del pacchetto di archiviazione

Mediante apposite procedure software del SdC, i PdV, opportunamente verificati e validati come descritto nelle sezioni precedenti, vengono trasformati in PdA e corredati delle ulteriori caratteristiche necessarie a soddisfare i requisiti previsti dalla normativa.

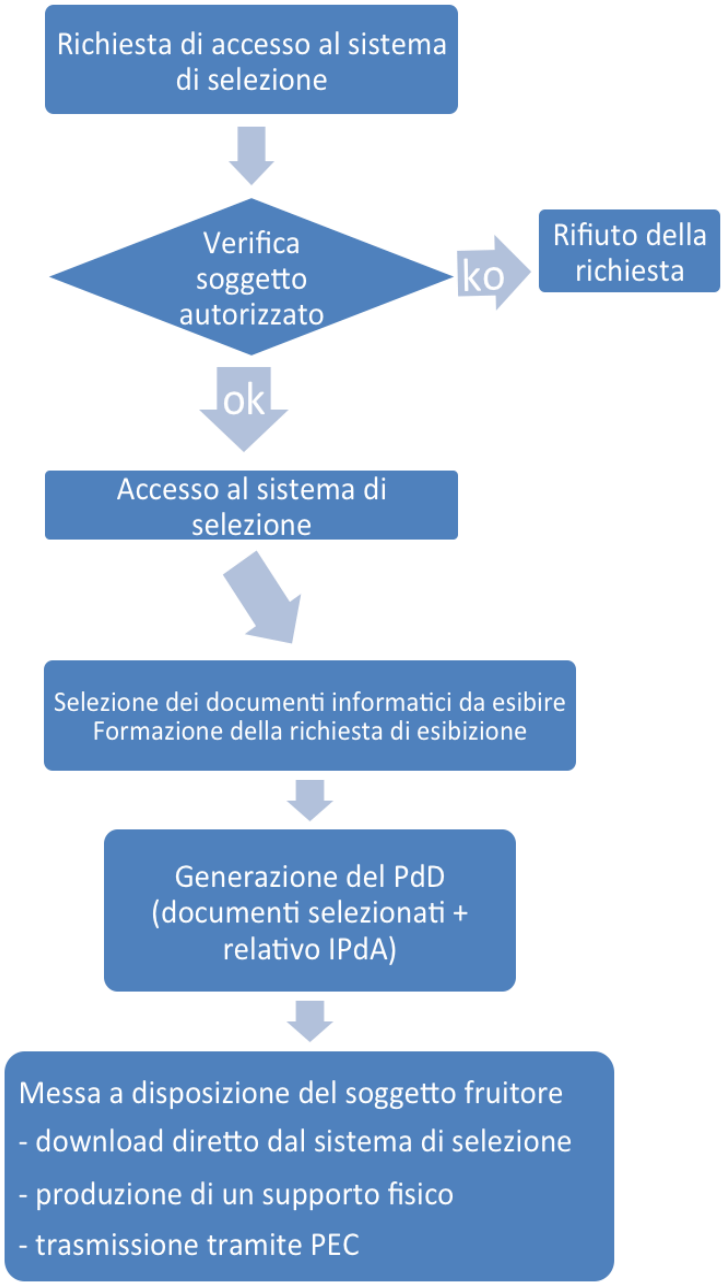
Qualora si rendano necessari interventi manuali di rettifica, integrazione di dati e metadati nei PdA, da parte degli operatori del SdC, tali operazioni sono tracciate su appositi log che includono, a titolo non esaustivo, le seguenti informazioni: data e ora di ogni singola operazione, utente/processo, codice cliente, tipo di operazione, metadati completi precedenti e successivi all'operazione, informazioni di sicurezza.

I PdA sono sottoscritti dal RSC e, ad essi, sono associate le relative marche temporali.
I PdA, così sottoposti al processo di conservazione digitale, sono custoditi, per i tempi previsti dalla normativa e dai Contratti di Servizio, nell'archivio informatico facente parte del SdC. Il sistema è implementato e sviluppato allo scopo di garantire e mantenere la disponibilità, la fruibilità, l'immodificabilità e l'autenticità dei documenti informatici in esso contenuti.
Le ulteriori informazioni peculiari contenute nel PdA, eventualmente concordate con il soggetto produttore, sono definite nei Contratti di Servizio.

Torna al sommario

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

Il processo di preparazione del PdD è attivato dalla ricezione di una richiesta di esibizione da parte dell'utente. Il SdC si occupa di verificare che il profilo dell'utente che accede abbia le necessarie autorizzazioni per effettuare l'estrazione.
L'utente, guidato dal sistema, opera la selezione dei documenti informatici da estrarre. Il sistema, sulla base della selezione, compone la richiesta di esibizione che specifica quali documenti informatici comporranno il PdD.
Il sistema provvede quindi a confezionare il PdD contenente i documenti informatici oggetto della selezione ed i relativi IPdA.
Gli IPdA contengono le impronte dei documenti richiesti per consentire all'utente la verifica autonoma e completa delle caratteristiche che determinano la corretta conservazione dei documenti.
Nel caso in cui si preveda l'utilizzo di supporti fisici rimovibili per la trasmissione dei pacchetti di distribuzione, si fa riferimento a quanto previsto nel contratto di servizio.
I supporti fisici non presentano riferimenti esterni che possano permettere l'identificazione dell'ente produttore, dei dati contenuti, della loro tipologia, ecc.
I supporti fisici sono trasportati a cura e responsabilità del personale di Prodeo o incaricato da Prodeo sulla base di specifici requisiti definiti dal RdC nella procedura PCD.
I dati richiesti sono crittografati e firmati digitalmente prima della loro spedizione/trasmissione allo stesso.
Nel caso in cui i contratti di servizio implichino la consegna dei PdD via email, viene utilizzata la posta certificata per permettere di tracciare l'intera trasmissione e sono conservate le sole ricevute di invio e consegna.
Tutti le informazioni relative ai PdD richiesti, generati, esportati dal SdC vengono storicizzate su appositi log. Tra queste, a titolo non esaustivo, citiamo: data e ora di ogni singola operazione, utente/processo, codice cliente, tipo di operazione, metadati completi, informazioni di sicurezza.



Schema 2 - Processo di preparazione e gestione del PdD

Torna al sommario

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

Il SdC prevede specifiche procedure per la generazione e produzione di duplicati informatici e copie informatiche sulla base delle modalità definite dall'art. 22 del CAD.

Produzione di duplicati informatici

Il procedimento di produzione di duplicati informatici consente di ottenere dal SdC i duplicati informatici aventi il medesimo valore giuridico, ad ogni effetto di legge, dei documenti informatici dai quali sono tratti in conformità con le regole tecniche vigenti. I duplicati di documenti informatici hanno il medesimo contenuto e la medesima rappresentazione informatica degli originali dai quali sono tratti.
Il procedimento di produzione di duplicati si attiva automaticamente:

- ogni volta che l'utente accede al sistema di selezione per ottenere uno o più PdD contenenti i documenti informatici di interesse;
- in occasione dei backup e delle repliche perpetrate sui PdA allo scopo di garantirne la permanenza dei requisiti essenziali di fruibilità e verificabilità.

Produzione di copie informatiche/analogiche ed estratti di documenti informatici

Il procedimento di produzione di copie informatiche ed estratti di documenti informatici consente di ottenere documenti aventi la stessa efficacia probatoria dei documenti informatici dai quali sono tratte. Le copie e gli estratti di documenti informatici hanno il medesimo contenuto degli originali da cui sono tratte ma diversa rappresentazione informatica.
Il procedimento di generazione di copie informatiche ed estratti viene di norma attivato:

- ogni qual volta sia richiesto dai soggetti fruitori e specificamente previsto dal contratto di servizio in relazione agli accordi;
- quando, per motivi legati all'evoluzione tecnologica e/o normativa, la rappresentazione informatica dei documenti originali non sia più fruibile dai sistemi di consultazione utilizzati e sia necessario adeguarne il formato.

Il procedimento di generazione di copie informatiche prevede la possibilità di richiedere l'intervento di un pubblico ufficiale allo scopo di attestare la conformità di queste con gli originali.

Produzione di copie informatiche di documenti analogici

Il procedimento di produzione di copie informatiche di documenti analogici consente di generare documenti informatici aventi la stessa efficacia probatoria degli originali analogici da cui sono tratti. Le modalità tecniche di ottenimento delle suddette copie sono costituite da procedure di digitalizzazione che avvengono tramite appositi dispositivi scanner o mediante procedure di rielaborazione delle informazioni che costituiscono i contenuti dei documenti analogici originali.
Il SdC prevede espressamente la possibilità di conservare dette fattispecie documentali e le procedure di digitalizzazione utilizzate sono ampiamente descritte nel SGI (Sistema Gestione Integrato Qualità - Ambiente) Procedura Operativa PO/11 – "Programmazione DB, Data Entry e Scansione Ottica", afferenti al ISMS.
Le procedure di elaborazione di un documento analogico in informatico, menzionate al paragrafo precedente, sono invece gestite da un apposito modulo software del SdC.
Il procedimento di produzione di copie informatiche di documenti analogici viene attivato quando il soggetto produttore conferisce al SdC documenti espressi su supporti analogici.

Torna al sommario

7.8. Scarto dei pacchetti di archiviazione

Il SdC effettua lo scarto dei pacchetti di archiviazione sulla base di quanto espresso nei Contratti di Servizio. L'eliminazione dei pacchetti informativi scartati e delle eventuali relative informazioni a corredo viene eseguita tramite una procedura di distruzione sicura dei dati, in linea con la vigente normativa sulla sicurezza dei dati e privacy. La procedura di scarto dei pacchetti di archiviazione viene operata e coordinata da RSC sulla base delle disposizioni ricevute dal soggetto produttore, delle disposizioni contenute nei contratti di servizio e in ottemperanza a quanto sancito dal panorama normativo vigente.
RFA e RSS coadiuvano RSC nella ponderazione delle azioni da intraprendere a fronte dell'attuazione di un procedimento di scarto. Tale procedimento viene operativamente attuato da RSI coadiuvato dagli addetti opportunamente individuati dell'area gestione sviluppo software e manutenzione e consiste nelle seguenti fasi:

- interrogazione del database del SdC per l'estrazione dei documenti che hanno superato la soglia temporale di scarto;
- informazione del soggetto produttore tramite interlocuzione diretta con RSC (o operatore incaricato) ed invio di una comunicazione formale tramite PEC;

- esecuzione della procedura batch (configurata ad hoc) per la cancellazione dei documenti condotta manualmente dagli operatori incaricati.

Nel caso di archivi pubblici o privati di particolare interesse culturale, le procedure di scarto avvengono previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo. La gestione della richiesta di autorizzazione è a carico dell'Ente pubblico produttore.

Torna al sommario

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

Prodeo, al fine di garantire l'interoperabilità del proprio sistema di conservazione e la trasferibilità di archivi informatici ad altri eventuali soggetti conservatori ha predisposto le seguenti misure:

- Adozione conformemente a quanto determinato dallo standard SInCRO, di tracciati XML omogenei relativi ai PdD e PdA.
- Generazione di tracciati XML (conformi allo standard SInCRO) privi di informazioni non standardizzate e/o arbitrariamente definite e/o ridondanti, salvo il caso in cui la presenza di esse sia espressamente richiesta dal soggetto produttore e palesata nelle specificità contrattuali;
- Mantenimento, per i PdD, della medesima struttura di dati espressa dal DPCM per la configurazione dei PdA (vedasi paragrafi 6.4 e 6.5);
- Mantenimento di identità tra Indice IPdA del PdA ed il medesimo presente nel PdD;
- Gestione dei metadati dei documenti informatici esterna al PdA tramite la corretta valorizzazione della sezione <MoreInfo>.

Il SdC è in grado di accettare il versamento di PdD prodotti da altri sistemi di conservazione se in formato standard SInCRO. Eventuali altri formati dovranno essere sottoposti ad analisi e valutazione tecnica prima dell'ingresso nel SdC allo scopo di programmare e svolgere le opportune attività volte all'adeguamento ai formati standard.

In caso di conclusione del contratto di servizio, Prodeo si impegna a rendere disponibili al produttore i PdD, coincidenti con i PdA conservati, tramite i canali e nelle modalità definite negli specifici accordi contrattuali e previa sottoscrizione dei relativi verbali di consegna. Ove previsto dalla natura dei dati riprodotti, sarà effettuata la cifratura degli stessi e la comunicazione, con canale distinto, della relativa chiave per la decifratura e la fruizione esclusiva da parte del titolare dell'archivio.

Torna al sommario

7.10. Conservazione delle comunicazioni intercorrenti tra il SdC e i fruitori del servizio di conservazione.

Tutte le comunicazioni prodotte durante le transazioni di pacchetti informativi tra Prodeo e il produttore (log applicativi, log di sistema, mail, mail pec) sono conservate mediante il SdC stesso.

Torna al sommario

8. Sistema di conservazione

Il sistema di conservazione, di seguito descritto nelle sue modalità di accesso, utilizzo e protezione è composto da:

- Componenti Logiche e Tecnologiche: Informazioni e dati, prodotti/servizi di software installati presso Prodeo;
- Componenti Fisiche: architettura informatica aziendale in tutti le sue componenti hardware, reti (aziendali ed esterne);
- Procedure di gestione e di evoluzione: procedure di produzione del software aziendale e della sua manutenzione, procedure di conservazione, procedure di Audit, Riesame della Direzione.

Torna al sommario

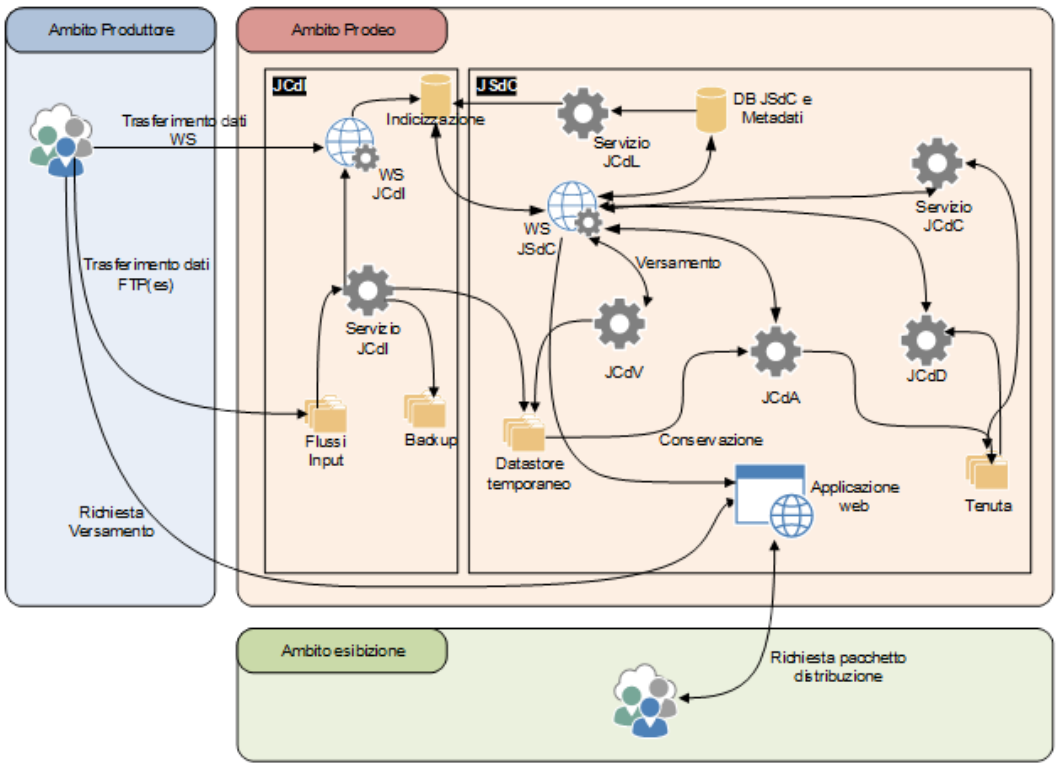
8.1. Componenti logiche

Il SdC è composto, a livello logico, dai seguenti oggetti:

- produttore: effettuano il versamento dei nuovi PdV generati al SdC;
- Componente di Indicizzazione (JCdI): componente che gestisce il monitoraggio, il controllo e l'indicizzazione dei flussi in ingresso;
- Componente di Versamento (JCdV): componente che gestisce la generazione dei PdV e dei rapporti di versmamento;
- Componente di Archiviazione (JCdA): componente che gestisce la trasformazione da PdV a PdA utilizzando i servizi di firma digitale dei documenti implementati con tecnologia HSM presso una CA accreditata;
- Componente di Distribuzione (JCdD): componente che gestisce la generazione e la ricerca dei PdD;
- Utenti: fruiscono del SdC, accedendo alla piattaforma di front-end gestita tramite applicazioni web-based.

Tutte le funzionalità gestite dal sistema sono erogate in modalità di servizio.

Lo schema riportato di seguito rappresenta l'architettura logico-funzionale del SdC.



Schema 3 - Componenti logiche del SdC

Torna al sommario

8.2. Componenti Tecnologiche

Il SdC è implementato attraverso una serie di moduli applicativi tra cui si riportano i principali:

- JCdI: è il modulo che realizza la componente di indicizzazione;
- JCdV: è il modulo che realizza la componente di versamento;
- JCdD: è il modulo che realizza la componente di distribuzione;
- JCdL (componente di logging): è il modulo che consente di gestire le funzionalità di logging;
- JCdC (componente di controllo): è il modulo che consente di gestire le funzionalità di controllo dei pacchetti.

Torna al sommario

8.3. Componenti fisiche

Si riportano lo schema e la descrizione dei siti di conservazione e delle connessioni tra i diversi siti e tra i diversi attori del sistema, con riferimento alle componenti tecnologiche del paragrafo precedente.
A questi si aggiungono lo schema e la descrizione delle componenti fisiche presenti in ciascuno dei siti di conservazione.

Il sistema di conservazione è ospitato presso i data center di Prodeo SpA sito in Bari. Tale sito è attrezzato con tecnologie innovative in termini di affidabilità, sicurezza, scalabilità e ridondanza e sono certificati secondo lo Standard UNI CEI ISO/IEC 27001:2014. La strategia per la continuità del servizio (*Business continuity plan*), che ha portato allo sviluppo del piano di continuità, prevede la disponibilità di un sito alternativo per il *disaster recovery*. Prodeo SpA dispone, infatti, di due siti: il sito primario, che rappresenta il sito operativo normalmente utilizzato per l'esposizione e la fruizione dei servizi ed il Disaster Recovery, allocato presso il Datacenter Fastweb di Milano, che è speculare al primo in termini di risorse e di servizi, ma che diventa "operativo" solo in caso di disastro del sito primario. La distanza di oltre 800km tra il sito primario ed il sito disaster recovery è tale da garantire la continuità del servizio anche a fronte di eventi catastrofici.

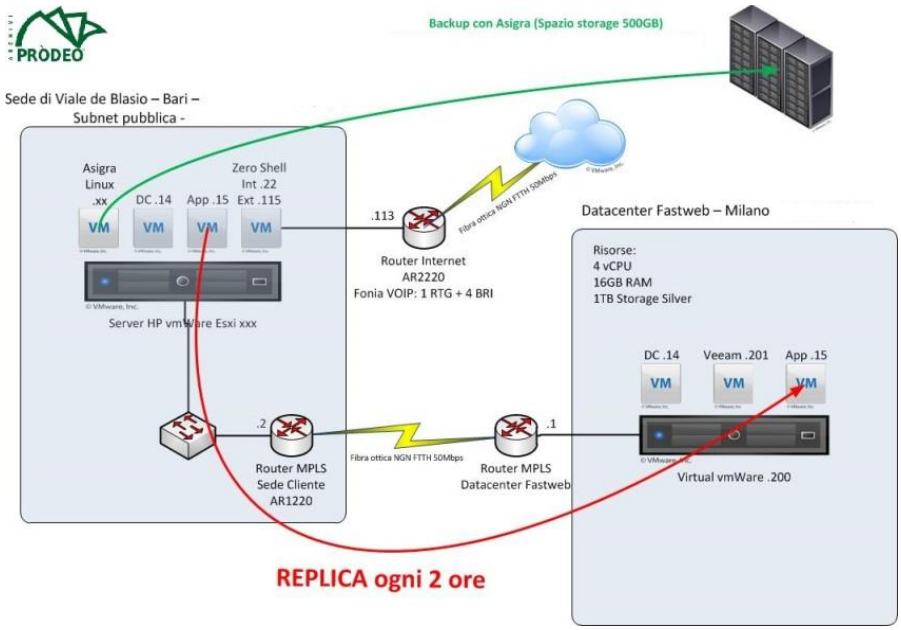


Figura 9: schema dell'infrastruttura della farm di DR

Entrambi i siti dispongono di connessioni ridondate in fibra ottica ad alte prestazioni che garantiscono servizi di replica sincrona, maggiore resilienza ed alta affidabilità. Sia i locali che ospitano i siti, sia le macchine e gli apparati che compongono l'infrastruttura sono controllati H 24x7x365 da un sistema distribuito per il monitoraggio ed il controllo. L'infrastruttura tecnologica dei data center è caratterizzata da:

- architettura *multitier;*
- affidabilità;
- scalabilità;
- sicurezza dei dati;
- manutenibilità;
- flessibilità;
- qualità e certificazione dei componenti.

Il sistema di alimentazione della sala server è costituito da due apparati UPS on-line da 10.000 VA e batterie supplementari che garantiscono su due linee separate l'alimentazione di tutte le apparecchiature per circa 60 minuti insieme ad un gruppo elettrogeno diesel che permette di estendere ulteriormente l'autonomia a tempo indeterminato. Tali gruppi sono sottoposti a rigorosi controlli periodici con la sostituzione di parti consumabili (batterie, etc.).
Il sistema di conservazione del "Sito primario" è basato su un cluster di server HP DL380 di ultima generazione (Gen9), ogni nodo è dotato di doppio processore INTEL XEON ES-2609v3 Six Core 1,90 GHz e 64 GB di RAM ciascuno per garantire la massima capacità e velocità di calcolo, storage HP StoreEasy 1650, controller e switch ridondati.

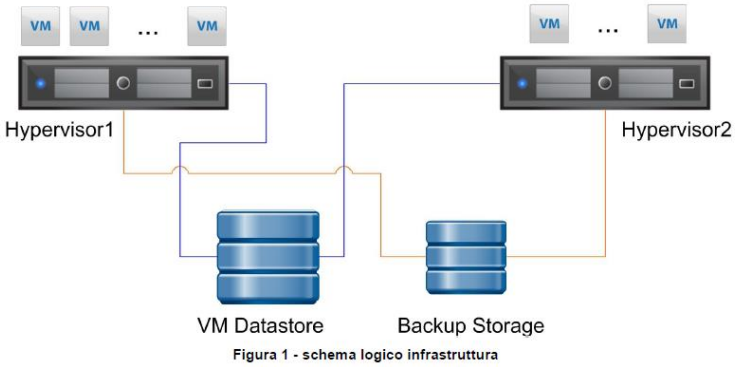


Figura 10: Schema logico dell'infrastruttura Pròdeo S.p.A.

Il cluster è basato su architettura VMware Vsphere e lo storage è costituito da dischi SAS in configurazione RAID6 + Spare.
Il sistema può essere ampliato con l'aggiunta di altri sistemi di storage da collegare in fibra ottica al cluster fino a raggiungere la capienza di decine di TB. La scalabilità del cluster è garantita dalla possibilità di aggiungere ulteriori nodi al crescere delle necessità di calcolo.
I sistemi operativi installati sono aggiornati all'ultima release stabile di Windows Server e Red Hat Linux e CentOS. La conservazione logica dei dati è affidata alla piattaforma JSDC di EnerJ.

Per un maggior dettaglio dei sistemi di sito primario e secondario si rimanda alla copia del piano per la sicurezza.

Torna al sommario

8.4. Procedure di gestione e di evoluzione

Descrizione delle procedure di gestione e di evoluzione, e della relativa documentazione prevista, inerenti le componenti logiche, tecnologiche e fisiche del sistema di conservazione relativamente a:

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

I processi di gestione coprono tutto il ciclo di vita del servizio di conservazione e consentono di monitorarne e controllarne tutti gli aspetti. Le procedure di gestione operative del servizio e dei relativi sistemi a supporto del sistema di conservazione sono gestite secondo il Piano per la sicurezza di Pròdeo S.p.A. che include riferimenti a:

- Conduzione e manutenzione del sistema di conservazione;
- Gestione e conservazione dei *log;*
- Monitoraggio del sistema di conservazione;
- *Change management;*
- Verifica periodica di conformità a normativa e standard di riferimento;
- Manutenzione evolutiva ed adeguativa del software;
- Manutenzione correttiva del software;
- Manutenzione dell'infrastruttura

Conduzione e manutenzione del sistema di conservazione

Le procedure di conduzione e manutenzione del sistema di conservazione rientrano nel perimetro della certificazione ISO/IEC 27001:2014 così anche le attività di sviluppo e adeguamento software e sono affidate al Responsabile dello Sviluppo e della manutenzione del sistema di conservazione, in collaborazione con il Responsabile della Sicurezza dei sistemi per la conservazione.

L'obiettivo della manutenzione e mantenimento dell'infrastruttura hardware e software, è garantire il corretto funzionamento degli apparati del sistema di conservazione e di sicurezza ambientale e perimetrali secondo le specifiche tecniche dei fornitori e quanto previsto dalla Politica per la Sicurezza, al fine di evitare perdite preventive, danni, furti o interruzioni delle attività.

Eventuali incidenti o interruzioni sono gestiti dal Responsabile della sicurezza il quale ne definisce la codifica preventiva e la gestione degli stessi.

Gestione e conservazione dei log

Il Sistema di "log management" di Pròdeo è descritto nel Manuale di Gestione della Sicurezza delle Informazioni e dei Documenti di Archivio (MSGSI).

In particolare, il sistema di "log management" del SdC traccia tutte le operazioni e le transazioni informatiche inerenti a:

- versamento di pacchetti informativi;
- trasformazioni di pacchetti informativi in PdA;
- conservazione dei PdA;
- comunicazioni ed esiti relativi ai pacchetti informativi scambiati con produttori e fruitori;
- gestione della firma digitale e della marcatura temporale;
- produzione e distribuzione dei PdD;
- controllo e verifica dei PdA;
- eventi di carattere sistemistico quali: accessi a risorse informatiche, incidenti di sicurezza, interruzione dell'operatività dei servizi, ecc.;
- accessi fisici ai locali.

Monitoraggio del sistema di conservazione
Il sistema di conservazione è sottoposto a controlli automatici e manuali che ne garantiscono la disponibilità e la corretta funzionalità. In particolare, il monitoraggio è effettuato su:

- servizi attivi sui singoli server
- traffico di rete in ingresso ed uscita
- banda totale e residua disponibile
- storage (spazio disponibile, funzionalità dei dischi, stato del RAID, etc.)
- server (occupazione CPU, memoria idle di sistema, etc)
- apparati critici (stato degli UPS, stato dei firewall, etc.)
- fattori ambientali (rete elettrica generale, alimentazione rack, temperatura ambiente, temperatura rack, rilevazione fumi, controllo intrusioni, etc.)
- apparati di rete

Ricadono nel "monitoraggio e controllo" l'hardware, il software e l'insieme delle attività e delle procedure che gli operatori sono tenuti ad eseguire per il corretto funzionamento dei data center.
Il controllo è finalizzato alla produzione di allarmi in caso di anomalie ed eventi che non solo possono compromettere il corretto funzionamento delle macchine, ma anche eventuali guasti o malfunzionamenti delle macchine stesse.

Il sistema di monitoraggio e controllo utilizza i seguenti sensori:

- **Sensore di temperatura** - la collocazione dei sensori garantisce la possibilità di un pronto intervento in caso di guasto ai condizionatori d'aria o di un'anomalia che possa provocare un inatteso aumento di temperatura localizzato in uno degli armadi rack (es.: ostacolo imprevisto davanti le condotte aeree dell'armadio).
- **Videocamera** - un sistema di videocamere consente la verifica visiva da parte del responsabile di controllo. Il sottosistema dispone della funzione "motion detection" per la segnalazione di eventuali intrusioni non autorizzate.
- **Rilevatore di presenza di energia elettrica** - i sensori sono collocati in modo tale da prescindere dalle informazioni fornite dai gruppo di continuità. La soluzione adottata consente di verificare la disponibilità o meno della corrente elettrica a livello di distribuzione e a livello di uscita di ogni singolo gruppo.

Il sistema di monitoraggio e controllo è dotato, inoltre, di **dispositivi di emergenza** per sopperire alla mancanza di alcune risorse necessarie come l'energia elettrica o l'accesso alla rete pubblica.

Change management
Tutte le modifiche che interessano gli *asset* vengono gestite nell'ambito del sistema di qualità aziendale Pròdeo S.p.A. In particolare, tutti i cambiamenti significativi (non di routine) alle infrastrutture per l'elaborazione delle informazioni sono soggette al controllo del cambiamento. Il processo di **Change Management** specifica le modalità da seguire per le richieste dei cambiamenti, per la verifica degli aggiornamenti dovuti alle nuove *release*, per il passaggio dall'ambiente di test a quello di produzione e per l'installazione della nuova *release*.

La procedura prevede i seguenti passi:

1. per ogni richiesta di cambiamento la valutazione di costi di esercizio ed i potenziali benefici

2. valutazione del rischio
3. creazione di opportuni “punti di ripristino”
4. elaborazione di un piano di test completo
5. il test avviene nell’ambiente di test
6. i cambiamenti vengono trasferiti all’ambiente reale di produzione

Inoltre gli aggiornamenti software sono versionati secondo una rigorosa politica di *versioning*.
Per ulteriori approfondimenti si faccia riferimento alle procedure di change management del sistema JSDC di proprietà di EnerJ Srl.

Verifica periodica di conformità a normativa e standard di riferimento

Il Responsabile di servizio di conservazione, il Responsabile della funzione archivistica di conservazione ed il Responsabile della Sicurezza controllano costantemente l’evoluzione normativa ed il quadro regolamentare per tenere il sistema e la sua gestione aggiornati con le specifiche e i vincoli derivanti da Leggi dello Stato e Regolamenti europei.

Manutenzione evolutiva ed adeguativa del software
Il servizio di manutenzione dei prodotti software garantisce la manutenzione per il software di base e d’ambiente, installato sui sistemi serventi, tramite contratti di manutenzione con le Aziende produttrici dei prodotti stessi.
L’aggiornamento all’ultima release disponibile del software di terze parti utilizzato sarà effettuato, di volta in volta e successivamente alle seguenti verifiche:

- fattibilità tecnica;
- salvaguardia della stabilità complessiva del sistema;
- salvaguardia dell’integrità e completezza delle basi dati;
- compatibilità tra le versioni del software dei prodotti da aggiornare e il resto dei prodotti installati.

Gli aggiornamenti dei sistemi/ambienti operativi includeranno le seguenti attività:

- Pianificazione degli interventi di manutenzione sul software;
- Esecuzione dell’intervento che potrà consistere nell’introduzione di service pack, installazione, personalizzazione e configurazione dei prodotti (SO, software middleware, Web Server, Application Server, ecc.);
- Controllo degli interventi di manutenzione effettuati.

La presente sezione descrive dunque le modalità e le caratteristiche del ***processo integrato*** di assistenza e manutenzione raffigurato nel seguente diagramma:

Figura 11: Processo integrato di assistenza e manutenzione

Nella fase di ***Assessment*** le istanze di intervento manutentivo vengono vagliate per essere indirizzate alle fasi successive o rigettate. Nelle fasi di ***Design*** e ***Build & Test*** l’istanza di manutenzione viene implementa, validata e collaudata. Nella fase di ***Deploy*** le componenti applicative vengono portate in esercizio

produttivo e rilasciate alla gestione operativa (fase ***Operate***). Le componenti in esercizio sono assoggettate al controllo e monitoraggio (fase di ***Monitoring***). In particolare, la fase di Monitoring ha anche il compito di effettuare un monitoraggio proattivo delle potenziali vulnerabilità di sicurezza del Sistema e delle sue componenti infrastrutturali, nonché individuare preventivamente possibili interventi evolutivi sul Sistema.
La Manutenzione Evolutiva permette l'implementazione di modifiche dell'applicazione preesistente, secondo la struttura dei modelli di sviluppo software. Le principali differenze rispetto a sviluppi ex-novo sono legate al fatto che il punto di partenza per le attività è la presenza di un'applicazione preesistente, che viene dunque mantenuta come base per la soluzione futura. Inoltre, la manutenzione evolutiva ed adeguativa prevede il costante sviluppo e/o aggiornamenti delle procedure software, dovuti al presentarsi di nuovi adempimenti normativi sulla conservazione.

Manutenzione correttiva del software
Il servizio di Manutenzione correttiva del software include:

- correzione del software su segnalazione di eventuali malfunzionamenti;
- aggiornamento costante delle versioni del software che l'azienda fornitrice rilascerà nel corso dell'anno;
- intervento tecnico per verifiche, installazioni, formazione.

Gli interventi di manutenzione correttiva sono i seguenti:

- Analisi del malfunzionamento e determinazione della causa;
- Identificazione soluzioni temporanee (Workaround) atte a ripristinare nel più breve tempo possibile l'operatività e che saranno sostituite dall'intervento definitivo;
- Revisione della priorità assegnata nel caso dell'esistenza di un Workaround;
- Correzione di codice di eventuali componenti SW custom, correzioni nelle configurazioni di sistema e applicazione di eventuali patch a correzione di errori nel software standard di base;
- Supporto alla definizione delle attività da effettuare per la correzione dei dati (es. riesecuzione flussi di interfaccia errati) a seguito di comportamento anomalo del componente in errore.

La manutenzione correttiva è attivata a seguito di una segnalazione di malfunzionamento proveniente dagli utenti che impediscono l'uso dell'applicazione o di alcune funzioni dell'applicazione. Gli interventi saranno eseguiti da personale specializzato dei fornitori terzi, con contratti di manutenzione sugli applicativi software. Gli interventi saranno sempre conclusi con il completo ripristino della piena operatività del software. Un intervento di manutenzione correttiva si chiude quando viene soddisfatta la richiesta di assistenza con la risoluzione del problema.

Manutenzione dell'infrastruttura
Il servizio di manutenzione ha l'obiettivo di garantire la piena operatività di tutti i prodotti hardware resi disponibili per la conservazione e comprende la manutenzione preventiva, ordinaria e correttiva degli apparati con personale in possesso delle professionalità e delle certificazioni necessarie allo svolgimento delle attività di manutenzione hardware con elevati livelli di qualità.
Il completamento dell'intervento, e conseguente ripristino della funzionalità ed operatività è previsto entro 24h successivi la segnalazione del malfunzionamento attraverso il Sistema di Monitoraggio e Controllo.
Il servizio prevede la stipula di contratti di manutenzione con i produttori delle apparecchiature, il che comporta la disponibilità di personale altamente specializzato su varie marche di prodotti hw e sugli apparati di storage in uso.
Riguardo agli interventi di manutenzione hardware si precisa quanto segue:

- per quanto riguarda la manutenzione delle apparecchiature la Pròdeo S.p.A. richiederà l'intervento dei fornitori di hw per attivare le procedure di ripristino funzionale delle apparecchiature in errore;

- le componenti utilizzate in sostituzione di quelle guaste sono di nuova fabbricazione, originale e coperte dalla garanzia ufficiale della casa madre;
- tutti gli interventi relativi alle attività di manutenzione preventiva/ordinaria/correttiva, saranno eseguiti evitando qualsiasi interruzione del servizio e, in caso di apparati "critici", potranno essere eseguiti anche in orario notturno.
-

Manutenzione preventiva
La manutenzione preventiva ha lo scopo, mediante interventi on-site, di assicurare uno stato di funzionamento degli apparati costantemente regolare e crescente in termini di efficienza, nonché di prevenire gli interventi di tipo correttivo in modo da ridurre i tempi di non operatività degli apparati stessi.

In funzione dei metodi d'analisi utilizzati può essere suddivisa in:

- *preventiva basata su metodi statistici* (frequenza dei guasti): a data costante se l'intervento di manutenzione è realizzato dopo un periodo prefissato (sulla base per es. della criticità dell'apparato), indipendentemente dal reale tempo di funzionamento, oppure a ciclo costante se l'intervento di manutenzione è realizzato quando il componente raggiunge un prefissato tempo di funzionamento;
- *preventiva basata sui controlli previsti dai produttori* delle apparecchiature nelle specifiche tecniche; in questo caso si provvede alla pianificazione delle attività, da effettuarsi almeno una volta l'anno, non coincidenti con gli interventi di tipo correttivo.

Manutenzione ordinaria
La manutenzione ordinaria prevede l'esecuzione degli interventi necessari per assicurare la costante aderenza delle apparecchiature all'evoluzione dell'ambiente tecnologico e del sistema informatico oltre che il rispetto delle vigenti leggi e normative in merito alla sicurezza delle informazioni e alla tutela della privacy. Tale manutenzione comprende gli interventi che possono emergere dalla segnalazione da parte dei produttori dell'HW della necessità di aggiornamenti di BIOS, installazioni di patch del firmware, ecc. al fine di assicurare un livello adeguato di aggiornamento dell'infrastruttura ed eliminare eventuali vulnerabilità.

Manutenzione correttiva
Il servizio comprende la riparazione dei guasti che dovessero identificarsi durante il funzionamento delle apparecchiature. Gli interventi comprendono diagnosi dei malfunzionamenti delle apparecchiature e/o sistemi, sostituzione e/o riparazione di parti e/o componenti difettosi o guasti.
Gli interventi di manutenzione correttiva sono i seguenti:

- Analisi del malfunzionamento e determinazione della causa;
- Identificazione soluzioni temporanee (Workaround) atte a ripristinare nel più breve tempo possibile l'operatività e che saranno sostituite dall'intervento definitivo;
- Revisione della priorità assegnata nel caso dell'esistenza di un Workaround;
- Correzione di codice di eventuali componenti custom, correzioni nelle configurazioni di sistema e applicazione di eventuali patch a correzione di errori nel software standard di base;
- Supporto alla definizione delle attività da effettuare per la correzione dei dati (es. ri-esecuzione flussi di interfaccia errati) a seguito di comportamento anomalo del componente in errore.

Tipicamente la manutenzione correttiva è una politica di manutenzione che prevede un intervento di riparazione, sostituzione o revisione, solo a guasto avvenuto. L'azione manutentiva è quindi subordinata all'attesa del manifestarsi del guasto. Solo a guasto avvenuto viene preparato ed eseguito un intervento di

"ripristino" che riporta la prestazione del sistema al livello che aveva prima del manifestarsi del guasto in un suo componente.
La manutenzione correttiva è attivata a seguito di una segnalazione di malfunzionamento proveniente dagli utenti, o dal sistema di monitoraggio dell'infrastruttura informatica. Gli interventi saranno eseguiti da personale specializzato dei fornitori terzi, con contratti di manutenzione sugli apparati. Gli interventi saranno sempre conclusi con il completo ripristino della piena operatività hardware dell'apparato.
Un intervento di manutenzione correttiva si chiude quando viene soddisfatta la richiesta di assistenza con la risoluzione del problema e la riattivazione dell'apparecchiatura.

Torna al sommario

9. Monitoraggio e controlli

Descrizione generale della strategia della conservazione e dei conseguenti obiettivi di monitoraggio e controllo (Regole Tecniche: art. 8, comma 2, lettera h).

Torna al sommario

9.1. Procedure di monitoraggio

Gli applicativi software del SdC producono i log delle transazioni dei pacchetti informativi (di cui alla sezione 8.4 del presente manuale), dall'elaborazione dei quali si traggono le informazioni necessarie per valutare nel tempo il mantenimento dell'efficacia del sistema, nonché dell'efficienza e della rispondenza dello stesso ai livelli di prestazioni previsti nei Contratti di Servizio.

La direzione, in sede di riesame, individua i conseguenti interventi sullo sviluppo e la manutenzione del software, sia gli investimenti necessari nell'infrastruttura tecnologica.

Torna al sommario

9.2. Verifica dell'integrità degli archivi

La funzionalità di verifica di integrità degli archivi, permette di verificare l'integrità del documento dal momento della sua conservazione, confrontando l'impronta attuale con quella contenuta nell'indice di conservazione. Tale funzionalità viene applicata durante il processo di conservazione subito dopo la fase di memorizzazione nel file system, e risulta poi utile, nell'assolvimento dei requisiti di verifica periodica della leggibilità dei documenti, come richiesto dalla normativa.
Questa funzionalità è presente nel sistema di conservazione, come processo schedulabile, e può essere quindi pianificata da parte del responsabile del servizio di conservazione.
A ogni verifica effettuata i risultati vengono collezionati all'interno di un database, che può essere consultato da parte del responsabile del servizio di conservazione per attestare la corretta esecuzione della verifica o per diagnosticare eventuali anomalie.

Torna al sommario

9.3. Soluzioni adottate in caso di anomalie

Di seguito vengono descritte le soluzioni che vengono adottate a fronte di anomalie riscontrate a seguito del monitoraggio delle funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi.
Accordi specifici concordati con il soggetto produttore possono essere descritti nell'allegato "Specificità del contratto".

Anomalia dovute a malfunzionamento dell'impianto
I servizi del sistema di conservazione sono continuamente monitorati e controllati al fine di verificarne la conformità agli SLA definiti ed il mantenimento dei livelli di riservatezza, integrità e disponibilità dei dati. Inoltre il conservatore mette a disposizione del cliente il servizio di assistenza disponibile attraverso il portale web aziendale (www.prodeo.it), attraverso l'invio di mail alla casella di posta elettronica assistenza@prodeo.it, o chiamando il centralino telefonico negli orari di ufficio. I ticket di assistenza aperti sono ricevuti su dispositivi mobile e presi in consegna dal Responsabile della Conservazione che provvede ad attivare la relativa assistenza. Tale servizio garantisce una tempestiva risposta sia alle problematiche tecniche sia a quelle applicative relative all'uso del sistema. Vengono subito analizzati i log di sistema alla ricerca degli eventi anomali. Le anomalie riscontrate vengono classificate per stabilirne la priorità. In base alla classificazione ed alla tipologia di evento, vengono invocate le azioni correttive previste dalle istruzioni operative e ripristinati i sistemi. Dopo che l'incidente è stato contenuto e le correzioni richieste completate, si individuano le cause per garantire una adeguata azione correttiva.
Le anomalie sono classificate con le seguenti tipologie e risolte con le seguenti tempistiche:

- **Severità 1**: L'anomalia non consente all'utente l'utilizzo del sistema (Sistema di esercizio, Piattaforma per l'addestramento, ecc.) in quanto non consente di completare l'operazione voluta o di ottenere il risultato richiesto o di ottenere le prestazioni attese e non esistono soluzioni alternative per ovviare al problema (Anomalia bloccante);
- **Severità 2**: L'anomalia non consente all'utente l'utilizzo del sistema (Sistema di esercizio, Piattaforma per l'addestramento, ecc.) in quanto non consente di completare l'operazione o di ottenere il risultato richiesto o di ottenere le prestazioni attese, ma esistono soluzioni alternative per ovviare temporaneamente al problema (Anomalia non bloccante);
- **Severità 3**: L'anomalia non ha effetti sulla correttezza dei risultati attesi (Anomalia minore).

Alla segnalazione viene inoltre assegnata una priorità di lavorazione che tiene conto oltre che del livello di severità assegnato, anche dei carichi di lavoro nel rispetto dei livelli di servizio previsti per i servizi di Assistenza tecnico-applicativa e Manutenzione.

Torna al sommario