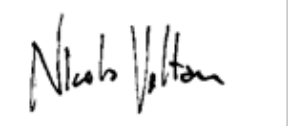
SIAV S.P.A.

MANUALE DI CONSERVAZIONE



NICOLA VOLTAN
SIAV SPA
Amministratore Delegato
18.09.2020 08:43:37 UTC

SIAV S.p.A.
Via Rossi, 5
35030 – Rubano (PD)
www.siav.it

+ 39 049 897 9797
+ 39 049 897 8800
info@siav.it

C.C.I.A.A.: PD 223442
Cap. Soc. € 250.000,00
C.F/P. IVA e R.I. 02334550288

Emissione del documento

Azione	Data	Nominativo	Funzione
Revisione e aggiornamento	16/09/2020	Rosalia Telese	Responsabile della funzione archivistica di conservazione
Verifica	16/09/2020	Alberto Veratelli	Responsabile dei sistemi informativi per la conservazione
		Davide Mietto	Responsabile della sicurezza dei sistemi per la conservazione
		Morgan Rizzolo	Responsabile dello sviluppo e della manutenzione del sistema di conservazione
		Daniela Perrone	Consulente interno
Approvazione	17/09/2020	Nicola Voltan	Responsabile del servizio di conservazione

Registro delle versioni

Versione	Data emissione	Descrizione
1.0	01/10/2014	Emissione del Manuale per Accreditamento AGID
2.0	28/03/2018	Revisioni varie in tutti i capitoli del Manuale
3.0	19/09/2019	Riferimenti al nuovo Responsabile dei sistemi informativi per la conservazione; riferimenti al DPO (Data Protection Officer)
4.0	17/09/2020	Inserito il riferimento alle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici; riferimento alla versione dello standard UNI SInCRO norma UNI 11386:2020

Sommario

1 SCOPO E AMBITO DEL DOCUMENTO

Il presente documento rappresenta il Manuale di Conservazione di Siav S.p.A. e descrive il servizio di conservazione di documenti informatici per soggetti terzi, sia pubblici che privati, che decidono di affidare il servizio di conservazione del proprio archivio digitale al Conservatore Siav.

Il Manuale di Conservazione (d'ora in poi Manuale) illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, la comunità di riferimento, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del processo di conservazione.

Torna al sommario

1.1 Premessa

Il Manuale, per alcuni aspetti specifici, rimanda alla documentazione di seguito elencata:

- Organigramma e funzionigramma del Conservatore;
- Nomine, deleghe e incarichi interni al Conservatore;
- Piano della sicurezza;
- *Accordi di servizio* concordati con il Cliente (pubblica amministrazione o soggetto privato) affidatario del servizio di conservazione in outsourcing presso Siav;
- Manuale utente per l'utilizzo del Sistema di conservazione.

Per motivi di riservatezza tale documentazione è disponibile soltanto a seguito di una richiesta trasmessa dal Cliente al Conservatore tramite messaggio di posta elettronica certificata.

Il Conservatore esegue periodicamente un controllo di conformità del processo di erogazione del servizio di conservazione aggiornando periodicamente il presente documento anche in considerazione dell'evoluzione della normativa e degli standard tecnologici.

Per ciascun contratto relativo al servizio di conservazione, il Conservatore condivide con il Responsabile della conservazione dell'organizzazione gli "Accordi di servizio", un documento inclusivo delle specifiche operative, metadati, formati e modalità di versamento al sistema di conservazione delle tipologie documentali e delle aggregazioni informatiche. La documentazione approvata dal Cliente (d'ora in poi Produttore) è trasmessa tramite posta elettronica certificata.

Eventuali modifiche al Manuale di conservazione comportano una nuova versione dello stesso; le variazioni sono sottoposte all'Agenzia per l'Italia Digitale per l'approvazione prima della loro adozione.

1.2 Ambito

Siav S.p.A. con sede direzionale a Rubano (PD) è un'azienda di sviluppo software e di servizi informatici specializzata nella dematerializzazione e nella gestione documentale e nei processi digitali. Si caratterizza per le competenze specialistiche maturate nella realizzazione di progetti complessi e si distingue per la capacità di garantire con risorse proprie le attività di analisi, implementazione, personalizzazione, formazione e supporto.

Nell'ambito dei servizi eseguiti in outsourcing, a titolo indicativo e non esaustivo, sono citati:

- dematerializzazione dei documenti;
- elaborazione di documenti digitali e relativa gestione;
- registrazione di documenti contabili;
- gestione della fatturazione elettronica.

La divisione Digital Services Outsourcing (DSO) si occupa del servizio di "Conservazione digitale a norma dei documenti informatici" per gli archivi affidati in outsourcing al Conservatore Siav; tale servizio è stato sviluppato e progettato secondo la normativa vigente e i requisiti espressi dalla Circolare n. 65 del 10 aprile 2014 dell'Agenzia per l'Italia Digitale.

Il sistema di conservazione, per i documenti sottoposti a processo, assicura il mantenimento delle seguenti caratteristiche:

- affidabilità;
- leggibilità;
- reperibilità;
- autenticità;
- integrità.

2 TERMINOLOGIA (GLOSSARIO E ACRONIMI)

Di seguito sono elencate le definizioni e gli acronimi ricorrenti nel presente Manuale e negli Accordi di servizio.

Accesso	Operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici

Accreditamento	Riconoscimento 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 o alle funzioni dell'ente
AGID	Agenzia per l'Italia Digitale
AIP	Archival information package (Pacchetto di archiviazione) ossia il pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento all'interno del sistema di conservazione
AOO	Area organizzativa omogenea intesa come insieme di funzioni e di strutture, individuate all'interno dell'amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 445/2000
Archiflow	Sistema di gestione informatica dei documenti sviluppato da SIAV S.P.A.
Archivio	Complesso organico di documenti, fascicoli e aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività
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 al documento informatico e/o al processo
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
CA	Certification Authority
CAD o Codice	Codice dell'amministrazione digitale, Decreto legislativo n. 82 del 7 marzo 2005, aggiornato con Decreto legislativo n. 217 del 13 dicembre 2017
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 di voci individuate attraverso specifici metadati
Codice eseguibile	Insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici
Comunità di riferimento	Secondo lo standard OAIS è da intendersi come l'insieme degli utenti in grado di comprendere autonomamente l'informazione archiviata nella forma in cui è conservata e resa disponibile dal Sistema di conservazione
Conservatore accreditato	Soggetto, pubblico o privato, che svolge le attività di conservazione al quale sia stato riconosciuto, dall'AGID, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza. Le pubbliche amministrazioni che affidano a terzi la conservazione hanno l'obbligo di rivolgersi esclusivamente a conservatori accreditati
Conservazione	Insieme delle attività finalizzate a definire le politiche complessive del sistema di conservazione e a governare la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione
Contenuto informativo	È l'oggetto che si vuole conservare ossia un *Information Object* eventualmente al suo interno strutturato
Copia informatica di documento analogico	Documento informatico avente contenuto identico a quello del documento analogico da cui è tratto
Copia per immagine su supporto informatico di documento analogico	Documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto; tipicamente viene ottenuto mediante scansione del cartaceo

Copia informatica di documento informatico	Documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari
Copia di sicurezza	Copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 del DPCM 3 dicembre 2013
CRL	Certificate revocation list, ossia la lista dei certificati revocati o sospesi
Data center	Struttura utilizzata per ospitare computer e componenti associati quali dispositivi di telecomunicazioni e di storage, con adeguati livelli di prestazioni e di sicurezza
Data Protection Officer (DPO)	Persona giuridica individuata dal Conservatore all'esterno della propria struttura con l'assegnazione delle attività indicate dal Regolamento generale sulla protezione dei dati 2016/679, art. 39
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale
Dematerializzazione	Progressivo incremento della gestione documentale informatizzata all'interno delle organizzazioni (pubbliche amministrazioni e privati) e la conseguente sostituzione del supporto cartaceo in favore del documento informatico
Destinatario	Identifica il soggetto/sistema al quale il documento informatico è indirizzato
Digitalizzazione	Processo che, mediante opportuni strumenti tecnologici e un sistema documentale, consente la produzione nativa digitale dei documenti
DIP	Dissemination information package (Pacchetto di distribuzione) ossia il pacchetto informativo generato dal sistema di conservazione a seguito di una specifica richiesta effettuata da un utente

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
Documento analogico	La rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti; è unico quando non è possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi
Documento informatico	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Documento elettronico	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva
Domicilio digitale	Un indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal Regolamento (UE) 23 luglio 2014 n. 910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno valido ai fini delle comunicazioni elettroniche aventi valore legale (noto come Regolamento EIDAS)
DSO	Digital Services Outsourcing di Siav S.p.A.
Duplicato informatico	Documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario
Esibizione	Operazione che consente di visualizzare un documento conservato e di ottenerne copia
Estratto per riassunto	Documento nel quale si attestano in maniera sintetica ma esaustiva fatti, stati o qualità desunti da dati o documenti in possesso di soggetti pubblici
Evidenza informatica	Sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica

Extensible Markup Language	Linguaggio di markup (marcatura) il cui scopo è quello di consentire a sua volta la definizione di linguaggi di markup personalizzati attraverso l'utilizzo di markup tags
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
Firma elettronica	Insieme di dati in forma elettronica utilizzati come metodo di autenticazione informatica. Di fatto, si utilizza la firma elettronica nella digitazione del codice PIN oppure nell'inserimento delle credenziali, quali l'identificativo utente e password
Firma elettronica avanzata	Insieme di dati in firma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi per i quali il firmatario può conservare un controllo esclusivo
Firma elettronica qualificata	Si tratta di una firma elettronica avanzata creata da un dispositivo per la generazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche
Firma digitale	Particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e l'altra privata correlate tra loro che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici
Formato	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
FTP server	Programma che permette di accettare le connessioni in entrata e di comunicare con un client attraverso protocolli criptati S-FTP/FTPS
Formazione	Include le modalità di generazione del documento informatico, di un'aggregazione informatica o del pacchetto informativo previste dalla normativa vigente

Fruibilità	Indica la possibilità di accedere ai dati conservati e, in modo intelligibile, alle informazioni che contengono, che li accompagnano o che li correlano tra loro
Gestione documentale	Attività finalizzate alla registrazione di protocollo, alla classificazione, fascicolazione, assegnazione, reperimento, accesso e consultazione dei documenti amministrativi prodotti o acquisiti da un ente nell'esercizio delle sue funzioni
Hash	Funzione matematica che genera, a partire da una evidenza informatica, un'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
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
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 in maniera univoca
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 di un'opportuna funzione di hash su un'altra sequenza di bit
Insieme minimo di metadati del documento informatico	Complesso di informazioni minime da associare al documento informatico per identificarne la provenienza e garantirne la gestione, conservazione e accesso
Integrità	Insieme delle caratteristiche di un documento informatico che ne dichiarano le 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
Indice delle Pubbliche amministrazioni (IPA)	Sito web che riporta informazioni dettagliate sulle Pubbliche amministrazioni censite, quali strutture organizzative, contatti, indirizzi, uffici, etc.
Indice del pacchetto di archiviazione	File xml generato in fase di certificazione dei PDA che garantisce la possibilità di verificare la validità del dato conservato al momento dell'esibizione del documento
IPDA	Cfr. Indice del pacchetto di archiviazione
ISO	International Organization for Standardization ovvero l'Organizzazione internazionale per la normazione (Organizzazione per la definizione di norme tecniche)
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 da 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 e il processo di conservazione dei documenti informatici
Manuale di gestione	Strumento che descrive la gestione documentale (Regole tecniche per il protocollo informatico, DPCM 3 dicembre 2013, art. 5)
Marcatura temporale	Permette di associare data e ora certe e legalmente valide ad un documento informatico, consentendo quindi di associare una validazione temporale opponibile a terzi
Memorizzazione	Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici

Metadati	Insieme di dati associati al contenuto informativo (documento, fascicolo o aggregazione documentale informatica) per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la consultazione nel tempo.
Modello organizzativo	I modelli organizzativi possibili per l'espletamento del processo di conservazione prevedono l'affidamento del servizio in outsourcing oppure la gestione in house
OAIS	Open Archival Information System – ISO 14721:2012; standard di riferimento per lo sviluppo di Sistemi di Conservazione digitale
Originali non unici	I documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione
Pacchetto di archiviazione	Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento (PdA) – Cfr. AIP
Pacchetto di distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta (PdD) – Cfr. DIP
Pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato con il Conservatore (PdV) – Cfr. SIP
Pacchetto informativo	Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche)
PEC	Posta elettronica certificata
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'art. 68 del D.P.R. 28 dicembre 2000, n. 445

Piano generale della sicurezza	Documento per la pianificazione delle attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza
Presa in carico	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione
Processo di conservazione	Insieme delle attività finalizzate alla conservazione di dati, documenti e aggregazioni informatiche
Produttore	Persona fisica o giuridica, di norma diversa dal soggetto che ha firmato 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
Pubblico ufficiale	Il Responsabile della conservazione assicura la presenza di un pubblico ufficiale quando prevista
Rapporto di versamento (RdV)	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento trasmessi dal produttore
Registrazione informatica	Insieme delle informazioni risultanti da transazioni informatiche o dalla presentazione in via telematica di dati attraverso moduli o formulari resi disponibili in vario modo all'utente
Registro particolare	Registro informatico di particolari tipologie di atti o documenti; nell'ambito della pubblica amministrazione è previsto ai sensi dell'art. 53 del D.P.R. 28 dicembre 2000, n. 445
Registro di protocollo	Registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti
Repertorio informatico	Registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche con cui si formano atti e documenti secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica

Responsabile della conservazione (RDC)	Persona fisica i cui compiti generali sono quelli di definire e attuare le politiche complessive del Sistema di conservazione e di governarne la gestione con piena responsabilità e autonomia, in relazione al modello organizzativo della conservazione adottato. I compiti e il ruolo del Responsabile della conservazione, persona fisica designata dal Soggetto produttore dei documenti, sono stabiliti dall'art. 7, c. 1, del DPCM 3 dicembre 2013
Responsabile della funzione archivistica di conservazione (RFA)	Persona fisica individuata dal Conservatore con l'assegnazione delle attività indicate nel documento "Profili professionali", allegato alla circolare AGID n. 65/2014
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'art. 61 del D.P.R. 28 dicembre 2000, n. 445, che produce il pacchetto di versamento e ne effettua il suo trasferimento al sistema di conservazione
Responsabile del servizio di conservazione (RSC)	Persona fisica individuata dal Conservatore con l'assegnazione delle attività indicate nel documento "Profili professionali", allegato alla circolare AGID n. 65/2014
Responsabile del trattamento dei dati personali (RTD)	Persona fisica individuata dal Conservatore con l'assegnazione delle attività indicate nel documento "Profili professionali", allegato alla circolare AGID n. 65/2014
Responsabile della sicurezza dei sistemi per la conservazione (RSS)	Persona fisica individuata dal Conservatore con l'assegnazione delle attività indicate nel documento "Profili professionali", allegato alla circolare AGID n. 65/2014
Responsabile dei sistemi informativi per la conservazione (RSI)	Persona fisica individuata dal Conservatore con l'assegnazione delle attività indicate nel documento "Profili professionali", allegato alla circolare AGID n. 65/2014
Responsabile sviluppo e manutenzione del sistema di conservazione (RSM)	Persona fisica individuata dal Conservatore con l'assegnazione delle attività indicate nel documento "Profili professionali", allegato alla circolare AGID n. 65/2014
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; cfr. validazione temporale

Scarto	Distruzione di documenti e/o fascicoli ritenuti privi di valore amministrativo e di interesse storico culturale
Sistema di classificazione o titolario	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 (SDC)	Sistema di conservazione a norma dei documenti informatici, sviluppato e implementato da Siav; cfr. "Virgilio".
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
SIP	Submission Information Package (Pacchetto di versamento) ovvero il pacchetto informativo trasmesso dal Produttore al sistema di conservazione secondo un formato predefinito concordato con il Conservatore
Soggetto Produttore o Cliente	Cfr. Produttore
Staticità	Caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione
Titolare di firma elettronica	La persona fisica cui è attribuita la firma elettronica con accesso al dispositivo per la sua creazione, nonché alle applicazioni per la sua sottoscrizione
Transazione informatica	Particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche alla base dati
TSA	La Time Stamping Authority (TSA) è una organizzazione che rilascia marche temporali sincronizzate con il segnale emesso da un Istituto accreditato
Utente	Persona, ente o sistema che interagisce con i servizi di un sistema per la conservazione dei documenti informatici, al fine di fruire le informazioni di interesse

URL	Uniform Resource Locator - Sistema standard di nomenclatura per identificare in maniera univoca una risorsa su Internet
Validazione temporale elettronica	Dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento
Validazione temporale elettronica qualificata	Una validazione temporale elettronica qualificata collega la data e ora ai dati in modo da escludere la possibilità di modifiche non rilevabili dei dati; si basa su una fonte accurata di misurazione del tempo collegata al tempo universale coordinato ed è apposta mediante una firma elettronica avanzata
Versamento agli Archivi di Stato	Trasmissione, ad opera dei Responsabili della gestione documentale e della conservazione, della documentazione agli Archivi di Stato o all'Archivio Centrale dello Stato secondo quanto previsto dalla normativa in materia di beni culturali
Virgilio	Sistema di conservazione a norma dei documenti informatici sviluppato da SIAV S.p.A.

Torna al sommario

3 NORMATIVA E STANDARD DI RIFERIMENTO

Di seguito sono riportati i principali riferimenti normativi e standard inerenti il processo di conservazione.

3.1 Normativa di riferimento

- Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- Legge 7 agosto 1990, n. 241, Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi e successive modificazioni;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa e successive modificazioni;
- Decreto legislativo 22 gennaio 2004, n. 42 e s.m.i., Codice dei Beni Culturali e del Paesaggio;
- Decreto legislativo 7 marzo 2005 n. 82, Codice dell'amministrazione digitale, aggiornato con Decreto legislativo n. 217 del 13 dicembre 2017, pubblicato in Gazzetta ufficiale n. 9 del 12 gennaio 2018;
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013, Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71 del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni;
- Decreto del Presidente del Consiglio dei Ministri 21 marzo 2013, Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico, oppure in caso di conservazione digitale, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013, Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'Amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013, Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1

e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82;

- Decreto Presidente del Consiglio dei Ministri 13 novembre 2014, Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23 -bis, 23 -ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82.

Le Regole tecniche in materia di formazione, protocollo informatico e conservazione (DPCM 13 novembre 2014 e DPCM 3 dicembre 2013) condividono i seguenti allegati:

- *Allegato 1 "Glossario",* contiene la descrizione dei termini maggiormente utilizzati nei testi normativi in ambito di formazione, gestione e conservazione dei documenti informatici;

- *Allegato 2 "Formati",* fornisce indicazioni per i formati da adottare nelle fasi di formazione, gestione e conservazione;

- *Allegato 3 "Standard e specifiche tecniche"* fornisce indicazioni sugli standard e le specifiche tecniche da ritenersi coerenti con le regole tecniche del documento informatico e del sistema di conservazione;

- *Allegato 4 "Specifiche tecniche del Pacchetto di archiviazione",* illustra la struttura descrittiva dell'indice del pacchetto di archiviazione;

- *Allegato 5 "Metadati del documento e del fascicolo",* illustra la struttura dei metadati relativi al documento informatico, al documento amministrativo informatico e al fascicolo informatico o aggregazione documentale informatica.

- Circolare AGID 10 aprile 2014, n. 65 (G.U. n. 89 del 16/04/2014), Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82;
- Decreto del Ministero dell'Economia e delle Finanze del 17 giugno 2014, Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto;
- Regolamento (UE) n. 910/2014 eIDAS (electronic IDentification Authentication and Signature), base normativa comune per i Paesi membri dell'U.E. per quanto riguarda i servizi fiduciari, i mezzi di identificazione elettronica e le modalità di interazioni elettroniche sicure fra cittadini, imprese e pubbliche amministrazioni;
- Decreto Legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali, aggiornato con Decreto Legislativo 10 agosto 2018 n. 101;
- Regolamento generale sulla protezione dei dati n. 679 del 27 aprile 2016 (GDPR) pubblicato in Gazzetta ufficiale europea L. 119 il 4 maggio 2016;
- Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, articolate in un documento principale e in sei allegati che ne costituiscono parte integrante.

  Gli allegati sono i seguenti:

- Allegato 1 - Glossario dei termini e degli acronimi
- Allegato 2 - Formati di file e riversamento
- Allegato 3 - Certificazione di processo
- Allegato 4 - Standard e specifiche tecniche
- Allegato 5 – Metadati
- Allegato 6 - Comunicazione tra AOO di Documenti amministrativi protocollati.

Le Linee Guida sulla formazione, gestione e conservazione dei documenti informatici sono state pubblicate sul sito dell'Agenzia per l'Italia digitale il 9 settembre 2020 e si applicano a partire dal duecento settantesimo giorno successivo alla loro entrata in vigore. Siav procederà con l'adeguamento del presente documento e di quanto previsto dalle Linee Guida entro tale termine.

Torna al sommario

3.2 Standard di riferimento

Di seguito gli standard di riferimento previsti dalla normativa vigente.

- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ISO/IEC 27001:2017, 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;
- UNI ISO 15489-1: 2006 Informazione e documentazione - Gestione dei documenti di archivio - Principi generali sul record management;
- UNI ISO 15489-2: 2007 Informazione e documentazione - Gestione dei documenti di archivio – Linee Guida sul record management;
- ISO/TS 23081-1:2006 Information and documentation - Records management processes – Metadata for records – Part 1 – Principles, Quadro di riferimento per lo sviluppo di un sistema di metadati per la gestione documentale;

- ISO/TS 23081-2:2007 Information and documentation - Records management processes – Metadata for records – Part 2 – Conceptual and implementation issues, Guida pratica per l'implementazione.

Il 7 maggio 2020 è stata emessa una nuova versione dello standard UNI SInCRO, norma UNI 11386:2020 "Supporto all'interoperabilità nella conservazione e recupero degli oggetti digitali (SInCRO)". I conservatori accreditati che erogano il servizio di conservazione dovranno continuare a riferirsi alla versione 2010 dello standard SInCRO e procedere con l'adeguamento alla versione del 2020 entro il termine previsto per l'applicazione delle Linee Guida ossia a partire dal duecento settantesimo giorno successivo alla loro entrata in vigore. Per un approfondimento sulla nuova versione dello standard si rimanda al sito dell'Osservatorio normativo SIAV, https://www.siav.com/it/unisincro-evoluzione-conservazione-supporto-interoperabilita/.

Torna al sommario

4 RUOLI E RESPONSABILITÀ

4.1 Dati identificativi del Conservatore

Siav S.p.A. progetta e sviluppa software e soluzioni informatiche ad alto valore tecnologico grazie all'esperienza maturata nel tempo per lo svolgimento delle attività legate alla gestione e conservazione dei documenti.

Il Conservatore possiede la certificazione UNI CEI EN ISO/IEC 27001:2017 il cui ambito di applicazione è la progettazione ed erogazione di servizi di dematerializzazione, gestione documentale e conservazione digitale; erogazione del servizio di registrazione documenti contabili e del servizio di trasmissione delle fatture elettroniche da e verso soggetti pubblici e privati.

Denominazione	SIAV S.P.A.
Partita IVA e Codice Fiscale	02334550288
Indirizzo sede legale	Via Rossi 5/n - 35030 Rubano (PD)
Legale rappresentante	Nicola Voltan
Referente tecnico (Operations Manager)	Roberto Pinelli

Posta elettronica	info@siav.it
Posta elettronica certificata	siav@pec.siav.it
Sito web istituzionale	www.siav.it
Telefono	049 897 97 97
Fax	049 897 88 00

I riferimenti al sito primario e al sito secondario sono indicati nel Piano della sicurezza e negli Accordi di servizio.

Nel processo di conservazione interviene il personale afferente a diverse aree dell'organigramma aziendale che partecipa al processo di conservazione condividendo metodologie e specifiche procedure. Gli operatori della divisione DSO sono stati individuati e formalmente incaricati per svolgere le attività relative al servizio di conservazione dal Responsabile dello sviluppo e della manutenzione del sistema di conservazione. L'Operations manager, d'intesa con il Responsabile del servizio di conservazione, ha individuato i profili dei responsabili previsti dalla Circolare AGID n. 65/2014 indicati di seguito.

Ruolo	Nominativo	Attività di competenza	Periodo nel ruolo	Eventuali deleghe
Responsabile del servizio di conservazione (RSC)	Nicola Voltan	• Definisce le politiche complessive del sistema di conservazione e la gestione del sistema di conservazione; • Definisce le caratteristiche e i requisiti del sistema di conservazione in conformità alla normativa vigente; • Assicura la corretta erogazione del servizio di conservazione in outsourcing; • Definisce le convenzioni e gli aspetti tecnico-operativi; convalida i disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione	Dal 28 settembre 2006[1]	
Responsabile del trattamento dei dati personali (RTD)	Nicola Voltan	• Garantisce il rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; • Garantisce che il trattamento dei dati avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza	Dal 28 settembre 2006	

[1] Atto aggiornato il 12 settembre 2017 registrato nel Libro dei verbali del Consiglio di amministrazione.

Ruolo	Nominativo	Attività di competenza	Periodo nel ruolo	Eventuali deleghe
Responsabile dello sviluppo e della manutenzione del sistema di conservazione (RSM)	Morgan Rizzolo	• Coordina lo sviluppo e la manutenzione delle componenti hardware e software del sistema di conservazione; • Pianifica e monitora i progetti di sviluppo del sistema di conservazione; •Monitora la documentazione relativa alla manutenzione del sistema di conservazione; • Si interfaccia con l'ente produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche; • Gestisce lo sviluppo di siti web e portali connessi al servizio di conservazione d'intesa con l'Area Sviluppo	Dal 1 ottobre 2014	Lettere di incarico per gli operatori della divisione DSO

Ruolo	Nominativo	Attività di competenza	Periodo nel ruolo	Eventuali deleghe
Responsabile della funzione archivistica di conservazione (RFA)	Rosalia Telese	•Collabora all'implementazione delle procedure relative al processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, descrizione archivistica dei documenti e delle aggregazioni documentali trasferite, di esibizione, accesso e fruizione del patrimonio documentario e informativo conservato; • Definisce il set di metadati di conservazione dei documenti e dei fascicoli informatici; • Monitora il processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione; • Collabora con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza	Dal 1 ottobre 2014	

Ruolo	Nominativo	Attività di competenza	Periodo nel ruolo	Eventuali deleghe
Responsabile dei sistemi informativi per la conservazione (RSI)	Alberto Veratelli	• Effettua il monitoraggio delle componenti hardware e software del sistema di conservazione; • Effettua il monitoraggio del mantenimento dei livelli di servizio concordati con l'ente produttore; • Segnala eventuali difformità delle componenti del sistema al Responsabile del servizio di conservazione e pianifica le azioni correttive; • Pianifica lo sviluppo delle infrastrutture tecnologiche del sistema di conservazione; • Controlla e verifica i livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione	Dal 10 settembre 2019	
Responsabile della sicurezza dei sistemi per la conservazione (RSS)	Davide Mietto	• Effettua il monitoraggio per garantire i requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; • Segnala eventuali difformità al Responsabile del servizio di conservazione individuando e pianificando le azioni correttive	Dal 1 ottobre 2014	

Ruolo	Nominativo	Attività di competenza	Periodo nel ruolo	Eventuali deleghe
Consulente interno	Daniela Perrone	Supporto tecnico – normativo per le attività afferenti il servizio di conservazione dei documenti fiscali.	Dal 3 novembre 2014	

L'Area risorse umane effettua l'aggiornamento e l'archiviazione degli atti di delega del Responsabile del servizio di conservazione per i Responsabili e delle lettere di incarico da parte del Responsabile dello sviluppo e della manutenzione.

Torna al sommario

4.1 Modelli organizzativi

Una qualsiasi organizzazione, pubblica amministrazione o soggetto privato, può eseguire il processo di conservazione adottando uno dei seguenti modelli:

- in house;
- in outsourcing.

Il modello in house prevede l'installazione del sistema di conservazione Virgilio presso la sede del Cliente e l'espletamento del processo di conservazione all'interno della struttura organizzativa attraverso il Responsabile della conservazione ed eventuali delegati; in questo caso Siav S.p.A., in qualità di fornitore del sistema di conservazione a norma, svolge attività di supporto per la redazione del Manuale e/o eventuali servizi concordati nel contratto di fornitura. I profili coinvolti nelle varie fasi di processo sono indicati nella tabella sottostante.

Modello organizzativo in house	
Ruolo	***Organizzazione di appartenenza (Conservatore – Produttore)***
Responsabile della conservazione	Produttore
Delegati del Responsabile della conservazione	Produttore
Utenti	Interni al Produttore o esterni

Il presente Manuale descrive il processo di conservazione eseguito per i Clienti che affidano il servizio in outsourcing al Conservatore Siav S.p.A. L'affidamento del servizio viene formalizzato e sottoscritto tra

Produttore e Conservatore; il Produttore, ente pubblico o soggetto privato, adotta un proprio Manuale di conservazione e sottoscrive il documento “Accordi di servizio” predisposto dal Conservatore. Il servizio è erogato dalla divisione Digital services outsourcing (DSO) di Siav nel rispetto dei requisiti di continuità, sicurezza fisica e logica, backup, monitoraggio, presidio operativo-sistemistico. Siav garantisce nel tempo l’aderenza del servizio offerto alla vigente normativa, aggiornando il software e informando tempestivamente i Clienti di ogni variazione di rilievo.

I profili coinvolti nelle varie fasi del processo in caso di affidamento in outsourcing sono indicati nella tabella sottostante.

Modello organizzativo in outsourcing	
Ruolo	***Organizzazione di appartenenza (Conservatore – Produttore)***
Responsabile della conservazione	Produttore
Eventuali Delegati o Referenti	Produttore
Responsabile del servizio di conservazione	Conservatore
Responsabili, delegati e incaricati coinvolti	Conservatore
Responsabile per l'attivazione del servizio	Conservatore (Project Manager)
Utenti	Interni al Produttore o esterni

A prescindere dal modello organizzativo adottato, il Produttore individua al proprio interno il Responsabile della conservazione e lo nomina con atto formale. Il Produttore che affida il servizio di conservazione all'outsourcer (conservatore accreditato) resta titolare e responsabile dei dati, documenti e aggregazioni sottoposte a processo di conservazione.

Di seguito i dettagli dei soggetti coinvolti nel processo di conservazione:

- il Titolare dei documenti informatici trasmessi in conservazione è il Produttore (il Cliente), che attraverso il proprio Responsabile della conservazione affida al Conservatore la gestione del servizio di conservazione;
- il Conservatore Siav S.p.A. ha individuato al proprio interno gli incaricati e i responsabili previsti dalla normativa;
- il Responsabile del servizio di conservazione (RSC) è la persona fisica del Conservatore che attraverso i propri delegati svolge le attività connesse al servizio di conservazione come descritto nel presente Manuale. Le attività affidate al Responsabile del servizio di conservazione sono elencate nell'atto di affidamento sottoscritto con il Referente o Responsabile della conservazione del produttore;
- l'utente *(consumer)* è il ruolo esercitato da una persona, ente o sistema che richiede l'accesso alle informazioni conservate e che quindi interagisce con il SDC. Non necessariamente il *consumer* coincide con il *producer* in quanto la comunità di riferimento potrebbe essere molto vasta, basti pensare ad esempio alla condivisione di un fascicolo/aggregazione documentale tra più Amministrazioni. Il sistema di conservazione permette ai soggetti autorizzati dal RDC

l'accesso diretto, anche da remoto, ai documenti informatici conservati e consente la produzione di un pacchetto di distribuzione; negli "Accordi di servizio" sono indicati i nominativi delle persone abilitate all'accesso al SDC;

- l'Organismo di tutela e vigilanza (in riferimento alle amministrazioni pubbliche) è da intendersi il Ministero per i beni e le attività culturali e per il turismo (MiBACT) che esercita funzioni di tutela e vigilanza degli archivi di enti pubblici o di enti privati dichiarati di interesse storico particolarmente rilevante e autorizza le operazioni di scarto e trasferimento della documentazione conservata ai sensi del Codice dei beni culturali. La tutela e vigilanza sugli archivi di enti pubblici non statali è esercitata dal MiBACT, tramite le Soprintendenze archivistiche competenti territorialmente;

- l'Agenzia per l'Italia digitale (AGID) svolge le attività di controllo e richiede ai conservatori accreditati un report con l'elenco dei contratti attivi e i dati afferenti il servizio di conservazione.

Infine le terze parti interessate sono:

- Certification Authority accreditate AGID per i certificati crittografici utilizzati nel processo di firma;
- Time Stamping Authority utilizzate nel processo di apposizione del riferimento temporale.

Torna al sommario

4.2 Suddivisione delle responsabilità

Il Produttore dei documenti informatici è il Cliente che affida al Conservatore la gestione del servizio di conservazione secondo le politiche complessive in uso presso lo stesso.

Il Conservatore Siav S.p.A. ha individuato all'interno della propria divisione DSO il personale coinvolto nelle varie fasi di processo come indicato nelle lettere di incarico predisposte dal Responsabile dello sviluppo e manutenzione; il sistema di conservazione sviluppato dal Conservatore per l'espletamento del servizio di conservazione sia in house che in outsourcing è Virgilio.

Il Conservatore è responsabile in merito alle procedure adottate nell'espletamento del processo di conservazione mentre la responsabilità del contenuto dei documenti traferiti al sistema di conservazione è in carico al Produttore dell'archivio.

È obbligo del Conservatore effettuare la conservazione dei documenti informatici trasmessi dal Produttore allo scopo di assicurare, dalla presa in carico fino allo scarto, la conservazione a norma, garantendone, tramite l'adozione di regole, procedure e tecnologie, le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità.

Il Conservatore è il soggetto giuridico al quale sono affidate contrattualmente le attività previste per l'espletamento del processo di conservazione.

Le attività in carico al Produttore dell'archivio sono:

- verifica e approvazione del documento *Accordi di servizio* contenente la descrizione delle tipologie documentali con relativi tempi di versamento e conservazione, formati e metadati;

- produzione del Pacchetto di versamento con documenti da sottoporre a conservazione e relativi metadati descrittivi;

- trasmissione del Pacchetto di versamento al Conservatore e verifica dell'esito tramite la visualizzazione del Rapporto di versamento prodotto in automatico dal Sistema di conservazione.

Alcune attività, quali ad esempio l'estrazione dei PdV dai sistemi in uso presso il Produttore e successivo versamento, possono essere effettuate dal Conservatore in base a quanto previsto dal contratto di fornitura. Il Conservatore garantisce la tutela degli interessati in ottemperanza a quanto disposto dal D. Lgs. 196/2003, dal D. Lgs. 101/2018 e dal Regolamento generale sulla protezione dei dati n. 679 del 27 aprile 2016 (GDPR); il Produttore è quindi informato sui diritti di accesso ai dati personali e quanto previsto dalla normativa vigente. Nelle Pubbliche amministrazioni è il Responsabile di conservazione del Soggetto Produttore che, d'intesa con il Responsabile della gestione documentale, con il Responsabile privacy e con il Responsabile della funzione archivistica, tutti appartenenti alla medesima organizzazione, affida al Conservatore accreditato alcune attività concernenti il Servizio, nominandolo Responsabile del trattamento ai sensi dell'art. 28 del Regolamento 679/2016/UE per le tipologie documentali, per i dati e per la durata indicati nel contratto e negli "Accordi di servizio".

I dati personali sono trattati dal Conservatore con strumenti automatizzati ai sensi della normativa in vigore per il tempo strettamente necessario a conseguire gli scopi per cui sono stati raccolti e nel rispetto delle indicazioni impartite dal Titolare , attuando specifiche misure di sicurezza per prevenire la perdita dei dati, usi illeciti o non corretti e accessi non autorizzati.

In particolare:

- Responsabile al trattamento: Siav S.p.A. con sede legale in Rubano (PD), via Rossi n. 5, nella persona dell'Amministratore delegato, dott. Nicola Voltan;

- Responsabile del servizio di conservazione: dott. Nicola Voltan;

- DPO (Responsabile della protezione dei dati): dott. Luigi Recupero;

- Scopo del trattamento: servizio di conservazione digitale a norma di documenti informatici.

Di seguito i contatti del DPO (Responsabile della protezione dei dati) individuato dal Conservatore:

DPO	Partiva IVA	Via/Piazza	CAP	Comune	Nominativo del DPO
Società LTA S.r.l.	14243311009	Via della Conciliazione n. 10	00193	Roma	Luigi Recupero

Torna al sommario

5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Organigramma

Di seguito l'estratto dell'organigramma del Conservatore con indicazione delle varie divisioni aziendali di riferimento.

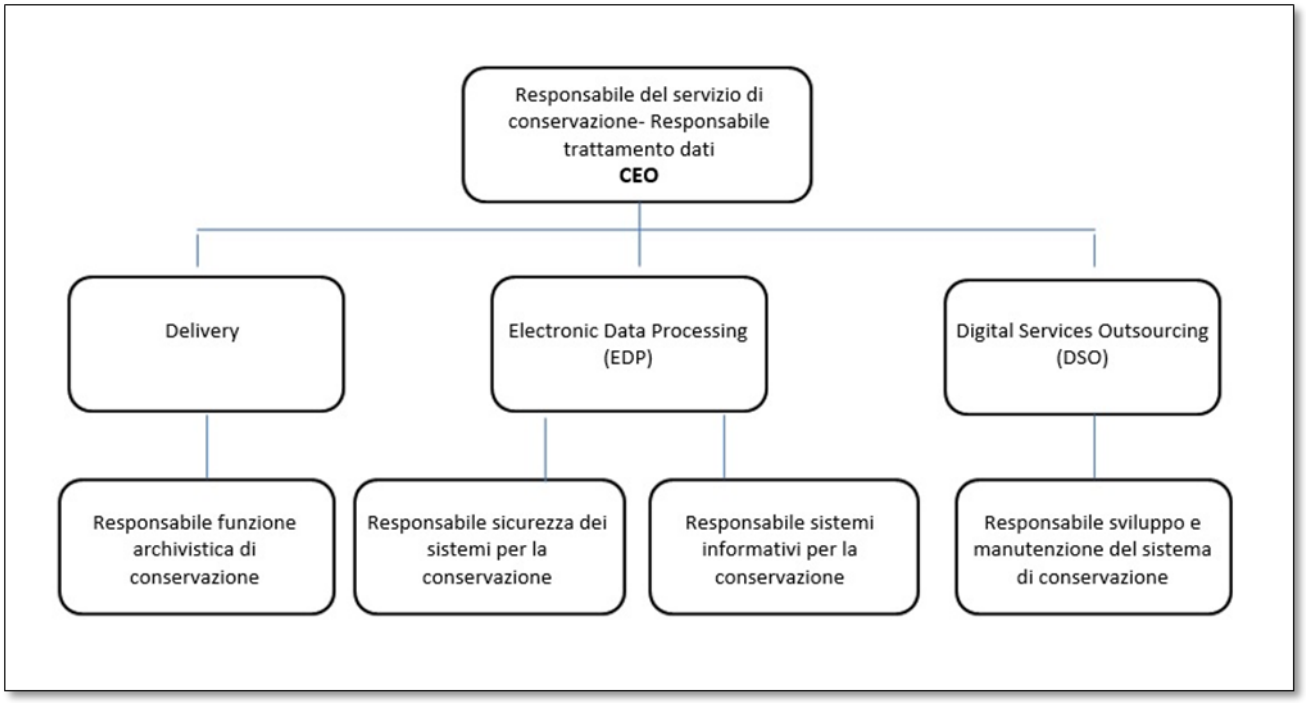


Figura 1 – Organigramma

Torna al sommario

5.2 Strutture organizzative

In questo paragrafo sono descritte le strutture organizzative che intervengono nelle principali attività del servizio di conservazione. Le aree interessate sono:

- Direzione (CEO);
- Area commerciale;
- Delivery e Area operativa (DSO);
- Sistemi informativi (EDP).

Il servizio di conservazione effettuato dal Conservatore include un complesso di attività sintetizzate nella tabella sottostante con relativa area competente e il personale coinvolto.

Attività proprie di ciascun contratto di servizio		
FASE 1: *Attività preliminari all'avvio del servizio*		
Attività	***Area competente***	***Personale coinvolto***
Richiesta di attivazione del servizio di conservazione mediante la contrattualizzazione dell'attività in outsourcing	Area Commerciale	Project manager (Responsabile di progetto)
Analisi delle tipologie documentali da conservare e relativi requisiti tecnici-archivistici; assessment delle componenti hardware e software coinvolte	Delivery e Area operativa	RFA, RSM e Responsabile di progetto
Predisposizione dell'infrastruttura hardware e software e analisi dei costi di manutenzione	Sistemi informativi	RSS, RSI
Definizione delle procedure operative e analisi di eventuali pre-lavorazioni	Delivery e Area operativa	Ogni responsabile interviene per la parte di propria competenza
Variazioni e/o implementazioni di ulteriori procedure	Area Commerciale, Delivery e Area operativa	Ogni responsabile interviene per la parte di propria competenza
FASE 2: *Attivazione del servizio*		
Attività	***Area competente***	***Personale coinvolto***
Redazione della documentazione (Accordi di servizio e atto di affidamento)	Delivery e Area operativa	RFA, RSM, Responsabile di progetto
Raccolta requisiti e informazioni del Produttore e dell'archivio sottoposto a	Conservatore e Produttore	RDC del produttore e Responsabile di progetto

conservazione		
Approvazione e trasmissione degli Accordi di servizio e atto di affidamento	Produttore	RDC del produttore sottoscrive e trasmette la documentazione al Conservatore tramite PEC
Attività di test per interfaccia tra i sistemi e verifica rispondenza delle specifiche concordate	Sistemi informativi e Area operativa	RSS, RSM
Generazione e invio delle credenziali di accesso al SDC	Sistemi informativi e Area operativa	RSS, RSM
Assistenza per configurazione di moduli aggiuntivi e/o ulteriori funzionalità	Sistemi informativi e Area operativa	RSS, RSM, RFA, Responsabile di progetto
FASE 3: *Acquisizione, verifica e gestione PDV*		
Attività	***Area competente***	***Personale coinvolto***
Generazione e invio dei PdV secondo le modalità e le tempistiche concordate	Produttore	Sistemi
Acquisizione PdV e generazione del RdV	Area operativa	SDC Virgilio
Eventuale notifica di anomalia	Area operativa	SDC Virgilio
Risoluzione dell'anomalia in base alle specifiche concordate	Area operativa	RSM e operatori DSO
Eventuale re-invio del PdV in base alle specifiche concordate	Produttore	Sistemi
Presa visione del RdV	Produttore	Sistemi
FASE 4: *Preparazione e gestione PDA e PDD*		
Attività	***Area competente***	***Personale coinvolto***
Preparazione e gestione dei PdA	Area operativa	RSM e operatori DSO
Certificazione del PdA con apposizione di firma digitale e marca temporale	Area operativa	RSM e operatori DSO

Invio notifica al Produttore di avvenuta certificazione del PdA	Area operativa	RSM e operatori DSO
Generazione delle copie di sicurezza del PdA	Area operativa	RSM e operatori DSO
Gestione dei PdD e delle richieste di accesso al SDC per la consultazione e l'esibizione	Area operativa	RSM e operatori DSO
Produzione di duplicati e copie informatiche su richiesta	Area operativa	RSM e operatori DSO (lato applicativo); RSS per quanto riguarda l'infrastruttura
FASE 5: *Scarto*		
Attività	***Area competente***	***Personale coinvolto***
Scarto dei PdA a seguito della trasmissione dell'elenco di scarto approvato dalla Soprintendenza archivistica competente territorialmente	Delivery, Area operativa e Produttore	RSC, RSM, RFA
Conservazione degli elenchi di scarto e/o del piano di conservazione trasmesso dal Produttore	Delivery, Area operativa e Produttore	RSC, RSM, RFA
FASE 6: *Attività di monitoraggio e controllo*		
Attività	***Area competente***	***Personale coinvolto***
Verifica dell'integrità e leggibilità dei PdA conservati	Area operativa	RSM e operatori DSO
Verifica delle componenti del sistema di conservazione	Area operativa e Sistemi informativi	RSI, RSS e operatori DSO
Verifica periodica di conformità alla normativa e agli standard di riferimento	Delivery e Area operativa	RFA e Consulente interno
Conduzione e manutenzione del SDC e	Sistemi informativi	RSS, RSI

change management		
Monitoraggio del sistema di conservazione	Sistemi informativi e Area operativa	RSM e operatori DSO

Torna al sommario

Si precisa che in base ai contratti stipulati con i produttori, il personale coinvolto nelle fasi di processo potrebbe variare.

Ogni responsabile di Area informa i propri collaboratori in merito alle procedure per la gestione degli interventi ed eventuale variazione delle stesse; la Direzione e l'Area Risorse umane mettono a disposizione corsi di formazione, anche su diretta indicazione del collaboratore.

Il Conservatore attiva il servizio di conservazione ad avvenuta ricezione degli Accordi di servizio e dell'atto di affidamento, entrambi trasmessi tramite posta elettronica certificata dal Responsabile della conservazione del Produttore. La gestione e archiviazione di tale documentazione è in carico alla Segreteria della Sede Direzionale.

Le comunicazioni tecniche ed eventuali richieste dei produttori sono gestite tramite posta elettronica ordinaria (PEO) dal Responsabile di progetto.

6. TIPOLOGIE DOCUMENTALI SOTTOPOSTE A CONSERVAZIONE

Il sistema di conservazione *Virgilio* effettua la conservazione del contenuto informativo ossia dell'oggetto che si vuole conservare. Il contenuto informativo corrisponde a dati, documenti e aggregazioni con relativi metadati che garantiscono la corretta interpretazione e comprensione del content information per un periodo indefinito di tempo.

Le tipologie documentali sottoposte a conservazione sono di seguito elencate:

- documenti protocollati in entrata, in partenza e interni;
- registro giornaliero di protocollo;
- registro giornaliero delle modifiche di protocollo;
- provvedimenti, contratti, determine, ecc.;
- libri e registri sociali e contabili;
- libro unico del lavoro;

- messaggi di posta elettronica certificata;
- fatture attive e passive;
- documenti fiscali.

Per le Pubbliche amministrazioni si segnala l'obbligo di conservare a norma anche i fascicoli informatici.

Le informazioni di conservazione (PDI - Preservation Description Information) si applicano al contenuto informativo e sono necessarie per garantire che lo stesso sia chiaramente identificabile per comprenderne il contesto di creazione.

Le informazioni PDI, predisposte dal Produttore, costituiscono metadati rilevanti per la conservazione a lungo termine dei documenti; tali informazioni sono articolate in cinque sezioni:

- *Provenance information* - informazioni relative alla provenienza del contenuto informativo ovvero chi ne ha avuto la custodia;
- *Reference information* - informazioni che identificano in maniera univoca l'oggetto digitale sottoposto a conservazione (ad es. il numero e la data di protocollo);
- *Fixity information* - informazioni relative alla verifica di validità del certificato di firma e dell'impronta del documento;
- *Context information* - informazioni che mostrano le relazioni esistenti tra il contenuto informativo e il contesto in cui è stato prodotto;
- *Access rights information* - informazioni sulle restrizioni previste per l'accesso ai contenuti informativi, sia in fase di conservazione che di consultazione.

Le caratteristiche, i formati e metadati delle tipologie documentali sottoposte a conservazione sono condivisi con il Produttore e definiti negli "Accordi di servizio".

Torna al sommario

6.1 Metadati

Il contenuto informativo è caratterizzato da metadati minimi obbligatori e da eventuali metadati aggiuntivi. I metadati, anche noti come attributi o proprietà permettono la descrizione, gestione e consultazione dell'oggetto digitale sottoposto a conservazione.

Nei paragrafi a seguire sono riportati i metadati delle macro-tipologie documentali:

- documento informatico;
- fascicolo informatico;
- registro giornaliero di protocollo;
- documento informatico avente rilevanza fiscale.

Si precisa che eventuali metadati aggiuntivi delle tipologie documentali trasferite in conservazione sono indicati negli "Accordi di servizio" concordati tra Conservatore e Produttore. Negli Accordi di servizio sono riportate anche modalità e tempistiche di trasferimento dei pacchetti informativi. Il Produttore è responsabile della corretta valorizzazione dei metadati trasferiti al sistema di conservazione.

Torna al sommario

6.1.1 Documento informatico

Il set di metadati minimi del documento informatico è il seguente:

Metadato	Descrizione
Identificativo univoco	Sequenza di non oltre venti caratteri alfanumerici associati in maniera univoca e persistente al documento informatico così da garantirne l'identificazione
Data	Data di formazione del documento valorizzata con gg/mm/aaaa
Oggetto	Sintesi del contenuto del documento
Soggetto produttore	Responsabile della produzione del documento informatico
Destinatario	Se disponibile
Impronta	La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione di un'opportuna funzione di hash su un'altra sequenza di bit

Nelle specifiche predisposte dal Conservatore sono previsti ulteriori metadati quali:

- numero di protocollo;
- data di protocollo;
- indice di classificazione;
- indicazione degli allegati.

Inoltre è possibile personalizzare il set di metadati in base alle esigenze del Produttore e alle peculiarità della tipologia documentale sottoposta a conservazione.

L'apposizione di una firma digitale o di un altro tipo di firma elettronica qualificata, per il documento informatico, basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione; pertanto è necessario agire per preservare l'autenticità di un documento informatico sottoscritto oltre il termine di scadenza del certificato e per far ciò risulta necessario avvalersi di un riferimento temporale opponibile a terzi. Tra le diverse tipologie di riferimenti temporali opponibili a terzi, quello più conosciuto ed efficace è senza dubbio la cosiddetta "marca temporale", definita dall'art. 1, comma 1, lettera i), del DPCM 22 febbraio 2013, come "il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo." Considerato che le marche temporali devono essere conservate dal Certificatore Accreditato per un periodo non inferiore a 20 anni, la firma digitale mantiene la sua validità per un identico lasso temporale.

Torna al sommario

6.1.2 Fascicolo informatico

Il set di metadati minimi del fascicolo informatico è il seguente:

Metadato	Descrizione
Identificativo univoco	Sequenza di caratteri alfanumerici associati in maniera univoca e persistente al fascicolo informatico così da garantirne l'identificazione
Amministrazione titolare	Amministrazione titolare del procedimento che cura la costituzione e gestione del fascicolo
Amministrazione partecipante	Amministrazione che partecipa all'iter del procedimento
Responsabile del procedimento amministrativo	Responsabile del procedimento amministrativo
Oggetto	Sintesi del contenuto del fascicolo
Documento	Elenco degli identificativi dei documenti contenuti nel fascicolo

Possono essere previsti ulteriori metadati quali:

- tipologia di fascicolo (per affare, per procedimento, per persona fisica o giuridica, ecc.);
- data di apertura del fascicolo;
- data di chiusura del fascicolo;
- indice di classificazione.

Torna al sommario

6.1.3 Registro giornaliero di protocollo

Il set di metadati del registro giornaliero di protocollo è il seguente:

Metadato	Descrizione
Identificativo univoco	Identificativo univoco restituito dal Sistema di gestione documentale
Data di chiusura	Data di creazione del registro
Soggetto produttore	Nominativo dell'operatore oppure del Sistema che ha prodotto il registro
Impronta del documento informatico	Restituita automaticamente dal Sistema in fase di formazione del registro
Codice identificativo dell'amministrazione	Codice IPA
Denominazione dell'amministrazione	Denominazione dell'amministrazione (Produttore)
Codice identificativo dell'area organizzativa omogenea	Codice AOO (può coincidere con il codice IPA)
Denominazione Ufficio Responsabile	Ufficio che ha in carico la verifica del Registro giornaliero
Responsabile	Responsabile della gestione documentale o Responsabile della conservazione
Oggetto	Valorizzato con "Registro giornaliero di protocollo"
Codice identificativo del registro	Valorizzato con un codice alfanumerico
Numero progressivo del registro e anno	Numero progressivo e anno di riferimento
Numero della prima registrazione	Numero della prima registrazione effettuata sul registro nella giornata di riferimento
Numero dell'ultima registrazione	Numero dell'ultima registrazione effettuata sul registro nella giornata di riferimento
Data della prima registrazione	Data della prima registrazione effettuata sul registro nella giornata di riferimento
Data dell'ultima registrazione	Data dell'ultima registrazione effettuata sul registro nella giornata di riferimento

Il RdV restituito dal SDC e reso disponibile al Produttore include anche il numero di pagine del registro e l'indice di classificazione; il Produttore è responsabile della corretta valorizzazione dei metadati sopra elencati.

Torna al sommario

6.1.4 Documento informatico avente rilevanza fiscale

Il set di metadati previsto per il documento informatico con rilevanza fiscale è il seguente:

Metadato	**Descrizione**
Identificativo univoco	Identificativo univoco del documento calcolato dal SDC
Numero/Registro protocollo IVA	Numero di registrazione del documento nel sistema contabile
Data registrazione	Formato GG/MM/AAAA (data di contabilizzazione)
Numero Fattura	Numero univoco contabile del documento
Data Documento	Formato GG/MM/AAAA, la data riportata in fattura dal fornitore
Numero documento fornitore	Numero di fattura del fornitore
Ragione sociale/Partita IVA/Codice fiscale fornitore	Ragione sociale, partita iva e il codice fiscale del fornitore
Ragione sociale/Partita IVA/Codice fiscale Cliente	Ragione sociale, partita iva e il codice fiscale del cliente (destinatario fattura)

Negli Accordi di servizio predisposti dal Conservatore sono indicati ulteriori metadati valorizzati in base alle esigenze e richieste del Produttore; infine in base alle modalità di lavorazione e al contratto stipulato sono possibili eventuali pre-lavorazioni.

Torna al sommario

6.2 Formati

Il sistema di conservazione supporta e utilizza i formati previsti dalla normativa vigente identificandoli in fase di ricezione del PDV attraverso l'analisi del magic number o del contenuto del file, in modo tale da individuare lo specifico Mimetype. In linea di massima, per la produzione dei documenti informatici si privilegiano i formati elettronici che presentano le seguenti caratteristiche:

- **indipendenza dalle piattaforme tecnologiche** per non avere vincoli di natura informatica o di tipo economico;
- **apertura e standardizzazione**, intese come disponibilità delle specifiche tecniche in forma liberamente accessibile, completa ed esaustiva, con la garanzia del loro mantenimento nel tempo ad opera di un'organizzazione riconosciuta a livello internazionale, quale ad esempio l'International Organization for Standardization;
- **non proprietario,** cioè non appartenente a un solo fornitore che ne detiene i diritti d'uso;
- **robustezza** ossia il coefficiente di robustezza di un formato elettronico indica la probabilità, in caso di corruzione di un file, di recuperare tutto o parte del suo contenuto;
- **accuratezza e usabilità** laddove per accuratezza si intende la capacità di rappresentare un contenuto informativo digitale con una qualità adeguata alle esigenze della comunità di riferimento, mentre il requisito di usabilità si riferisce alla facilità di accesso, trasferimento e gestione dei file;
- **stabilità,** intesa come compatibilità con le versioni precedenti e quelle future;
- **sicurezza,** intesa come protezione da virus o da altro codice maligno;
- **inammissibilità di macroistruzioni** all'interno del file, o almeno disponibilità di strumenti capaci di rilevarne la presenza con sufficiente sicurezza;
- **capacità di memorizzare** nel *file* gli strumenti e i dettagli tecnici necessari per la rappresentazione del contenuto informativo, unitamente all'insieme dei metadati che lo descrivono e documentano il processo di produzione.

Torna al sommario

Di seguito è riportato l'elenco dei formati dei documenti accettati dal sistema di conservazione.

Formato del file	*Proprietario del formato*	*Estensione del file*	*Tipo Mime*	*Aperto*	*Visualizzatore*
PDF PDF/A	Adobe Systems	.pdf	Application/pdf	Sì	Adobe Reader
TIFF	Aldus Corporation	.tif	Image/tiff	No	Visualizzatori di immagini
JPEG	Joint photographic experts group	.jpeg .jpg	Image/jpeg	Sì	Visualizzatori di immagini
Office e Open XML	Microsoft	.docx, .xlxs, .pptx	MIME	Sì	Visualizzatori compatibili
XML	W3C	.xml	Application/xml text/xml	Sì	Web browser
TXT	txt/plain	.txt	ASCII, UTF-8, UNICODE	Sì	Visualizzatori di testo
PEC e EMAIL	Vari	.eml	RCF 2822/MIME (standard di riferimento per i messaggi di posta elettronica)	No	Client di posta elettronica che supportano la visualizzazione di file .eml
ODF	Consorzio OASIS OpenOffice.org	.ods, .odp, .odg, .odb	Application/vnd.oasis opendocument.text	Sì	Visualizzatori di immagini

Il sistema di conservazione utilizza librerie di sistema per il riconoscimento dei formati dei file ricevuti all'interno dei pacchetti di versamento. Queste librerie non si limitano a verificare l'estensione del file, ma ne verificano il contenuto, dando quindi un livello di sicurezza superiore rispetto al reale formato dei documenti trasferiti in conservazione.

Si suggerisce di trasferire gli archivi secondo i formati standard previsti dalla normativa vigente; si precisa che per alcuni formati si utilizzano visualizzatori installati su client e in questi casi il Conservatore fornisce la documentazione tecnica necessaria alla comprensione del viewer stesso.

Negli "Accordi di servizio" concordati tra Produttore e Conservatore per ciascuna tipologia documentale è specificato il formato del documento.

Il Produttore, responsabile della corretta formazione dei documenti, trasferisce gli stessi garantendone l'autenticità e l'integrità, nel rispetto delle norme in merito alla formazione dei documenti informatici.

Il Produttore garantisce che il versamento dei documenti informatici venga realizzato utilizzando formati compatibili con il sistema di conservazione rispondenti a quanto previsto dalla normativa vigente e dagli Accordi di servizio concordati con il Conservatore. Gli oggetti da conservare sono trasferiti dal Produttore al sistema di conservazione tramite Pacchetti informativi denominati Pacchetti di versamento.

Torna al sommario

6.3 Pacchetto di Versamento (PdV)

Il PdV è il pacchetto informativo proveniente dal soggetto produttore e versato al sistema di conservazione in formato .zip o .rar formato da:

- un insieme di file da conservare (content information), eventualmente firmati digitalmente;
- informazioni PDI associate al content information.

Il processo di acquisizione individua l'insieme delle attività finalizzate all'accettazione delle risorse digitali versate dal soggetto produttore e alla loro preparazione per la creazione del PdA.

Negli Accordi di servizio sono descritte le condizioni di versamento concordate con il produttore ovvero:

- aggregazioni e tipologie documentali da trasferire;
- tempistica di versamento (entro la giornata successiva a quella di generazione, settimanale, mensile, bimestrale, trimestrale, quadrimestrale, semestrale, annuale);
- formati e metadati;
- modalità di conferimento;
- ulteriori lavorazioni dei pacchetti.

Il modulo di accettazione del sistema di conservazione mette a disposizione del produttore una serie di funzionalità di validazione che gli consentono di modificare la composizione dei PdV prima della sua acquisizione da parte del Conservatore. Il Produttore quindi in base agli accordi concordati con il Conservatore procede alla conversione del formato, all'apposizione della firma digitale dei documenti, all'implementazione di metadati descrittivi, ecc.

Torna al sommario

6.3.1 Conferimento dei PDV documenti

Gli oggetti digitali sottoposti al processo di conservazione sono organizzati in pacchetti informativi, intesi come contenitori che racchiudono uno o più oggetti da trattare - documenti informatici, fascicoli informatici, aggregazioni informatiche - comprensivi delle informazioni per la loro interpretazione e rappresentazione. I pacchetti informativi quindi contengono non solo il documento e/o l'aggregazione ma anche i metadati necessari a garantirne la conservazione e l'accesso nel lungo periodo. Risulta necessario adottare procedure in grado di garantire la conservazione nel lungo periodo monitorando le attività connesse alle seguenti fasi:

- immissione nel sistema di conservazione;
- certificazione e conservazione;
- esibizione.

La trasmissione dei documenti tra Produttore e sistema di conservazione avviene tramite pacchetti informativi costituiti da singoli documenti o da cartelle zippate contenenti documenti, fascicoli o aggregazioni informatiche. A seconda della loro funzione i pacchetti informativi si distinguono in:

- Pacchetto di versamento (PdV);
- Pacchetto di archiviazione (PdA);
- Pacchetto di distribuzione (PdD).

I documenti digitali sono trasferiti al SDC tramite protocolli criptati di tipo FTPS ed S-FTP per garantire la sicurezza dei dati. Il Produttore trasferisce i propri documenti nell'area predisposta dal Conservatore per la presa in carico del PDV. Il trasferimento dei pacchetti e successiva presa in carico possono avvenire in modalità manuale, automatica oppure semi-automatica.

La trasmissione dei documenti avviene sotto forma di pacchetti rispondenti a precise caratteristiche quali l'essere in formato zip e recare un nome file senza spazi né caratteri speciali. Per ciascun documento versato in conservazione il SDC associa automaticamente i metadati di processo; tra questi si segnala il codice alfanumerico identificativo univoco (d'ora innanzi ID univoco) del soggetto produttore assegnato ad ogni oggetto/aggregazione documentale informatica. L'ID univoco, codice di venti caratteri alfanumerici, assume una duplice funzione:

- contrassegna la tracciabilità del documento durante l'intero processo di conservazione;
- identifica in modo univoco il documento informatico con l'associazione dei dati di provenienza del Produttore.

Per ulteriori dettagli sulle procedure per l'acquisizione del pacchetto di versamento si rimanda ai Manuali tecnici del sistema di conservazione.

Torna al sommario

6.3.2 Conferimento del PDV con fascicoli

Il fascicolo informatico contiene i documenti relativi allo stesso affare, procedimento amministrativo o persona (fisica o giuridica) prodotti nell'espletamento delle funzioni proprie del soggetto produttore.

Le tipologie di fascicolo si distinguono principalmente in:

- fascicoli di persona fisica;
- fascicoli di persona giuridica;
- fascicoli di affare;
- fascicoli di procedimento amministrativo.

I tempi di gestione del fascicolo nell'archivio corrente sono differenti a seconda della tipologia; in linea di massima la tempistica di conferimento dei fascicoli nel SDC è definita dal Produttore, fermo restando la possibilità di sottoporre a conservazione anche fascicoli relativi a procedimenti non conclusi.

La trasmissione dei fascicoli al SDC può avvenire tramite un modulo sviluppato dal Conservatore oppure con altre modalità definite di volta in volta in base alle esigenze del Produttore.

Torna al sommario

6.4 Rapporto di versamento (RdV)

Il rapporto di versamento è un file in formato .xml che attesta l'esito di versamento dei PdV trasferiti dal produttore al SDC.

In sostanza il RdV, per ciascun file incluso nel PdV, riporta le seguenti informazioni:

- URN, stringa univoca che identifica il documento;
- metadati del singolo file;
- impronta del file.

Il SDC genera in automatico il RdV che viene reso disponibile al produttore; al RdV è associato un preciso riferimento temporale specificato con un riferimento al Tempo universale coordinato (UTC).

Contestualmente alla generazione del RdV, viene segnalato anche l'esito del conferimento che può essere positivo, nel caso in cui non siano state evidenziate anomalie, oppure negativo se al contrario il sistema identifichi un errore o un'anomalia del PdV.

Negli Accordi di servizio concordati con il singolo Produttore è presente una tabella con la mappatura dei codici di errore che il SDC può riscontrare in fase di versamento. Inoltre il SDC per ogni Produttore d'archivio configurato, genera con cadenza periodica un PdA di tutti i RdV.

In fase di acquisizione del PdV, in base agli Accordi concordati tra Conservatore e Produttore, è possibile applicare la cifratura per i dati considerati sensibili; in questo caso il Produttore consegna al Conservatore la chiave di decriptazione dei PdA sottoposti a cifratura. In generale i dati sensibili sono trattati con tecniche di cifratura indipendenti dal sistema di database utilizzato e conformi alla normativa vigente.

Torna al sommario

6.5 Pacchetto di Archiviazione (PdA)

Il PdA si ottiene dalla trasformazione di uno o più PdV ed è il pacchetto di informazioni destinato alla conservazione nel lungo periodo.

Il singolo PdA include:

- gli oggetti sottoposti a conservazione;
- l'Indice del pacchetto di archiviazione (IPDA) in formato .xml, generato secondo lo schema dell'UNI SInCRO 11386:2010 per facilitare l'interoperabilità tra i sistemi di conservazione.

Qualora venissero riscontrate anomalie, il sistema provvede automaticamente a bloccare la formazione del PdA e a segnalare il problema; se previsto il Produttore può effettuare il re-invio del pacchetto. Successivamente sono effettuati ex novo i controlli concordati negli Accordi di servizio e in caso di esito positivo si procede alla formazione del PdA.

Le informazioni incluse nell'IPDA riguardano:

- il SDC ossia versione, produttore, identificativo;
- PDA;
- documenti contenuti nel PDA;
- metadati dei singoli documenti;
- soggetti che intervengono nel processo di conservazione con indicazione del ruolo svolto.

I PdA sottoposti a conservazione sono riepilogati nell'Indice del Pacchetto di archiviazione (IPdA), il quale costituisce l'evidenza informatica associata ad ogni PdA contenente un insieme di informazioni articolate come segue:

- Descrizione generale, comprende l'identificativo univoco dell'IPdA e le informazioni relative all'applicazione che lo ha generato (nome e versione dell'applicativo e produttore del software); possono eventualmente essere inclusi i riferimenti per collegare l'IPdA ad altri precedenti IPdA presenti all'interno del sistema di conservazione;
- Attributi del PdA cui l'IPdA è associato, comprendono l'identificativo univoco del PdA ed, eventualmente, i riferimenti che permettono di collegare tale PdA ad altri PdA presenti nel sistema di conservazione;
- File gruppo, questo campo permette di aggregare più oggetti documentali presenti all'interno del PdA indicandone l'identificativo univoco e l'impronta; tale attributo consente di formare degli insiemi di oggetti sulla base di criteri funzionali;
- Processo, attraverso questo attributo vengono inserite le informazioni riguardanti il processo di conservazione dello specifico PdA cui l'IPdA fa riferimento; sono riportati i dati dei soggetti intervenuti durante il processo di formazione del PdA, le informazioni relative a data e ora di produzione dell'IPdA sotto forma di riferimento e marca temporale;
- Extrainfo in cui il sistema riporta le informazioni utili a richiamare i log di sistema salvati e conservati nel database Oracle.

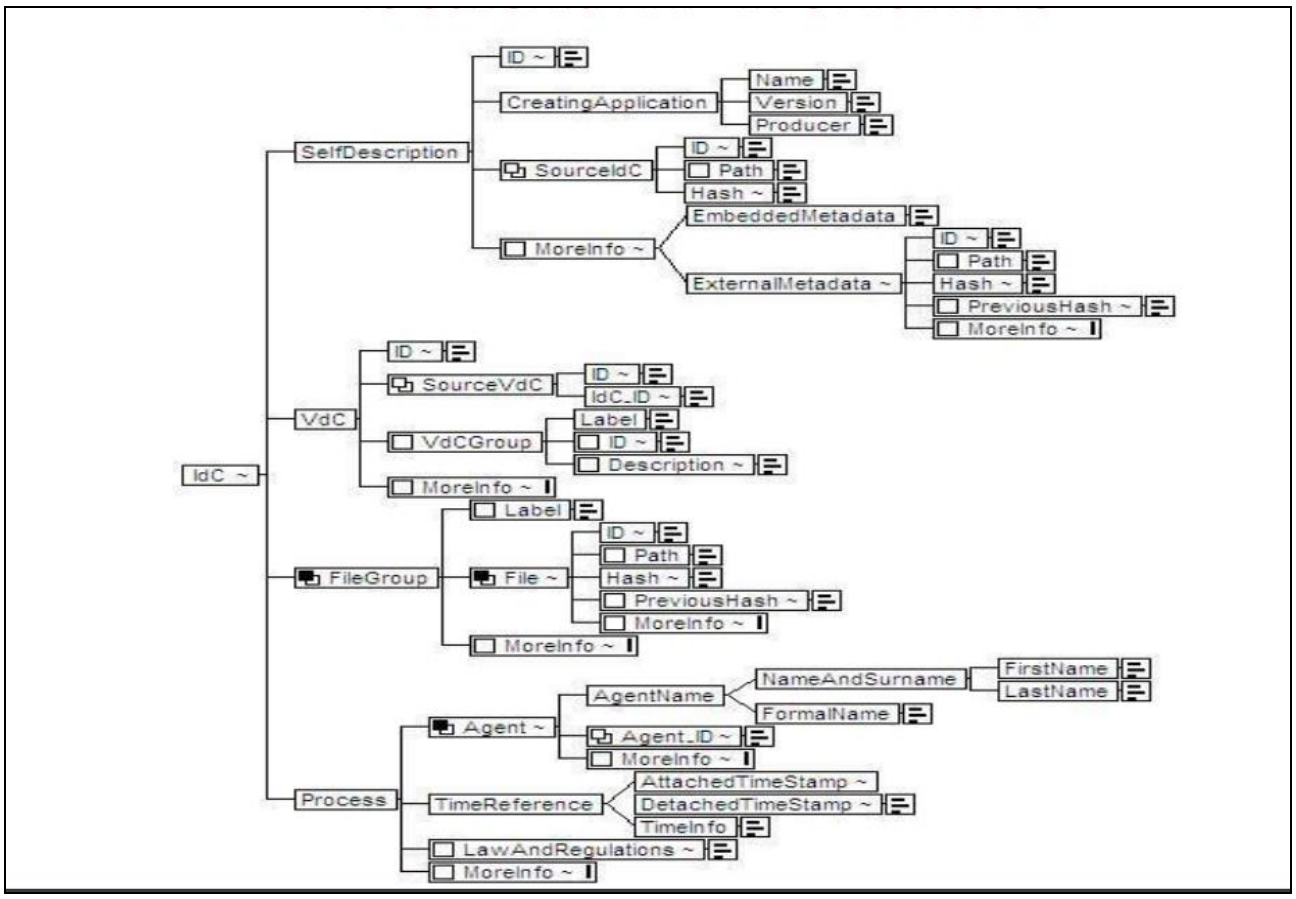


Figura 2 - Struttura IPDA

L'IPdA è l'evidenza informatica nel formato xml associata ad ogni PdA, contenente un insieme di informazioni descritte nelle regole tecniche, cui sopra è riportata la figura.

Al termine del processo, per ciascun IPdA viene apposta una marca temporale e la firma digitale del Responsabile del servizio di conservazione o delegato.

La procedura si conclude con l'invio di una PEC al Produttore che notifica l'avvenuta formazione e certificazione di uno o più PdA.

[Torna al sommario]

6.6 Pacchetto di Distribuzione (PdD)

Il pacchetto di distribuzione (PdD) è generato dal SDC contestualmente al PdA.

L'utente effettua la ricerca in base ai diritti di accesso assegnati, effettuando se previsto l'accesso alla console di esibizione del SDC.

In base alle informazioni concordate negli Accordi di servizio il SDC localizza i documenti conservati nei diversi PdA e su richiesta effettua il PdD selettivo; tale pacchetto informativo viene firmato digitalmente dal Responsabile del servizio di conservazione e salvato nel formato di file immagine .iso

L'esibizione del PdD è garantita tramite console web; se la richiesta è pervenuta tramite PEC il responsabile del servizio di conservazione o delegato, nella PEC di risposta, indica il link da cui il Produttore può accedere per effettuare il download del pacchetto.

Infine se previsto da contratto, il file immagine .iso può essere masterizzato su un supporto ottico (DVD) e trasmesso al responsabile della conservazione; tali informazioni sono riportate negli Accordi di servizio.

La materializzazione dei supporti certificati avviene attraverso la produzione automatica di una loro copia .iso che risiede sul server stesso del sistema di conservazione.

Il PdD contiene:

- i documenti richiesti nel formato previsto per la loro visualizzazione;
- un'estrazione dei metadati associati ai documenti;
- l'indice di conservazione firmato e marcato;
- i viewer necessari alla visualizzazione dei documenti conservati.

Come già detto, l'utente è il ruolo svolto da persone o sistemi che interagiscono con il sistema di conservazione al fine di accedere e ricercare le informazioni di interesse.

Il documento conservato deve essere leggibile in qualunque momento presso il sistema di conservazione e disponibile su richiesta anche su supporto ottico e/o analogico.

La richiesta di esibizione può essere inoltrata dal soggetto produttore o dai soggetti autorizzati tramite due modalità:

- i soggetti inviano una PEC allegando alla richiesta di consultazione l'elenco dei PdA o dei documenti di cui richiedono l'esibizione. Il Conservatore individua tali documenti attraverso l'ID univoco e li predispone per l'esibizione creando il PdD;
- i soggetti effettuano il login con username e password forniti dal Conservatore ed effettuano l'accesso alla console web di esibizione di Virgilio; il firewall del sistema riconosce l'indirizzo IP da cui viene effettuata la richiesta di esibizione e la concede solo se l'indirizzo è tra quelli dichiarati dal soggetto produttore negli Accordi di servizio. Attraverso la console di esibizione il Produttore procede alla ricerca e alla selezione dei documenti di cui richiede l'esibizione.

Il soggetto produttore stabilisce i livelli di accesso e di consultabilità della propria documentazione affidata al conservatore soprattutto in casi di PdV contenenti dati sensibili.

Il responsabile della conservazione del produttore comunica i nominativi e gli indirizzi di posta elettronica delle persone che devono accedere al sistema di conservazione. Nel documento “Piano della sicurezza” di Siav sono definite le politiche di gestione degli accessi, riviste periodicamente, che assicurano la disponibilità delle informazioni al personale autorizzato in base a specifiche policy aziendali. Il Conservatore verifica periodicamente le credenziali di accesso al sistema di conservazione, sulla base della periodicità di consultazione indicata nella richiesta, proprio per accertare che la necessità di accesso sia ancora valida. La documentazione e i log di analisi e verifica sono accessibili soltanto al personale autorizzato dal RSI.

Torna al sommario

7 IL PROCESSO DI CONSERVAZIONE

Il processo di conservazione implementato dal Conservatore è rappresentato nella figura 3.

Figura 3 – Fasi del servizio di conservazione

Il servizio di conservazione viene attivato a seguito di sottoscrizione dell'atto di affidamento del servizio di conservazione e della documentazione a corredo (Accordi di servizio e Manuale di conservazione). Il Conservatore rende disponibili e consultabili i documenti conservati per l'intera durata del servizio previsto dal contratto.

Le principali fasi del processo di conservazione, dettagliatamente descritte nei paragrafi successivi, sono:

- ricezione del PdV;
- verifica della correttezza del PdV e segnalazione di eventuali anomalie;
- generazione del RdV;
- generazione del PdA;
- certificazione del PdA e generazione dell'IPdA;
- generazione del PdD;
- gestione e scarto del PdA.

Torna al sommario

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

La produzione del PdV si ottiene a seguito del processo di estrazione dei documenti/fascicoli/aggregazioni documentali e relativi metadati dalle varie applicazioni informatiche adottate dal Produttore e successivo trasferimento al SDC. Negli Accordi di servizio sono formalizzate le specifiche concordate con il Produttore in termini di:

- contenuto, tipologia documentale, metadati obbligatori ed aggiuntivi, modalità di estrazione dei metadati, formati dei documenti ed eventuali conversioni;
- tempistica per l'invio dei pacchetti;
- autenticazione e canale di versamento.

Le possibili modalità di versamento sono:

- S-FTP – caricamento via file system;
- web service – caricamento automatico tramite interfaccia tra applicativi;
- upload manuale del file – caricamento da interfaccia grafica.

In caso di versamento tramite canale Ftp criptato sono assegnate le credenziali di accesso per effettuare il conferimento. Il PdV deve essere conferito compresso, eventualmente criptato, preferibilmente con classi documentali omogenee. L'estrazione dei metadati può avvenire mediante normalizzazioni a cura del Conservatore; il trasferimento dei documenti su canale è quindi ottimale in caso siano previste delle pre-lavorazioni. I PdV conferiti sono presi in carico da un servizio per il versamento nel Sistema dunque esso è asincrono. I log degli accessi e dei conferimenti ai server ftp/ftps sono conservati nel SDC; inoltre è possibile concordare una notifica via PEC della presa in carico dei pacchetti di versamento. Nel caso di versamento tramite web services, il soggetto produttore dialoga in modo sincrono con le interfacce del SDC. In fase di redazione degli Accordi di servizio, il produttore dichiara gli indirizzi IP da cui intende connettersi al server scelto e riceve le credenziali di accesso all'area web. Il produttore può effettuare la connessione esclusivamente da uno degli indirizzi dichiarati. Il conservatore può offrire strumenti di supporto alla generazione del PdV che dialogano con i sistemi del produttore:

- servizio di Middleware denominato Orchestrator e realizzato da Siav per un dialogo diretto tra i sistemi produttori della documentazione ubicati, da adattare secondo le caratteristiche dell'applicazione di provenienza (query su database, chiamate webservices etc.);
- qualora il Produttore utilizzasse come repository documentale il Sistema documentale Archiflow, vi è un software dedicato sviluppato da Siav, che estrae i documenti e relativi metadati per trasmetterli al SDC secondo le due forme alternative ftps/webservices.

Torna al sommario

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

L'acquisizione del PdV nel SDC avviene con cadenza programmata, concordata con il produttore in base alla natura dei documenti trasferiti e secondo i termini previsti dalla legge.

L'identificazione del Produttore viene effettuata a monte tramite le credenziali di accesso all'FTP Server o web services del SDC.

Per ciascun pacchetto ricevuto, il sistema verifica che il contenuto sia rispondente a quanto definito negli Accordi di servizio, inoltre effettua le seguenti verifiche:

- formato dei file;
- validità della firma.

Il sistema notifica eventuali anomalie tramite messaggio PEC al responsabile della conservazione del produttore. Le verifiche sopra indicate possono dare anche esito negativo e quindi il sistema segnala la presenza di un'anomalia. I documenti con anomalia possono presentare dati illeggibili o incompleti, dati memorizzati su formati non compatibili, certificati di firma scaduta, ecc. In questi casi il sistema procede a "rifiutare" i documenti con anomalia e a generare contestualmente il RdV che contiene indicazione delle anomalie riscontrate. L'esito del versamento di uno o più PdV è notificato al Produttore tramite email generata in automatico dal sistema.

Negli Accordi di servizio è definito l'elenco dei formati dei documenti che il soggetto produttore sottopone al processo di conservazione. Il Conservatore effettua periodicamente i controlli sui documenti e sulle aggregazioni documentali presenti nel sistema, in modo da identificare eventuali anomalie.

Le eccezioni sono riferibili alla necessità, da parte del soggetto produttore, di conservare i documenti in formati non compatibili con la conservazione a lungo termine e sui quali non sia possibile effettuare una conversione di formato senza alterarne la leggibilità e la forma. In questo caso il responsabile del servizio di conservazione ammette tali documenti nel sistema di conservazione specificando però che, per queste eccezioni, non sarà possibile assicurare l'integrità e la leggibilità per la conservazione nel lungo periodo. I controlli effettuati dal SDC sui documenti e sulle aggregazioni informatiche comprendono anche le verifiche volte ad identificare il formato dei file. Comunemente il formato di un file è riconosciuto attraverso la sua estensione; ai fini di una corretta identificazione questo non è però sufficiente in quanto l'estensione di un file può essere modificata, volontariamente o involontariamente, ad esempio a causa di una ridenominazione accidentale o per l'intervento di un virus. In ogni caso, anche se eseguita correttamente, l'identificazione del file tramite l'estensione permette di riconoscere solo la famiglia di formati cui appartiene e non la specifica versione, utile ai fini di una corretta rappresentazione del file.

Torna al sommario

7.3 Accettazione dei pacchetti di versamento e generazione del Rapporto di versamento

Il SDC per ciascun PdV accettato effettua le verifiche di cui sopra e genera in automatico il rapporto di versamento che contiene:

- identificativo univoco;
- metadati dei documenti contenuti;
- impronte dei documenti contenuti;
- riferimento temporale.

Il RdV attesta la presa in carico di uno o più pacchetti trasmessi dal Produttore.

Torna al sommario

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

Il PdV è sottoposto ai controlli descritti nel precedente paragrafo, alcuni di questi sono eseguiti obbligatoriamente, altri invece concordati negli Accordi di servizio.

Ulteriori controlli effettuati dal sistema riguardano la nomenclatura dei pacchetti conferiti in cartelle zippate e successivamente anche il loro contenuto. Il SDC in caso di errori restituisce un RdV con esito negativo; l'anomalia viene quindi evidenziata direttamente nel RdV. Si evidenziano documenti anomali quando avviene una corruzione o perdita di dati, ad esempio i dati sono memorizzati su formati non compatibili, sono presenti fatture discontinue, metadati mancanti, documenti con certificati di firma scaduta, etc. In questi casi il sistema procede a "rifiutare" i documenti su cui sono state riscontrate le anomalie; il RdV è reso disponibile al Produttore.

Torna al sommario

7.5 Preparazione e gestione del pacchetto di archiviazione

Conseguentemente all'acquisizione del PdV e alla restituzione del RdV il Conservatore procede alla certificazione degli oggetti digitali contenuti nei pacchetti. Le modalità e tempistiche per la creazione del PdA sono definite negli Accordi di servizio, nello specifico il PdA può coincidere con il PdV trasferito ma può comprendere anche più PdV. La tempistica per la formazione del PdA è variabile in base ai tempi di conferimento, alle esigenze del Produttore e alla normativa vigente.

La struttura dei PdA "certificati" ossia sottoporti a processo di conservazione, rispecchia lo standard SInCRO UNI 11386:2010, norma riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione. In sintesi il PdA è un'entità logica contenuta in un'alberatura di file e cartelle, definita nel file indice UNI SInCRO generato al termine del processo di conservazione.

La gestione del PdA termina con la generazione dell'IPdA che viene firmato e marcato dal Responsabile del servizio di conservazione o delegato. Il SDC si occupa autonomamente di gestire tutte le fasi del processo di conservazione, tracciandone ogni passaggio e ogni esito nei file di log.

Torna al sommario

7.6 Preparazione e gestione del PdD ai fini dell'esibizione

Il SDC è in grado di restituire in qualsiasi momento la documentazione richiesta dall'utente generando PdD coincidenti con PdA oppure PdD selettivi, formati da diverse tipologie documentali e aggregazioni estratte da differenti PdA. La formazione del PdD è quindi condizionata dal soggetto richiedente e dagli obiettivi per i quali si richiede l'esibizione che può essere un'ispezione di un'Autorità piuttosto che una richiesta di consultazione o di accesso agli atti. Per le modalità di esibizione si rimanda al paragrafo 6.6.

In generale il sistema di conservazione è in grado di esibire tutti i documenti informatici in esso conservati in qualsiasi momento del periodo di conservazione, secondo le richieste di accesso ed esibizione eseguite dai soggetti debitamente autorizzati.

Torna al sommario

7.7 Produzione di duplicati e copie informatiche

La divisione DSO, d'intesa con i Sistemi informativi, effettua periodicamente il salvataggio dei dati e monitora le procedure per la generazione di copie e duplicati dei PdA, previa richiesta trasmessa con PEC dal Produttore. Le copie informatiche dei documenti contenuti in un PdA sono identiche ai documenti informatici originari.

Il duplicato informatico è il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della stessa sequenza di valori binari del documento informatico originario.

Le copie di sicurezza dei PdA sono prodotte nel momento in cui il PdA è generato e memorizzato automaticamente sui server.

È possibile, previa richiesta del Produttore oppure in situazioni particolari, generare le copie anche su supporti ottici (DVD).

I PdD trasmessi su supporto ottico (DVD) sono crittografati e protetti da password.

Torna al sommario

7.8 Scarto dei pacchetti di archiviazione

Nessun documento o dato conservato può essere cancellato o modificato, se non in occasione della cessazione del contratto o per le procedure di selezione e scarto richieste tramite PEC dal Produttore. Il processo di selezione e scarto include gli interventi finalizzati da una parte alla conservazione della documentazione avente valore giuridicamente e storicamente rilevante, e dall'altra alla selezione per la

distruzione di documentazione giudicata irrilevante dal punto di vista amministrativo-legale e storico. Ai sensi della normativa vigente la pubblica amministrazione adotta il Piano di conservazione (anche noto come Massimario di selezione e scarto); tale strumento, approvato dalla Soprintendenza archivistica competente territorialmente, indica il tempo di conservazione di documenti e fascicoli prodotti dall'ente nello svolgimento delle sue funzioni. L'ente richiede l'autorizzazione alla Soprintendenza archivistica competente territorialmente trasmettendo l'elenco di scarto che include almeno i seguenti dati: tipologia dei documenti proposti per lo scarto, la quantità, la classificazione, gli estremi cronologici, la motivazione, il peso e i metri lineari. Il Produttore effettua lo scarto dei PdA conservati in Virgilio, se previsto da contratto; in questo caso il procedimento prende avvio dalla richiesta formale di scarto trasmessa dal Produttore al Conservatore tramite PEC. La richiesta, sottoscritta dai responsabili della gestione documentale e della conservazione del soggetto produttore, include l'elenco dei PdA proposti per la distruzione.

Il Conservatore riceve la richiesta di scarto verificando che sia presente anche l'autorizzazione della Soprintendenza. Qualora venissero rilevate delle anomalie il Conservatore può chiedere documentazione integrativa al Produttore.

Si precisa che l'autorizzazione della Soprintendenza è necessaria anche per gli archivi prodotti da soggetti giuridici privati sottoposti a vigilanza a seguito della dichiarazione di notevole interesse culturale da parte del MiBACT (D. Lgs. 22 gennaio 2044, n. 42 art. 13).

Torna al sommario

7.9 Modalità di intervento del pubblico ufficiale

Il Produttore di documenti trasmessi in conservazione assicura la presenza del pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite. Il Conservatore supporta il Produttore per le attività di esibizione e generazione dei pacchetti di distribuzione.

Torna al sommario

7.10 Verifica di firme e marche

La procedura adottata per la verifica delle firme prevede i seguenti passaggi:

- verifica che il formato della firma sia aderente a quanto richiesto dai requisiti cioè si controlla l'algoritmo utilizzato e che gli attributi firmati siano quelli necessari (data, impronta, etc.);

- verifica che il certificato non sia scaduto (data di inizio e fine validità);

- verifica che il certificato sia stato emesso da una CA autorizzata e per far questo si utilizza l'elenco delle CA dal sito istituzionale AGID;

- verifica che il certificato non sia stato revocato e questo viene fatto scaricando la CRL relativa al certificato seguendo le informazioni contenute nel certificato stesso.

La procedura adottata per la verifica delle marche temporali è la seguente:

- si verifica che il formato della marcatura sia aderente a quanto richiesto dalla normativa;
- si verifica che la TSA sia stata accreditata da AGID come per i certificati.

Il sistema di conservazione è in grado di applicare la firma digitale utilizzando i certificati rilasciati da tutte le Certification Authority accreditate presso AGID.

Torna al sommario

7.11 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità verso altri conservatori

Ai fini dell'interoperabilità tra i sistemi di conservazione sono stati adottati i criteri indicati di seguito.

I formati adottati per gli oggetti documentali predisposti dal Sistema di conservazione e quelli ammessi per i documenti di cui è richiesta la conservazione sono previsti dall'*Allegato 2* delle Regole tecniche a garanzia dei principi dell'interoperabilità tra i sistemi di conservazione.

I pacchetti di archiviazione sono realizzati secondo i requisiti previsti dalle "Specifiche tecniche del pacchetto di archiviazione" (DPCM 3 dicembre 2013, allegato 4); tali specifiche fanno riferimento allo standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali

(UNI 11386:2010), che costituisce lo standard nazionale riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione. In analogia allo standard SInCRO, la struttura utilizzata prevede una specifica articolazione tramite il linguaggio di marcatura XML.

Torna al sommario

7.11.1 Esportazione di un archivio informatico

In caso di cessazione del servizio, il Conservatore procede alla restituzione dei PdA secondo la seguente modalità operativa:

- ricezione tramite PEC delle modalità di trasferimento e relative coordinate;
- il Conservatore effettua l'estrazione dell'archivio digitale da restituire al Produttore;
- il RSM accedendo alla console del sistema di conservazione individua l'elenco dei Pacchetti di archiviazione certificati che compongono l'archivio ed esegue una procedura di materializzazione su supporto ottico (DVD) o storage;
- generazione di un report che contiene l'elenco di tutti i PdA con i relativi estremi di certificazione;
- in caso di restituzione di archivi memorizzati su supporti ottici il servizio avviene attraverso la spedizione degli stessi all'indirizzo indicato negli Accordi di servizio;
- in caso di trasmissione telematica, si effettua l'upload dei PdA nell'area FTP del Cliente; viene trasmessa una PEC con il report dell'avvenuto deposito nell'area di download.

In alcuni casi, il Produttore può richiedere al Conservatore una relazione archivistica afferente l'archivio digitale restituito. Tale relazione, elaborata dal responsabile della funzione archivistica di conservazione, contiene una sintesi della documentazione sottoposta a conservazione: descrizione dei metadati, dei formati, degli estremi cronologici, dei soggetti intervenuti nel processo di conservazione, gli interventi effettuati, etc.

In caso di cessazione del servizio si effettua la cancellazione dei PDA previa comunicazione formale al Produttore.

Torna al sommario

7.11.2 Importazione di un archivio informatico

La richiesta di importazione di un archivio informatico nel sistema di conservazione prevede una serie di controlli effettuati dal Conservatore quali:

- un'analisi preventiva dell'archivio per la rilevazione delle criticità;
- la redazione di un'analisi tecnica dettagliata sulle modalità di importazione;
- la definizione e configurazione dell'archivio nel sistema di conservazione;

- la verifica delle tipologie documentali trasferite;
- il monitoraggio della procedura di versamento dei PdA nel sistema di conservazione effettuando verifiche dell'integrità fisica e logica dei documenti/fascicoli in essi contenuti;
- l'analisi della consistenza e completezza degli oggetti digitali costituenti l'archivio da importare;
- relazione tecnica.

Torna al sommario

7.11.3 Interoperabilità applicativa tra i sistemi

Il sistema di conservazione e in particolare le sue componenti applicative, mettono a disposizione un insieme di API (Application Programming Interface) esposte sotto forma di web services. Tramite i suddetti web services è possibile costruire integrazioni che permettono ad altri sistemi di accedere da remoto all'intero archivio oppure a porzioni di esso.

Torna al sommario

8 IL SISTEMA DI CONSERVAZIONE (SdC)

Il sistema di conservazione (Virgilio) è basato su un'architettura modulare service-based pensata per soddisfare la gestione delle procedure di conservazione dei documenti a norma.

Il Sistema gestisce archivi di più soggetti produttori, applicando agli stessi regole differenti ed è possibile associare tipologie documentali con gli attributi appropriati a ciascuna Azienda.

L'architettura del sistema di conservazione può essere suddivisa in tre livelli dedicati rispettivamente all'interfaccia utente (Presentation layer), alla logica funzionale (System Services) e alla gestione dei dati e dei documenti (Repository).

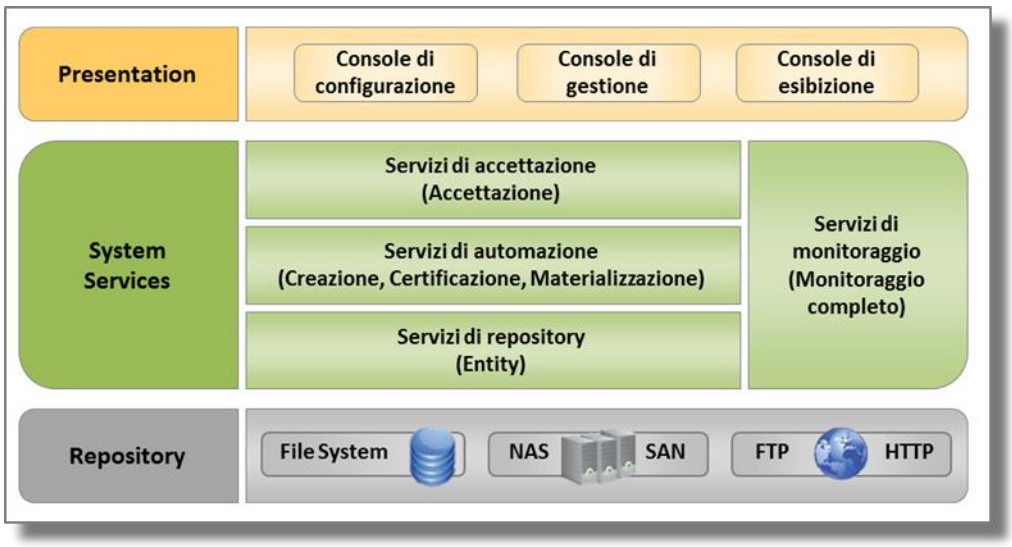


Figura 4 – Architettura three-tier

Lo strato di Presentation è costituito dalle interfacce di gestione e di utilizzo del sistema (console) accessibili solo dagli utenti autorizzati via client Windows e/o via web (ad esempio per esibire un documento a prescindere dal luogo fisico di conservazione). In particolare, Virgilio supporta diverse interfacce che permettono ai responsabili e agli utenti abilitati di amministrare e monitorare opportunamente il processo di conservazione:

- la **console di configurazione** (disponibile solo sul client Windows), utilizzata dai responsabili del sistema per accedere a tutte le funzionalità di amministrazione;
- la **console di esibizione** (disponibile via web), per la ricerca e l'esibizione dei PdD;
- la **console di gestione** specificatamente predisposta per gli operatori DSO e delegato RSC, che, oltre ad includere tutte le funzionalità disponibili nella console di esibizione, permette sia di gestire i PdA logici di conservazione per le operazioni di creazione, certificazione, materializzazione sia di monitorare lo stato di avanzamento del processo di conservazione e lo stato fisico e logico di tutto l'archivio.

Lo strato System Services è costituito da un insieme di servizi che supportano il sistema nello svolgimento di tutte le fasi del processo di conservazione, presidiando controlli e automatizzando alcune attività, così come nel monitoraggio dello stato dei documenti e dei supporti utilizzati. In generale opera su tre diverse console:

- **Console di Accettazione e Consolidamento** (disponibile anche nella versione web), permette la firma digitale, dove richiesta, sui documenti da importare in Virgilio;
- **Console di import dei PdA**, permette di effettuare l'upload di PdA di conservazione generati con sistemi diversi da Virgilio e di inserirli nel ciclo di controllo del sistema;
- **Console correzione anomalie e PdA**: permette di gestire le eventuali anomalie nel processo di conservazione.

Lo strato di Repository infine, sotto il controllo del servizio Gestione PdA, gestisce la consistenza e il mantenimento dell'archivio del sistema di conservazione a norma, sfruttando le risorse storage a disposizione (NAS ed eventuali sistemi remoti accessibili via S-FTP e HTTPS).

Virgilio si propone come sistema dedicato alla conservazione che può operare in modalità stand-alone o connesso ad un qualsiasi sistema di gestione informatica dei documenti. In entrambi i casi il SDC effettua le operazioni necessarie alla conservazione e garantisce quanto previsto dalla normativa vigente.

La conservazione degli oggetti digitali nel SDC è riassumibile nelle seguenti fasi di processo:

- definizione delle regole di conservazione che il documento deve osservare (variabili in base alla tipologia documentale e all'ambito di riferimento quale ad es. fiscale, amministrativo, etc.);
- associazione delle tipologie documentali al soggetto produttore;
- verifica delle regole di conservazione ed esecuzione delle eventuali operazioni necessarie (firma, marca) in base alla tipologia documentale di appartenenza del documento;
- acquisizione del documento nel sistema Virgilio;
- archiviazione del documento in un PdA con creazione dell'IPdA;
- certificazione dell'IPdA;
- creazione delle copie dei PdA (copie automatiche di backup);
- verifica dell'integrità dei documenti non oltre i cinque anni dalla data di certificazione del pacchetto.

Torna al sommario

8.1 Componenti logiche

I servizi Windows sono utilizzati per effettuare le operazioni di conservazione (creazione PdA, etc.) e per l'esecuzione delle attività di Virgilio (monitoraggio, etc.). I servizi gestiti attraverso la console di configurazione del sistema sono i seguenti:

1) *Accettazione* - Servizio usato per inserire nuovi documenti in Virgilio: come sistemi di input può utilizzare dei file di testo (stile CSV con separatore o a lunghezza fissa) e/o può interfacciarsi direttamente ad Archiflow (oppure ad altro Sistema documentale) attraverso l'utilizzo di un modulo specifico;

2) *Creazione PdA* - Servizio per la creazione dei PdA in base a modelli predefiniti;

3) *Certificazione* - Servizio per la certificazione automatica dei PdA con apposizione di firma digitale e marca temporale degli IPdA;

4) *Materializzazione* - Creazione delle copie fisiche dei PdA virtuali in base alle regole impostate;

5) *Monitoraggio* - Servizio di monitoraggio dell'archivio digitale; viene pianificato periodicamente dal responsabile della manutenzione del SdC e prevede la verifica della consistenza e coerenza dei documenti;

6) *Operazioni generiche* - Servizio per la gestione delle operazioni generiche quali ad esempio la cancellazione, le richieste effettuate dal web, etc;

7) *WCF per il Web* -Servizi WCF per il web; può essere definito una volta sola per tutto l'impianto;

8) *WCF di amministrazione*- I servizi WCF di amministrazione dispongono una serie di funzionalità per la creazione di Aziende, tipologie documentali, etc.; può essere definito una volta sola per tutto l'impianto;

9) *WCF per i Gadget*- Espone i servizi per l'utilizzo dei Gadget di Virgilio; può essere definito una volta sola per tutto l'impianto;

10) *FTP HTTPS*- Non è un servizio Windows; viene utilizzato dal SdC per identificare la modalità di trasporto delle copie ISO sul server web tramite il protocollo HTTPS;

11) *Gestione PdA*- Questo servizio gestisce la storicizzazione dei PdA correnti delle immagini.

Tali servizi, in ambienti che utilizzano più server, possono essere definiti più volte in modo da parallelizzare le operazioni su entità differenti.

Le funzionalità che caratterizzano il SDC e rese disponibili, sono di seguito sintetizzate:

- verifica dei documenti in termini di leggibilità, integrità, etc.;
- gestione dei PdA di documenti;
- certificazione dei PdA;
- materializzazione dei PdA certificati;

- ricerca ed esibizione dei documenti;
- monitoraggio sullo stato logico e fisico del sistema;
- amministrazione e configurazione del sistema.

Torna al sommario

8.2 Componenti tecnologiche

Nell'architettura di Virgilio, i servizi caratterizzanti sono interoperabili secondo una definizione formale indipendente dalla piattaforma e dalle tecnologie di sviluppo (come Java, .NET, etc.) dato che viene applicata una logica comunemente conosciuta come Service-Oriented Architecture (SOA). Ciò significa che ogni servizio può essere richiamato per eseguire i propri compiti senza avere conoscenza dell'applicazione chiamante e senza che l'applicazione, a sua volta, abbia conoscenza del servizio che effettivamente esegue l'operazione.

Il SOA funziona attraverso l'uso di un componente di orchestrazione, secondo il modello dell'Enterprise Service Bus, che opera nel rispetto dei principi di cooperazione applicativa basati sullo standard xml.

L'implicazione principale di un tale approccio, grazie alla possibilità di modificare in maniera semplice le modalità di interazione tra i servizi e in generale la loro combinazione (per soddisfare le esigenze dei processi che implementano), prevede che la logica di business sia svincolata dalla tecnologia utilizzata, per cui è possibile realizzare la separazione tra "cosa un'applicazione fa" da "come lo fa".

Un ulteriore vantaggio di un'architettura a servizi è l'integrazione immediata con altri applicativi via web services; in sintesi altri applicativi, indipendentemente dal linguaggio di programmazione in cui sono stati scritti e dalla piattaforma su cui sono implementati, possono utilizzare i servizi messi a disposizione attraverso l'invio tramite HTTPS di messaggi in formato xml.

L'organizzazione in servizi, interagenti tra loro e attivabili in funzione delle esigenze, permette di massimizzare anche la modularità e l'estensibilità della soluzione, ottimizzando da una parte il carico di lavoro e soddisfacendo dall'altra tutte le esigenze di amministrazione delle attività di conservazione a norma degli archivi digitali.

In particolare in Virgilio sono attivi i seguenti moduli:

- Accettazione PdV;
- Generazione PdA;
- Certificazione PdA;
- Materializzazione PdA;
- Monitoraggio;
- Gestione PdA.

Si riporta la descrizione dettagliata degli stessi:

- **il Modulo di Accettazione** gestisce l'importazione dei documenti versati, procedendo alle verifiche formali sui documenti e, nel caso siano firmati digitalmente, effettua le verifiche sulla validità del certificato di firma;

- **il Modulo di Generazione dei PdA**, gestisce la trasformazione dei PdV in PdA, supportando la creazione di PdA differenti in funzione della tipologia di documenti che dovranno contenere;

- **il Modulo di Certificazione** gestisce l'attività di chiusura dell'IPdA, avvisando il responsabile del servizio di conservazione o delegato alla firma della presenza di nuovi PdA logici da certificare, permettendo a quest'ultimo di monitorare il processo e di firmare digitalmente gli IPdA e di procedere all'apposizione della firma digitale e marca temporale;

- **il Modulo di Materializzazione** gestisce l'attività di materializzazione dei PdA su file system, o su supporto (DVD) in modalità istantanea o schedulata;

- **il Modulo di Monitoraggio** controlla con cadenza configurabile l'integrità dei PdA e dei documenti in esso contenuti;

- **il Modulo di Gestione PdA** viene utilizzato per la gestione dei dati e dei PdA e in particolare dei flussi di informazioni che da Virgilio spostano o copiano i PdA (e quindi i documenti ivi contenuti) verso gli storage di storicizzazione (NAS).

Torna al sommario

8.2.1 Infrastruttura di Disaster Recovery

Il sistema di conservazione si presenta da un punto di vista di componenti fisiche (in realtà virtualizzate) come descritto nel paragrafo precedente. Tale architettura, pur essendo già dimensionata per supportare il volume atteso nel medio periodo, può essere estesa semplicemente scalando orizzontalmente ed aumentando, eventualmente, le risorse fisiche sottostanti (RAM, Storage, ecc.). Il sistema di conservazione è logicamente e fisicamente replicato in un sito secondario di Disaster Recovery posizionato ad una distanza in linea d'aria superiore a 200 km dal sito primario.

Al fine di ottenere prestazioni e sicurezza è stata contrattualizzata una linea "dedicata" in fibra e la replica delle informazioni avviene direttamente tra i due apparati di storage (SAN) identici per marca e modello. Questo permette di garantire prestazione, affidabilità, scalabilità e robustezza.

La figura sottostante mostra lo schema, semplificato, dei due siti fisici utilizzati per l'erogazione del servizio.

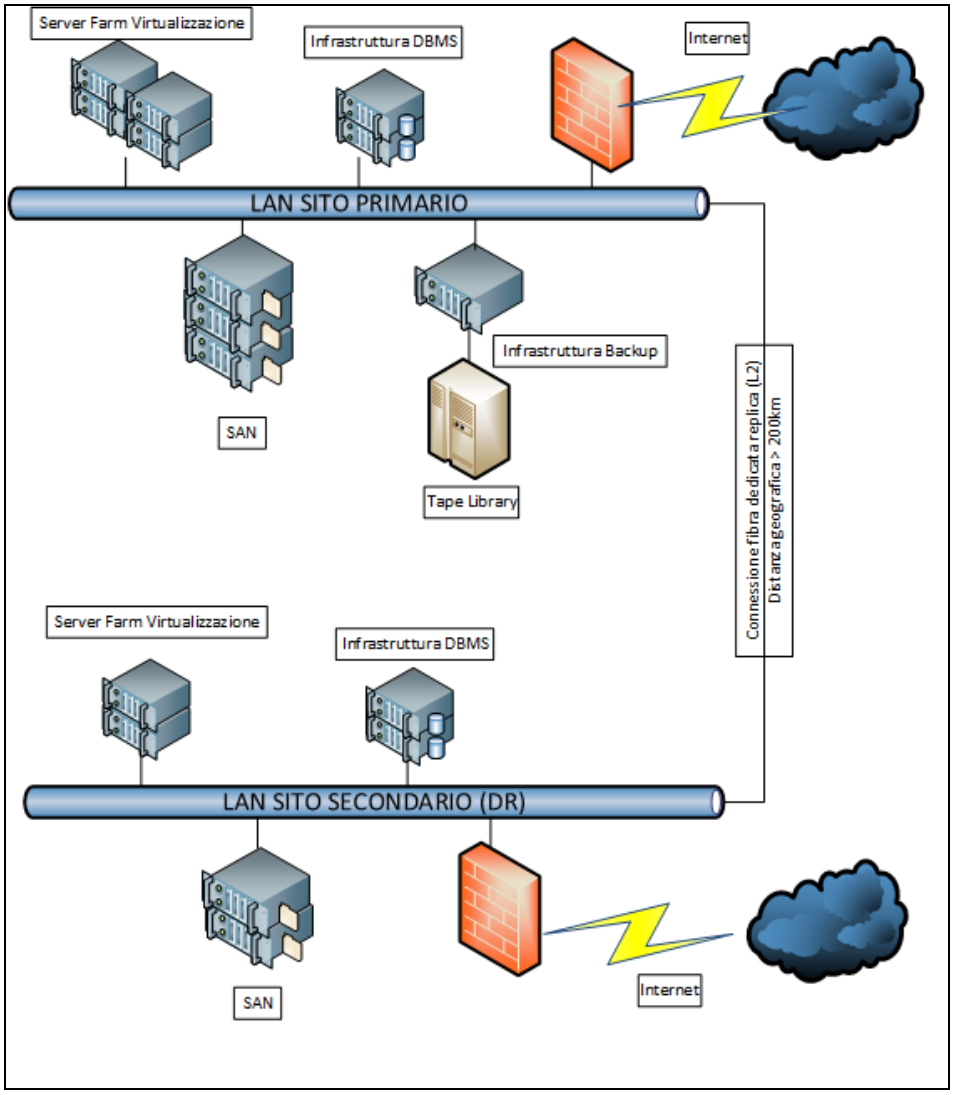


Figura 5 – Infrastruttura Disaster Recovery

8.3 Componenti fisiche

L'architettura di Virgilio è stata progettata per gestire in modo ottimale le performance dei processi di conservazione e di esibizione applicando un approccio multi-server e tecniche di bilanciamento intelligente del carico di lavoro.

In particolare essa garantisce:

- l'estensibilità della soluzione, grazie alla possibilità di attivare solo i moduli necessari per la specifica implementazione;
- l'alta affidabilità, grazie alla possibilità di distribuire i moduli su server indipendenti e di clusterizzare tutti i suoi componenti;
- la scalabilità, grazie alla possibilità di distribuire i vari moduli su più server al crescere del carico di lavoro e di sfruttare la piena compatibilità con i più diffusi e affidabili sistemi NAS e SAN per la gestione dello storage.

Si precisa che le diverse componenti critiche e significative ("sensitive") del sistema di conservazione sono isolate da altri ambienti, organizzativamente, fisicamente e logicamente, in quanto organizzativamente il DSO è un settore specifico con personale dedicato; dal punto di vista logico Virgilio è configurato su macchine dedicate, gli schemi database e le reti sono separate, la SAN è frazionata, etc.

Per quanto riguarda l'isolamento fisico:

- gli apparati del SDC sono collocati in un'area sorvegliata, accessibile soltanto al personale autorizzato;
- il sito di Disaster Recovery è ospitato nei locali di un Data Center certificato, posizionato ad una distanza in linea d'aria superiore ai 200 km dal sito primario.

Per ulteriori dettagli si rimanda al Piano della sicurezza.

Torna al sommario

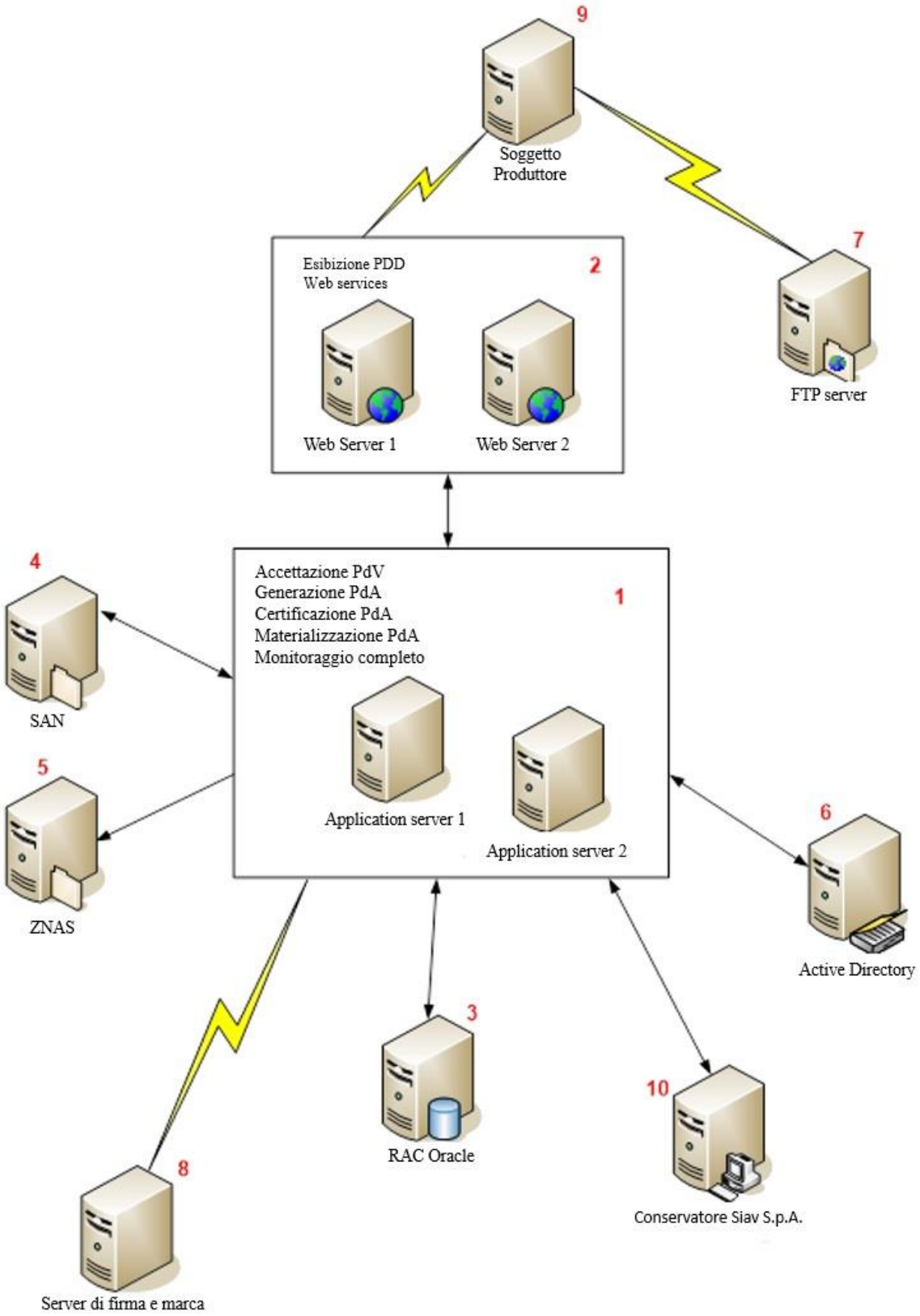


Figura 6 – Architettura base del sistema

Descrizione della figura:

1) i servizi di Virgilio sono installati su due diversi Application Server che lavorano in parallelo;

2) il servizio di esibizione del PdD e i web services, accessibili dal soggetto produttore, operano attraverso due web server che lavorano in parallelo;

3) sul cluster Oracle risiedono i metadati, i dati, i log di sistema e le path utili a collegare i metadati ai relativi documenti;

4) area di storage in cui vengono salvati i documenti;

5) area di storage dove risiedono le immagini storicizzate dei documenti;

6) attraverso il protocollo LDAP, l'active directory è utilizzata come base dati per memorizzare in forma centralizzata tutte le informazioni del dominio di rete relativamente all'autenticazione e all'accesso degli utenti;

7) il server FTP permette di accettare le connessioni in entrata e di comunicare con un client attraverso protocollo S-FTP/FTP-S;

8) per il controlli sulle firme e marche temporali, il sistema si collega ad un server esterno e relativi distribution points presenti all'interno dei certificati di firma e di marca (per le sole C.A. riconosciute da AgID - "https://eidas.agid.gov.it/TL/TSL-IT.xml"). Lo stesso server è utilizzato dal responsabile del servizio di conservazione e delegato per apporre la firma digitale in maniera automatica e massiva attraverso l'utilizzo del dispositivo HSM.

Torna al sommario

8.4 Procedure di gestione ed evoluzione

Nel documento "Piano della sicurezza" sono descritte nel dettaglio:

- le attività espletate per la conduzione e manutenzione del servizio di conservazione e del SDC;
- le procedure attinenti al piano di continuità operativa e Disaster Recovery;
- le procedure di backup e di gestione dei log.

La procedura di rilascio dei pacchetti evolutivi del SDC segue i requisiti imposti dalla certificazione UNI CEI EN ISO/IEC 27001:2017, pertanto ogni nuova release del software viene testata e approvata dalla divisione "Quality Assurance Software".

Per quanto riguarda la descrizione della gestione della sicurezza aziendale, dell'analisi dei rischi e della continuità operativa si rimanda al Piano della sicurezza.

Torna al sommario

8.5 Change management

Di seguito sono descritte le modalità attuate dal Conservatore per la gestione dei cambiamenti al sistema informatico a supporto del sistema di conservazione. Il responsabile del servizio di conservazione autorizza la procedura di change management che solitamente viene gestita dal RSI d'intesa con il RSS e il RSM.

Il sistema informatico viene aggiornato principalmente per due motivi:

- correzione di malfunzionamenti riscontrati;
- evoluzioni, miglioramenti e adeguamenti normativi.

I componenti informatici oggetto del cambiamento sono:

- sistemi operativi;
- software applicativi a supporto del processo di gestione e conservazione dell'archivio digitale.

L'aggiornamento dei sistemi server side avviene sfruttando l'infrastruttura di virtualizzazione e relativo sistema di *Business Continuity*; tutti i sistemi sono duplicati su due nodi distribuiti su differenti macchine fisiche. Per un approfondimento si rimanda al Piano della sicurezza.

Torna al sommario

8.5.1 Aggiornamento dei sistemi operativi

Il RSI con il proprio team, procede come di seguito:

- aggiornamento del nodo passivo;
- promozione del nodo passivo a nodo attivo;
- esecuzione di uno specifico piano di test.

Nel caso in cui non siano rilevati errori, avviene l'aggiornamento del nodo passivo; in caso di problemi il nodo passivo ritorna attivo bloccando di fatto l'aggiornamento e ripristinando la precedente versione.

Torna al sommario

8.5.2 Aggiornamento applicativo

L'aggiornamento applicativo si distingue in:

- manutenzione correttiva;
- manutenzione adattiva;
- manutenzione evolutiva.

La manutenzione del sistema include tutti gli interventi finalizzati al miglioramento e all'evoluzione del software e può essere di tre tipi:

- **manutenzione correttiva**, comprende la diagnosi e la rimozione delle cause e degli effetti dei malfunzionamenti dalle procedure e programmi;
- **manutenzione adattiva**, comprende l'attività di manutenzione volta ad assicurare la costante aderenza delle procedure e dei programmi all'evoluzione dell'ambiente tecnologico del sistema informativo e al cambiamento dei requisiti (organizzativi, normativi, etc.);
- **manutenzione evolutiva**, prevede il miglioramento della soluzione a fronte di nuovi processi e quindi include l'introduzione di nuove funzionalità e/o il miglioramento di quelle esistenti e in alcuni casi anche la rimozione.

Il responsabile dello sviluppo e della manutenzione del sistema di conservazione effettua l'aggiornamento del sistema direttamente e/o coinvolgendo uno o più incaricati della divisione DSO. Per un approfondimento si rimanda ai Manuali operativi del SDC.

Le componenti da modificare possono essere più o meno estese ma generalmente la procedura articolata in questo modo:

- aggiornamento dell'ambiente di test dell'applicativo;
- esecuzione di un piano di test estratto dal piano di test generato in funzione delle componenti da aggiornare;
- in caso di fallimento viene redatto un verbale con i problemi riscontrati;
- individuazione della "finestra temporale" di minor impatto, tipicamente durante il fine settimana per gli aggiornamenti rilevanti;
- backup a caldo differenziale della base di dati;
- aggiornamento del nodo passivo;
- promozione del nodo passivo a nodo attivo;
- esecuzione di un test relativo alle funzioni critiche impattate dall'aggiornamento;

- in caso di fallimento viene redatto il verbale con l'elenco dei problemi riscontrati e si procede al ripristino dal backup della macchina virtuale;
- nel caso in cui non siano rilevati errori, viene effettuato l'aggiornamento del nodo passivo (precedentemente attivo);
- aggiornamento del registro delle versioni installate nei vari ambienti;
- monitoraggio del funzionamento del sistema per 48-72 ore successive all'aggiornamento.

Periodicamente il responsabile dello sviluppo e della manutenzione effettua un aggiornamento della base dati del sistema di test per adeguarlo alle nuove esigenze; la periodicità standard è di 12 mesi salvo situazioni particolari.

Esistono casi specifici per i quali il processo di aggiornamento applicativo richiede l'intervento diretto della divisione "*Software Development*".

Torna al sommario

8.6 Conformità a normativa e standard

Il Conservatore pianifica processi di audit interni riguardanti aspetti normativi, di processo, organizzativi, tecnologici e logistici. L'obiettivo di tali processi è accertare la conformità del sistema alla normativa e agli standard vigenti. Le attività sono riepilogate nel verbale di audit e nella documentazione tecnica per il rilascio delle versioni aggiornate del SDC.

Il Conservatore monitora costantemente l'evoluzione della normativa di settore, al fine di garantire la compliance del Sistema e dei processi. A tale attività contribuisce l'Osservatorio normativo, che ha l'obiettivo di monitorare di norme, regolamenti, regole tecniche, circolari, e più in generale la normativa che ha impatto sulla dematerializzazione e conservazione digitale dei documenti. L'Osservatorio pubblica periodicamente articoli tematici accessibili dal sito istituzionale https://www.siav.com/it/articoli-osservatorio-normativo/.

Eventuali nuovi requisiti conseguenti al monitoraggio normativo vengono condivisi con la divisione Software Development. Successivamente tra le divisioni coinvolte è approvata una roadmap con la pianificazione degli interventi e la relativa tempistica di realizzazione.

Torna al sommario

9 MONITORAGGIO E CONTROLLI

9.1 Procedure di monitoraggio

Conservare un contenuto informativo digitale significa mantenere nel tempo la capacità di riprodurlo con il contenuto e la forma originaria. L'obiettivo del processo di conservazione è quello di mantenere nel tempo il valore giuridico probatorio dei documenti e la capacità di leggerne la sequenza binaria nella sua interezza, di interpretarla con le regole del formato elettronico e di visualizzare il documento originale.

Per mantenere nel lungo periodo l'autenticità, l'integrità e la leggibilità di tutti i documenti conservati nel sistema, il Conservatore attua il piano della sicurezza volto ad individuare e correggere tempestivamente eventuali processi di corruzione dei documenti e dei PdA.

Il responsabile della sicurezza d'intesa con il responsabile dello sviluppo e manutenzione pianifica la tempistica e le attività inerenti i controlli per la verifica dei documenti conservati. Alcune verifiche sono effettuate automaticamente dal sistema che seleziona un campione schedulato di documenti sull'intero archivio di ciascun soggetto produttore, calcola l'impronta di ogni documento e la confronta con quella rilevata al momento dell'acquisizione del documento stesso da parte del sistema di conservazione e memorizzata tra i metadati del documento. Attraverso il confronto delle impronte è possibile verificare l'integrità e l'autenticità del documento.

La leggibilità dei documenti conservati è assicurata dal confronto dell'impronta, in quanto la corruzione della stringa di bit che compone il documento provocherebbe la visualizzazione del file in maniera distorta.

Il Conservatore effettua periodici controlli per prevenire l'obsolescenza tecnologica, un processo causato dalla velocità del progresso tecnologico che, a seguito dell'introduzione sul mercato di tecnologie sempre più avanzate, causa il disuso dei formati. Il Conservatore monitora l'elenco dei formati adottati per la conservazione dei documenti e, qualora venisse prospettato un caso di obsolescenza tecnologica, procede con le attività di riversamento, ovvero il processo che trasferisce uno o più documenti conservati da un supporto di memorizzazione ad un altro, modificando la loro rappresentazione informatica, garantendo il mantenimento dell'integrità del contenuto. Qualora venisse riscontrata la modifica dell'hash del documento, il Produttore coinvolge un pubblico ufficiale per attestarne la conformità della copia all'originale.

Torna al sommario

9.2 Verifica dell'integrità degli archivi

Il Conservatore effettua le verifiche di integrità e leggibilità dei PdA e in caso di obsolescenza degli stessi procede alla generazione delle copie.

Periodicamente viene garantita la conformità degli archivi digitali conservati attraverso i seguenti interventi:

- **controlli di processo**, per lo più automatizzati dal sistema, delle fasi operative del processo di conservazione e gestione delle anomalie;
- **controlli periodici pianificati** preventivamente dai responsabili della conservazione e dei sistemi informativi;
- **controlli e manutenzione** delle strutture hardware e software.

I responsabili della sicurezza e dei sistemi informativi effettuano e monitorano le procedure di backup; inoltre coordinano anche le attività previste per la gestione del piano di continuità operativa e del risk assessment.

Il SDC effettua diverse tipologie di monitoraggio:

- tracciatura e monitoraggio di tutte le attività del processo di conservazione e di gestione dei PdA, notificando gli esiti delle diverse attività svolte, così come eventuali problemi, anomalie e criticità;
- effettuando query ad hoc si possono individuare i documenti con formato non a norma e procedere al riversamento;
- rinnovo automatico del periodo di validità dei certificati e delle marche temporali dei documenti (mediante accesso alla CA e alla TSA certificate), tracciando e segnalando gli esiti;
- gli esiti delle operazioni svolte, incluse le anomalie e le situazioni critiche o potenzialmente rischiose evidenziate dal sistema di conservazione sono visualizzabili nei file di log. Le notifiche di errori o anomalie riscontrati durante la presa in carico dei PdV sono evidenziate anche nei RdV.

Con periodicità definita dal Conservatore si effettua un riesame generale del servizio, al fine di accertare la conformità del sistema al livello di servizio atteso, analizzare le cause di eventuali incidenti o disservizi e promuovere attività di prevenzione e/o miglioramento.

Torna al sommario

9.3 Soluzioni adottate in caso di anomalie

La casistica delle anomalie è abbastanza ampia per cui differenti sono le procedure adottate per la risoluzione.

Di seguito è riportata la procedura di risoluzione delle principali anomalie che generalmente si verificano in fase di versamento.

Fase di versamento		
Anomalia	***Area competente***	***Procedura***
Verifica della nomenclatura dei pacchetti e dei file	Area operativa	Il SDC rileva eventuali incongruenze rifiutando il PdV
Verifica dell'impronta	Area operativa	Viene verificata l'impronta dei documenti versati (se disponibile) effettuandone il confronto con quella calcolata dal SDC
Verifica del formato del file	Area operativa	In presenza di formato non a norma o di file corrotto viene richiesto al produttore un nuovo invio del pacchetto
Errori non previsti	Produttore e Area operativa	Il produttore evidenzia il problema al conservatore che pianifica la procedura per la risoluzione; il verbale di anomalia con il dettaglio dell'anomalia e la soluzione adottata viene inserito nel PdA di riferimento.

Torna al sommario