SIAV S.p.A.

MANUALE DI CONSERVAZIONE

Emissione del documento

Azione	Data	Nominativo	Funzione
Aggiornamento	14/06/2022	Nicola Voltan	Responsabile del servizio di conservazione
Presa visione	14/06/2022	Matteo Fiocchi	Responsabile dei sistemi informativi per la conservazione
		Davide Mietto	Responsabile della sicurezza dei sistemi per la conservazione
		Arianna Santin	Responsabile della funzione archivistica di conservazione
		Morgan Rizzolo	Responsabile dello sviluppo e della manutenzione del sistema di conservazione
		Daniela Perrone	Consulente interno
Approvazione	15/06/2022	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	Riferimenti alle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici; riferimento alla versione dello standard UNI SInCRO norma UNI 11386:2020
5.0	13/09/2021	Aggiornamenti normativi e revisione complessiva del documento; variazione del Responsabile dei sistemi informativi
6.0	17/01/2022	Variazione del Responsabile della funzione archivistica di conservazione
7.0	15/06/2022	Ulteriore variazione del Responsabile della funzione archivistica di conservazione

Sommario

1 SCOPO E AMBITO DEL DOCUMENTO

Il presente documento rappresenta il Manuale di conservazione di Siav S.p.A. e descrive il processo di conservazione di documenti e aggregazioni informatiche per le organizzazioni che affidano il servizio a Siav S.p.A.

Il Manuale di conservazione (d'ora in poi Manuale) illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, la descrizione delle varie fasi di processo, la descrizione delle architetture e delle infrastrutture, le misure di sicurezza adottate e ogni altra informazione utile alla comprensione 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;
- Nomine, deleghe e incarichi interni;
- Piano della sicurezza;
- *Accordi di servizio* concordati con il Cliente, nonché Titolare dell'archivio;
- Manuale utente per la descrizione del Sistema di conservazione.

Per motivi di riservatezza tale documentazione risulta disponibile a seguito di una richiesta trasmessa dal Titolare 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 il presente documento anche a seguito 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 delle tipologie documentali e delle aggregazioni informatiche al sistema di conservazione. La documentazione approvata dal Cliente (d'ora in poi Titolare) viene inviata al Conservatore tramite posta elettronica certificata.

Eventuali modifiche al Manuale di conservazione comportano una nuova versione dello stesso; ogni versione viene trasmessa all'Agenzia per l'Italia digitale che procede con l'approvazione e la pubblicazione del Manuale sul proprio sito istituzionale.

Torna al sommario

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, gestione documentale e 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.

Il sistema di conservazione assicura, dalla presa in carico fino all'eventuale scarto, la conservazione degli oggetti digitali nello stesso conservati, tramite l'adozione di regole, procedure e tecnologie, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità.

2 GLOSSARIO

Di seguito sono elencate le definizioni ricorrenti nel presente Manuale e negli Accordi di servizio così come elencate nel documento "Glossario dei termini e degli acronimi", allegato 1 - Linee Guida sulla formazione, gestione e conservazione dei documenti informatici.

Accesso	Operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici
Affidabilità	Caratteristica che, con riferimento al sistema di gestione documentale o di conservazione, esprime il livello di fiducia che l'utente ripone nel sistema stesso, mentre con riferimento al documento informatico esprime la credibilità e l'accuratezza della rappresentazione di atti e fatti in esso contenuta
Aggregazione documentale informatica	Insieme di documenti informatici o insieme di fascicoli informatici riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente
AGID	Agenzia per l'Italia digitale

Area Organizzativa Omogenea (AOO)	Un insieme di funzioni e di uffici individuati dall'ente al fine di gestire i documenti in modo unitario e coordinato, secondo quanto disposto dall'art. 50 comma 4 del D.P.R. 28 dicembre 2000, n. 445. Essa rappresenta il canale ufficiale per l'invio di istanze e l'avvio di procedimenti amministrativi
Archiflow	Sistema di gestione informatica dei documenti sviluppato da SIAV S.p.A.
Archivio	Complesso dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria 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 o asseverata al documento informatico
Autenticità	Caratteristica in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto, un oggetto è autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze
Certificazione	Attestazione di terza parte relativa alla conformità all'elenco di requisiti specifici
Classificazione	Attività di organizzazione di tutti i documenti secondo uno schema costituito da un insieme di voci articolate in modo gerarchico e che individuano, in astratto, le funzioni, competenze e attività del Titolare
Cloud della PA	Ambiente virtuale che consente alle Pubbliche Amministrazioni di erogare servizi digitali a cittadini e imprese nel rispetto dei requisiti minimi di sicurezza e affidabilità
Codice o CAD	Codice dell'amministrazione digitale, Decreto legislativo n. 82 del 7 marzo 2005, aggiornato con il Decreto Legge n. 76 del 16 luglio 2020 noto come Decreto Semplificazioni
Codec	Algoritmo di codifica e decodifica che consente di generare flussi binari, eventualmente imbustarli in un file o in un wrapper (codifica), così come di estrarli da esso (decodifica)
Conservatore	Soggetto pubblico o privato che svolge attività di conservazione di documenti e aggregazioni informatiche
Conservazione	Attività finalizzate a definire le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione
Convenzioni di denominazione del file	Insieme di regole sintattiche che definisce il nome dei file all'interno di un filesystem o pacchetto

Coordinatore della Gestione Documentale	Soggetto responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 nei casi di amministrazioni che abbiano istituito più AOO
Destinatario	Soggetto o sistema al quale il documento informatico viene indirizzato
Digest	Vedi "Impronta crittografica"
CRL	Certificate revocation list, ossia la lista dei certificati revocati o sospesi
Documento amministrativo informatico	Ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa
Documento elettronico	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva
Documento informatico	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Duplicato informatico	Il documento informatico ottenuto mediante la memorizzazione sullo stesso dispositivo o su dispositivi diversi della medesima sequenza di valori binari del documento originario
DSO	Digital Services Outsourcing di Siav S.p.A.
eSeal	Vedi sigillo elettronico
Esibizione	Operazione che consente di visualizzare un documento conservato
eSignature	Vedi firma elettronica
Estratto informatico	Parte del documento con una diversa evidenza informatica rispetto al documento da cui è tratto
Estratto per riassunto di documento informatico	Documento nel quale si attestano in maniera sintetica fatti, stati o qualità desunti da documenti informatici
Estrazione statica dei dati	Estrazione di informazioni utili da grandi quantità di dati (es. database, datawarehouse ecc...), attraverso metodi automatici o semi-automatici

Evidenza informatica	Sequenza finita di bit che può essere elaborata da una procedura informatica
Fascicolo informatico	Aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento
File	Insieme di informazioni, dati o comandi logicamente correlati, raccolti sotto un unico nome e registrati, per mezzo di un programma di elaborazione o di scrittura, nella memoria di un computer
File-manifesto	File che contiene metadati riferiti ad un file o ad un pacchetto di file
Filesystem	Sistema di gestione dei file, strutturato mediante una o più gerarchie ad albero, che determina le modalità di assegnazione dei nomi, memorizzazione e organizzazione all'interno di uno storage
Firma elettronica	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare
Firma elettronica avanzata	Una firma elettronica avanzata soddisfa i seguenti requisiti: a) è connessa unicamente al firmatario; b) è idonea a identificare il firmatario; c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.
Firma elettronica qualificata	Una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche
Firma digitale	Un particolare tipo di firma qualificata basata su un su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo 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
Flusso (binario)	Sequenza di bit prodotta in un intervallo temporale finito e continuativo che ha origine precisa ma di cui potrebbe non essere predeterminato il suo istante di interruzione
Formato contenitore	Formato di file progettato per consentire l'inclusione ("imbustamento" o wrapping), in uno stesso file, di una o più evidenze informatiche soggette a differenti tipi di codifica e al quale possono essere associati specifici metadati

Formato del documento informatico	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
Formato "deprecato"	Formato in passato considerato ufficiale il cui uso è attualmente sconsigliato a favore di una versione più recente
FTP server	Programma che permette di accettare le connessioni in entrata e di comunicare con un client attraverso protocolli criptati S-FTP/FTPS
Funzione di *hash* crittografica	Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o digest (vedi) in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
Gestione documentale	Processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta, uso, selezione e conservazione dei documenti
Hash	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
Identificativo univoco	Sequenza di numeri o caratteri alfanumerici associata in modo univoco e persistente ad un'entità all'interno di uno specifico ambito di applicazione
Impronta crittografica	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di hash crittografica a un'evidenza informatica
Integrità	Caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità
Interoperabilità	Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi
Leggibilità	Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica

Metadati	Dati associati a un o documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017
Indice del pacchetto di archiviazione	File xml generato in fase di firma e marca temporale del 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
Naming convention	Vedi "Convenzioni di denominazione"
Oggetto di conservazione	Oggetto digitale versato in un sistema di conservazione
Oggetto digitale	Oggetto informativo digitale, che può assumere varie forme tra le quali quelle di documento informatico, fascicolo informatico, aggregazione documentale informatica o archivio informatico
ISO	International Organization for Standardization (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	Documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture
Manuale di gestione	Documento informatico che descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi
Pacchetto di archiviazione	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel manuale di conservazione
Pacchetto di distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione

Pacchetto di file (*file package)*	Insieme finito di più file (possibilmente organizzati in una struttura di sottoalbero all'interno di un filesystem) che costituiscono, collettivamente oltre che individualmente, un contenuto informativo unitario e auto-consistente
Pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione
Pacchetto informativo	Contenitore logico che racchiude uno o più oggetti di conservazione con i relativi metadati, oppure anche i soli metadati riferiti agli oggetti di conservazione
Percorso	Informazioni relative alla localizzazione virtuale del file all'interno del filesystem espressa come concatenazione ordinata del nome dei nodi del percorso
Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi
Piano di classificazione (Titolario)	Struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata
Piano di conservazione	Documento, allegato al manuale di gestione e integrato con il sistema di classificazione, in cui sono definiti i criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445
Piano di organizzazione delle aggregazioni documentali	Strumento integrato con il sistema di classificazione a partire dai livelli gerarchici inferiori di quest'ultimo e finalizzato a individuare le tipologie di aggregazioni documentali (tipologie di serie e tipologie di fascicoli) che devono essere prodotte e gestite in rapporto ai procedimenti e attività in cui si declinano le funzioni svolte dall'ente
Piano generale della sicurezza	Documento 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 e, in caso di affidamento del servizio all'esterno, dagli accordi stipulati tra il titolare dell'oggetto di conservazione e il responsabile del servizio di conservazione
Processo	Insieme di attività correlate o interagenti che trasformano elementi in ingresso in elementi in uscita

Produttore del PdV	Persona fisica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con il responsabile della gestione documentale
qSeal	Sigillo elettronico qualificato, come da art. 35 del Regolamento eIDAS
qSignature	Firma elettronica qualificata, come da art. 25 del Regolamento eIDAS
Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore
Registro particolare	Registro informatico individuato da una pubblica amministrazione per la memorizzazione delle informazioni relative a documenti soggetti a registrazione particolare
Registro di protocollo	Registro informatico ove sono memorizzate le informazioni prescritte dalla normativa per tutti i documenti ricevuti e spediti da un ente e per tutti i documenti informatici dell'ente stesso
Repertorio	Registro su cui vengono annotati con un numero progressivo i fascicoli secondo l'ordine cronologico in cui si costituiscono all'interno delle suddivisioni del piano di classificazione
Regolamento eIDAS	electronic IDentification Authentication and Signature, Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE
Responsabile del servizio di conservazione (RSC)	Soggetto che coordina il processo di conservazione all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Responsabile della conservazione (RDC)	Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia
Responsabile della funzione archivistica di conservazione (RFA)	Soggetto che coordina il processo di conservazione dal punto di vista archivistico all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Responsabile della gestione documentale (RGD)	Soggetto responsabile della gestione del sistema documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445

Responsabile della protezione dei dati (RPD)	Persona con conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, in grado di assolvere i compiti di cui all'articolo 39 del Regolamento (UE) 2016/679
Responsabile dei sistemi informativi per la conservazione (RSI)	Soggetto che coordina i sistemi informativi all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Responsabile della sicurezza dei sistemi per la conservazione (RSS)	Soggetto che assicura il rispetto dei requisiti di sicurezza all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Responsabile dello sviluppo e della manutenzione del sistema di conservazione (RSM)	Soggetto che assicura lo sviluppo e la manutenzione del sistema all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Riferimento temporale	Insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC)
Riversamento	Procedura mediante la quale uno o più documenti informatici sono convertiti da un formato di file (ovvero di busta, ovvero di pacchetto di file) ad un altro, lasciandone invariato il contenuto per quanto possibilmente permesso dalle caratteristiche tecniche del formato (ovvero dei formati) dei file e delle codifiche di destinazione
Scarto	Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico-culturale
Serie	Raggruppamento di documenti con caratteristiche omogenee (vedi anche aggregazione documentale informatica)
Sigillo elettronico	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi
Sistema di conservazione (SDC)	Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, comma 1, del CAD
Sistema di gestione informatica dei documenti	Insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle organizzazioni per la gestione dei documenti. Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445
Timeline	Linea temporale virtuale su cui sono disposti degli eventi relativi ad un sistema informativo o a un documento informatico. Costituiscono esempi molto diversi di timeline un file di log di sistema, un flusso multimediale contenente essenze audio\video sincronizzate

Titolare dell'oggetto di conservazione	Soggetto produttore degli oggetti sottoposti a conservazione
Trasferimento	Passaggio di custodia dei documenti da una persona o un ente ad un'altra persona o un altro ente
Ufficio	Riferito ad un'area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico
Utente abilitato	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse
Versamento	Passaggio di custodia, di proprietà e/o di responsabilità dei documenti. Nel caso di un organo giudiziario e amministrativo dello Stato operazione con la quale il responsabile della conservazione trasferisce agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali
Virgilio	Sistema di conservazione 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 (anche noto come TUDA);

- 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 frequentemente, l'ultima revisione è avvenuta con l'emanazione del D. Lgs. n. 217 del 13 dicembre 2017, pubblicato in GU n. 9 del 12 gennaio 2018 e infine con il D.L. n. 76 del 16 luglio 2020 noto come *Decreto Semplificazioni*

- 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.

- 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, formate da un documento principale e da 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 10 settembre 2020.

A partire dalla data di attuazione (1° gennaio 2022) saranno abrogati i seguenti decreti:

- il DPCM 13 novembre 2014 contenente "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici";
- il DPCM 3 dicembre 2013 contenente "Regole tecniche in materia di sistema di conservazione";
- Circolare AGID n. 60 del 23 gennaio 2013 in materia di "Formato e definizione dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le Pubbliche amministrazioni" che viene sostituita dall'allegato 6 "Comunicazione tra AOO di documenti amministrativi protocollati".

Per quanto riguarda il DPCM del 3 dicembre 2013 "Regole tecniche in materia di protocollo informatico" a partire dalla data di applicazione delle Linee guida sono abrogate tutte le disposizioni del DPCM fatte salve le seguenti:

- art. 2 comma 1, Oggetto e ambito di applicazione;
- art. 6, Funzionalità;
- art. 9, Formato della segnatura di protocollo;
- art. 18 commi 1 e 5, Modalità di registrazione dei documenti informatici;
- art. 20, Segnatura di protocollo dei documenti trasmessi;
- art. 21, Informazioni da includere nella segnatura.

- Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici pubblicato il 25 giugno 2021 con determinazione AGID n. 455/2021. Tale Regolamento definisce i nuovi criteri per la fornitura del servizio di conservazione dei documenti informatici, fissando in un apposito allegato i requisiti generali nonché i requisiti di qualità, di sicurezza e organizzazione necessari per la fornitura del servizio. Composto di due allegati tecnici, il Regolamento è emanato secondo quanto previsto dall'articolo 34, comma 1-bis del Decreto legislativo n. 82/2005, come integrato e modificato dal Decreto Semplificazione (D.L. 76/2020), convertito con Legge n. 120/2020 ed entrerà in vigore il 1° gennaio 2022, data a partire dalla quale è abrogata la Circolare n. 65/2014 "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".

Torna al sommario

3.2 Standard per la conservazione digitale

Di seguito gli standard per la conservazione digitale previsti dalla normativa vigente (Allegato 4 "Standard e Specifiche tecniche" - Linee Guida sulla formazione, gestione e conservazione dei documenti informatici).

- **UNI 11386** - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali

- **ISO 14721** - OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione

- **ISO 15836** - Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core
- **ISO/TR 18492** - Long-term preservation of electronic document-based information
- **ISO 20652** - Space data and information transfer systems - Producer-Archive interface - Methodology abstract standard
- **ISO 20104** - Space data and information transfer systems — Producer-Archive Interface Specification (PAIS)
- **ISO/CD TR 26102** - Requirements for long-term preservation of electronic records
- **SIARD** Software Independent Archiving of Relational Databases 2.0
- **Ministère de la culture et de la communication**, Service interministériel des Archives de France, Standard d'échange de donnéès pour l'archivage. Transfert – Communication – Élimination – Restitution - Modification, ver. 2.1, 2018
- **METS -** Metadata Encoding and Transmission Standard
- **PREMIS –** PREservation Metadata: Implementation Strategies
- **EAD (3)/ISAD (G)**
- **EAC (CPF)/ISAAR (CPF)/NIERA (CPF)**
- **SCONS2/EAG/ISDIAH**

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 elettronici.

Il Conservatore possiede la certificazione UNI CEI EN ISO/IEC 27001 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 in possesso dei requisiti professionali indicati dalla Circolare AGID; di seguito l'elenco dettagliato.

Ruolo	Nominativo	Attività di competenza	Data di decorrenza
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]

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

Ruolo	Nominativo	Attività di competenza	Data di decorrenza
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 il Titolare 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
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 del Titolare, 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; • Attività di supporto al Titolare per il trasferimento al sistema di	Dal 1°ottobre 2014

	Giulia Colombo	conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza	Dal 14 gennaio 2022
	Arianna Santin		Dal 14 giugno 2022

Ruolo	Nominativo	Attività di competenza	Data di decorrenza
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 il Titolare; • 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
	Matteo Fiocchi		Dal 3 agosto 2021
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
Consulente interno	Daniela Perrone	Supporto tecnico – normativo per le attività afferenti al servizio di conservazione di documenti fiscali	Dal 3 novembre 2014

L'Ufficio Risorse umane aggiorna e conserva gli atti di delega e le lettere di incarico.

Torna al sommario

4.2 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 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 a 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 – Titolare)***
Responsabile della conservazione	Per le Pubbliche amministrazioni è un ruolo previsto dall'organigramma del Titolare dell'oggetto di conservazione; per i soggetti diversi dalla Pubblica Amministrazione, il ruolo del responsabile della conservazione può essere svolto da un soggetto esterno all'organizzazione, in possesso di idonee competenze giuridiche, informatiche ed archivistiche, purché terzo rispetto al Conservatore al fine di garantire la funzione del Titolare dell'oggetto di conservazione rispetto al sistema di conservazione
Delegati del Responsabile della conservazione	Il responsabile della conservazione, sotto la propria responsabilità, può delegare lo svolgimento delle proprie attività o parte di esse ad uno o più soggetti, che all'interno della struttura organizzativa, abbiano specifiche competenze ed esperienze. Tale delega, riportata nel manuale di conservazione, deve individuare le specifiche funzioni e competenze delegate
Utente abilitato	Può essere interno oppure esterno al Titolare

Il presente Manuale descrive il processo di conservazione svolto per i Clienti che affidano il servizio in outsourcing al Conservatore Siav S.p.A. L'affidamento del servizio viene formalizzato e sottoscritto tra le parti; il Titolare, ente pubblico o soggetto privato, adotta un proprio Manuale di conservazione e sottoscrive il documento "Accordi di servizio" predisposto dal Conservatore. Il servizio viene erogato dal DSO Siav nel rispetto dei requisiti di continuità, sicurezza fisica e logica, backup, monitoraggio, presidio operativo-sistemistico. Siav garantisce l'aderenza del servizio alla normativa vigente, aggiornando il software e informando tempestivamente i Clienti per eventuali variazioni 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 – Titolare)***
Responsabile della conservazione	Per le Pubbliche amministrazioni è un ruolo previsto dall'organigramma del Titolare dell'oggetto di conservazione; per i soggetti diversi dalla Pubblica Amministrazione, il ruolo del responsabile della conservazione può essere svolto da un soggetto esterno all'organizzazione, in possesso di idonee competenze giuridiche, informatiche ed archivistiche, purché terzo rispetto al Conservatore al fine di garantire la funzione del Titolare dell'oggetto di conservazione rispetto al sistema di conservazione
Eventuali delegati del Responsabile della conservazione	Il responsabile della conservazione, sotto la propria responsabilità, può delegare lo svolgimento delle proprie attività o parte di esse a uno o più soggetti, che all'interno della struttura organizzativa, abbiano specifiche competenze ed esperienze. Tale delega, riportata nel manuale di conservazione, deve individuare le specifiche funzioni e competenze delegate
Responsabile del servizio di conservazione	Conservatore
Responsabili, delegati e incaricati coinvolti	Conservatore
Responsabile per l'attivazione del servizio	Project Manager del Conservatore
Utente abilitato	Può essere interno oppure esterno al Titolare

A prescindere dal modello organizzativo adottato, il Titolare individua il Responsabile della conservazione con un atto formale. Nel caso di affidamento a terzi, il produttore del PdV provvede a generare e trasmettere al sistema di conservazione i pacchetti di versamento nelle modalità e con i formati concordati con il conservatore e descritti nel manuale di conservazione. Provvede inoltre a verificare il buon esito della operazione di trasferimento al sistema di conservazione tramite la presa visione del rapporto di versamento prodotto dal sistema di conservazione stesso.

I ruoli individuati nel processo di conservazione sono:

- titolare dell'oggetto della conservazione;
- produttore del PdV;
- utente abilitato;
- responsabile della conservazione;
- conservatore.

Viene di seguito fornita una descrizione dettagliata:

- Il Titolare rappresenta il Soggetto produttore degli oggetti di conservazione il cui Responsabile della conservazione affida al Conservatore la gestione del servizio di conservazione;
- il Produttore del PdV rappresenta la persona fisica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con il responsabile della gestione documentale;
- l'utente abilitato rappresenta la persona, l'ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse;
- il responsabile della conservazione rappresenta il soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia;
- il Conservatore rappresenta il soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici.

Coerentemente con quanto stabilito dal Codice dei beni culturali, il trasferimento al sistema di conservazione di documenti e aggregazioni documentali informatiche, appartenenti ad archivi pubblici e privati dichiarati di interesse storico particolarmente importante, è assoggettato all'obbligo di cui all'art. 21 del Codice dei Beni Culturali di comunicazione agli organi competenti in materia di tutela dei beni archivistici o, nel caso di affidamento esterno, alla loro autorizzazione.

Torna al sommario

4.3 Suddivisione delle responsabilità

Il Titolare a seguito della sottoscrizione di un contratto può affidare al Conservatore la gestione del servizio di conservazione secondo le modalità concordate negli Accordi di servizio.

Il Conservatore Siav S.p.A. individua nell'area DSO il personale coinvolto nelle varie fasi di processo come indicato nelle lettere di incarico predisposte dal Responsabile dello sviluppo e manutenzione; Virgilio è il nome del sistema di conservazione sviluppato da Siav per l'espletamento del servizio di conservazione.

Il Conservatore esegue le fasi previste dal processo di conservazione rimanendo in ogni caso inteso che la responsabilità giuridica generale sul processo di conservazione, non essendo delegabile, rimane in capo al responsabile della conservazione, chiamato altresì a svolgere le necessarie attività di verifica e controllo.

Il Conservatore esegue il servizio di conservazione dei documenti informatici trasmessi dal Titolare allo scopo di assicurarne la conservazione e di garantire le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità.

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

Le attività in carico al Titolare sono:

- approvazione del documento *Accordi di servizio* contenente la descrizione delle tipologie documentali con relativi formati e metadati, tempi di versamento e di conservazione;
- produzione del Pacchetto di versamento con i 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;
- assistenza al Pubblico ufficiale ed esibizione alle Autorità competenti.

Alcune attività, quali ad esempio l'estrazione del PdV dal sistema 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 Titolare dell'archivio è quindi informato sui diritti di accesso ai dati personali e quanto previsto dalla normativa vigente.

Il nuovo Regolamento europeo sulla protezione dei dati personali (Regolamento (UE) 2016/679 – cd. "GDPR"), ha definito le seguenti figure:

- Titolare del Trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (art. 4, par. 1, n. 7 GDPR);
- Responsabile del trattamento: la persona fisica, giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (art. 4, par. 1, n. 8 GDPR);
- Responsabile della Protezione dei Dati (c.d. Data Protection Officer o D.P.O.): figura prevista dagli artt. 37 e seguenti del GDPR che ne disciplinano compiti, funzioni e responsabilità.

Al Titolare del Trattamento, ai sensi dell'art. 24 del GDPR, spetta l'adozione di misure tecniche e organizzative atte a garantire ed essere in grado di dimostrare che il trattamento effettuato è conforme al Regolamento ed in particolare:

- gli interventi normativi necessari per l'adeguamento al GDPR;
- l'attribuzione di funzioni e compiti ai "soggetti attuatori" per gli adempimenti previsti dal GDPR.

Il Responsabile del Trattamento, ai sensi dell'art. 28 del GDPR, è un soggetto esterno, con esperienza, capacità e conoscenza necessarie per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del Regolamento comunitario, anche relativamente al profilo della sicurezza, il quale effettua

trattamenti di dati personali per conto del Titolare sulla base di un contratto o da altro atto giuridico che determini la materia del trattamento, la durata, la finalità, le categorie di dati personali trattati, le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento.

I dati sono trattati dal Conservatore con strumenti automatizzati ai sensi della normativa vigente 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, l'utilizzo illecito o non corretto e gli accessi non autorizzati.

Di seguito il dettaglio.

- 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;
- 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 Responsabile della protezione dei dati individuato dal Conservatore.

Responsabile della protezione dei dati	**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 le sezioni dell'organigramma coinvolte nel servizio di conservazione.

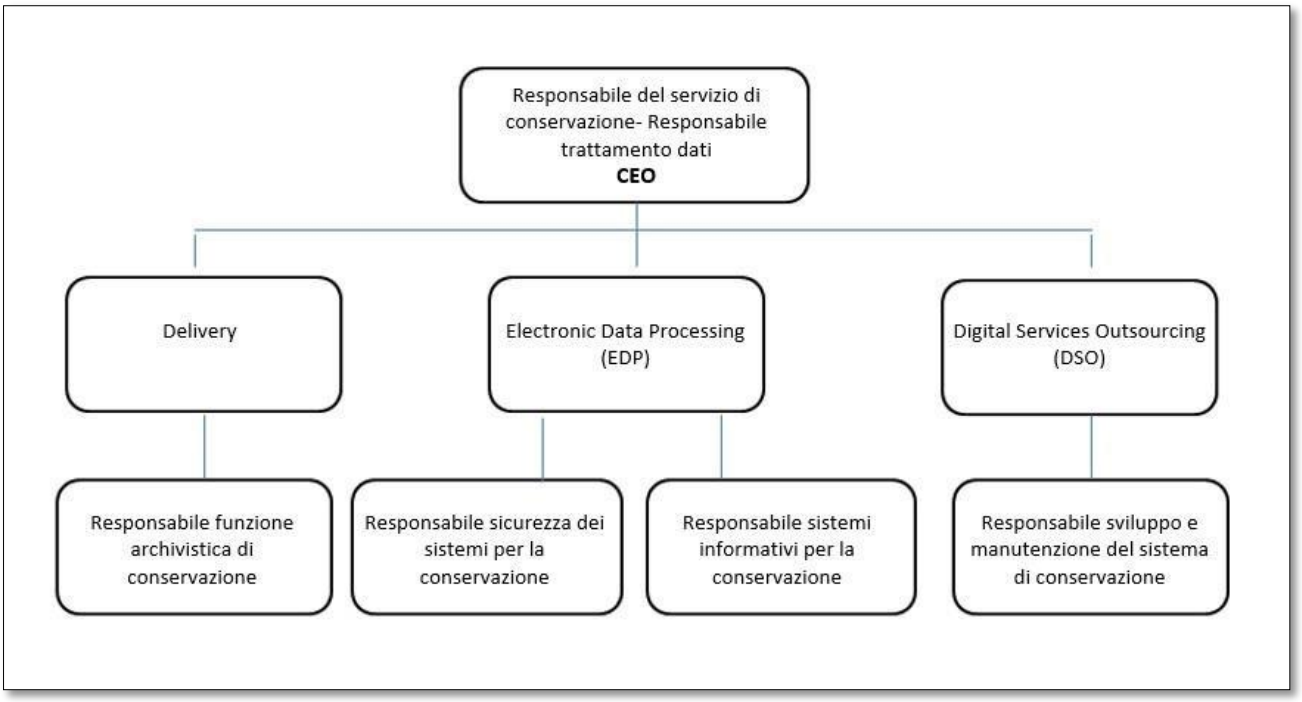

Figura 1 – Organigramma

Torna al sommario

5.2 Strutture organizzative

In questo paragrafo sono descritte le strutture organizzative coinvolte 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 elencate nella tabella sottostante con relativa area competente e il personale coinvolto.

Attività afferenti al singolo 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 tecnico - 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 del costo 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 inerenti le tipologie documentali da sottoporre a conservazione digitale	Conservatore e Titolare	Responsabile di progetto
Approvazione e trasmissione degli Accordi di servizio e atto di affidamento	Titolare	Il RDC del Titolare
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 del PDV*		
Attività	***Area competente***	***Personale coinvolto***
Generazione e invio del PdV secondo le modalità e le tempistiche concordate	Produttore PdV - Titolare	Sistemi
Acquisizione del 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 PdV - Titolare	Sistemi
Presa visione del RdV	Produttore PdV - Titolare	Sistemi
FASE 4: *Preparazione e gestione del PDA e del PDD*		
Attività	***Area competente***	***Personale coinvolto***
Preparazione e gestione del 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 del 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: *Selezione e scarto*		
Attività	***Area competente***	***Personale coinvolto***
Scarto della documentazione indicata nell'elenco di scarto approvato dalla Soprintendenza archivistica competente territorialmente	Titolare, Delivery, Area operativa	RSC, RSM, RFA
Conservazione degli elenchi di scarto e del Piano di conservazione del Titolare dell'archivio	Titolare, Delivery, Area operativa	RSC, RSM, RFA
FASE 6: *Attività di monitoraggio e controllo*		
Attività	***Area competente***	***Personale coinvolto***
Verifica dell'integrità e leggibilità del PdA conservato	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
Conduzione e manutenzione del SDC e change management	Sistemi informativi	RSS, RSI
Monitoraggio del sistema di conservazione	Sistemi informativi e Area operativa	RSM e operatori DSO

Torna al sommario

Ogni responsabile di area informa i propri collaboratori in merito alle procedure per la gestione degli interventi ed eventuale variazione delle stesse.

Il Conservatore pianifica il servizio di conservazione a seguito dell'avvenuta ricezione degli Accordi di servizio e dell'atto di affidamento, entrambi trasmessi tramite posta elettronica certificata dal Responsabile della conservazione del Titolare. Le comunicazioni tecniche ed eventuali richieste sono gestite tramite posta elettronica ordinaria 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 può essere un dato elettronico oppure un documento o un'aggregazione con relativi metadati che ne garantiscono la corretta interpretazione e comprensione del content information per un periodo indefinito di tempo.

Le principali tipologie documentali sottoposte a conservazione sono di seguito elencate:

- documenti protocollati;
- registro giornaliero di protocollo;
- provvedimenti, contratti, determine, ecc.;
- libri sociali e contabili;
- libro unico del lavoro;
- messaggi di posta elettronica certificata;
- fatture elettroniche e altra documentazione fiscale.

Per le Pubbliche amministrazioni si segnala l'obbligo di conservare anche le aggregazioni documentali informatiche.

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 Titolare, costituiscono metadati rilevanti per la conservazione nel lungo termine della documentazione; 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 al contenuto informativo, sia in fase di conservazione che di consultazione.

Le caratteristiche, i formati e metadati delle tipologie documentali sottoposte a conservazione sono descritti dettagliatamente nel documento "Accordi di servizio", predisposto dal Conservatore e firmato dal Titolare.

Torna al sommario

6.1 Metadati

Il contenuto informativo risulta caratterizzato da un insieme di 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.

Il set di metadati delle tipologie documentali trasferite in conservazione sono indicati negli "Accordi di servizio", documento concordato tra il Conservatore e il Titolare dell'archivio.

Si rimanda alle Linee Guida sulla formazione, gestione e conservazione dei documenti, Allegato 5 *"I metadati"* per consultare l'elenco dettagliato del set di metadati previsto per il documento informatico, per il documento amministrativo informatico e per l'aggregazione documentale informatica.

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 formazione del documento informatico 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**, ossia 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 ad un solo fornitore che ne detiene i diritti d'uso;
- **robustezza** ossia il coefficiente di robustezza di un formato elettronico che ne indica la probabilità, in caso di corruzione di un file, per il recupero parziale o totale 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 del file;
- **stabilità,** intesa come compatibilità con le versioni precedenti e quelle attuali;
- **sicurezza,** intesa come protezione da virus;
- **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.

Di seguito è riportato l'elenco dei formati 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 del formato per i file ricevuti all'interno del pacchetto 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 della documentazione versata 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.

I formati delle tipologie documentali trasferite in conservazione sono indicati negli "Accordi di servizio", documento concordato tra il Conservatore e il Titolare dell'archivio.

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

Il Titolare garantisce che il versamento dei documenti informatici avvenga tramite l'utilizzo di 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 sono versati dal Titolare al sistema di conservazione tramite Pacchetti informativi denominati Pacchetti di versamento.

Per maggiori dettagli si rimanda alle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, Allegato 2 "*Formati di File e Riversamento*".

Torna al sommario

6.3 Pacchetto di Versamento (PdV)

Il PdV rappresenta il pacchetto informativo proveniente dal Titolare, versato al sistema di conservazione e 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 Titolare e alla loro preparazione per la creazione del PdA.

Il documento "Accordi di servizio" include le condizioni di versamento concordate con il Titolare ovvero:

- aggregazioni e tipologie documentali da versare al sistema di conservazione;
- 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 del pacchetto informativo.

Il modulo di accettazione del sistema di conservazione mette a disposizione del Titolare una serie di funzionalità di validazione che gli consentono di modificare la composizione del PdV prima della sua acquisizione da parte del Conservatore. Il Titolare quindi sulla base degli accordi convenuti con il Conservatore può eseguire la conversione di formato oppure implementare i metadati descrittivi, ecc.

Torna al sommario

6.3.1 Conferimento del PDV con 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 documentali 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 del PdV 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 Titolare trasferisce i propri documenti nell'area predisposta dal Conservatore per la presa in carico del PDV. Il trasferimento del pacchetto e successiva presa in carico avviene in modalità manuale, automatica oppure semi-automatica.

La trasmissione del pacchetto risponde a precise caratteristiche quali ad esempio il formato zip e il nome del file non devono contenere spazi e 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 (ID univoco) del Titolare assegnato ad ogni oggetto/aggregazione documentale informatica.

L'ID univoco 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.

Per ulteriori dettagli sulle procedure per l'acquisizione del pacchetto di versamento si rimanda al Manuale tecnico del sistema di conservazione.

Torna al sommario

6.3.2 Conferimento del PDV con aggregazioni

Il fascicolo informatico rappresenta un'aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento.

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

Le tipologie di fascicolo si distinguono principalmente in:

- fascicolo di persona (fisica o giuridica);
- fascicolo di affare/attività;
- fascicolo di procedimento amministrativo.

I tempi di gestione del fascicolo nella fase corrente sono differenti a seconda della tipologia; in linea di massima la tempistica di conferimento del fascicolo nel SDC viene definita dal Titolare, fermo restando la possibilità di sottoporre a conservazione anche fascicoli relativi a procedimenti non conclusi.

La trasmissione del fascicolo al SDC può avvenire tramite un modulo sviluppato dal Conservatore oppure con altre modalità definite di volta in volta sulla base delle esigenze del Titolare.

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 del PdV trasferito dal Titolare 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 Titolare; 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.

Il documento "Accordi di servizio" include una tabella con la mappatura dei codici di errore che il SDC può riscontrare in fase di versamento.

In fase di acquisizione del PdV, in base agli accordi concordati tra le parti, è possibile applicare la cifratura per i dati considerati sensibili; in questo caso il Titolare consegna al Conservatore la chiave di decriptazione del PdA sottoposto 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 e rappresenta 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 11386:2020 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 del PdV può effettuare il re-invio del pacchetto. Successivamente sono effettuati ex novo i controlli definiti 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 rappresenta 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 alla data e all'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.

L'IPdA rappresenta l'evidenza informatica nel formato xml associata ad ogni PdA, contenente un insieme di informazioni definite dallo standard UNI 11386:2020 Standard SInCRO.

Al termine del processo il PDA viene firmato digitalmente dal Responsabile del servizio di conservazione o delegato e viene apposta una marca temporale.

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

Torna al sommario

6.6 Pacchetto di Distribuzione (PdD)

Il pacchetto di distribuzione (PdD) viene generato dal SDC contestualmente al PdA. L'utente abilitato effettua la ricerca dell'oggetto digitale in base al profilo di accesso configurato effettuando se previsto l'accesso alla console di esibizione del SDC.

Sulla base delle informazioni concordate nel documento "Accordi di servizio" il SDC localizza i documenti conservati in più PdA e su richiesta effettua il PdD selettivo.

Il PdD viene firmato digitalmente dal Responsabile del servizio di conservazione, memorizzato nel formato di file immagine .iso e messo a disposizione nell'area FTP.

L'esibizione del PdD è garantita anche attraverso la console web; se la richiesta arriva tramite PEC il responsabile del servizio di conservazione o delegato indicherà il link da cui il Titolare può accedere per effettuare il download del pacchetto.

Il PdD contiene:

- i documenti richiesti nel formato previsto per la loro visualizzazione;
- una estrazione di metadati associati agli oggetti digitali;
- l'indice di conservazione firmato e marcato;
- i viewer necessari alla visualizzazione degli oggetti digitali conservati.

Come già detto, l'utente rappresenta 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 nel sistema di conservazione e disponibile su richiesta anche su supporto ottico e/o analogico.

La richiesta di esibizione può essere inoltrata dal Titolare a Conservatore tramite due modalità:

- trasmissione di una PEC inclusiva dell'elenco del PdA o della documentazione di cui si richiede l'esibizione;
- effettuando l'accesso al sistema di conservazione tramite credenziali assegnate all'utente abilitato in fase di configurazione; 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 Titolare negli Accordi di servizio. Attraverso la console di esibizione il Titolare procede con la ricerca e la selezione della documentazione di cui richiede l'esibizione.

Il Titolare stabilisce i livelli di accesso e di consultabilità della propria documentazione soprattutto in casi di PdV contenenti dati sensibili.

Il responsabile della conservazione del Titolare comunica i nominativi e gli indirizzi di posta elettronica delle persone che dovranno 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 sintetizzato di seguito.

Figura 2 – Fasi del servizio di conservazione

Il servizio di conservazione si attiva a seguito di una 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 del pacchetto di versamento per la presa in carico

La produzione del PdV si ottiene a seguito del processo di estrazione degli oggetti digitali e relativi metadati dalle varie applicazioni informatiche adottate dal Titolare e dal successivo trasferimento al SDC. Il documento "Accordi di servizio" include la descrizione dettagliata afferente a:

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

Le modalità di versamento sono le seguenti:

- 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 viene conferito compresso, eventualmente criptato, preferibilmente con classi documentali omogenee. L'estrazione di metadati può avvenire mediante normalizzazioni a cura del Conservatore. I PdV conferiti sono presi in carico da un servizio per il versamento nel Sistema dunque esso è asincrono. I log degli accessi e conferimenti al server ftp/ftps sono conservati nel SDC; inoltre è possibile concordare una notifica via mail per la presa in carico del pacchetto di versamento. Nel caso di versamento tramite web services, il Titolare dialoga in modo sincrono con le interfacce del SDC. In fase di redazione degli Accordi di servizio, il Titolare dichiara gli indirizzi IP da cui intende connettersi al server scelto e riceve le credenziali di accesso all'area web. Il Titolare può effettuare la connessione esclusivamente da uno degli indirizzi dichiarati. Il Conservatore può offrire strumenti di supporto per la generazione del PdV che dialogano con i sistemi del Titolare:

- 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, ecc.);
- se il Titolare utilizza il Sistema documentale Archiflow viene predisposto un software apposito, sviluppato da Siav, che effettua l'estrazione degli oggetti digitali e relativi metadati per eseguire il versamento al SDC secondo le due forme alternative ftps/webservices.

Torna al sommario

7.2 Verifiche effettuate sul pacchetto di versamento e gli oggetti in esso contenuti

L'acquisizione del PdV nel SDC avviene con cadenza programmata, concordata con il Titolare sulla base della natura della documentazione versata e secondo i termini previsti dalla legge.

L'identificazione del Titolare 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 ed effettua i seguenti controlli:

- formato del file;
- validità della firma.

Il sistema notifica eventuali anomalie al responsabile della conservazione del Titolare tramite email generata in automatico; le verifiche sopra indicate possono restituire anche un esito negativo e quindi il sistema segnala la presenza di un'anomalia. I documenti sono anomali quando presentano dati illeggibili o incompleti, dati memorizzati su formati non compatibili, certificati di firma scaduta, ecc. In questi casi il sistema "rifiuta" i documenti con presenza di anomalia e genera contestualmente il RdV che contiene indicazioni afferenti le anomalie riscontrate. Il documento "Accordi di servizio" include l'elenco dei formati dei documenti che il Titolare sottopone al processo di conservazione.

Le eccezioni circa l'utilizzo di altri formati da parte del Titolare includono la possibilità di conservare i documenti in formati non compatibili con la conservazione a lungo termine per i quali non è 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 comprendono anche le verifiche volte ad identificare il formato del file. Comunemente il formato di un file viene riconosciuto attraverso la sua estensione; al fine di una corretta identificazione questo però non è 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 al fine di una corretta rappresentazione del file.

Torna al sommario

7.3 Accettazione del pacchetto 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 Titolare.

Torna al sommario

7.4 Rifiuto del pacchetto di versamento e modalità di comunicazione delle anomalie

Il PdV viene sottoposto ad una serie di controlli descritti nel precedente paragrafo, alcuni di questi sono eseguiti obbligatoriamente, altri invece concordati nel documento "Accordi di servizio".

Ulteriori controlli effettuati dal sistema riguardano la nomenclatura del pacchetto conferito 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 oppure una 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, ecc. In questi casi il sistema procede con un "rifiuto" di documenti per i quali sono state riscontrate le anomalie; il RdV rimane memorizzato nel SDC e reso disponibile al Titolare.

Torna al sommario

7.5 Preparazione e gestione del pacchetto di archiviazione

Conseguentemente all'acquisizione del PdV e produzione del RdV il Conservatore procede alla certificazione degli oggetti digitali contenuti nel pacchetto. Le modalità e le 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 risulta variabile a seconda del tempo di conferimento, in base alle esigenze del Titolare e alla normativa vigente.

La struttura del PdA "certificato" ovvero il PdA sottoposto a conservazione, rispecchia lo standard SInCRO UNI 11386:2020, norma riguardante la struttura dell'insieme del dato a supporto del processo di conservazione. In sintesi, il PdA rappresenta 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 nel file di log.

Torna al sommario

7.6 Preparazione e gestione del PdD ai fini dell'esibizione

Il sistema di conservazione restituisce in qualsiasi momento la documentazione richiesta dall'utente abilitato generando un PdD coincidente con il PdA oppure un PdD selettivo, formato da tipologie documentali e aggregazioni estratte da un numero variabile di PdA. La formazione del PdD risulta quindi condizionata dal soggetto richiedente e dallo scopo per il quale viene richiesta l'esibizione che può essere una verifica da parte dell'Autorità di controllo 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 può esibire tutti i documenti informatici nello stesso conservati in qualsiasi momento del periodo di conservazione, sulla base delle richieste di accesso e di esibizione eseguite dal soggetto abilitato/autorizzato.

Torna al sommario

7.7 Produzione di duplicati e copie informatiche

La divisione DSO, d'intesa con i Sistemi informativi, effettua il salvataggio dei dati e monitora le procedure per la generazione di copie e duplicati del PdA, previa richiesta trasmessa con PEC dal Titolare.

Il duplicato informatico rappresenta 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 del PdA sono prodotte nel momento in cui il PdA viene generato e memorizzato automaticamente sul server.

È possibile, previa richiesta del Titolare oppure in situazioni particolari, generare le copie anche su supporto ottico (DVD).

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

Torna al sommario

7.8 Scarto del pacchetto di archiviazione

Nessun documento o dato conservato può essere cancellato o modificato, se non in occasione della cessazione del contratto o delle procedure di selezione e scarto richieste tramite PEC dal Titolare. 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 considerata irrilevante dal punto di vista amministrativo, legale e storico.

La normativa vigente prevede l'obbligo per la pubblica amministrazione di adottare 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 aggregazioni documentali prodotte 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 documentale proposta per lo scarto, la quantità, la classificazione, gli estremi cronologici, la motivazione, il peso e i metri lineari. Il Titolare effettua lo scarto di uno o più PdA conservati in Virgilio; in questo caso il procedimento prende avvio dalla richiesta formale di scarto trasmessa dal Titolare al Conservatore tramite PEC. La richiesta, sottoscritta dal responsabile della gestione documentale del Titolare, include l'elenco di documenti, aggregazioni e relativi PdA proposti per lo scarto.

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 Titolare.

Si precisa che l'autorizzazione della Soprintendenza risulta necessaria anche per gli archivi prodotti da soggetti giuridici privati sottoposti a vigilanza a seguito della dichiarazione di notevole interesse culturale da parte del Ministero della Cultura ai sensi del D. Lgs. 22 gennaio 2004, n. 42 art. 13.

Torna al sommario

7.9 Modalità di intervento del pubblico ufficiale

Il Titolare assicura la presenza del pubblico ufficiale, nel caso 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 Titolare per le attività di esibizione e generazione del pacchetto di distribuzione.

Torna al sommario

7.10 Controlli di firme e marche

I soggetti che desiderano dotarsi di un dispositivo di firma digitale devono rivolgersi ai prestatori di servizi fiduciari accreditati, soggetti pubblici o privati che, sotto la vigilanza di AGID, emettono certificati qualificati (per la firma digitale) e certificati di autenticazione (per le carte nazionali dei servizi).

La firma digitale viene generata grazie ad una coppia di chiavi digitali asimmetriche attribuite in maniera univoca ad un soggetto, detto titolare:

- la **chiave privata** è conosciuta solo dal titolare ed è usata per generare la firma digitale da apporre al documento;
- la **chiave da rendere pubblica** è usata per verificare l'autenticità della firma.

Questo metodo è conosciuto come crittografia a doppia chiave e garantisce la piena sicurezza visto che la chiave pubblica non può essere utilizzata per ricostruire la chiave privata.

Vi sono due modalità di utilizzare la firma digitale:

- **in "locale":** si intende la firma digitale generata in uno strumento nel possesso fisico del titolare, smartcard o token
- **da "remoto":** si intende la firma digitale generata usando strumenti di autenticazione (tipicamente user id, password, OTP o telefono cellulare) che consentono la generazione della propria firma su un dispositivo (HSM) custodito dal certificatore (in terminologia europea, prestatore del servizio fiduciario qualificato).

Possono dotarsi di firma digitale tutte le persone fisiche: cittadini, amministratori e dipendenti di società e pubbliche amministrazioni. È possibile rivolgersi ai **prestatori di servizi fiduciari qualificati** autorizzati da AGID che garantiscono l'identità dei soggetti che utilizzano la firma digitale.

Per orientarsi in tale scelta, dalla pagina web del sito AGID "**Prestatori di servizi fiduciari attivi in Italia**" è possibile accedere ai siti web dei certificatori qualificati e scaricare i rispettivi Manuali operativi aggiornati.

La procedura adottata per i controlli sulle firme prevede la verifica dell'algoritmo utilizzato e la validità del certificato.

Inoltre, si procede con la verifica della Certification Authority autorizzata al rilascio di firme e per far questosi utilizza l'elenco dei soggetti inseriti nella lista ufficiale pubblicata sul sito istituzionale AGID.

I certificati delle chiavi di certificazione devono essere resi pubblici per verificare la validità dei certificati emessi dai certificatori autorizzati.

La marca temporale è un servizio offerto da un Certificatore accreditato, che consente di associare data e ora, certe e legalmente valide, a un documento informatico, permettendo una validazione temporale del documento opponibile a terzi.

Il servizio di Marcatura Temporale può essere utilizzato anche su documenti non firmati digitalmente. Il Regolamento eIDAS introduce due definizioni:

- **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 che soddisfa i requisiti di cui all'articolo 42 del Regolamento eIDAS.

La validazione temporale elettronica dà luogo a una presunzione legale relativa alla certezza della data e dell'ora. Se i prestatori di servizi fiduciari (Trust Service Providers - TSP) intendono avviare la prestazione di un servizio fiduciario qualificato dovranno trasmettere all'Organismo di vigilanza (AGID) l'intenzione di "Avviare un servizio fiduciario qualificato", allegando anche una relazione di valutazione di conformità (Conformity Assessment Report) rilasciata da un organismo di valutazione di conformità (Conformity Assessment Body – CAB) accreditato da Organismi di accreditamento riconosciuti dagli Stati membri. Per l'Italia l'organismo di accreditamento è Accredia. Se l'Organismo di vigilanza conclude che il Prestatore di servizi fiduciari e i servizi fiduciari da esso prestati rispettano i requisiti previsti nel regolamento per i prestatori di servizi fiduciari qualificati e per i servizi fiduciari qualificati, concede la qualifica. La marcatura temporale è normata dagli articoli 41 e 42 del Regolamento eIDAS.

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 Linee Guida a garanzia del principio di interoperabilità tra sistemi di conservazione.

I pacchetti di archiviazione sono realizzati secondo i requisiti previsti dallo standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2020), che rappresenta descrive 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 del PdA secondo le modalità elencate:

- ricezione tramite PEC delle modalità di trasferimento e ulteriori informazioni;
- il Conservatore effettua l'estrazione dell'archivio digitale da restituire al Titolare;
- il RSM accedendo alla console del sistema di conservazione individua i Pacchetti di archiviazione che compongono l'archivio sottoposto a conservazione ed esegue una procedura di materializzazione su supporto ottico (DVD) oppure di storage;
- generazione di un report che contiene l'elenco di tutti i PdA con gli estremi di certificazione;
- in caso di restituzione degli 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 nell'area FTP del Titolare; viene trasmessa una PEC con il report dell'avvenuto deposito nell'area di download.

In alcuni casi, il Titolare può richiedere al Conservatore una relazione archivistica afferente all'archivio digitale restituito. In caso di cessazione del servizio, si effettua la cancellazione di tutti i dati previa comunicazione formale al Titolare. Per ulteriori approfondimenti si rimanda al Piano di cessazione del servizio di conservazione di Siav S.p.A.

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 del PdA nel sistema di conservazione effettuando verifiche dell'integrità fisica e logica dei documenti/fascicoli negli stessi contenuti;
- l'analisi della consistenza e completezza degli oggetti digitali e dell'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 si possono realizzare integrazioni che permettono ad altri sistemi di accedere da remoto alla documentazione.

Torna al sommario

8 IL SISTEMA DI CONSERVAZIONE

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

Il Sistema è in grado di gestire archivi di molteplici organizzazioni, applicando regole differenti e associando le tipologie documentali con gli attributi appropriati per 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).

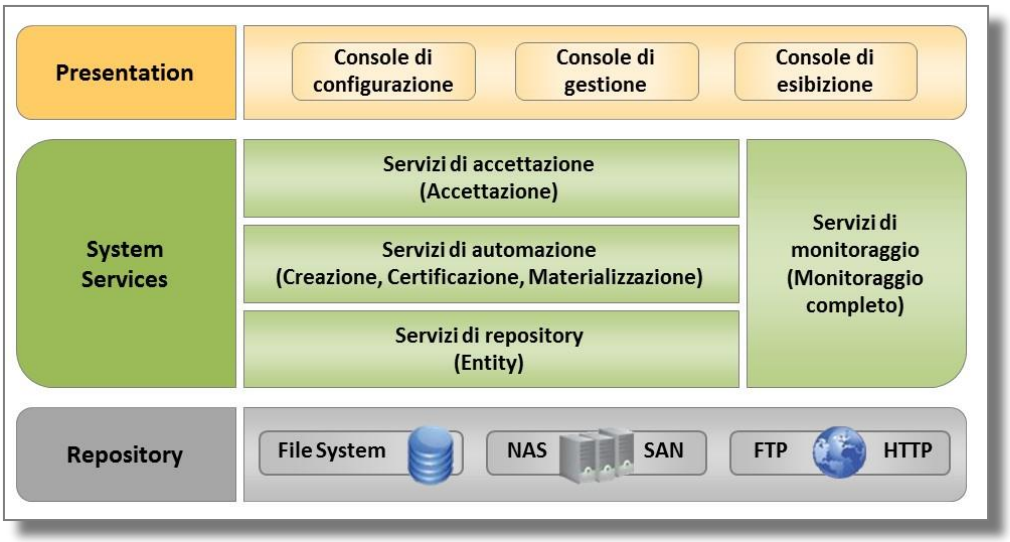

Figura 3 – Architettura three-tier

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 a responsabili e utenti abilitati di monitorare opportunamente il processo di conservazione accedendo alle seguenti console:

- **Console di configurazione** (disponibile solo sul client Windows), utilizzata dal responsabile del sistema per accedere a tutte le funzionalità di amministrazione;
- **Console di esibizione** (disponibile via web), per la ricerca e l'esibizione del PdD;
- **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 il PdA logico 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 del supporto utilizzato. In generale esso opera su tre diverse console:

- **Console di Accettazione e Consolidamento** (disponibile anche nella versione web), permette la firma digitale, dove richiesta, per documenti da importare in Virgilio;
- **Console di import del PdA**, permette di effettuare l'upload del 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 del 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 per il processo di 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, ecc.);
- associazione delle tipologie documentali al soggetto Titolare;
- verifica delle regole di conservazione ed esecuzione delle eventuali operazioni necessarie (firma e marca) in base alla tipologia documentale di appartenenza del documento;
- acquisizione del documento nel sistema Virgilio;
- archiviazione del documento in un PdA con generazione dell'IPdA;
- certificazione dell'IPdA;
- creazione delle copie del PdA (copie automatiche di backup);
- verifica dell'integrità di documenti informatici 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 del PdA, ecc.) e per l'esecuzione delle attività di Virgilio (monitoraggio, ecc.). 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 file di testo (stile CSV con separatore o a lunghezza fissa) e/o può interfacciarsi direttamente con Archiflow (oppure con un altro Sistema documentale) attraverso l'utilizzo di un modulo specifico;

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

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

4) *Materializzazione* - Creazione delle copie fisiche 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, ecc;

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 di una serie di funzionalità per la creazione di Aziende, tipologie documentali, ecc.; 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 del PdA corrente 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, ecc.;
- gestione del PdA di documenti;
- certificazione del PdA;
- materializzazione del PdA certificato;
- 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 di validità del certificato di firma;

- **il Modulo di Generazione del PdA** gestisce la trasformazione del 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 generazione dell'IPdA, avvisando il responsabile del servizio di conservazione della presenza di un nuovo PdA da certificare, permettendo allo stesso di monitorare il processo, firmare digitalmente e procedere con l'apposizione della firma digitale e marca temporale;

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

- **il Modulo di Monitoraggio** controlla con cadenza configurabile l'integrità del PdA e della documentazione in esso contenuti;

- **il Modulo di Gestione PdA** viene utilizzato per la gestione di dati e PdA ed in particolare per le informazioni versate e/o copiate 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 con la replica delle informazioni e ciò 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, con i due siti fisici utilizzati per l'erogazione del servizio.

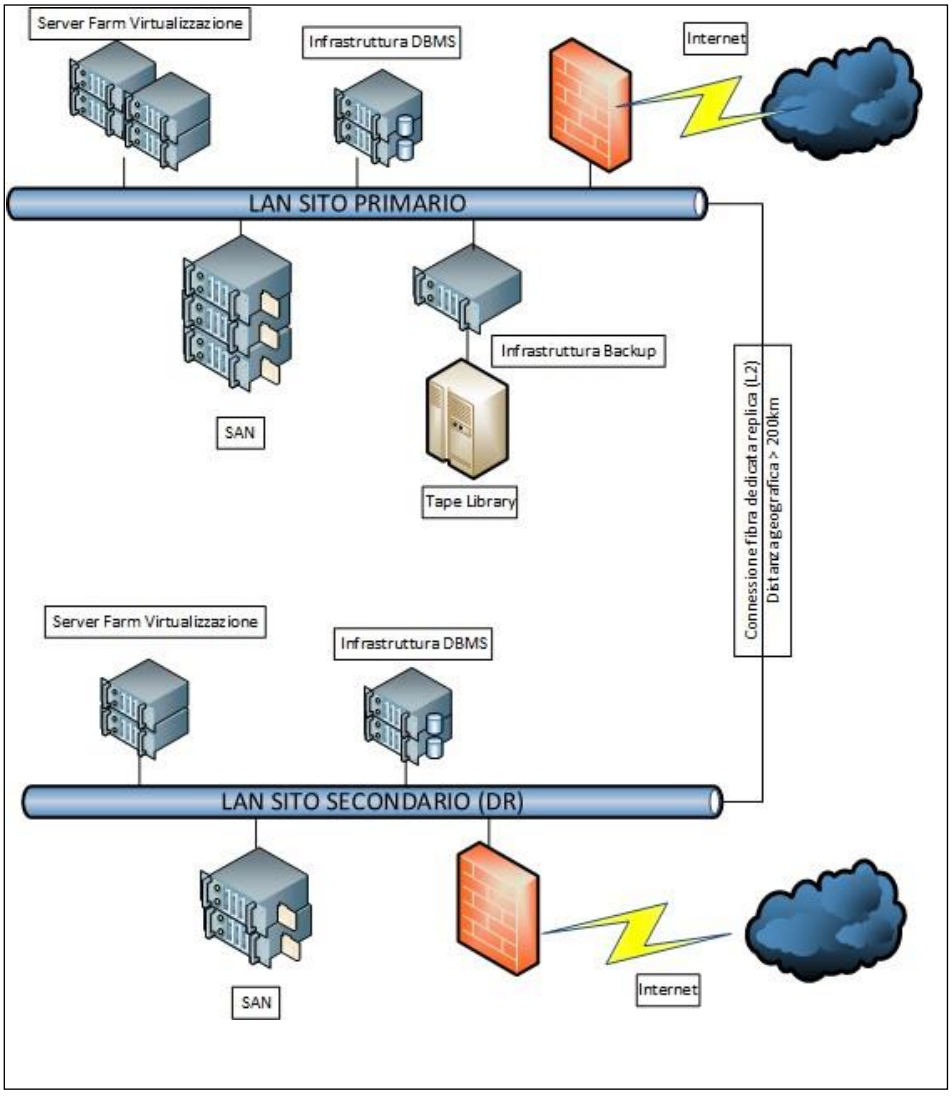

Figura 4 – Infrastruttura Disaster Recovery

8.3 Componenti fisiche

L'architettura del SDC è stata progettata per gestire in modo ottimale la performance del processo 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 il SDC risulta configurato su macchine dedicate, gli schemi database e le reti sono separate, la SAN è frazionata, ecc.

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 a 200 km dal sito primario.

Per ulteriori dettagli si rimanda al Piano della sicurezza.

Torna al sommario

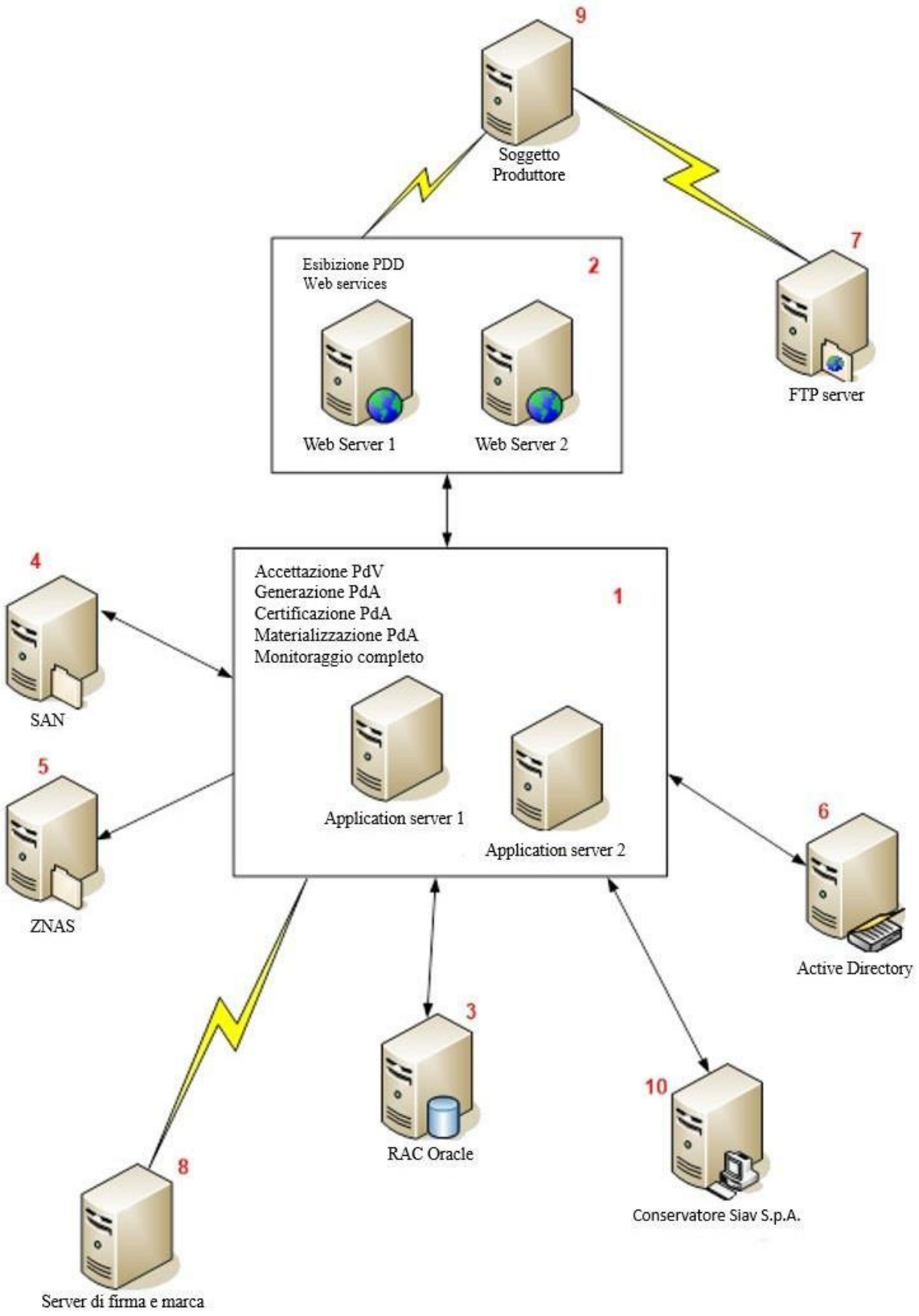

Figura 5 – Architettura base del sistema

Di seguito una rapida descrizione della figura 5:

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 viene 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 il protocollo S-FTP/FTP-S;

8) per i controlli di 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 (URL di riferimento "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

Il documento "Piano della sicurezza di Siav S.p.A." include descrizioni dettagliate quali a titolo indicativo e non esaustivo:

- 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 file di log.

La procedura di rilascio di pacchetti con evolutive del SDC segue i requisiti imposti dalla certificazione UNI CEI EN ISO/IEC 27001, 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 del cambiamento 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 del sistema 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 del sistema operativo

Il RSI con il proprio team procede all'occorrenza con le seguenti azioni:

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

Nel caso in cui non siano stati rilevati errori si procede con 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 del malfunzionamento dalle procedure e programmi;
- **manutenzione adattiva**, comprende l'attività di manutenzione volta ad assicurare la costante aderenza delle procedure e del programma all'evoluzione dell'ambiente tecnologico del sistema informativo e al cambiamento dei requisiti (organizzativi, normativi, ecc.);
- **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 al Manuale operativo del SDC.

Le componenti da modificare possono essere più o meno estese ma generalmente la procedura include i seguenti passaggi:

- 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 al nodo attivo;
- esecuzione di un test relativo alle funzioni critiche impattate dall'aggiornamento;
- in caso di fallimento viene redatto il verbale con l'elenco delle problematiche riscontrate 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 ha una durata pari a 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 Adeguamenti normativi

Il Conservatore pianifica processi di audit interni riguardanti aspetti normativi, di processo, organizzativi, tecnologici e logistici. L'obiettivo di tali processi è quello di accertare la conformità del sistema alla normativa e agli standard in vigore. 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 del processo. Siav, forte della sua ventennale competenza in ambito normativo e archivistico, ha costituito un *Osservatorio Normativo*, un organo di consulenza che offre la solida conoscenza di normative e leggi italiane riguardo la gestione e conservazione dei documenti con l'obiettivo di monitorare norme, regolamenti, circolari, e più in generale la normativa avente un 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 requisiti conseguenti al monitoraggio normativo vengono condivisi con la divisione Software Development; successivamente tra le divisioni coinvolte viene approvata una roadmap con la pianificazione degli interventi e 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 di documenti e 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 Titolare, 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 si ottiene la verifica dell'integrità e dell'autenticità del documento.

La leggibilità della documentazione conservata 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 Titolare coinvolge un pubblico ufficiale per produrre l'attestazione di conformità della copia all'originale.

Torna al sommario

9.2 Verifica dell'integrità dell'archivio

Il Conservatore effettua le verifiche di integrità e leggibilità del PdA e in caso di obsolescenza dello stesso procede con la 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 dal responsabile della conservazione e/o dal responsabile dei sistemi informativi;
- **controlli e manutenzione** delle strutture hardware e software.

I responsabili della sicurezza e 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 del 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 di certificati e 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 del PdV sono evidenziate anche nel 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 viene illustrata la procedura di risoluzione delle principali anomalie che possono verificarsi in fase di versamento.

Fase di versamento		
Anomalia	***Area competente***	***Procedura***
Verifica della nomenclatura del pacchetto e degli oggetti digitali contenuti	Area operativa	Il SDC rileva eventuali incongruenze rifiutando il PdV
Verifica dell'impronta	Area operativa	Viene verificata l'impronta della documentazione versata 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 del PdV un nuovo invio del PdV
Errori non previsti	Produttore e Area operativa	Il Titolare evidenzia il problema al conservatore che pianifica la procedura per la risoluzione. Il verbale di anomalia contenente la descizione dell'anomalia e relativa soluzione adottata viene inserito nel PdA di riferimento.

Torna al sommario