

MANUALE DI CONSERVAZIONE

di TEAMSYSTEM SERVICE S.R.L.



EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	04/12/2025	Stefano Franzoso	Responsabile Funzione Archivistica di Conservazione
Verifica e Approvazione	17/12/2025	Paola Lavezzaro	Responsabile del Servizio di Conservazione

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche sostanziali apportate	Osservazioni
1.0	21/04/2015	Prima versione del Manuale della Conservazione conforme allo schema del Manuale pubblicato da AgID per la procedura di accreditamento ai sensi dell'art. 44-bis del CAD e della Circolare AgID n. 65/2014	
2.0	09/10/2015	- Aggiornamento dei requisiti normativi (parag. 3.1); - Revisione struttura modello-dati del Pacchetto di Versamento e Archiviazione (parag 6.4, 6.6); - Inserimento maggior dettagli su gestione dei fascicoli informatici nel manuale (parag. 6.2.3, 6.4, 6.5, 6.6, 6.7, 7.5, 7.8); - Aggiunta di maggiori informazioni esplicative nel Manuale in relazione alla struttura dati dell'Indice del Pacchetto di Versamento (parag. 6.4).	
2.1	20/01/2016	- Revisione per specificazione della natura del Responsabile della Conservazione interno al Produttore e del Responsabile del Servizio di	

		Conservazione interno al Conservatore (parag. 4, 5.2, 6.5, 6.6, 6.7, 7.3, 7.5 e 7.6) - Modifiche di carattere formale e di formattazione al fine di garantire i requisiti di accessibilità al manuale	
2.2	12/02/2016	- Applicazione di testo alternativo alle figure per rendere il contenuto del documento completamente accessibile	
2.3	23/01/2017	- Modifica del Data Center secondario	
2.4	31/07/2017	- Modifica del Responsabile sviluppo e manutenzione del sistema di conservazione - Integrazione agli standard di riferimento	
2.5	07/05/2018	- Modifica del Responsabile Sicurezza del sistema per la conservazione e del Responsabile Sistemi Informativi per la conservazione - Aggiornamento variazione della sede legale ed operativa di Teamsystem Service S.r.l. - Aggiunta di tre risoluzioni dell'Agenzia delle Entrate nel paragrafo 3.1 "Normativa di Riferimento"	
2.6	28/09/2018	- Aggiornamento organigramma con inserimento del nominativo del Responsabile Sicurezza del sistema per la conservazione e del Responsabile Sistemi Informativi per la conservazione - Nuova nomina responsabile del trattamento dei dati	
2.7	05/08/2019	- Aggiornamento della Normativa di Riferimento (par.3.1) - Modifica delegati operativi del Responsabile del Servizio di Conservazione (tabella al Capitolo 4) - Aggiunti controlli di validità sui Pacchetti di Versamento (Par.7.2) - Inserimento Piano di Cessazione (Par. 7.10) - Modifiche alle componenti logiche, tecnologiche e fisiche del sistema (Capitolo 8) - Modifiche ad alcune figure	
2.8	09/04/2020	- Aggiornamento relativo al ruolo del Responsabile della Conservazione (Capitolo 4)	
2.9	05/11/2021	- Revisione sostanziale di tutto il documento per adeguamento a nuove Linee Guida AgID - Aggiornamento relativo ai ruoli della struttura organizzativa del Conservatore Teamsystem Service (Capitolo 4) - Variazioni dell'infrastruttura del sistema di conservazione (Capitolo 8) - Modifiche nella gestione dei log (Paragrafo 9.1.4)	
2.10	30/01/2023	- Aggiornamento degli standard di riferimento (Paragrafo 3.2)	

		- Aggiornamento relativo al Ruolo del Responsabile dello Sviluppo (Capitolo 4)	
2.11	04/10/2023	- Aggiornamento paragrafo 5.2- Strutture organizzative, per la parte di attivazione del Servizio - Aggiornamento paragrafo 8.1- Componenti logiche	
2.12	01/10/2025	- Aggiornamento paragrafo 5.2- Strutture organizzative - Aggiornamento paragrafo 7.8- Scarto dei Pacchetti di Archiviazione - Aggiornamento paragrafo 8.1-Componenti logiche - Aggiornamento paragrafo 8.2-Componenti tecnologiche - Aggiornamento paragrafo 8.3-Componenti fisiche	
3.0	17/12/2025	- Aggiornamento relativo ai ruoli della struttura organizzativa del Conservatore Teamsystem Service (Capitolo 4)	

Sommario

1.	SCOPO E AMBITO DEL DOCUMENTO	5
2.	TERMINOLOGIA (GLOSSARIO, ACRONIMI)	7
2.1	GLOSSARIO	7
2.2	ACRONIMI	11
3.	NORMATIVA E STANDARD DI RIFERIMENTO.....	12
3.1	NORMATIVA DI RIFERIMENTO	12
3.2	STANDARD DI RIFERIMENTO	14
4.	RUOLI E RESPONSABILITÀ.....	16
5.	STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE	20
5.1	ORGANIGRAMMA	20
5.2	STRUTTURE ORGANIZZATIVE	22
6.	OGGETTI SOTTOPOSTI A CONSERVAZIONE.....	28
6.1	OGGETTI CONSERVATI	28
6.2	METADATI	30
6.3	FORMATI	30
6.4	PACCHETTO DI VERSAMENTO	33
6.5	RAPPORTO DI VERSAMENTO	33
6.6	PACCHETTO DI ARCHIVIAZIONE	34
6.7	PACCHETTO DI DISTRIBUZIONE	37
7.	PROCESSO DI CONSERVAZIONE	39
7.1	MODALITÀ DI ACQUISIZIONE DEI PACCHETTI DI VERSAMENTO PER LA LORO PRESA IN CARICO	40
7.2	VERIFICHE EFFETTUATE SUI PACCHETTI DI VERSAMENTO E SUGLI OGGETTI IN ESSI CONTENUTI	42
7.3	ACCETTAZIONE DEI PACCHETTI DI VERSAMENTO E GENERAZIONE DEL RAPPORTO DI VERSAMENTO DI PRESA IN CARICO	42
7.4	RIFIUTO DEI PACCHETTI DI VERSAMENTO E RELATIVA COMUNICAZIONE	43
7.5	PREPARAZIONE E GESTIONE DEL PACCHETTO DI ARCHIVIAZIONE	43
7.6	PREPARAZIONE E GESTIONE DEL PACCHETTO DI DISTRIBUZIONE AI FINI DELL'ESIBIZIONE	44
7.7	PRODUZIONE DI DUPLICATI E COPIE INFORMATICHE E DESCRIZIONE DELL'EVENTUALE INTERVENTO DEL PUBBLICO UFFICIALE NEI CASI PREVISTI	45
7.8	SCARTO DEI PACCHETTI DI ARCHIVIAZIONE	45
7.9	PREDISPOSIZIONE DI MISURE A GARANZIA DELL'INTEROPERABILITÀ E TRASFERIBILITÀ AD ALTRI CONSERVATORI	47
8.	IL SISTEMA DI CONSERVAZIONE.....	48
8.1	COMPONENTI LOGICHE	48
8.2	COMPONENTI TECNOLOGICHE	50
8.3	COMPONENTI FISICHE	50
9.	MONITORAGGIO E CONTROLLI.....	52
9.1	PROCEDURE DI MONITORAGGIO	52
9.1.1	Procedure di audit interno	52
9.1.2	Procedure di audit sui fornitori	54
9.1.3	Monitoraggio dei fornitori	54
9.1.4	Monitoraggio delle operazioni nel sistema di log	54
9.1.5	Monitoraggio componenti hardware del sistema di Conservazione	56
9.1.6	Controllo autenticazione ed accesso al Servizio	57
9.1.7	Procedura di verifica periodica dei permessi di accesso alla piattaforma	58
9.1.8	Procedure di sicurezza	58
9.2	VERIFICA DELL'INTEGRITÀ DEGLI ARCHIVI	59
9.3	SOLUZIONI ADOTTATE IN CASO DI ANOMALIE	60
9.4	PROCESSO DI GESTIONE DEI CAMBIAMENTI HARDWARE, SOFTWARE E FIRMWARE	61

1. SCOPO E AMBITO DEL DOCUMENTO

Il presente documento ha lo scopo di descrivere, sulla base di quanto previsto dalle Linee Guida AgID in materia, la struttura organizzativa ed il funzionamento del sistema di conservazione del Conservatore **TEAMSYSTEM SERVICE S.r.l.**, che realizza e gestisce il processo di conservazione:

DATI DEL CONSERVATORE	
<i>Denominazione</i>	TeamSystem Service S.r.l. con Unico Socio Società del Gruppo TeamSystem controllata al 100% da TeamSystem S.p.A.
<i>Rappresentante Legale</i>	Fulvio Talucci
<i>Sede legale ed operativa</i>	Viale Giuseppe Ferro 86100 Campobasso (CB)
<i>Codice Fiscale e Partita Iva</i>	01641790702
<i>Registro Imprese</i>	Iscritta al Registro Imprese di Campobasso n. 01641790702
<i>Repertorio Economico Amministrativo</i>	Nr. R.E.A. 124222
<i>Capitale Sociale</i>	€ 200.000 Interamente versato
<i>Contatti</i>	teamsystemsrl@pecsicura.it

Più nel dettaglio, ai sensi delle Linee Guida AgID, il presente documento illustra 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 utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione denominato TeamSystem Archive.

La redazione del Manuale di Conservazione si basa sui principi dell'aggiornamento e della trasparenza al fine di garantire al Titolare e al suo Responsabile della Conservazione, al Produttore dei PdV e all'Utente fruitore del Servizio di Conservazione una descrizione fedele del sistema di Conservazione adottato e gestito dal Conservatore TeamSystem Service.

Il principio della completezza nella redazione del presente Manuale è soddisfatto da Teamsystem Service per il tramite di documenti allegati al Manuale, che rappresentano parti integranti e sostanziali del manuale stesso.

I documenti allegati, di seguito riportati, vengono condivisi e concordati tra Conservatore e Titolare e Produttore dei PdV in fase di attivazione del Servizio ed aggiornati nel tempo al verificarsi di variazioni nelle condizioni del Servizio stesso.

Documenti allegati	Descrizione
Documento Specificità del Contratto - Disciplinare	Le Specificità del Contratto possono essere contenute in alcuni documenti caratteristici del Servizio di Conservazione erogato da TeamSystem Service (quali ordini di acquisto, schede servizio, disciplinari tecnici, ecc.) condivisi con il Cliente. In particolare, sono i documenti correlati alle condizioni generali di Servizio che, a seconda della natura delle tipologie documentali sottoposte a conservazione e del contesto, definiscono le condizioni specifiche per ciascun Produttore.
Manuale Utente/Help center	È il manuale che il Conservatore mette a disposizione dell'Utente fruitore del Servizio e rappresenta una guida per ricercare, consultare ed esibire i documenti conservati e distribuire i pacchetti ai soggetti autorizzati che ne fanno espressa richiesta al sistema di conservazione. Le istruzioni e le procedure pubblicate nell'area della piattaforma denominata "Help center" rappresentano la forma con cui viene esposto il Manuale Utente.

[Torna al sommario](#)

2. TERMINOLOGIA (GLOSSARIO, ACRONIMI)

2.1 Glossario

Accesso: operazione che consente a chi ne ha diritto di prendere visione dei documenti informatici;

Affidabilità: caratteristica che, con riferimento a un sistema di gestione 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;

Acquisizione: procedura di acquisizione e presa in carico del sistema di conservazione, a seguito di verifica di coerenza, dei Pacchetti di Versamento conformi allo standard UNI SInCRO 11386, come indicato nel presente manuale;

Aggregazione documentale informatica: aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente;

Archivio informatico: complesso organico di documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico da un soggetto pubblico o privato durante lo svolgimento della propria attività;

Autenticità: caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico;

Conservazione: insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel presente Manuale di Conservazione, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti;

Copia di sicurezza: copia di backup degli archivi del sistema di conservazione prodotta ai sensi delle Linee Guida AgID;

Copia informatica di documento analogico: il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto;

Copia per immagine su supporto informatico di documento analogico: il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto;

Copia informatica di documento informatico: il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari;

Conformità della copia: la conformità della copia di un documento informatico o di un documento analogico assicurata secondo le disposizioni del Codice dell'Amministrazione Digitale e delle Linee Guida AgID attuative in materia;

Destinatario: Soggetto o sistema al quale il documento informatico è indirizzato;

Documento informatico: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;

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 analogico: la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti;

Documento statico non modificabile: documento informatico redatto in modo tale per cui il contenuto risulti non alterabile durante le fasi di accesso e di conservazione nonché immutabile nel tempo; a tal fine il documento informatico versato al sistema di conservazione deve rispettare i formati idonei e quindi non deve contenere macroistruzioni o codice eseguibile, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati;

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;

Esibizione: operazione che consente di visualizzare un documento conservato e di ottenerne copia;

Evidenza informatica: sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica;

Fascicolo informatico (unità archivistica): 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.

Firma elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica;

Firma elettronica avanzata: firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati;

Firma elettronica qualificata: firma elettronica avanzata che sia basata su un certificato qualificato e creata mediante un dispositivo sicuro per la creazione della firma;

Firma digitale: particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al Titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare l'autenticità e l'integrità di un documento informatico o di un insieme di documenti informatici;

Formato del documento informatico: modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file;

Funzione di hash: funzione matematica che genera, a partire da una generica sequenza di simboli binari, un'impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari (bit) che la generi, ed altresì risulti di fatto impossibile determinare una coppia di sequenze di simboli binari per le quali la funzione generi impronte uguali;

Immodificabilità: caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso;

Impronta: sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima sequenza di un'opportuna funzione di hash;

Insieme minimo di metadati del documento informatico: complesso dei metadati, la cui struttura è descritta nelle Linee Guida AgID, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta. Ulteriori metadati minimi obbligatori possono essere associati al documento informatico, in ottemperanza a normative settoriali, quali a titolo di esempio non esaustivo quelle vigenti in ambito tributario;

Integrità: insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato;

Leggibilità: Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica;

Linee Guida AgID: sono le regole tecniche attuative in materia di formazione gestione e conservazione dei documenti informatici adottate ai sensi dell'art. 71 del Codice dell'Amministrazione Digitale.

Marca temporale: evidenza informatica che consente di rendere opponibile a terzi un riferimento temporale;

Metadati: Dati associati a un 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;

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.

Pacchetto di Archiviazione: pacchetto informativo composto dalla trasformazione di uno o più Pacchetti di Versamento secondo lo standard UNI SInCRO 11386 e secondo le modalità riportate nel Manuale di Conservazione;

Pacchetto di Distribuzione: pacchetto informativo inviato dal sistema di conservazione di TeamSystem Service all'Utente in risposta ad una sua richiesta;

Pacchetto di Versamento: pacchetto informativo inviato dal Produttore dei PdV al sistema di conservazione di TeamSystem Service secondo un formato predefinito e concordato descritto nel Manuale di Conservazione e nelle Specificità del Contratto;

Pacchetto Informativo: contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare;

Pacchetto di Input: Pacchetto di Versamento di Input definito nel sistema di conservazione di TeamSystem Service che racchiude uno o più oggetti da conservare oppure anche i soli metadati riferiti agli oggetti da conservare ed è versato dal Produttore dei PdV al sistema di conservazione nella fase di pre-acquisizione e secondo le specifiche e le condizioni concordate nelle Specificità del Contratto;

Pre-acquisizione e presa in carico: procedura di acquisizione e presa in carico, a seguito di pre-verifica di coerenza, del sistema di conservazione dei Pacchetti di Input ricevuti dal Produttore ed elaborati successivamente per essere normalizzati e conformi allo standard UNI SinCRO 11386 per poter essere così accettati dal sistema di conservazione. La presa in carico definitiva e quindi l'accettazione da parte del sistema di conservazione di TeamSystem Service di un pacchetto di versamento in quanto conforme alle modalità previste dal presente manuale di conservazione e agli accordi stipulati tra il Titolare dell'oggetto di conservazione e il Conservatore, si ha solo in caso di generazione da parte del sistema di conservazione del rapporto di versamento con esito positivo.

Processo di conservazione: insieme delle attività correlate e interagenti alla conservazione dei documenti informatici secondo le Linee Guida AgID;

Produttore dei PdV (nel seguito anche **Produttore**): persona fisica che produce il pacchetto di versamento di input ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione;

Rapporto di Versamento: documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione di TeamSystem Service dei Pacchetti di Versamento inviati dal Produttore dei PdV e normalizzati secondo lo standard UNI SinCRO 11386;

Riferimento temporale: informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento;

Scarto: operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico-culturale.

Servizio: si intende il Servizio di Conservazione svolto dal Conservatore TeamSystem Service S.r.l.

Utente: persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.

[Torna al sommario](#)

2.2 Acronimi

AgID: Agenzia per l'Italia Digitale (già DigitPA e CNIPA);

CA: Certification Authority;

CAD: Codice dell'Amministrazione Digitale;

CNIPA: Centro Nazionale per l'Informatica della Pubblica Amministrazione, ora AgID;

D.Lgs.: Decreto Legislativo;

D.M.: Decreto Ministeriale;

D.P.C.M.: Decreto del Presidente del Consiglio dei Ministri;

HTTPS: HyperText Transfer Protocol over Secure Socket Layer;

IDM: Identity Management;

IPdA: Indice del Pacchetto di Archiviazione;

IPdD: Indice del Pacchetto di Distribuzione;

IdS: Indice di Scarto;

IPdV: Indice del Pacchetto di Versamento;

ISAD(G): General International Standard Archival Description;

MT: Marca temporale;

OAIS: Open Archival Information System (ISO 14721:2012);

PdA: Pacchetto di Archiviazione;

PdD: Pacchetto di Distribuzione;

PdI: Pacchetto di Input;

PdV: Pacchetto di Versamento;

RdV: Rapporto di Versamento;

RdC: Responsabile della conservazione;

RT: Riferimento temporale;

SGSI: Sistema di Gestione della Sicurezza delle Informazioni;

SLA: Service Level Agreement;

TSA: Time Stamping Authority;

UTC: Universal Time Coordinated.

[Torna al sommario](#)

3. NORMATIVA E STANDARD DI RIFERIMENTO

3.1 Normativa di riferimento

Di seguito è riportata la normativa generale di riferimento per l'attività di conservazione a livello nazionale:

Codice Civile

[Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica.

Legge 7 agosto 1990, n. 241 e s.m.i.

Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.

Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i.

Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.

Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i.

Codice in materia di protezione dei dati personali.

Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i.

Codice dei Beni Culturali e del Paesaggio.

Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i.

Codice dell'amministrazione digitale (CAD).

Deliberazione CNIPA 21 maggio 2009 n. 45 e s.m.i.

Regole per il riconoscimento e la verifica del documento informatico. Abrogata e sostituita dalle Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate del 20 giugno 2019

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.

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 sostitutiva, 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.

Linee Guida AgID in materia di formazione gestione e conservazione dei documenti informatici

Regole tecniche attuative del CAD adottate con Determinazione dirigenziale n. 407/2020 del 9 settembre 2020, entrate in vigore il 10 settembre 2020 con adozione obbligatoria entro il 1 gennaio 2022.

Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013

Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005. Abrogato e sostituito dalle Linee Guida AgID a partire dal 1 gennaio 2022.

Circolare AGID 10 aprile 2014, n. 65

Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82. Abrogata a partire dal 1 gennaio 2022.

Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014

Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005. Abrogato e sostituito dalle Linee Guida AgID a partire dal 1 gennaio 2022.

Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014

Regolamento europeo eIDAS (electronic IDentification Authentication and Signature) in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.

Regolamento di esecuzione (UE) 2015/1501 della Commissione, dell'8 settembre 2015

Relativo al quadro di interoperabilità di cui all'articolo 12, paragrafo 8, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno. Per l'attuazione del regolamento eIDAS la Commissione europea ha emanato alcuni provvedimenti attuativi riportati nell'apposita sezione del sito istituzionale di AgID "Atti esecutivi eIDAS".

Linee guida contenenti le Regole Tecniche e Raccomandazioni

Regolamento afferente la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate del 20 giugno 2019, che con la sua entrata in vigore abroga la Deliberazione CNIPA 21 maggio 2009, n. 45.

Ulteriori riferimenti normativi necessari per la definizione del quadro normativo completo in relazione a determinati casi specifici e alla natura degli oggetti digitali sottoposti al processo di conservazione sono riportati nell'allegato "Specificità del Contratto" condiviso con il Titolare e il suo Responsabile della Conservazione e con il Produttore dei PdV.

[Torna al sommario](#)

3.2 Standard di riferimento

Di seguito sono riportati gli standard elencati nell'allegato specifico delle Linee Guida AgID a cui l'attività di conservazione del Conservatore TeamSystem Service si riferisce:

UNI 11386:2020

Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;

ISO 14721:2012

OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;

ISO/IEC 27001:2013

Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);

ISO/IEC 27002:2013

Information Technology - Security Techniques - Code of practice for information security controls;

ISO/IEC 27017:2015

Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

ISO/IEC 27018:2019

Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO/IEC 27035:2011,

Information Technology - Security Techniques - Information Security Incident Management;

ISF SGP 2014

Information Security Forum – Standard of Good Practice for Information Security

ISO/IEC 31000:2018

Risk management – Principles and guidelines;

ETSI TS 101 533-1 V 1.3.1 (2012-04)

Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;

ETSI TR 101 533-2 V 1.3.1 (2012-04)

Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;

ISO 9001

Sistemi di gestione per la qualità per i servizi di conservazione di documenti informatici;

ISO 15836:2009

Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core;

UNI ISO 15489-1

Informazione e documentazione - Gestione dei documenti di archivio -Principi generali sul record management.

UNI ISO 15489-2

Informazione e documentazione - Gestione dei documenti di archivio –Linee Guida sul record management.

[Torna al sommario](#)

4. RUOLI E RESPONSABILITÀ

Il sistema di Conservazione descritto nel presente documento adotta ai sensi delle Linee Guida AgID un modello organizzativo conforme al modello di riferimento Open Archival Information System (ISO 14721), il quale prevede l'interazione e la collaborazione tra vari soggetti esterni ed interni al sistema al fine garantire la conservazione a lungo termine degli oggetti digitali sottoposti al Servizio.

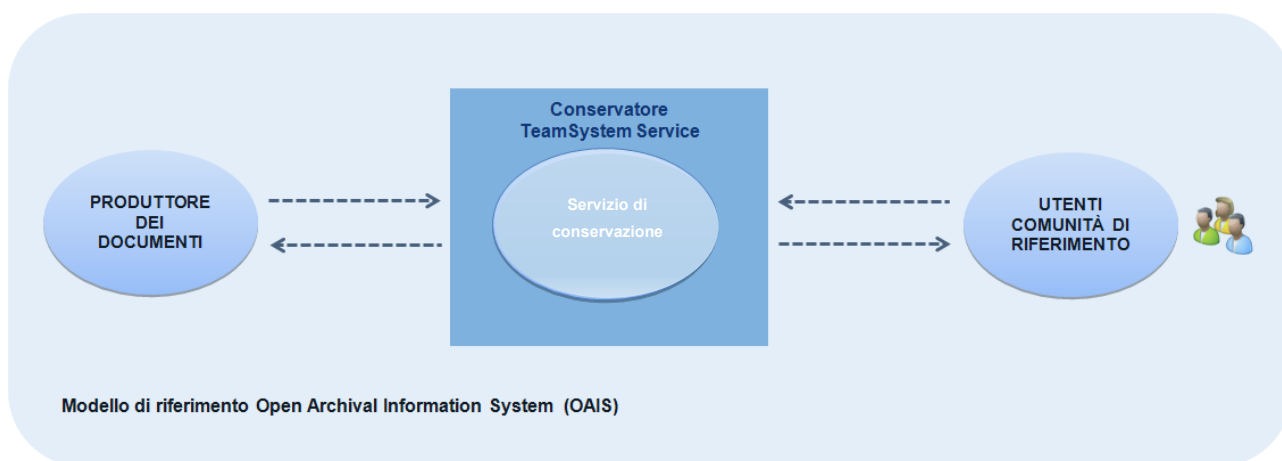


Fig. 1 – Modello di riferimento organizzativo del sistema Archive

Nel sistema di conservazione di TeamSystem Service si individuano i seguenti ruoli:

- **Titolare degli oggetti di conservazione:** è il soggetto responsabile del contenuto degli oggetti digitali di conservazione (ad esempio dei documenti informatici), della loro autenticità dell'origine, emissione/formazione. È il soggetto obbligato per legge o regolamenti alla conservazione degli oggetti stessi.

La corretta e certa individuazione del Titolare dei documenti da parte del sistema di conservazione avviene nella fase di attivazione del Servizio e in ciascuna sessione di versamento tramite i dati identificativi contenuti nell'Indice del Pacchetto di Versamento.
- **Produttore dei PdV:** è il soggetto responsabile del versamento (trasferimento) del Pacchetto di Versamento di Input al sistema di conservazione di TeamSystem Service e della verifica del buon esito dell'operazione di versamento tramite la presa visione del Rapporto di Versamento prodotto dal sistema di conservazione.

Il Produttore dei PdV può coincidere con il Titolare oppure può essere delegato ad un soggetto terzo. La corretta e certa individuazione del Produttore dei PdV da parte del sistema di conservazione avviene nella fase di attivazione del Servizio e in ciascuna sessione di versamento normalizzata tramite i dati identificativi contenuti nell'Indice del Pacchetto di Versamento.

Per i soggetti diversi dalle Pubbliche Amministrazioni, la persona fisica del Produttore dei PdV indicata dalle Linee Guida AgID è rappresentata dal legale rappresentante del Produttore dei PdV (nella sezione Submitter degli indici nello standard UNI SiNCRO e nell'anagrafica del sistema di conservazione sarà sempre indicata l'organizzazione).

- **Responsabile della Conservazione:** soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia. È il soggetto responsabile dell'insieme delle attività stabilite dalle Linee Guida AgID.
Il Responsabile della Conservazione è una persona fisica che opera presso l'organizzazione del Titolare (Soggetto Produttore). Nelle Pubbliche Amministrazioni, il ruolo del Responsabile della Conservazione è svolto da un dirigente o da un funzionario formalmente designato.
Per i soggetti diversi dalle Pubbliche Amministrazioni, il ruolo del Responsabile della Conservazione può essere altresì svolto da un soggetto esterno all'organizzazione del Titolare, purché in possesso di idonee competenze giuridiche, informatiche ed archivistiche e purché sia un soggetto terzo rispetto al Conservatore, in modo da garantire la funzione del Titolare dell'oggetto di conservazione rispetto al sistema di conservazione.
Il Responsabile della Conservazione, di una Pubblica Amministrazione o anche di un Soggetto Privato, sotto la propria responsabilità ai sensi delle Linee Guida AgID affida il processo di conservazione al Conservatore TeamSystem Service e al suo Responsabile del Servizio di Conservazione, rimanendo in ogni caso inteso che la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile, rimane in capo al responsabile della conservazione, chiamato altresì a svolgere le necessarie attività di verifica e controllo in ossequio alle norme vigenti sui servizi affidati in outsourcing.
- **Conservatore:** è TeamSystem Service S.r.l. che eroga, previo contratto di servizio e specifico affidamento, il Servizio di Conservazione svolgendo di fatto tutte le attività e compiti previsti dalle Linee Guida AgID, come meglio specificati nella delega, attraverso una propria struttura organizzativa descritta nel seguito.
Inoltre, il Conservatore esegue una normalizzazione dei Pacchetti di Input trasformandoli in Pacchetti di Versamento standard UNI SInCRO 11386 prima di sottoporli alla verifica di coerenza definitiva e quindi di generare il Rapporto di Versamento quale esito di acquisizione o rifiuto.
- **Utente abilitato:** persona, ente o sistema che interagisce con i servizi del sistema per la conservazione al fine di fruire delle informazioni di interesse.
- **Comunità di riferimento:** gruppi o insiemi di utenti autorizzati che possiedono i diritti per l'accesso ai documenti.

Internamente, il Conservatore TeamSystem Service ha adottato un modello organizzativo a supporto dell'erogazione del Servizio e delle attività di conservazione in coerenza con quanto previsto dalla normativa vigente. Tale modello prevede una struttura organizzativa della conservazione, che in base alle competenze ed esperienze specifiche, presenta dei responsabili che operano d'intesa tra di loro e svolgono le attività assegnategli per il raggiungimento di obiettivi comuni.

A tal fine TeamSystem Service ha adottato il documento "MANSIONARIO – FIGURE PROFESSIONALI PER LA CONSERVAZIONE" che mantiene aggiornato nel tempo.

Gli obiettivi comuni dell'attività svolte dai singoli responsabili e dai loro team operativi sono parte di un obiettivo generale del Conservatore TeamSystem Service di garantire con qualità ed affidabilità quanto stabilito dalla normativa di riferimento e l'esecuzione dei compiti a lui affidati.

Nello specifico il Conservatore, nel rispetto dei requisiti di organizzazione previsti dalle Linee Guida AgID e dall'Allegato A al Regolamento AgID sui criteri per la fornitura dei servizi di conservazione dei documenti informatici, ha nominato nella propria struttura organizzativa le figure professionali di seguito elencate:

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo	Eventuali deleghe
Responsabile del servizio di conservazione	Michele Di Rienzo - Contratto di tre anni rinnovabile -----	- Definizione ed attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione; - Definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente; - Corretta erogazione del Servizio di Conservazione all'Ente Produttore; - Gestione delle convenzioni, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei Servizi di Conservazione.	Dal 02/03/2015 al 16/12/2025 ----- Dal 17/12/2025	
	Ilaria Bruno - Contratto di tre anni rinnovabile ----- Paola Lavezzaro - Contratto di tre anni rinnovabile -----	Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'Ente Produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato;	Dal 02/03/2015 al 14/10/2021 ----- Dal 15/10/2021 al 16/12/2025	

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo	Eventuali deleghe
	Stefano Franzoso - Contratto di tre anni rinnovabile	▪ Definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici; ▪ Monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione; ▪ Collaborazione con l'Ente Produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.	Dal 17/12/2025	

[Torna al sommario](#)

5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Organigramma

TeamSystem Service S.r.l. è la società del Gruppo TeamSystem specializzata nell'erogazione e nella delivery dei Servizi in outsourcing. La realizzazione delle attività di Conservatore richiede la presenza di più funzioni aziendali coinvolte, ognuna delle quali ha la responsabilità di specifici ambiti di intervento.

La figura di seguito riassume le principali funzioni coinvolte nell'erogazione del Servizio di Conservazione.

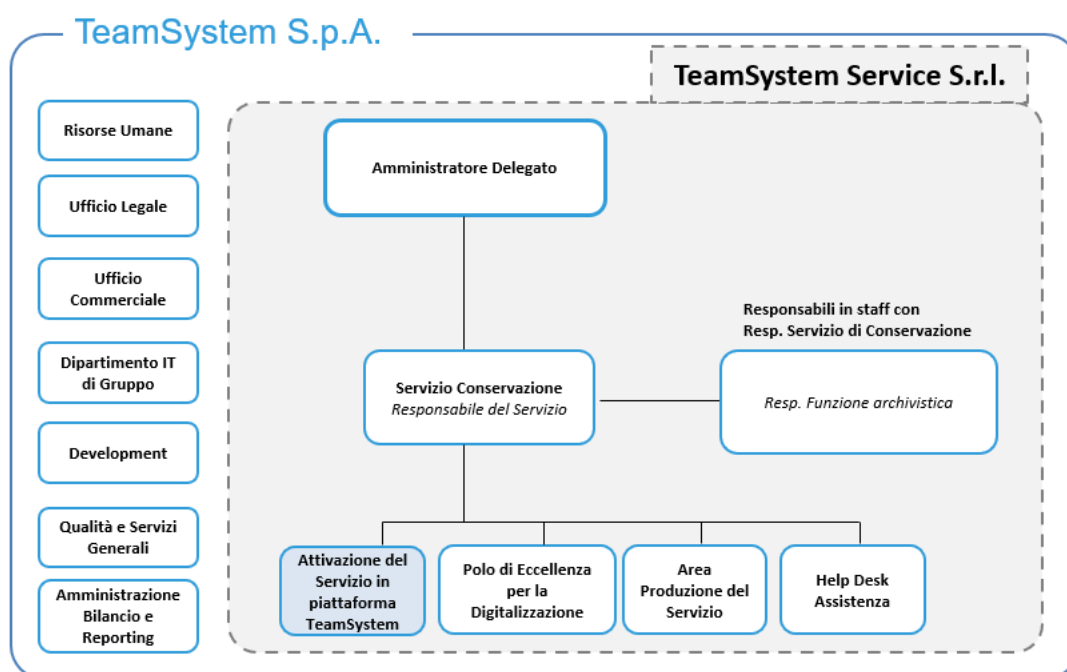


Fig. 2 – Funzioni organizzative coinvolte nell'erogazione del Servizio

In particolare, le aree primarie interne alla TeamSystem Service S.r.l. interessate all'erogazione del Servizio di Conservazione sono:

- **Polo di Eccellenza per la Digitalizzazione:** costituito in modo permanente dal Responsabile del Servizio di Conservazione e dal Responsabile della Funzione Archivistica di TeamSystem Service con il supporto a richiesta di consulenti ed esperti della materia, del team di Compliance e di Regulatory e dei Responsabili della Sicurezza e del Trattamento dei dati del Conservatore. Il Polo di Eccellenza ha il compito di garantire la verifica periodica e contribuire a preservare nel tempo la conformità del sistema e del processo di conservazione ed in generale della dematerializzazione alle normative vigenti e agli standard di settore. Periodicamente vengono organizzati dei meeting di review con tutti i responsabili nel modello organizzativo in cui si

analizzano con il Polo di Eccellenza tutte le tematiche di gestione del Servizio e di analisi per le scelte decisionali future.

Il Polo di Eccellenza può, inoltre, erogare servizi consulenziali sulle tematiche di digitalizzazione alla Clientela.

- **Area Attivazione del Servizio:** costituito dagli operatori delegati che si occupano prevalentemente delle operazioni di back end funzionali alla gestione dei rapporti contrattuali. Nello specifico sono responsabili della gestione della documentazione utile all'avvio dei contratti con i Clienti e delle pratiche ad esse connesse. È in comune con tutta la piattaforma TeamSystem di cui il servizio di conservazione fa parte.
- **Area Produzione del Servizio:** costituito dagli operatori delegati che si occupano prevalentemente di monitorare l'esercizio del processo di conservazione (produzione).
- **Area Help Desk / Assistenza:** costituito da operatori specializzati responsabili di assistere gli Utenti nell'utilizzo quotidiano del servizio. Le attività di Help Desk ed assistenza (front end) in relazione ai Servizi che prevedono la conservazione dei documenti informatici sono svolte in collaborazione anche con la società controllante TeamSystem S.p.A.
Il servizio di assistenza viene attivato attraverso l'apertura di un ticket on line.

Le altre funzioni a supporto dell'erogazione del Servizio di Conservazione (e.g. Risorse Umane, Ufficio Legale, ecc.) sono condivise a livello di Gruppo con apposito contratto di servizio tra la controllata TeamSystem Service S.r.l. e la controllante TeamSystem S.p.A., garantendo la standardizzazione di procedure e prassi comuni su temi trasversali quali, a titolo esemplificativo, la predisposizione della contrattualistica di Servizio, la formazione del personale, la gestione dei sistemi IT e l'attuazione di verifiche ispettive interne. Di seguito viene riportata una descrizione delle principali attività assegnate alle singole funzioni di Gruppo:

- **Risorse Umane:** responsabile dei processi di selezione dei candidati idonei alla funzione delle competenze necessarie, come stabilito all'interno della procedura di Selezione Assunzione e Gestione del personale e annesso mansionari. Inoltre, tale funzione è responsabile del processo di formazione e sensibilizzazione del personale tramite la partecipazione a corsi e seminari, l'organizzazione di corsi in aula e/o in modalità e-learning.
La funzione, in relazione al Servizio di Conservazione, si occupa di aggiornare il mansionario delle figure professionali in cui sono definiti ruoli ed attività connesse (job description);
- **Ufficio Legale:** fornisce supporto in tema di predisposizione della contrattualistica, analisi della conformità alle normative cogenti e contributi su eventuali dubbi interpretativi, collaborando a stretto contatto con il Polo di Eccellenza per la Digitalizzazione;
- **Ufficio Commerciale:** responsabile della vendita del Servizio di Conservazione, interagisce all'occorrenza con la rete di Rivenditori ed Intermediati TeamSystem per facilitare la capillarità dell'azione commerciale e coadiuvare il contatto con il Cliente finale;
- **Dipartimento IT di Gruppo:** responsabile della gestione degli apparati e delle applicazioni utilizzate per l'erogazione del Servizio di Conservazione. In tale contesto, i termini e le condizioni di erogazione delle attività che TeamSystem S.p.A. eroga a favore di TeamSystem Service S.r.l.

sono stabilite all'interno del contratto Intercompany di servizio per la fornitura e la gestione dei servizi ICT. Tale contratto regola inoltre i livelli di servizio richiesti alla Capo Gruppo, attraverso la formalizzazione ed il monitoraggio di specifici SLA (o Service Level Agreement). L'unità di Planning, Management & Governance è responsabile della gestione delle verifiche ispettive interne volte a valutare la conformità alle normative e agli standard di settore adottati a livello di Gruppo;

- **Software Factory:** responsabile dello sviluppo applicativo della piattaforma proprietaria dedicata all'erogazione del Servizio di Conservazione in conformità con quanto previsto dalla normativa vigente e con quanto specificato nel presente Manuale. Tale funzione, su richiesta della TeamSystem Service che detiene la licenza della piattaforma, è inoltre responsabile degli interventi applicativi necessari a garantire l'aggiornamento tecnologico e funzionale della piattaforma, anche in relazione agli eventuali adeguamenti normativi e tecnici e/o al miglioramento di specifiche funzionalità;
- **Amministrazione, Bilancio e Reporting:** responsabile di tutte le attività e i servizi amministrativi, contabili e finanziari dell'azienda;
- **DPO:** responsabile di osservare, valutare e organizzare la gestione del trattamento di dati personali (e la loro protezione) affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali.

[Torna al sommario](#)

5.2 Strutture organizzative

TeamSystem Service è una società del Gruppo TeamSystem dedicata all'erogazione dei servizi in *outsourcing* che richiedono una forte competenza e correlazione con la normativa, tra cui la conservazione dei documenti informatici.

Il *business process* della conservazione in TeamSystem Service è costituito da un insieme di attività organizzate al fine di realizzare un Servizio di Conservazione affidabile, sicuro e di qualità, che soddisfi le esigenze e le aspettative del Cliente.

Nel modello TeamSystem Service il Responsabile del Servizio di Conservazione è il *process owner* o *service manager* che garantisce attraverso la collaborazione con gli altri Responsabili individuati e del Polo di Eccellenza per la Digitalizzazione il controllo di tutto il processo e una gestione orientata all'erogazione del Servizio.

Per il Servizio di Conservazione è stato identificato da TeamSystem Service un *lifecycle* costituito da tre fasi principali:



Fig. 3 – Lifecycle del Servizio di Conservazione

Di seguito viene descritto e graficato il *business process* organizzativo della Conservazione attraverso tre *flow chart*, uno per ciascuna fase del ciclo di vita del Servizio, caratterizzata da un insieme di attività assegnate e svolte dalle aree organizzative.

La **fase di Attivazione** si avvia con una richiesta di adesione al Servizio da parte del Cliente.

Il Servizio di Conservazione fa parte della piattaforma TeamSystem, contenente altri servizi (per es. la Fatturazione, la Firma ecc.) per i quali mette a disposizione tutta una serie di servizi comuni che consentono di ottimizzare e di migliorare l'esperienza per il cliente, che fruisce di un solo ambiente di lavoro.

Per esempio, l'accesso alla piattaforma TeamSystem viene gestita attraverso il TeamSystem ID, l'utenza unica che permette di connettersi in modo sicuro ai vari software TeamSystem (<https://agyo.elevio.help/it/articles/246>)

Anche la fase di attivazione del Servizio Archive coincide con quella di piattaforma e viene descritta in una specifica sezione dell'Help Center: <https://agyo.elevio.help/it/categories/19-primi-passi-su-ts-digital>

In questa fase rientra anche l'attività di Back office relativa al controllo della documentazione contrattuale e le eventuali comunicazioni delle irregolarità emerse. Vi è una uniformità anche a livello contrattuale, nel senso che esiste un solo contratto per tutti i servizi della piattaforma che contiene le condizioni generali comuni e le varie specificità dei Servizi che lo compongono.

Con l'attivazione del Servizio TS Archive, a seguito della stipula del contratto e l'accettazione delle condizioni generali, **il Responsabile della Conservazione (RdC) del Cliente (e dei relativi Terzi Beneficiari) designato dal Cliente si presume che sia:**

- il Cliente medesimo nel caso in cui quest'ultimo agisca in nome proprio (es. professionista persona fisica);
- il Legale Rappresentante del Cliente nel caso in cui quest'ultimo agisca per il tramite di un Legale Rappresentante (es. Cliente persona giuridica).

La suddetta presunzione non troverà applicazione laddove il Cliente abbia fornito a TeamSystem una Delega rilasciata da un diverso RdC, in questo caso il RdC è la persona fisica firmataria della Delega.

Tutti i passi necessari per la corretta attivazione sono specificati nell'Help Center:

<https://agyo.elevio.help/it/categories/163-configurazione-del-servizio-archive>

Una volta attivato il Servizio, il Produttore dei PdV può iniziare a versare i Pacchetti di Input (PdI) secondo il formato e le specificità concordate nelle Specificità del Contratto (Scheda Servizio e/o ordine di acquisto) ed attivare un processo di conservazione periodico conforme alle Linee Guida AgID e meglio descritto nei capitoli successivi.

La seconda fase del Servizio riguarda la fase produttiva denominata della **Conservazione** ed in particolare l'insieme delle attività operative di cui è responsabile della corretta esecuzione l'**Area di Produzione** con owner, coordinatore e supervisore il Responsabile del Servizio di Conservazione del Conservatore, previa delega da parte del Responsabile della Conservazione del Titolare. Questa fase si suddivide nelle seguenti sotto-fasi:

- Durante la chiamata di versamento via web services o da interfaccia, esecuzione delle pre verifiche sui Pacchetti di Versamento di Input (PdI) e in caso di riscontro di errori, non accettazione del versamento e segnalazione dell'errore al Produttore dei PdV;
- normalizzazione dei Pacchetti di Versamento di Input (PdI) ricevuti e che hanno superato la pre-verifica al fine di trasformarli in PdV standard UNI SInCRO 11386;
- verifica sui PdV standard e generazione del Rapporto di Versamento (RdV) standard UNI SInCRO 11386 quale esito delle verifiche di validità;
- generazione del Pacchetto di Archiviazione standard UNI SInCRO 11386, firmato o sigillato e marcato temporalmente secondo la normativa di riferimento;
- pubblicazione web dei documenti e dei Pacchetti per la ricerca, consultazione ed esibizione;
- presidio, monitoraggio e controlli sulla conservazione degli oggetti digitali;
- generazione del Pacchetto di Distribuzione (PdD) standard UNI SInCRO 11386 su richiesta espressa dell'Utente;
- produzione di copie e duplicati su richiesta dell'Utente.

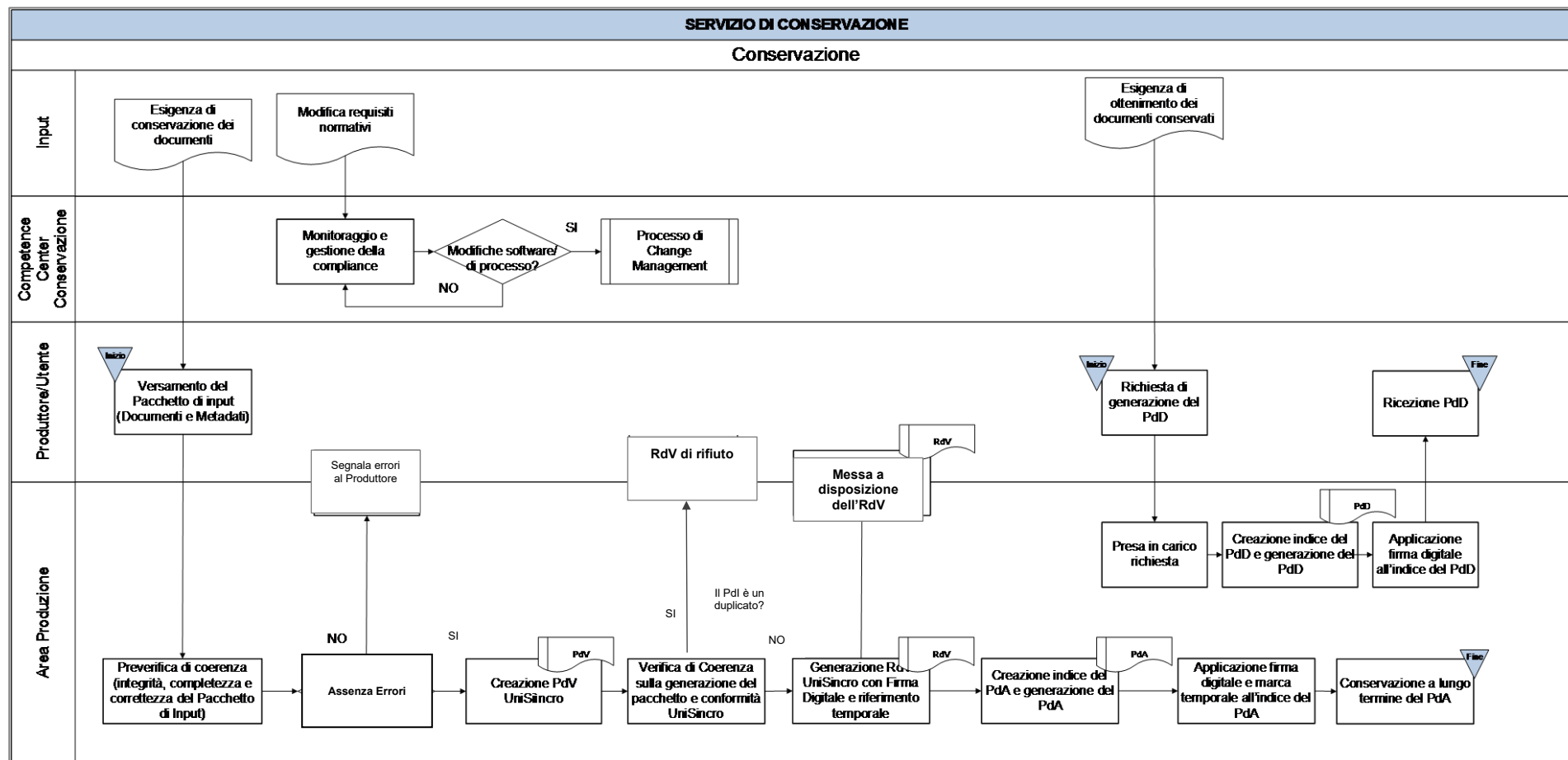


Fig. 4 – Diagramma di flusso della fase di conservazione

Successivamente alla fase produttiva della conservazione, il Conservatore TeamSystem Service espleta una serie di attività di monitoraggio e controllo per garantire l'osservanza di una serie di adempimenti legislativi, tra i quali:

- mantenimento per tutto il periodo di conservazione dei Pacchetti di Archiviazione e degli oggetti digitali conservati a seconda dei casi (documenti informatici, documenti amministrativi informatici, fascicoli, registri e repertori informatici), con tutti i relativi indici previsti dal processo secondo normativa;
- garanzia dell'integrità, dell'autenticità dell'origine e della leggibilità dei PdA e degli oggetti digitali per tutto il periodo di conservazione;
- garanzia di esibizione dei PdD e della ricerca dei documenti secondo le chiavi di ricerca previste dalla normativa;
- assistenza agli organi di controllo in caso di verifiche ed ispezioni.

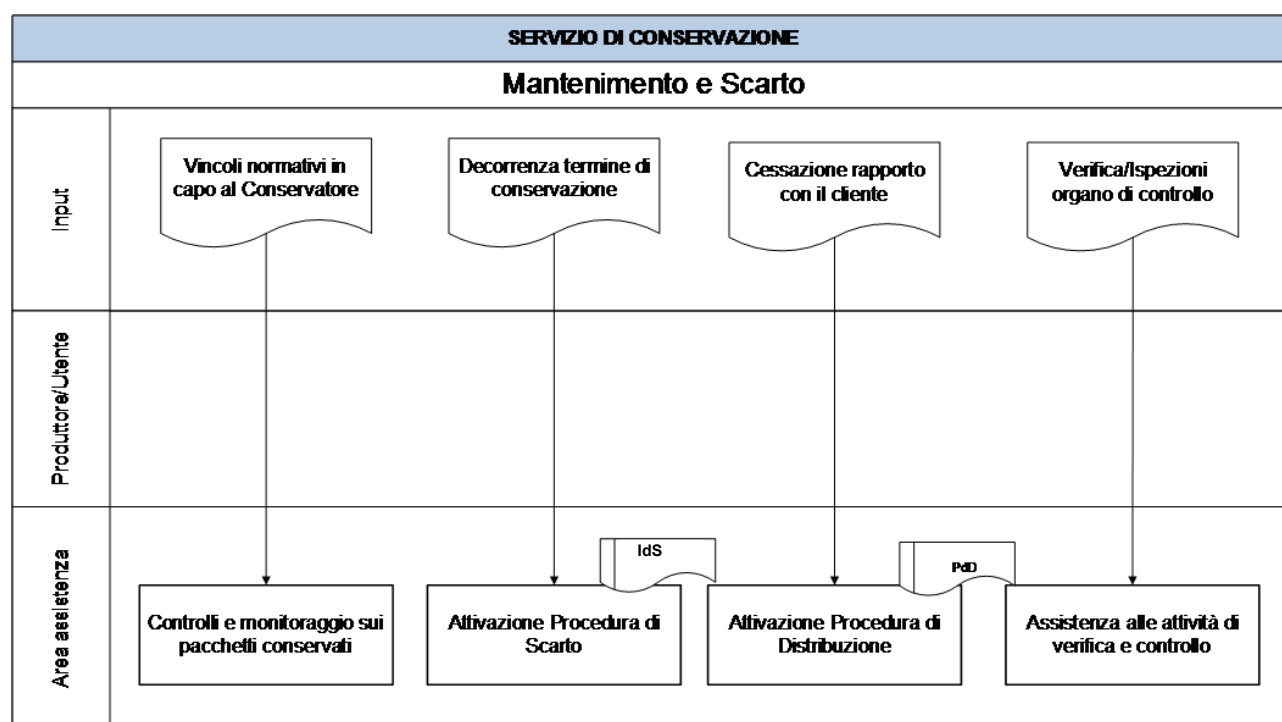


Fig. 5 – Diagramma di flusso della fase di mantenimento e scarto

Terminato il periodo di conservazione concordato contrattualmente, il Conservatore può provvedere alla procedura di **Scarto**.

In tutte le tre fasi sopra descritte relative al *lifecycle* del Servizio di Conservazione le **aree funzionali di Gruppo** (Dipartimento IT di Gruppo, Ufficio Legale, Amministrazione Bilancio e Reporting, Risorse Umane, Qualità e Servizi generali, Ufficio Commerciale e Development) supportano le attività

erogate dal Conservatore TeamSystem Service.

Le attività di **gestione ICT del sistema di conservazione** a supporto del processo di conservazione eseguite dall'**Area Dipartimento IT di Gruppo** sulla base di uno specifico contratto di Servizi e coordinate dai Responsabili indicati nei ruoli del Conservatore TeamSystem Service sono principalmente le seguenti:

- conduzione e manutenzione del sistema di conservazione;
- monitoraggio dei processi e dei sistemi dell'infrastruttura;
- gestione del *Change Management* secondo quanto già previsto dalla certificazione ISO IEC 27001.

Le modalità di sviluppo e di manutenzione delle risorse informatiche giocano un ruolo determinante ai fini della garanzia di elevati livelli di affidabilità, sicurezza e qualità. Qualsiasi cambiamento significativo apportato ai sistemi informatici segue uno specifico iter procedurale ed è preventivamente approvato dai soggetti incaricati a valle di una valutazione sulla fattibilità dell'intervento e di un'analisi degli impatti che esso comporterebbe sul livello di sicurezza degli stessi. La struttura organizzativa di TeamSystem Service ha redatto la procedura di *Change Management* proprio per definire i passaggi operativi da eseguire in caso del verificarsi del change;

- verifica dei reporting sugli SLA relativi al Servizio di Conservazione erogato;
- misurazione delle attività eseguite e dei carichi delle risorse;
- gestione delle componenti hardware e software e loro sviluppo a garanzia dell'evoluzione tecnologica e normativa;
- verifica e pianificazione delle misure di sicurezza dell'infrastruttura.

La struttura organizzativa del Conservatore prevede che periodicamente siano organizzati meeting **Stato Avanzamento Lavori (SAL)** del Servizio tra le varie aree funzionali interessate, coordinati dal Responsabile del Servizio di Conservazione, per la condivisione dell'andamento della gestione del Servizio del Conservatore TeamSystem Service, per l'individuazione e la condivisione delle criticità, per l'analisi degli indicatori di performance e delle statistiche sulle eventuali anomalie riscontrate. Inoltre grazie alle riunioni di Sprint Review, cadenziate ogni due settimane, il team di sviluppo condivide con i principali stakeholder del Servizio (Responsabile del Servizio, Polo di eccellenza, Operation, Divisione Commerciale, Direzione) l'avanzamento degli sviluppi software in corso e non ancora messi in produzione.

In ultimo, la documentazione relativa al Servizio di Conservazione dell'ente conservatore TeamSystem Service è mantenuta attraverso strumenti e sistemi che rispettano le regole indicate nella parte 1, capitolo 5 e capitolo 7 dello standard ISO 15489 (rispettivamente Regulatory Environment e Records Management Requirements).

[Torna al sommario](#)

6. OGGETTI SOTTOPOSTI A CONSERVAZIONE

6.1 Oggetti conservati

Gli oggetti sottoposti a conservazione sono trattati dal sistema *Archive* di TeamSystem Service in pacchetti informativi e si distinguono in Pacchetti di Versamento (PdV), Pacchetti di Archiviazione (PdA) e Pacchetti di Distribuzione (PdD).

Per garantire l'interoperabilità nella conservazione e nel recupero degli oggetti digitali in caso di migrazioni da un sistema di conservazione all'altro, il Conservatore TeamSystem Service ha adottato la struttura dati conforme allo standard UNI SInCRO 11386 per tutti gli Indici XML dei pacchetti informativi PdV, PdA, PdD ed anche per il Rapporto di Versamento (RdV) e l'Indice di Scarto (IdS) generato dalla procedura di scarto.

Un Pacchetto Informativo racchiude il **contenuto informativo**, ovvero uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), ed **informazioni di descrizione della conservazione** come, ad esempio, i metadati riferiti agli oggetti da conservare.

Il contenuto informativo è costituito dagli **oggetti dati** e dalle **informazioni sulla rappresentazione**: informazioni che rappresentano e servono a dare un significato ad un oggetto dati ovvero lo associano a concetti più significativi (es: formato, tipi di dato).

Gli oggetti dati gestiti dal sistema di conservazione di TeamSystem Service possono essere costituiti da **documenti informatici** (di varia natura quale ad esempio tributaria, civilistica, lavoristica, assicurativa, bancaria, ecc.).

Per garantire l'autonomia nella gestione conservativa degli oggetti dati rispetto alle soluzioni tecnologiche, il Conservatore TeamSystem Service assicura di includere nei pacchetti informativi (PdV, PdA e PdD) le **informazioni di descrizione della conservazione** in base alla natura dell'oggetto da conservare, in conformità con l'allegato 5 delle Linee Guida AgID.

L'obiettivo del Conservatore TeamSystem è stato quello di progettare le strutture dati degli XML dei pacchetti informativi in modo da essere **auto-sufficienti** nel senso di contenere tutte le informazioni di descrizione della conservazione e quindi tutte le informazioni archivistiche e previste dalle Linee Guida necessarie al processo di formazione, tenuta e conservazione degli oggetti digitali.

Le informazioni di descrizione della conservazione sono l'insieme complessivo delle informazioni, riportate nell'immagine seguente, necessarie per comprendere il contenuto informativo.

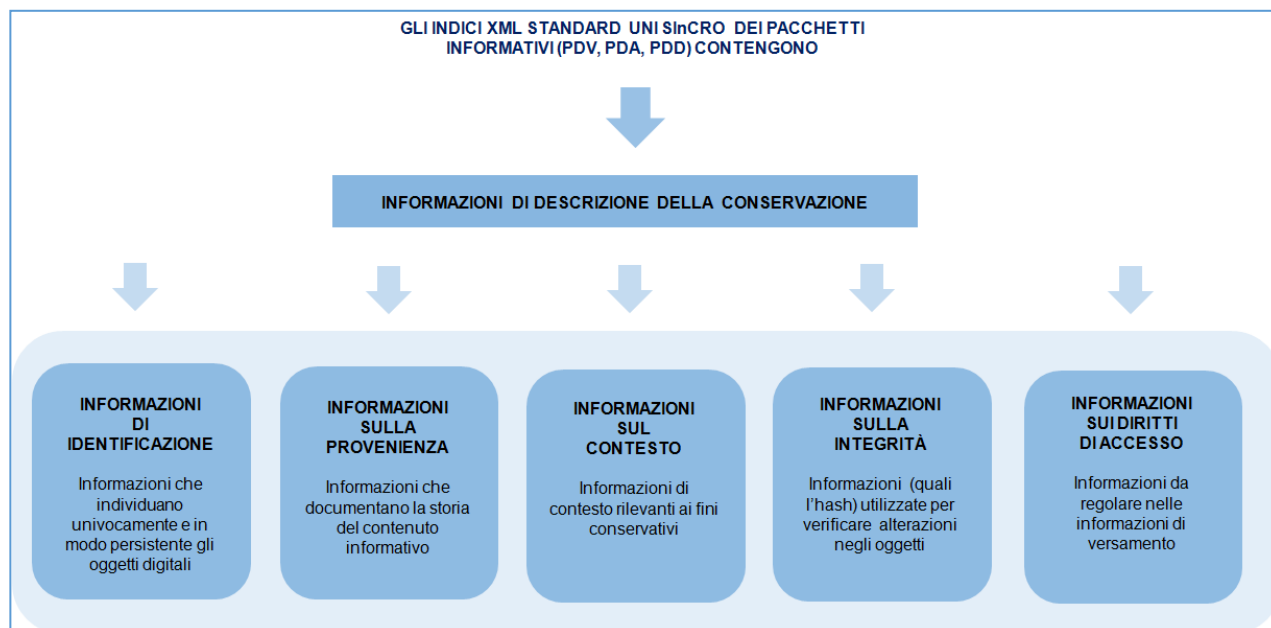


Fig. 6 – Informazioni descrittive della conservazione correlati agli oggetti sottoposti a *conservazione*

L'obiettivo delle predette informazioni descrittive della conservazione che il Conservatore TeamSystem Service inserisce **negli Indici XML standard UNI SInCRO dei Pacchetti Informativi (PdV, PdA, Pdd)** durante il processo è quello di garantire agli oggetti sottoposti a conservazione le caratteristiche di autenticità, integrità, interoperabilità, affidabilità, leggibilità e reperibilità.

In fase di attivazione del Servizio, nel **Disciplinare Specificità del Contratto (denominato Scheda Servizio)**, il Conservatore ed il Produttore definiscono e concordano sugli oggetti da conservare quanto segue:

- natura dei documenti informatici (individuazione della natura dei documenti ed individuazione della normativa settoriale da applicare eventualmente nel processo di formazione, gestione e conservazione);
- eventuale presenza di documenti informatici amministrativi;
- formati degli oggetti sottoposti a conservazione;
- periodo di conservazione;
- metadati associati agli oggetti. Vengono definiti i metadati minimi obbligatori in conformità alla normativa vigente e quelli aggiuntivi facoltativi da valorizzare nell'IPdV in modo da associare delle chiavi descrittive agli oggetti digitale di conservazione.
- soggetti coinvolti nel processo (Titolare, Responsabile della Conservazione (RdC), Produttore dei PdV, il delegato Conservatore e il suo Responsabile del Servizio di Conservazione, ecc.)

- Utenti che possono accedere al sistema di conservazione per quel determinato titolare dei documenti e loro diritti di accesso.

Eventuali ulteriori specifiche ed informazioni in merito alle descrizioni associate agli oggetti digitali da sottoporre alla conservazione sono contenute nel Disciplinare Specificità del Contratto.

[Torna al sommario](#)

6.2 Metadati

La normativa di riferimento dispone di associare ai documenti informatici dei metadati che li accompagneranno dal momento della formazione e per tutto il loro ciclo di vita, quindi anche durante la conservazione, in modo da identificarli univocamente, da classificarli con una descrizione archivistica e permettere la loro corretta gestione nel sistema documentale e in quello di conservazione.

Quindi il Conservatore TeamSystem Service, il Responsabile della Conservazione del Titolare e il Produttore dei PdV definiscono nel **Disciplinare Specificità del Contratto** (Scheda Servizio) la classificazione logica delle tipologie documentali secondo uno schema articolato in campi individuati attraverso specifici metadati.

Si evidenzia che la struttura **dell'insieme minimo di metadati** del documento informatico, da associare all'oggetto digitale per identificarne provenienza e natura e per garantirne la tenuta, è definita e descritta dall'apposito allegato delle Linee Guida AgID. Ulteriori metadati aggiuntivi, richiesti dalla normativa in virtù della diversa natura delle tipologie documentali o richiesti dal Produttore dei PdV per proprie esigenze, sono definiti nel Disciplinare Specificità del Contratto.

Ad esempio, i **documenti di rilevanza tributaria** (a titolo non esaustivo fatture attive e passive, ddt, libri e registri contabili, dichiarazioni, comunicazioni, ecc.) devono soddisfare anche quanto richiesto in merito all'obbligo di garantire l'esibizione (ricerca ed estrazione) attraverso delle chiavi di ricerca (metadati) in ottemperanza alle disposizioni del Decreto ministeriale in materia.

[Torna al sommario](#)

6.3 Formati

Il formato di un documento informatico è la modalità di rappresentazione della sequenza di bit che costituisce il documento informatico stesso ed è comunemente rappresentato attraverso l'estensione del file.

L'Allegato 2 delle Linee Guida AgID fornisce le indicazioni sui formati dei file con cui devono essere rappresentati i documenti informatici oggetto di conservazione.

Al fine di assicurare una corretta gestione degli oggetti conservati, i formati idonei devono garantire le seguenti caratteristiche:

- apertura;

- sicurezza;
- portabilità o interoperabilità;
- funzionalità;
- supporto allo sviluppo;
- diffusione.

Nella scelta dei formati idonei si è rispettato il principio di interoperabilità e di mitigazione del rischio di “obsolescenza tecnologica”, la caratteristica di apertura e di essere formati non proprietari, ossia liberamente utilizzabili e non coperti da brevetto, e di essere reperibili online diversi software applicativi open-source in grado di leggere i predetti formati.

Il Conservatore TeamSystem Service adotta misure di controllo periodiche per evitare l'obsolescenza dei formati in relazione all'evoluzione tecnologica.

Inoltre, il Titolare e il Produttore dei PdV sono obbligati ad utilizzare sempre **font interoperabili standard** come da disposizioni delle Linee Guida AgID.

I formati idonei alla conservazione che il sistema di conservazione di TeamSystem Service accetta e che quindi possono essere utilizzati dal Produttore dei PdV per il versamento al sistema predetto, sono indicati nel **Disciplinare Specificità del Contratto**.

Il **formato TXT** è ammesso dal sistema di conservazione di Teamsystem Service, dato che è un formato molto diffuso in vari ambiti, ma non è espressamente riportato dalle nuove Linee Guida AgID, che tuttavia prevedono la **possibilità di utilizzare formati diversi** da quelli elencati nell'Allegato 2 “Formati di file e riversamento”, **effettuando una valutazione di interoperabilità**. Per tal motivo il sistema di conservazione Teamsystem Service ha deciso di accettare anche il formato TXT, come da suddetto elenco, in continuità con le previgenti regole tecniche, riportando di seguito un'adeguata valutazione di interoperabilità e relativo indice di interoperabilità:

Caratteristica	Intervallo	Valutazione	Valore
Standardizzazione	da 0 a 3	Il formato TXT è basato su codifica ASCII riconosciuta come standard dall'ISO. Ad esempio, la versione UNICODE, sviluppata nel 1991, è riconosciuta come standard ISO 8859-1.	3
Apertura	da 0 a 3	Il formato TXT è un formato aperto	3
Non proprietà	da 0 a 4	Il formato TXT è un formato non proprietario	2
Estendibilità	da 0 a 2	Il formato TXT è estensibile	2

Livello di metadati	da 0 a 3	Non è ammesso incorporare metadati all'interno del file	0
Robustezza	da 0 a 2	Essendo un formato testuale (non binario) è un formato molto robusto	2
Indipendenza da dispositivi	da 0 a 4	È un formato leggibile in qualunque ambiente operativo o tramite qualsiasi dispositivo.	4
Compatibilità in avanti e all'indietro	Non specificato	Il formato TXT è un file testuale e sono diffusi molteplici software di elaborazione testi open source, installabili su piattaforma di sistema Android, Windows, Windows Phone, Linux, Mac OS al fine di accedere e visualizzare i file nel formato TXT.	2
Testuale o binario	Non specificato	Formato puramente testuale (ASCII), quindi non formattato.	2
TOTALE INDICE DI INTEROPERABILITÀ			20

LEGENDA: nel calcolo del suddetto indice di interoperabilità è stata applicata la scala indicata dalle Linee Guida AgID che prevede:

- formato più interoperabile = indice pari a 20;
- formato meno interoperabile = indice pari a 0;
- un valore pari a 12 o superiore può essere considerato sufficiente dal punto di vista dell'impatto di tale formato relativamente ad interoperabilità e obsolescenza;
- valori inferiori indicano problematiche oggettive che vanno affrontate il prima possibile in ottica di riversamento o altre metodologie.

Quindi, in conclusione, la valutazione di interoperabilità ha portato al risultato che il formato TXT ha ottenuto un indice di interoperabilità pari a 20 qualificandosi come ottimo dal punto di vista dell'interoperabilità e dell'obsolescenza.

[Torna al sommario](#)

6.4 Pacchetto di Versamento

Il PdV nel formato XML standard UNI SInCRO 11386 che riceve il Sistema di Conservazione di TeamSystem Service trae origine dal Pacchetto di Input (PdI), un Pacchetto che il Produttore del PdV versa al Conservatore e che contiene il contenuto informativo (documenti informatici) e le informazioni della conservazione, quali i metadati, da sottoporre al processo di conservazione.

Una volta eseguite le pre-verifiche di coerenza da parte del Conservatore sui Pacchetti di Input ricevuti dal Produttore e solo in caso di esito positivo, viene normalizzato e generato il **Pacchetto di Versamento standard UNI SInCRO 11386**, nel seguito **PdV UNI-SInCRO** o semplicemente **PdV**.

Il PdV UNI-SInCRO adottato dal sistema di conservazione è costituito principalmente da:

- **Oggetti Dati** (ad esempio documenti informatici, documenti informatici amministrativi);
- **Indice del Pacchetto di Versamento (IPdV)** nel formato XML generato secondo un modello-dati conforme allo standard UNI SInCRO 11386 e sulla base degli oggetti e delle informazioni contenute nel Pacchetto di Input (PdI). All'IPdV è associato un Riferimento Temporale, specificato con riferimento al Tempo Universale Coordinato (UTC). A tal riguardo tutti i sistemi di TeamSystem Service a supporto del Servizio della Conservazione sono sincronizzati con lo stesso NTP Server (verso UTC pubblico).

La struttura-dati del IPdV UNI-SInCRO dettagliata ed ulteriori specifiche ed informazioni di dettaglio in merito al Pacchetto di Versamento sono riportate nel Disciplinare Specificità del Contratto (Scheda Servizio), parte integrante e sostanziale del Manuale.

[Torna al sommario](#)

6.5 Rapporto di Versamento

Il Rapporto di Versamento è un file di esito che il Conservatore TeamSystem Service produce quale esito definitivo delle verifiche di coerenza eseguite sui Pacchetti di Versamento ricevuti, in osservanza a quanto disposto dalle Linee Guida AgID.

Nel processo TeamSystem Service viene generato un RdV in corrispondenza di un unico PdV. In conformità con lo standard ISO 14721 (Open Archival Information System OAIS) e per garantire l'interoperabilità di tutti gli oggetti che caratterizzano il processo, il Conservatore ha adottato la conformità allo standard UNI SInCRO 11386 per tutti gli Indici dei Pacchetti Informativi.

La stessa scelta è stata adottata anche per il Rapporto di Versamento che è costituito da un file XML generato in conformità allo Standard UNI SInCRO 11386 con una struttura dati simile all'IPdV. Il suo Vocabolario e gli elementi della struttura dati sono, pertanto, simili a quelli dell'IPdV anche se in questo caso si riferiscono alla generazione del RdV.

La differenza sostanziale è che sul RdV, una volta generato, è apposta una firma digitale del Responsabile del Servizio di Conservazione prima di metterlo nella disponibilità del Produttore dei

PdV. Anche in questo caso al file RdV è associato un Riferimento Temporale specificato con riferimento al Tempo Universale Coordinato (UTC).

Inoltre, il RdV riporta nella sua struttura dati l'esito delle verifiche eseguite sul PdV ricevuto ai fini della presa in carico. L'esito può essere positivo (<Esito>PdV Acquisito</Esito>) o negativo <Esito>ER001 - PdV Scartato per errore</Esito>.

Le casistiche di rifiuto in questa fase si limitano al caso di PdV duplicato, in quanto tutte le possibili altre cause di rifiuto vengono precedentemente intercettate al momento del versamento del Pdl impedendone il versamento stesso.

In ottemperanza alle Linee Guida AgID, il buon esito dell'operazione di versamento è verificato tramite il Rapporto di Versamento prodotto dal sistema di conservazione. La responsabilità di tale verifica è in carico al Produttore dei PdV in quanto se il sistema non produce un RdV con esito positivo ciò significa che gli oggetti dati contenuti nel Pdl e quindi nel PdV versati non saranno acquisiti per l'erogazione del Servizio e di conseguenza non saranno conservati.

La struttura-dati del RdV UNI-SInCRO dettagliata ed ulteriori specifiche ed informazioni di dettaglio in merito al Rapporto di Versamento sono riportate nel Disciplinare Specificità del Contratto.

[Torna al sommario](#)

6.6 Pacchetto di Archiviazione

Il Pacchetto di Archiviazione, il cui indice è generato nel formato XML in conformità allo Standard UNI SInCRO 11386, è una trasformazione di uno o più Pacchetti di Versamento.

Il suo vocabolario e gli elementi della struttura dati sono, pertanto, simili a quelli dell'IPdV anche se in questo caso si riferiscono alla generazione del PdA.

La differenza sostanziale è che sull'Indice del Pacchetto di Archiviazione, una volta generato, è apposta una firma digitale del Responsabile del Servizio di Conservazione o in alternativa un sigillo elettronico qualificato del Conservatore.

Di seguito un esempio di indice PdA:

```
<?xml version="1.0" encoding="utf-8"?>
<sincro:PIndex xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:sincro="http://www.uni.com/U3011/sincro-v2/" sincro:uri="http://www.uni.com/U3011/sincro-v2/PIndex.xsd"
sincro:sincroVersion="2.0"
xmlns:tsFMI="http://teamsystem.com/conservazione/v2.0/DocumentoInformaticoExtensionTeamSystem/"
xmlns:tsVcEx="http://teamsystem.com/conservazione/v2.0/VdcInfoExtension/"
xmlns:tsPdAEx="http://teamsystem.com/conservazione/v2.0/PdAInfoExtension/"
xmlns:tsFgEx="http://teamsystem.com/conservazione/v2.0/FileGroupExtension/">
  <sincro:SelfDescription>
    <sincro:ID sincro:scheme="local">IdC_7e5ac473-a7f2-445d-8996-219b07fe4f59</sincro:ID>
    <sincro:CreatingApplication>
      <sincro:Name>Conservazione Cloud TeamSystem Service</sincro:Name>
      <sincro:Version>2.0.0</sincro:Version>
      <sincro:Producer>TeamSystem S.p.a.</sincro:Producer>
    </sincro:CreatingApplication>
  </sincro:SelfDescription>
```

```
<sincro:PVolume>
  <sincro:ID sincro:scheme="local">VdC_7e5ac473-a7f2-445d-8996-219b07fe4f59</sincro:ID>
  <sincro:PVolumeGroup>
    <sincro:ID sincro:scheme="local">PdA_7e5ac473-a7f2-445d-8996-219b07fe4f59</sincro:ID>
    <sincro:Label>PdA</sincro:Label>
    <sincro:Description>Pacchetto di Archiviazione</sincro:Description>
  </sincro:PVolumeGroup>
</sincro:PVolume>
<sincro:FileGroup>
  <sincro:ID sincro:scheme="local">PdV_95d2aae1-43e9-4f30-999c-9e95f90583dd</sincro:ID>
  <sincro:Label>PdV - Pacchetto di Versamento</sincro:Label>
  <sincro:File sincro:encoding="binary" sincro:extension="pdf" sincro:format="application/pdf">
    <sincro:ID sincro:scheme="local">PdI_2090266559</sincro:ID>
    <sincro:Path>test.pdf</sincro:Path>
    <sincro:Hash sincro:hashFunction="SHA-
256">77ad3210d085ba922d017345548ce258890ec1a7700fc4776b7356cea250502d</sincro:Hash>
    <sincro:MoreInfo sincro:xmlSchema="FileExtensionDigitalArchive.xsd">
      <sincro:EmbeddedMetadata>
        <tsFMI:DocumentoInformatico xsi:type="tsFMI:DocumentoInformaticoType">
          <tsFMI:IdDoc>
            <tsFMI:ImprontaCrittograficaDelDocumento>
              <tsFMI:Impronta>d60yENCfupItAXNFViziWiKOWadwD8R3a3NWzqJQUc0=</tsFMI:Impronta>
              <tsFMI:Algoritmo>SHA-256</tsFMI:Algoritmo>
            </tsFMI:ImprontaCrittograficaDelDocumento>
            <tsFMI:Identificativo>PdI_2090266559</tsFMI:Identificativo>
          </tsFMI:IdDoc>
          <tsFMI:ModalitaDiFormazione>creazione tramite utilizzo di strumenti software che assicurino la
produzione di documenti nei formati previsti in allegato 2</tsFMI:ModalitaDiFormazione>
          <tsFMI:TipologiaDocumentale>Fatture emesse B2B</tsFMI:TipologiaDocumentale>
          <tsFMI:DatiDiRegistrazione>
            <tsFMI:TipologiaDiFlusso>E</tsFMI:TipologiaDiFlusso>
            <tsFMI:TipoRegistro>
              <tsFMI:Nessuno>
                <tsFMI:TipoRegistro>Nessuno</tsFMI:TipoRegistro>
                <tsFMI>DataDocumento>2025-03-17</tsFMI>DataDocumento>
                <tsFMI:OraDocumento>15:26:49.263Z</tsFMI:OraDocumento>
                <tsFMI:NumeroDocumento>001 TEST</tsFMI:NumeroDocumento>
              </tsFMI:Nessuno>
            </tsFMI:TipoRegistro>
          </tsFMI:DatiDiRegistrazione>
          <tsFMI:Soggetti>
            <tsFMI:Ruolo>
              <tsFMI:Mittente>
                <tsFMI:TipoRuolo>Mittente</tsFMI:TipoRuolo>
                <tsFMI:PF>
                  <tsFMI:Cognome>XXXX</tsFMI:Cognome>
                  <tsFMI:Nome>Luca</tsFMI:Nome>
                </tsFMI:PF>
              </tsFMI:Mittente>
            </tsFMI:Ruolo>
            <tsFMI:Ruolo>
              <tsFMI:Destinatario>
                <tsFMI:TipoRuolo>Destinatario</tsFMI:TipoRuolo>
                <tsFMI:PF>
                  <tsFMI:Cognome>XXXX</tsFMI:Cognome>
                  <tsFMI:Nome>Hermione </tsFMI:Nome>
                </tsFMI:PF>
              </tsFMI:Destinatario>
            </tsFMI:Ruolo>
            <tsFMI:Ruolo>
              <tsFMI:SoggettoCheEffettuaLaRegistrazione>
                <tsFMI:TipoRuolo>Soggetto Che Effettua La Registrazione</tsFMI:TipoRuolo>
                <tsFMI:PF>
                  <tsFMI:Cognome>ZZZ</tsFMI:Cognome>
                  <tsFMI:Nome>Luca</tsFMI:Nome>
                </tsFMI:PF>
              </tsFMI:SoggettoCheEffettuaLaRegistrazione>
            </tsFMI:Ruolo>
          </tsFMI:Soggetti>
```

```
<tsFMI:ChiaveDescrittiva>
  <tsFMI:Oggetto>TEST</tsFMI:Oggetto>
</tsFMI:ChiaveDescrittiva>
<tsFMI:Allegati>
  <tsFMI:NumeroAllegati>0</tsFMI:NumeroAllegati>
</tsFMI:Allegati>
<tsFMI:Classificazione>
  <tsFMI:IndiceDiClassificazione/>
  <tsFMI:Descrizione/>
  <tsFMI:PianoDiClassificazione/>
</tsFMI:Classificazione>
<tsFMI:Riservato>>false</tsFMI:Riservato>
<tsFMI:IdentificativoDelFormato>
  <tsFMI:Formato>application/pdf</tsFMI:Formato>
  <tsFMI:ProdottoSoftware>
    <tsFMI:NomeProdotto/>
    <tsFMI:VersioneProdotto/>
    <tsFMI:Produttore/>
  </tsFMI:ProdottoSoftware>
</tsFMI:IdentificativoDelFormato>
<tsFMI:Verifica>
  <tsFMI:FirmatoDigitalmente>>false</tsFMI:FirmatoDigitalmente>
  <tsFMI:SigillatoElettronicamente>>false</tsFMI:SigillatoElettronicamente>
  <tsFMI:MarcaturaTemporale>>false</tsFMI:MarcaturaTemporale>
<tsFMI:ConformitaCopieImmagineSuSupportoInformatico>>false</tsFMI:ConformitaCopieImmagineSuSupporto
Informatico>
</tsFMI:Verifica>
<tsFMI:Agg/>
<tsFMI:NomeDelDocumento>test.pdf</tsFMI:NomeDelDocumento>
<tsFMI:VersioneDelDocumento>1</tsFMI:VersioneDelDocumento>
</tsFMI:DocumentoInformatico>
<tsFMI:AdditionalMetadata>
  <tsFMI:AdditionalSubjectMetadata index="1" label="partita_iva"/>
  <tsFMI:AdditionalSubjectMetadata index="1" label="codice_sdi"/>
  <tsFMI:AdditionalSubjectMetadata index="1" label="id_paese">IT</tsFMI:AdditionalSubjectMetadata>
  <tsFMI:AdditionalSubjectMetadata index="1" label="matricola"/>
  <tsFMI:AdditionalSubjectMetadata index="2" label="partita_iva"/>
  <tsFMI:AdditionalSubjectMetadata index="2" label="codice_sdi"/>
  <tsFMI:AdditionalSubjectMetadata index="2" label="id_paese">IT</tsFMI:AdditionalSubjectMetadata>
  <tsFMI:AdditionalSubjectMetadata index="2" label="matricola"/>
  <tsFMI:AdditionalSubjectMetadata index="3" label="partita_iva"/>
  <tsFMI:AdditionalSubjectMetadata index="3" label="codice_sdi"/>
  <tsFMI:AdditionalSubjectMetadata index="3" label="id_paese">IT</tsFMI:AdditionalSubjectMetadata>
  <tsFMI:AdditionalSubjectMetadata index="3" label="matricola"/>
  <tsFMI:Metadata tsFMI:Label="anno_riferimento">2026</tsFMI:Metadata>
</tsFMI:AdditionalMetadata>
</sincro:EmbeddedMetadata>
</sincro:MoreInfo>
</sincro:File>
<sincro:MoreInfo sincro:xmlSchema="FileGroupExtensionDigitalArchive.xsd">
  <sincro:EmbeddedMetadata>
    <sincro:CustomMetadata xsi:type="tsFgEx:FileGroupExtension">
      <tsFgEx:FileGroupMetadata>
        <tsFgEx:Item label="IdObject">95d2aae1-43e9-4f30-999c-9e95f90583dd</tsFgEx:Item>
        <tsFgEx:Item label="NomeFilePdV">IPdV_95d2aae1-43e9-4f30-999c-9e95f90583dd.xml</tsFgEx:Item>
        <tsFgEx:Item label="HashTypePdV">SHA-256</tsFgEx:Item>
        <tsFgEx:Item
label="HashValuePdV">2b5795512e5aeed3de2b80783d97e989f31e1c9241876e74b2cebd79b4f5804</tsFgEx:Item>
        <tsFgEx:Item label="NomeFileRdV">RdV_95d2aae1-43e9-4f30-999c-9e95f90583dd.xml.p7m</tsFgEx:Item>
        <tsFgEx:Item label="HashTypeRdV">SHA-256</tsFgEx:Item>
        <tsFgEx:Item
label="HashValueRdV">0b92c03896d9efae3ea2f2b3317bc5a30463fad7bb742b4f65ce3c3f91dbeab2</tsFgEx:Item>
      </tsFgEx:FileGroupMetadata>
    </sincro:CustomMetadata>
  </sincro:EmbeddedMetadata>
</sincro:MoreInfo>
</sincro:FileGroup>
<sincro:Process>
  <sincro:Submitter sincro:agentType="legal person">
```

```
<sincro:AgentID>VATIT-12345678903</sincro:AgentID>
<sincro:AgentName>
  <sincro:FormalName>TEST</sincro:FormalName>
</sincro:AgentName>
<sincro:RelevantDocument>Manuale di conservazione del conservatore Teamsystem
Service</sincro:RelevantDocument>
</sincro:Submitter>
<sincro:Holder sincro:agentType="legal person" sincro:holderRole="soggetto produttore">
  <sincro:AgentID>VATIT-12345678903</sincro:AgentID>
  <sincro:AgentName>
    <sincro:FormalName>TEST</sincro:FormalName>
  </sincro:AgentName>
  <sincro:RelevantDocument>Manuale di conservazione del conservatore Teamsystem
Service</sincro:RelevantDocument>
</sincro:Holder>
<sincro:AuthorizedSigner sincro:agentType="natural person" sincro:signerRole="PreservationManager">
  <sincro:AgentID>Tixxxxxxxxxxx3H</sincro:AgentID>
  <sincro:AgentName>
    <sincro:NameAndSurname>
      <sincro:FirstName>zzzz</sincro:FirstName>
      <sincro:LastName>NNNN</sincro:LastName>
    </sincro:NameAndSurname>
  </sincro:AgentName>
  <sincro:RelevantDocument>Manuale di conservazione del conservatore Teamsystem
Service</sincro:RelevantDocument>
</sincro:AuthorizedSigner>
<sincro:AuthorizedSigner sincro:agentType="legal person" sincro:signerRole="Delegate">
  <sincro:AgentID>VATIT-01641790702</sincro:AgentID>
  <sincro:AgentName>
    <sincro:FormalName>TeamSystem Service Srl</sincro:FormalName>
  </sincro:AgentName>
  <sincro:RelevantDocument>Manuale di conservazione del conservatore Teamsystem
Service</sincro:RelevantDocument>
</sincro:AuthorizedSigner>
<sincro:AuthorizedSigner sincro:agentType="natural person" sincro:signerRole="Delegate">
  <sincro:AgentID>TINNNNNNNNNNNNN1W</sincro:AgentID>
  <sincro:AgentName>
    <sincro:NameAndSurname>
      <sincro:FirstName>Responsabile</sincro:FirstName>
      <sincro:LastName>Del Servizio</sincro:LastName>
    </sincro:NameAndSurname>
  </sincro:AgentName>
  <sincro:RelevantDocument>Manuale di conservazione del conservatore Teamsystem
Service</sincro:RelevantDocument>
</sincro:AuthorizedSigner>
<sincro:TimeReference>
  <sincro:TimeInfo sincro:attachedTimeStamp="false">2025-04-14T15:29:09.643Z</sincro:TimeInfo>
</sincro:TimeReference>
<sincro:LawsAndRegulations>UNI 11386:2020 - Linee Guida AGID ex articolo 71 del
CAD</sincro:LawsAndRegulations>
</sincro:Process>
</sincro:PIndex>
```

[Torna al sommario](#)

6.7 Pacchetto di Distribuzione

Il Pacchetto di Distribuzione, il cui indice nel formato XML è generato in conformità allo Standard UNI SInCRO 11386, è una distribuzione di uno o più Pacchetti di Archiviazione, a seconda della richiesta eseguita dall'Utente al sistema di Conservazione.

L'Utente può eseguire una ricerca nell'interfaccia web del sistema di conservazione attraverso le chiavi di ricerca (metadati) associate ad una determinata tipologia documentale. Ottenuto il risultato

della ricerca, l'Utente ha la facoltà di richiedere la distribuzione dei documenti ottenuti nell'output di ricerca.

Il sistema di conservazione, presa in carico la richiesta, la evade generando e sottoscrivendo il Pacchetto di Distribuzione con firma digitale del Responsabile del Servizio di Conservazione o con sigillo elettronico qualificato del Conservatore, prima di distribuirlo all'Utente tramite canale sicuro.

Il Pacchetto di Distribuzione nel sistema *Archive* è quindi un pacchetto informativo prodotto per permettere lo svolgimento del processo di esibizione e di esportazione dal sistema di conservazione che può contenere un Pacchetto di Archiviazione o n Pacchetti di Archiviazione a seconda della richiesta dell'Utente.

Il Pacchetto di Distribuzione del sistema *Archive* può avere le seguenti caratteristiche, a seconda delle esigenze dell'Utente espresse attraverso una *request* al sistema:

- **PdD coincidente con un PdA** di cui si è richiesta la distribuzione (generalmente richiesto in caso di migrazioni);
- **PdD selettivo con un unico IPdA** (ricerca selettiva di singolo documento o più documenti appartenenti ad uno stesso PdA);
- **PdD selettivo con N IPdA** (ricerca selettiva di singolo documento o più documenti appartenenti a diversi PdA).

Nei predetti tre casi, l'oggetto Pacchetto di Distribuzione è costituito da un contenitore in formato compresso (ad esempio .zip) in cui sono contenuti i seguenti oggetti dati:

- i **documenti informatici** a cui il PdD si riferisce;
- **uno o più IPdA**, a cui si riferiscono i documenti, firmati digitalmente dal Responsabile del Servizio di Conservazione e marcati temporalmente;
- un **IPdD, Indice del Pacchetto di Distribuzione**, generato in conformità allo standard UNI SInCRO 11386 e contenente le informazioni relative alla sessione di distribuzione e i riferimenti agli oggetti dati distribuiti nel contenitore compresso .zip;
- un **PdD Viewer**, denominato "*CCT Explorer*", ovvero un file eseguibile che permette ad un Utente o ad un organo di controllo, in caso di verifiche ed ispezioni, la visualizzazione di tutti i predetti oggetti dati contenuti nel PdD e permette da qualsiasi PC, in cui è scaricato il PdD, di eseguire le ricerche dei documenti conservati attraverso le chiavi di ricerca (metadati) previste.

La struttura-dati dettagliata dell'IPdD UNI-SInCRO ed ulteriori specifiche ed informazioni di dettaglio in merito al Pacchetto di Distribuzione sono riportate nel Disciplinare Specificità del Contratto.

[Torna al sommario](#)

7. PROCESSO DI CONSERVAZIONE

Il processo di conservazione è conforme a quanto previsto dalle Linee Guida AgID ed ha la finalità di assicurare i requisiti di autenticità dell'origine, integrità, leggibilità, disponibilità e reperibilità degli oggetti sottoposti al processo per tutto il periodo di conservazione.

Le componenti funzionali del sistema *Archive* di TeamSystem Service assicurano il trattamento dell'intero ciclo di gestione dell'oggetto conservato nell'ambito del processo di conservazione, garantendo nel tempo la conformità alla normativa vigente. Il modello di riferimento adottato è quello dello standard ISO 14721 di seguito schematizzato:

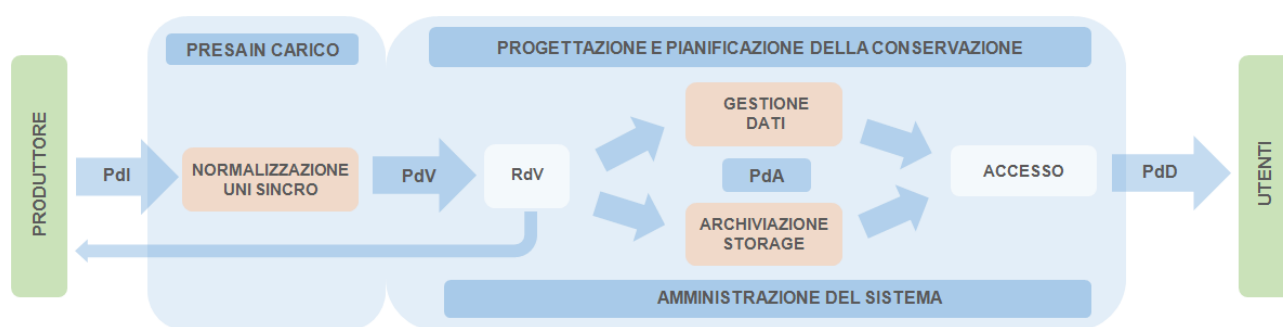


Fig. 7 – Modello di processo di conservazione adottato dal sistema *Archive*

Il Conservatore ed il suo Responsabile del Servizio di Conservazione, a ciò delegati dal Responsabile della Conservazione, gestiscono le varie sessioni del processo, i servizi e le funzioni per la gestione complessiva del sistema *Archive* in osservanza a quanto previsto dalle Linee Guida AgID.

Il processo di conservazione dei documenti informatici nel sistema *Archive* avviene attraverso le fasi graficate e dettagliate di seguito.

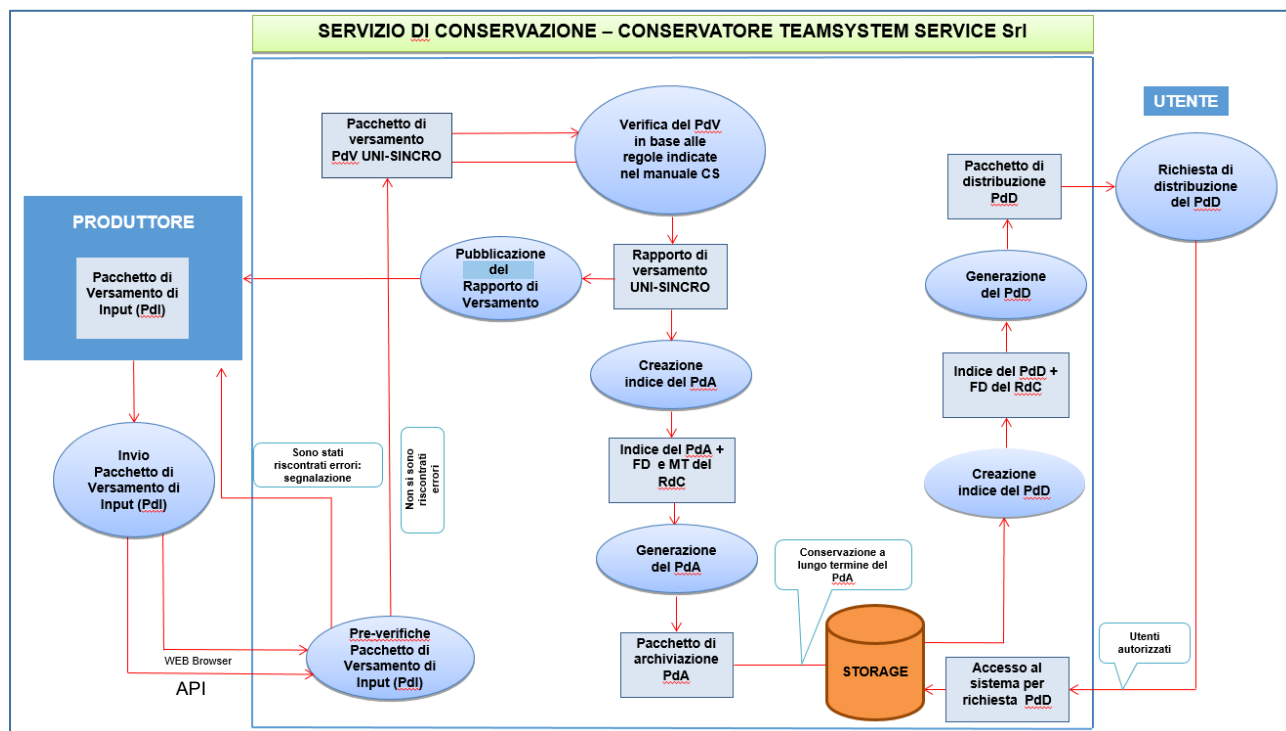


Fig. 8 – Schema di processo del Servizio di conservazione

[Torna al sommario](#)

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

Il Produttore dei PdV, preventivamente individuato dal sistema, può versare i **Pacchetti di Versamento di Input (PdI)** al sistema *Archive* attraverso modalità e canali trasmissivi sicuri:

- **Application Programming Interface (API) di tipo REST**
- **Uploader manuale** tramite interfaccia web del sistema *Archive*;

Il Servizio *Archive* consente di prendere in carico i Pacchetti di Input, costituiti dai documenti ed eventualmente dai loro metadati che ne consentono la classificazione e la relativa reperibilità, da sottoporre a Conservazione in modo distinti per ciascun Produttore dei PdV che abbia sottoscritto il relativo contratto di servizio e quindi settato e riconosciuto nel sistema nello stato “attivo”.

Una volta ricevuto il PdI, via web services o da interfaccia, il Servizio esegue le pre verifiche sui Pacchetti di Versamento di Input (PdI) e in caso di riscontro di errori non accetta il versamento e segnala l’errore al Produttore dei PdV;

Nel caso di trasmissione del PdI tramite **API** le stesse rispondono in modo sincrono con una segnalazione che riporta la descrizione dell’errore e quindi il motivo per cui non è stato preso in

carico il Pdl dal sistema. Nel caso di **upload del Pdl tramite interfaccia web**, l'esito di risposta verrà visualizzato in real time dall'Utente alla conferma dei dati di caricamento.

Se, al contrario, le **verifiche sul Pdl non hanno riscontrato errori** il sistema genera il PdV normalizzato nel formato XML conforme allo standard UNI SInCRO 11386 a partire da uno o più Pdl acquisiti.

I sistemi, presenti nell'infrastruttura di erogazione del Servizio, per la presa in carico dei Pdl, la normalizzazione dei PdV UNI SInCRO e la presa in carico di quest'ultimi, sono tutti in alta disponibilità e sono attive procedure di backup e replica dati sia a livello di storage che a livello di database che garantiscono la ridondanza dei dati e la sicura disponibilità, anche nei casi eventuali di disastro, come meglio specificato nell'ambito della documentazione relativa alla certificazione ISO IEC 27001.

[Torna al sommario](#)

7.2 Verifiche effettuate sui Pacchetti di Versamento e sugli oggetti in essi contenuti

Il sistema *Archive*, ricevuti dal Produttore i Pacchetti di Versamento di Input (PdI), esegue su di essi delle **verifiche di coerenza ed una serie di controlli di validità** rispetto alle specifiche concordate nel Disciplinare Specificità del Contratto che consistono nella:

- Verifica credenziali Utente e stato Utente attivo ed autorizzato;
- Verifica dell'idoneità del formato dei files contenuti nel PdI;
- Verifica della integrità del documento mediante il confronto tra l'impronta associata al file in ingresso e l'impronta ricalcolata dal sistema di conservazione;
- Verifica della eventuale presenza nel corrispondente archivio informatico di un documento o oggetto identico;
- Verifica della presenza dei dati anagrafici dei soggetti Produttore, Titolare dei documenti, Responsabile della Conservazione nel sistema di conservazione;
- Verifica della avvenuta compilazione dei metadati obbligatori per ogni tipo di documento o in generale oggetto digitale;
- PdI con estensione non valida: il documento PdI presenta un'estensione non coerente con la corrente Scheda Servizio;
- Errore durante l'esecuzione automatica del check di coerenza;
- Il contenuto del file non è coerente con l'estensione.

In caso di esito positivo, viene generato il PdV normalizzato standard UNI SInCRO.

Il sistema prende in carico il PdV normalizzato, verifica la sua coerenza e valida la conformità sintattica del XML allo schema UNI SInCRO di riferimento.

Quale esito definitivo del versamento del PdV (e quindi del PdI) da parte del Produttore dei PdV, il sistema genera un **Rapporto di Versamento** che ha lo scopo di rappresentare una **ricevuta di presa in carico** per l'erogazione del Servizio in caso di esito positivo delle verifiche o una **ricevuta di rifiuto dei PdV** elaborati in caso di esito negativo delle verifiche.

[Torna al sommario](#)

7.3 Accettazione dei Pacchetti di Versamento e generazione del Rapporto di Versamento di presa in carico

Il sistema *Archive* accetta i PdV e quindi il Conservatore si assume la responsabilità contrattuale di erogare il Servizio di Conservazione secondo gli SLA previsti dalla normativa e/o da quanto concordato con il Produttore nel Disciplinare Specificità del Contratto, esclusivamente se i Rapporti di Versamento prodotti sono con esito positivo in tal caso la **sessione di acquisizione e presa in carico** del processo è definitivamente conclusa e tracciata nel sistema di log.

Il RdV è un file XML, firmato digitalmente dal Responsabile del Servizio di Conservazione o sigillato con un sigillo elettronico qualificato del Conservatore e a cui è stato associato un Riferimento Temporale riferito al Tempo Universale Coordinato (UTC).

Il RdV è univocamente identificato come tutti gli oggetti del sistema, contiene il riferimento al PdV verificato, contiene l'esito della verifica e contiene negli elementi agent tutti i soggetti che intervengono nella fase di generazione del RdV e sono parte del processo. I Rapporti di Versamento sono documenti informatici ed il Conservatore mantiene nel tempo la prova della verifica eseguita. I RdV di rifiuto vengono conservati un anno e poi eliminati dal sistema.

I Rapporti di Versamento sono messi a disposizione del Produttore dei PdV e degli Utenti autorizzati attraverso l'apposita interfaccia web based del sistema *Archive*, che tramite la funzione di ricerca, ne consente la visualizzazione e l'eventuale download.

[Torna al sommario](#)

7.4 Rifiuto dei Pacchetti di Versamento e relativa comunicazione

L'esito delle verifiche riepilogative sul PdV UNI SInCRO sono comunicate attraverso la generazione del RdV. Il Produttore dei PdV ha il dovere di monitorare i RdV attraverso l'apposita interfaccia web based del sistema *Archive*, che tramite la funzione di ricerca, ne consente la visualizzazione e l'eventuale download.

Le casistiche di rifiuto in questa fase si limitano al caso di PdV duplicato, in quanto tutte le possibili altre cause di rifiuto vengono precedentemente intercettate al momento del versamento del Pdl impedendone il versamento stesso.

Ai sensi delle Linee Guida Agid il Servizio gestisce un numero massimo di rifiuti illimitato, ma con le seguenti regole:

dopo il primo versamento, eventuali duplicati inviati entro 5 giorni vengono automaticamente rifiutati. Se un versamento duplicato viene effettuato dopo il quinto giorno dal primo, esso verrà comunque acquisito e successivamente rifiutato; da questo momento decorrerà un nuovo termine di 5 giorni per controllare eventuali ulteriori duplicati

Il RdV di rifiuto viene messo a disposizione nell'interfaccia web.

[Torna al sommario](#)

7.5 Preparazione e gestione del Pacchetto di Archiviazione

Il Pacchetto di Archiviazione (PdA) costituisce l'elemento indispensabile per il sistema di conservazione, in quanto rappresenta il contenitore di tutti gli elementi necessari per una conservazione a norma e di lungo termine.

Secondo il piano di conservazione, configurato nel profilo del sistema in corrispondenza di ciascun Titolare e di ciascuna tipologia documentale, il processo di conservazione quindi si realizza appieno nel momento in cui viene apposta la firma digitale da parte del Responsabile del Servizio di Conservazione o del sigillo elettronico qualificato del Conservatore e l'apposizione della marca temporale sull'Indice del Pacchetto di Archiviazione.

La garanzia di sicurezza, immutabilità, integrità del processo e del PdA generato ai fini di mantenimento e conservazione (long-term preservation) sono garantiti nel sistema *Archive* attraverso la memorizzazione degli oggetti sottoposti al processo di conservazione in uno storage che garantisce **il massimo livello di sicurezza e integrità dei dati**. Tale sistema dedicato è dotato di una soluzione software specifica che **impedisce l'alterazione o l'eliminazione dei file prima di una data prestabilita** che corrisponde al periodo di conservazione (funzionalità di software **WORM**), come meglio specificato nella documentazione della certificazione ISO/IEC 27001.

La firma digitale o il sigillo elettronico qualificato e la marca temporale apposte sull'IPdA sono emesse, in conformità alla normativa vigente, da Certification Authority (CA) e de Time Stamping Authority, certificate da AgID e in conformità alla normativa vigente.

Il sistema di conservazione sovrintende a tutte le fasi del processo tracciandone ogni attività svolta ed ogni azione nei **file di log**.

Il sistema controlla automaticamente la validità dei certificati o dei sigilli al momento dell'apposizione della firma.

La connessione con la TSA per l'emissione delle marche temporali avviene tramite protocollo [HTTPS/SSL] cifrato per garantire la sicurezza e la riservatezza dell'operazione.

La marca temporale viene apposta dopo la firma del Responsabile del Servizio di Conservazione o il sigillo del Conservatore al fine di garantire una data opponibile a Terzi in cui la conservazione dei documenti era già avvenuta.

I controlli automatici del sistema *Archive* a completamento della generazione del IPdA garantiscono un intervento immediato degli operatori in caso di errori nell'apposizione della marca temporale, attivando il processo di gestione dell'anomalia dopo aver creato apposito ticket nel sistema di trouble ticketing aziendale.

[Torna al sommario](#)

7.6 Preparazione e gestione del Pacchetto di Distribuzione ai fini dell'esibizione

L'esibizione deve essere garantita dal sistema di conservazione e conforme a quanto previsto dalle Linee Guida AgID e da ulteriore normativa di riferimento settoriale.

Ai fini della distribuzione agli Utenti autorizzati il Sistema di Conservazione deve permettere l'accesso diretto ai documenti conservati, anche da remoto, mediante specifica azione di ricerca e selezione dei documenti conservati, richiesta del PdD e successiva produzione di un Pacchetto di Distribuzione (PdD) firmato digitalmente dal Responsabile del Servizio di Conservazione.

In maggior dettaglio, tramite accesso al Servizio, l'Utente può richiedere la visualizzazione di uno o più documenti conservati oppure può richiedere di scaricare il Pacchetto di Distribuzione.

Il Servizio richiede l'inserimento dei seguenti dati:

- Soggetto Titolare dei documenti;
- Anno
- Tipologia documentale del documento conservato da esibire;

- compilazione del filtro di ricerca, attraverso i metadati con cui i documenti sono stati indicizzati.

Il risultato della ricerca viene esposto in una vista che consente di:

- visualizzare i documenti ed i relativi metadati (eventualmente per consentire i controlli sulla leggibilità dei documenti) o la sua corretta conservazione e integrità
- selezionare i documenti che compongono il Pacchetto di Distribuzione.

Quando l'Utente richiede il Pacchetto di Distribuzione, i documenti selezionati vengono resi disponibili come download (zippati), con le caratteristiche descritte al paragrafo 6.7.

[Torna al sommario](#)

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

L'Utente accreditato per l'accesso al sistema *Archive*, tramite le proprie credenziali, può scaricare duplicati informatici secondo le proprie esigenze o richiedere Pacchetti di Distribuzione (PdD) che contengono anche i duplicati informatici.

Il processo di generazione del duplicato informatico, attraverso confronto degli hash, garantisce che il documento informatico ottenuto sullo stesso sistema di memorizzazione, o su un sistema diverso, contenga la stessa sequenza di bit del documento informatico di origine.

Per la produzione di copie informatiche, solo in caso di richiesta espressa dell'Utente sulla base di specifico accordo contrattuale, le procedure operative del sistema *Archive* fanno riferimento alle disposizioni delle Linee Guida AgID, permettendo:

- la generazione della copia informatica con l'apposizione della firma digitale del soggetto che ha effettuato la copia, mediante un processo che calcola l'hash della copia prodotta e dell'originale per garantire che il contenuto sia identico;
- la generazione, ove richiesto e previo raffronto tra l'originale e la copia, dell'attestazione di conformità inserita nel documento informatico che contiene la copia con l'apposizione della firma digitale del notaio o di un pubblico ufficiale. L'attestazione di conformità delle copie di uno o più documenti può essere altresì prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. Il documento informatico così prodotto è sottoscritto con firma digitale del notaio o del pubblico ufficiale a ciò autorizzato.

Tutte le operazioni eseguite nel sistema per la generazione dei duplicati informatici e/o delle copie vengono mantenute nel tempo nel sistema di log.

[Torna al sommario](#)

7.8 Scarto dei Pacchetti di Archiviazione

Successivamente alla scadenza dei termini di conservazione, in conformità alle Linee Guida AgID, viene effettuato lo scarto dei documenti conservati dal sistema di conservazione, dandone comunicazione con preavviso al Produttore dei PdV (Cliente) e al Responsabile della

Conservazione del Titolare, ad eccezione dei casi in cui lo scarto può avvenire solo previa autorizzazione del Ministero della Cultura (MIC) rilasciata al Titolare (Soggetto produttore) secondo quanto previsto dalla normativa vigente in materia di beni culturali, in quanto trattasi di archivi pubblici o privati che rivestono interesse storico particolarmente importante.

Nel Servizio Archive, ad ogni documento (PdI) viene associato dal sistema un Tempo di Conservazione fisso di 10 anni, per garantire la conservazione decennale prevista dalle condizioni contrattuali del Servizio, anche nei casi di disdetta o di recesso anticipato.

Superato il periodo di conservazione previsto, il Servizio produce un elenco dei Pacchetti di Archiviazione contenenti i documenti informatici destinati allo scarto e lo comunica al Responsabile della Conservazione del Titolare (se presente la sua mail) o altri destinatari del Produttore dei PdV.

Il destinatario della comunicazione di scarto, ricevuta la comunicazione prende visione dell'elenco dei documenti e pacchetti proposti per lo scarto e fa pervenire non oltre 60 giorni al Conservatore l'eventuale richiesta di proroga del periodo di conservazione (rinnovo). In caso di silenzio assenso il Conservatore è autorizzato trascorsi i 60 giorni dalla comunicazione ad avviare la procedura di scarto dei Pacchetti e documenti individuati.

In ogni caso l'invio della comunicazione di scarto avverrà sempre almeno 60 giorni prima della scadenza di conservazione e del conseguente scarto. Lo scarto avverrà sempre dopo la data di scadenza del periodo (tempo) di conservazione concordato.

La procedura di scarto prevede in particolare due scenari:

- Scarto automatico, che avviene dopo la scadenza di conservazione contrattuale (data di conservazione + 10 anni): l'eventuale rinnovo da parte dell'utente destinatario della comunicazione di scarto può essere richiesto massivamente per un ulteriore periodo;
- Scarto a richiesta: l'utente può richiedere al Servizio di modificare la scadenza per PdI, definendo una nuova data di scadenza per un documento già conservato. Il Servizio può accettare una data massima di 30 anni in più.

Nella richiesta è possibile anche anticipare la data di richiesta scarto, rispetto a quella precedentemente definita.

Al fine di soddisfare l'obbligo di tracciamento delle informazioni essenziali sullo scarto, la funzione di scarto di Archive provvede a generare un file Indice di Scarto (IdS) conforme allo standard UNI SInCRO 11386:2020

Nel caso di archivi pubblici o privati, che rivestono interesse storico particolarmente importante, il Conservatore TeamSystem ed il Responsabile della Conservazione concordano preventivamente nella Scheda Servizio che lo Scarto del Pacchetto di Archiviazione debba avvenire esclusivamente previa autorizzazione del Ministero della Cultura (MIC) rilasciata al Titolare secondo quanto previsto dalla normativa vigente in materia di beni culturali e secondo la procedura indicata nelle Linee Guida AgID.

[Torna al sommario](#)

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

Le scelte implementative del sistema e processo di Conservazione adottate da TeamSystem Service sono quelle di generare tutti gli indici dei pacchetti informativi ed anche il Rapporto di Versamento secondo lo standard UNI SInCRO 11386 proprio per garantire l'interoperabilità e la trasferibilità degli oggetti da un sistema ad un altro.

Il Conservatore TeamSystem Service è, altresì, responsabile della predisposizione della documentazione in cui sono riportate tutte le strutture-dati ed i vocabolari adottati, per agevolare le attività di corretta presa in carico ed interpretazione di un Produttore o di un altro Conservatore, secondo il principio della trasparenza e della collaborazione.

Il trasferimento dei PdA avviene sempre sottoforma di generazione dei PdD attraverso canali trasmissivi sicuri (ad esempio HTTPS) previa richiesta del Produttore.

In caso di recesso (o disdetta) dal contratto di affidamento del Servizio di conservazione, il Produttore dei PdV può scaricare i Pacchetti di Distribuzione di tutti i documenti e PdA sottoposti al processo di conservazione.

In ogni caso i documenti conservati saranno disponibili per la consultazione e l'esibizione fino al loro scarto. A seguito del recesso, al Produttore verrà inibita la possibilità di effettuare ulteriori versamenti.

[Torna al sommario](#)

8. IL SISTEMA DI CONSERVAZIONE

8.1 Componenti logiche

Da un punto di vista logico il Sistema Archive può essere schematizzato secondo il seguente grafico:

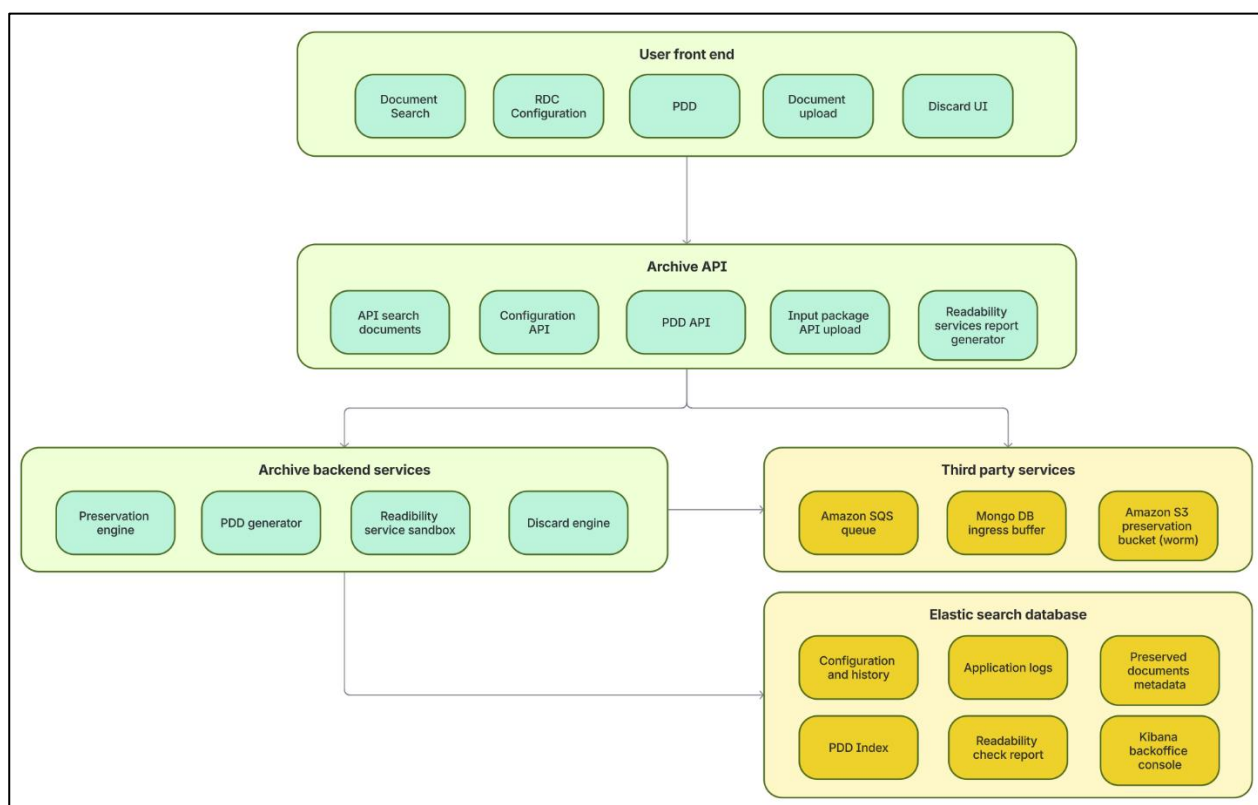


Fig. 9– Rappresentazione grafica delle componenti logiche del sistema Archive

L'applicazione può essere suddivisa nelle seguenti categorie di servizi:

- **User front end:** appartengono a questa categoria logica tutte le interfacce utente messe a disposizione sul portale web, per consentire agli utenti finali la consultazione di tutte le entità del sistema di conservazione. Il front end è esposto come applicazione web ed è accessibile ai clienti finali attraverso il sistema di autenticazione
- **Archive API:** le funzionalità del sistema di conservazione sono esposte online attraverso una serie di API. Le funzionalità offerte comprendono tutta l'operatività offerta agli utenti finali.
- **Archive Backoffice API:** alcune funzionalità del sistema di conservazione sono esposte online ma, grazie al sistema di autorizzazione, sono accessibili solo agli operatori di backoffice. Ad esempio, la validazione di una richiesta RDC.

- **Archive backend services:** i processi legati alla conservazione dei documenti versati o altre attività time expensive vengono eseguite in questa sezione della piattaforma.
- **Elastic search database:** il sistema si appoggia sullo stack elasticsearch.

Il sistema Archive sfrutta inoltre una serie di servizi della piattaforma TeamSystem:

- **Teamsystem auth services:** servizi legati al sistema di autenticazione, compreso il gestore delle credenziali, la gestione password o il sistema di creazione e autorizzazione degli utenti.
- **Company Registry:** servizi che hanno l'obiettivo di gestire, validare, mantenere le posizioni anagrafiche delle entità che utilizzano il sistema di conservazione.
- **Connection services:** attraverso questi servizi le entità descritte nella company registry possono essere collegate tra loro per creare relazioni di tipo "studio / gestita". Inoltre, attraverso il sistema di gestione delle connessioni è possibile gestire i servizi attivati su ciascuna entità.
- **Metering services:** il sistema del metering adempie a due funzionalità, la prima è contattare le API di configurazione dei prodotti comunicando quali entità hanno comprato e possono utilizzare il servizio. La seconda funzionalità svolta dal metering è quella di ricevere da parte dei prodotti la segnalazione dell'uso del servizio, segnalazione che il metering conterrà al fine di effettuare un puntuale conteggio dei consumi.
- **Helk log services:** i log applicativi sono registrati sullo stack elk, un elasticsearch dedicato alla sola registrazione dei log di sistema di tutti gli applicativi Teamsystem.
- **Backoffice front end:** gli operatori di backoffice hanno la possibilità di effettuare alcune operazioni per la gestione dei clienti di Archive. Il front end offerto agli operatori è totalmente autonomo e sfrutta le API offerte dal back-end di Archive per effettuare le operazioni consentite.

Le componenti direttamente coinvolte nello storage delle informazioni sono:

- **AWS S3:** i dati sono ridondati su più zone di disponibilità e sono georeplicati sul sito secondario con un ritardo massimo di 15 minuti, al fine di garantire una replica esatta dei dati presenti sul sito primario. I dati sono conservati su bucket configurato come WORM, rendendo di fatto impossibile la cancellazione delle informazioni.
- **Database server:** Le informazioni del sistema sono mantenute da un sistema Big data Elastic search.

In aggiunta alle componenti prettamente applicative possono essere evidenziati altri strumenti che partecipano al sistema di conservazione:

Notifier service: il sistema può emettere notifiche per avvisare utenti finali e gli operatori del back office nelle diverse fasi del processo di conservazione.

Digital sign/timestamp engine: motore e componenti dedicati all'apposizione della firma digitale di documenti e degli indici dei pacchetti, oltre all'apposizione della marca temporale, attraverso la connessione sicura con un certificatore accreditato.

[Torna al sommario](#)

8.2 Componenti tecnologiche

Il sistema di conservazione è basato su un'infrastruttura tecnologica complessa e composta da più elementi interoperanti tra loro.

Ricalcando la divisione delle componenti logiche, le seguenti sono le tecnologie di riferimento per l'implementazione di ogni livello di servizio:

- l'**interfaccia WEB** è sviluppata in linguaggio Javascript principalmente utilizzando React con un'interfaccia HTML5, operante su protocollo HTTPS e servito come single page application. L'autenticazione è effettuata tramite un sistema di gestione di chiavi ed utenze. Dialoga con la parte di API Rest tramite chiamate HTTPS;
- le interfacce **API Rest** esposte sul cloud sono tutte protette dal sistema di autenticazione Teamsystem Auth / TSID e consentono l'interazione tra il mondo esterno e il sistema di conservazione.
- i **Backend service** espongono i servizi che implementano la logica business e fanno da interfaccia verso il sistema Elasticsearch. Sono servizi scalabili che lavorano anch'essi in Load Balancing;
- tutti i sistemi sono operanti dietro dei **LoadBalancer** basati su tecnologia Linux e sono responsabili delle logiche di gestione dell'integrità di sessione e delle logiche di fault tolerance e fallback in caso di problemi sui singoli server;
- gli **ambienti di sviluppo e test** sono realizzati su una infrastruttura dati dedicata, e sono collegati su DMZ e VLAN riservate.

[Torna al sommario](#)

8.3 Componenti fisiche

L'architettura del Sistema di Conservazione è stata progettata per garantire i più elevanti standard di Qualità e Sicurezza, in linea con le migliori best practice e standard del settore.

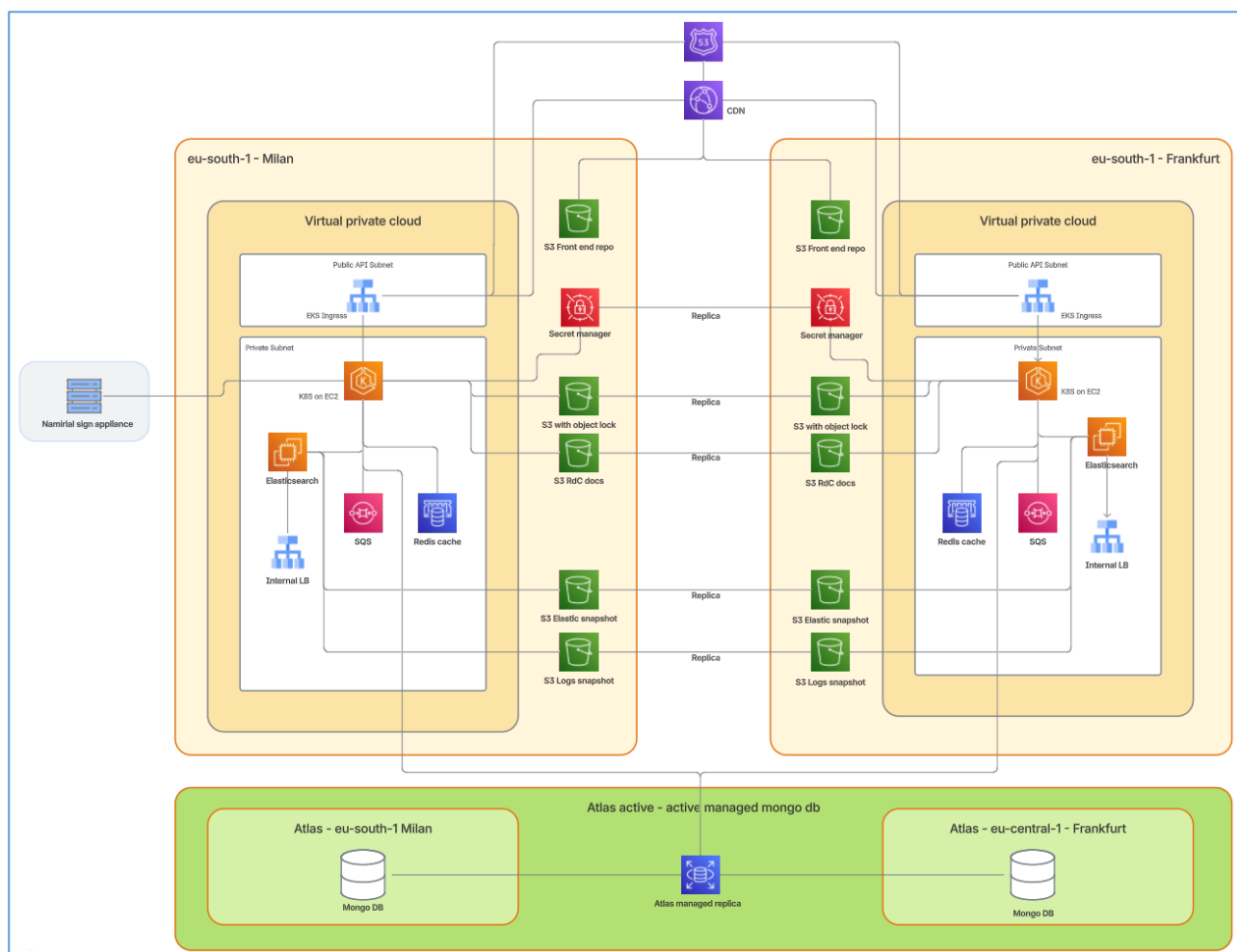


Fig. 10 – Rappresentazione grafica delle componenti fisiche del sistema Archive

L'immagine rappresenta l'infrastruttura cloud progettata per garantire massima affidabilità, resilienza e continuità operativa grazie a una solida architettura di duplicazione geografica.

La soluzione si sviluppa su due principali data center situati in due regioni europee distinte:

Milan (eu-south-1) e Frankfurt (eu-central-1).

Entrambi i siti ospitano repliche complete delle risorse e dei servizi applicativi, organizzate all'interno di ambienti virtualizzati (VPC) autonomi ma sincronizzati tra loro. In questo modo, ogni servizio fondamentale (come storage, database, sistemi di ricerca e code di messaggistica) risulta ridondato su entrambe le regioni, assicurando la disponibilità anche in caso di problemi localizzati su una singola area.

Un particolare accento viene dato al Disaster Recovery (DR): la presenza di copie (repliche) costanti tra le due regioni garantisce che, in caso di guasto o indisponibilità di un data center, l'infrastruttura possa continuare a operare senza interruzioni, grazie all'attivazione delle risorse replicate.

In sintesi, questa architettura offre:

- Duplicazione geografica delle risorse su due regioni UE distinte, per resilienza contro eventi locali;
- Ridondanza dei componenti critici (storage, database, cache, code, gestione dei segreti, bilanciatori di carico) distribuiti e replicati su entrambi i data center;
- Disaster Recovery: le repliche continue permettono di garantire continuità del servizio anche in condizioni di emergenza.

Queste caratteristiche complessive consentono all'infrastruttura di offrire un elevato livello di affidabilità e continuità operativa.

Ulteriori dettagli relativi all'infrastruttura hardware e di rete adottata per il sistema *Archive* sono contenuti nel SGSI del servizio.

[Torna al sommario](#)

9. MONITORAGGIO E CONTROLLI

Il Conservatore TeamSystem Service programma ed attua meccanismi di monitoraggio e controllo ed esegue un processo di gestione degli incidenti, assicurando l'individuazione delle soluzioni tecniche e operative per la prevenzione, la rilevazione, la pronta reazione ed il monitoraggio degli incidenti fino alla loro risoluzione.

9.1 Procedure di monitoraggio

9.1.1 Procedure di audit interno

Al fine di garantire il miglioramento continuo dei servizi e delle prestazioni delle attività di conservazione, TeamSystem Service ha pianificato ed eseguito, anche con l'ausilio di consulenti, delle verifiche ispettive interne, in linea con gli standard ISO/IEC 27007 e TR 101 533-02, per stabilire se i processi e le procedure siano efficacemente realizzati e conformi con quanto richiesto dalla normativa di riferimento.

Il processo utilizzato per lo svolgimento degli audit è basato sul processo di gestione delle verifiche ispettive interne definito centralmente dalla Capogruppo nell'ambito della conformità allo standard ISO 9001.

L'obiettivo degli audit interni è quello di:

- verificare e valutare:
 - l'efficienza ed efficacia del sistema SGSI;
 - il rispetto delle procedure aziendali del SGSI;
 - il rispetto della normativa cogente. In tale ambito, considerando l'elevato numero di standard e normative di riferimento che regolamentano l'erogazione dei servizi quali la fatturazione elettronica e la conservazione digitale a norma è stata definita una apposita procedura per la gestione delle conformità.
- avviare le azioni correttive e preventive identificate come necessarie per prevenire il ripetersi delle carenze e delle problematiche relative ai processi e/o sistemi analizzati. La gestione di tali azioni viene formalizzata all'interno di uno specifico documento;
- individuare le opportunità di miglioramento che consentirebbero di incrementare il livello complessivo di sicurezza, riservatezza ed integrità degli oggetti e delle informazioni.

Nel pianificare gli audit, l'organizzazione del Conservatore deve tenere in considerazione i seguenti criteri:

- devono essere oggetto di verifica tutti i processi aziendali coinvolti incluse le attività della Direzione Generale;
- devono essere verificati a campione tutti i processi predisposti per rispondere ai requisiti dello standard ISO/IEC 27001, del Manuale di Conservazione e del Disciplinare Specificità del Contratto;
- devono essere verificate le criticità emerse dai risultati delle precedenti verifiche ispettive interne;
- devono essere verificati i risultati delle verifiche ispettive dell'Organismo di Certificazione ove disponibili;
- devono essere selezionati dei valutatori indipendenti che non hanno alcuna responsabilità o rapporti di dipendenza diretta nell'attività sottoposta a verifica.

In tale contesto, il piano delle verifiche interne approvato dalla Direzione Aziendale del Conservatore, in accordo con il Responsabile del Servizio di Conservazione, prevede l'esecuzione periodica di audit specifici sui processi e sulle funzioni aziendali coinvolte nell'ambito di applicazione del SGSI e del sistema di conservazione.

In aggiunta, nell'ambito delle procedure di monitoraggio messe in campo dal Conservatore, viene eseguita anche una verifica periodica relativa alla consistenza e l'integrità dei Pacchetti di documenti e dei relativi indici. Tale attività prevede l'esecuzione o eventuale delega di esecuzione a consulenti esterni, di una procedura di controllo che interesserà un adeguato campione pseudo casuale degli oggetti sottoposti a Conservazione. Al fine di garantire un controllo esaustivo di consistenza e integrità, tale procedura sarà effettuata sui dati presenti all'interno del sistema di Storage e sulle copie di sicurezza.

In aggiunta all'adozione di specifiche procedure di controllo interno, sono state abilitate delle apposite funzionalità di logging che consentono di registrare, valutare ed analizzare periodicamente le performance del sistema di conservazione e, in generale, delle misure di sicurezza adottate in ambito SGSI. Nello specifico, le procedure di verifica, gli eventuali interventi sul software applicativo, le modifiche delle configurazioni, l'assegnazione delle deleghe a svolgere opportune operazioni,

nonché tutti eventi importanti o ritenuti tali dal Responsabile della Conservazione e da altri Responsabili della struttura organizzativa del Conservatore ai fini del corretto svolgimento del processo di conservazione saranno opportunamente tracciati nel sistema di log e se necessari in verbali appositamente redatti.

[Torna al sommario](#)

9.1.2 Procedure di audit sui fornitori

Al fine di garantire il miglioramento continuo dei servizi e delle prestazioni delle attività di conservazione, TeamSystem Service ha pianificato ed eseguito, anche con l'ausilio di consulenti, delle verifiche ispettive esterne sui principali fornitori, ossia quelli che hanno maggiore impatto sul servizio di conservazione, in linea con i requisiti AgID e ISO/IEC 27001, per stabilire se i processi e le procedure siano efficacemente realizzati e conformi con quanto richiesto dalla normative di riferimento.

Tali verifiche ispettive sono sancite nello specifico all'interno dei contratti di servizio con i fornitori. Si rimanda ai relativi contratti in essere per eventuali approfondimenti.

9.1.3 Monitoraggio dei fornitori

Nell'ambito delle attività svolte dal sistema di conservazione occorre porre particolare attenzione a due aspetti inerenti i fornitori chiave, ossia i fornitori la cui attività ha impatti diretti sul sistema di conservazione: Service Level Agreement (SLA) e Statement of Applicability (SOA).

Il processo di monitoraggio dei fornitori prevede il seguente approccio:

- Per quanto riguarda gli SLA occorre andare a monitorare periodicamente e puntualmente gli indicatori definiti all'interno degli specifici contratti, tracciando i risultati del monitoraggio all'interno del file "DC_MSA_02_Misure Service Level Agreement", in modo da valutare la fornitura del servizio.
- Per quanto riguarda invece i SOA, è necessario analizzare i controlli di sicurezza messi in atto dai fornitori e valutarli rispetto ai requisiti del sistema di conservazione in ottica ISO/IEC 27001.

Per ulteriori dettagli si rimanda agli specifici contratti stipulati con le terze parti.

9.1.4 Monitoraggio delle operazioni nel sistema di log

I log del servizio *Archive* vengono gestiti in accordo alla procedura di log management, in cui sono dettagliate le misure tecniche ed organizzative previste per una corretta gestione dei log stessi.

Sulla base di quanto definito all'interno di tale procedura, i file di log sono classificati al fine di differenziarne la gestione, in base alla categoria di appartenenza. Sono previsti tre livelli di classificazione in funzione della natura degli eventi/attività tracciate:

- Log di sistema
- Log applicativi
- Log di sicurezza

Sempre all'interno della procedura di log management sono definiti dal punto di vista organizzativo i ruoli e le responsabilità assegnate agli attori coinvolti nel processo di gestione dei log che a livello macroscopico prevede le seguenti fasi:

- raccolta;
- analisi;
- storicizzazione;
- gestione accesso ai log;
- distruzione.

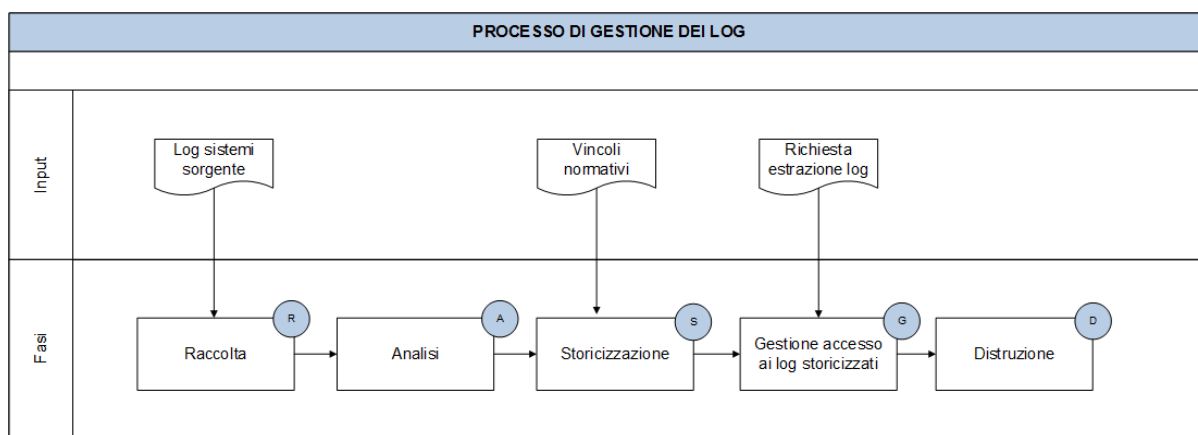


Fig. 11 – Processo di gestione dei log

I file di log sistemistici e di sicurezza, ove applicabile, sono raccolti e conservati mediante l'utilizzo di una piattaforma di log collection centralizzata, posizionata nel Data Center contenente l'ambiente di produzione. I dispositivi per i quali è prevista la raccolta centralizzata dei log devono essere configurati in modo da inviare i log raccolti in locale verso il sistema centrale, adottando il protocollo syslog. Gli eventi non inviati alla piattaforma centralizzata sono conservati in locale sui sistemi. I file di log di sicurezza dei server, ove presenti vengono inviati e conservati sulla piattaforma Cyberark.

La piattaforma centralizzata garantisce una serie di requisiti tecnici/normativi per la gestione sicura dei log, in particolare risponde ai seguenti requisiti:

- Completezza, inalterabilità ed integrità dei log;
- Tracciabilità di tutti gli accessi (Login) e di tutte le disconnessioni (Logout) eseguite da utenze con privilegi amministrativi sugli strumenti elettronici mediante cui vengono eseguiti trattamenti di dati personali;
- Cancellazione dei log raccolti in locale sulle sorgenti entro un tempo massimo prestabilito;
- Conservazione on line, per almeno 6 mesi, dei Log di Accesso (Log di sicurezza) delle utenze con privilegi di amministrazione

I file di log estratti dalla piattaforma utilizzata per erogare il Servizio di Conservazione sono strutturati in modo da fornire tutte le informazioni necessarie a ricostruire a posteriori i comportamenti dei sistemi o degli utilizzatori dei sistemi. Tali file di log consentono di rilevare almeno i seguenti eventi:

- il login ed il logout di ciascun utente;
- le attività svolte da ciascun utente nell'ambito dei flussi operativi;
- le azioni svolte nell'ambito dei vari work-flow operativi.

Sempre per ciò che riguarda i Log del Servizio di Conservazione, la procedura attuale di gestione prevede indici incrementali dei log; attualmente l'incremento dei log e degli indici viene effettuato su base mensile. Gli indici sono tenuti sullo stack Elastic e hanno una nomenclatura che richiama l'anno e il mese di creazione della riga di log secondo il pattern "cct_log_log_[anno][mese] "

Come primo livello di protezione, gli indici dei log su Elastic vengono messi in sola lettura allo scadere del mese. Tale attributo viene impostato automaticamente il giorno successivo al cambio mese. Quindi riscontreremo nel sistema un indice "attivo" su cui vengono versati i dati attuali e gli indici dei mesi precedenti, in sola lettura.

Per garantire l'immutabilità delle informazioni, al cambio mese una procedura automatica trasferisce lo snapshot contenente la replica dei log dei mesi in sola lettura su S3 in un bucket con objectlock attivo con data di retention di 10 anni. Questo consente di spostare e garantire che l'archivio su cui vengono tenuti gli indici dei log, e quindi il loro contenuto sia tecnicamente immutabile.

Dopo aver terminato il trasferimento su S3 degli indici e impostato l'objectlock, lo snapshot trasferito viene rianalizzato estraendo direttamente da S3 gli hashcode dei file archiviati. Tali hashcode sono direttamente riconducibili al contenuto dei file e quindi ai log in esso contenuti. L'insieme degli hashcode sono quindi riportati in un documento di testo che rappresenta l'indice dello snapshot, tale indice viene conservato digitalmente a norma, così da apporre a tali hashcode anche una firma digitale e una marcatura temporale che garantisca l'istante in cui le informazioni sono state congelate.

La catena dei riferimenti tra log, file, hashcode e firma digitale con conservazione digitale consente di garantire che i dati siano immutati rispetto all'istante di conservazione dell'indice dello snapshot.

Per le componenti di sistema ospitate su cloud provider pubblico AWS, i log vengono raccolti ed inviati real-time verso il servizio PaaS di TeamSystemHELK nonché inviati al database Elastic Search che colleziona i log da conservare.

Le modifiche di configurazione dei servizi offerti da AWS vengono registrate direttamente dal cloud provider e consultabili tramite il servizio AWS CloudWatch e AWS CloudTrail.

Per ogni ulteriore approfondimento si rimanda al documento di Procedura di Log Management del SGSI di TeamSystem Service.

[Torna al sommario](#)

9.1.5 Monitoraggio componenti hardware del sistema di Conservazione

Le procedure di monitoraggio hanno l'obiettivo di valutare ed analizzare periodicamente le performance del Sistema di Conservazione e, in generale, delle misure di sicurezza adottate in ambito SGSI.

Il processo di monitoraggio del sistema di conservazione prevede un approccio a più livelli:

- valutazione complessivo del livello sicurezza delle informazioni. Nello specifico, con cadenza annuale, si procede alla misura dei risultati conseguiti complessivamente in tema di raggiungimento degli obiettivi di sicurezza delle informazioni. Ulteriori dettagli sono riportati all'interno del SGSI, in cui è disponibile una descrizione di tale processo;
- valutazione di KPI relativi al livello di attuazione ed efficacia dei processi di sicurezza afferenti al SGSI. Tale analisi è pianificata con cadenza annuale. Per ulteriori dettagli si veda il documento che definisce i KPI del SGSI;
- valutazione effettiva sul campo tramite l'esecuzione di attività di verifiche ispettive interne, volte a valutare la corretta attuazione dei processi SGSI. Per ulteriori dettagli si veda il par. 9.1.1;
- identificazione di eventuali vulnerabilità o debolezze di sicurezza tramite l'esecuzione di attività di Vulnerability Assessment e Penetration Test, adottando strumenti dedicati e un processo formalizzato;
 - valutazione ed analisi di dettaglio dei log prodotti dai componenti che costituiscono la piattaforma adottata da TeamSystem Service per erogare il Servizio di Conservazione.

Le attività di monitoraggio prevedono l'identificazione di eventuali aree di debolezza, con la definizione, laddove necessario, di piani / proposte di miglioramento che costituiscono i principali input al Riesame della Direzione.

[Torna al sommario](#)

9.1.6 Controllo autenticazione ed accesso al Servizio

I controlli di accesso logico adottati dall'Organizzazione del Conservatore per salvaguardare la sicurezza delle informazioni gestite all'interno del sistema di conservazione sono molteplici:

- l'accesso alla piattaforma Web del sistema di conservazione (front end Archive) è protetto da un modulo di autenticazione, basato sull'utilizzo di credenziali di accesso (username e password), a cui si accede esclusivamente utilizzando il protocollo HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer);
- gli Utenti sono responsabili della scelta, gestione, utilizzo e modifica delle proprie credenziali di accesso, nel rispetto dei vincoli imposti dalla password policy che rappresenta lo standard di sicurezza aziendale per la gestione delle password. I principi definiti all'interno di tale documento sono in linea con quanto richiesto anche dalla normativa vigente in materia di protezione dei dati personali e dalla ISO/IEC 27001;
- il sottosistema autorizzativo, basato su logica RBAC, impone che ogni utente sia associato ad un ruolo e quindi ad un profilo di default, che può essere tuttavia modificato di volta in volta andando a gestire eventuali eccezioni;
- la piattaforma genera in autonomia i log necessari per monitorare la correttezza delle attività eseguite, sia a livello utente, sia a livello di utenze privilegiate, tracciando eventuali tentativi di compromissione. Tali log, oltre a consentire il monitoraggio delle operazioni di login e logout, come per altro richiesto anche dal Codice in materia di protezione dei dati personali (D. Lgs. 196/03), permettono anche la verifica delle operazioni eseguite dagli Amministratori di Sistema (e.g. modifica dei metadati, modifica parametri di configurazione);

- in casi specifici (e.g., 5 tentativi login falliti) è prevista la generazione di allarmi automatici che consentono di intervenire tempestivamente nelle fasi di contenimento e contrasto di un eventuale incidente di sicurezza informatica. Ulteriori dettagli sono riportati nel SGSI certificato ISO 27001;
- i sistemi anti-intrusione, quali Firewall e IDS/IPS, sono posizionati all'interno del segmento di rete che collega la piattaforma Archive con internet, al fine di intercettare ogni eventuale azione malevola volta a degradare, parzialmente o totalmente, l'erogazione del Servizio;
- la generazione dell'utenza avviene in conformità con le direttive indicate all'interno della procedura di controllo accessi, garantendo il rispetto dei principi di Segregation of Duties e Need to Know, come illustrato anche all'interno del SGSI:
 - la fase di inserimento di una nuova utenza interna (e.g., Operatore, Amministratore), avviene previa richiesta formale da parte di una figura individuata e riconosciuta come responsabile dell'utente, la quale ha l'obbligo di specificare alcuni dati, tra i quali il ruolo ed il profilo richiesto nel rispetto delle regole definite all'interno dell'apposita "Matrice ruoli – funzionalità" predisposta dall'Organizzazione, a garanzia del principio del RBAC;
 - per le utenze esterne (e.g., Clienti), a seguito dell'adesione al Servizio e il controllo di integrità e correttezza della documentazione contrattuale firmata, si procede con l'invio delle credenziali agli Utenti, ponendo l'obbligo del cambio password al primo accesso. Gli Operatori del Servizio non vengono mai a conoscenza della password utente al fine di assicurare la riservatezza delle informazioni trattate tramite il processo di conservazione;
- tutte le utenze abilitate sono sottoposte ad un processo di revisione periodico circa la sussistenza delle esigenze che hanno portato alla loro attivazione.

Per la descrizione dettagliata del processo di gestione degli accessi logici al sistema *Archive* si rimanda alla specifica procedura referenziata all'interno del SGSI certificato ISO27001.

[Torna al sommario](#)

9.1.7 Procedura di verifica periodica dei permessi di accesso alla piattaforma

Tutte le utenze abilitate all'accesso al sistema di conservazione, sia quelle interne che esterne, devono essere sottoposte a revisione circa la sussistenza delle esigenze che hanno portato alla loro attivazione.

La revisione delle utenze avviene periodicamente e con frequenza almeno semestrale.

Per ulteriori dettagli relativamente allo specifico processo di revisione, si rimanda al documento alla documentazione contenuta nel SGSI certificato ISO27001.

[Torna al sommario](#)

9.1.8 Procedure di sicurezza

La Direzione Aziendale, tramite l'adozione di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) conforme alla norma ISO/IEC 27001 e l'emissione della Information Security Policy ha delineato l'indirizzo generale e strategico da perseguire al fine di prevenire i rischi connessi al trattamento delle informazioni e di proteggere il patrimonio informativo aziendale e dei propri Clienti.

La suddetta politica si fonda sull'insieme di principi e requisiti necessari a proteggere e tutelare le informazioni, siano esse gestite in formato elettronico o cartaceo. Tale concetto può essere declinato con le seguenti proprietà (dette anche parametri o principi di sicurezza):

- **Confidenzialità:** assicurare che l'informazione sia accessibile solamente a coloro che hanno le dovute autorizzazioni;
- **Integrità:** salvaguardare la completezza e l'accuratezza dell'informazione;
- **Disponibilità:** assicurare che gli utenti autorizzati abbiano accesso alle informazioni, e agli elementi architetture associati, quando ne fanno richiesta.

Le tematiche specifiche che contribuiscono a vario titolo al fine comune di salvaguardia delle informazioni sono delineate all'interno della documentazione di dettaglio contenuta nel SGSI, certificato ISO/IEC 27001, a cui si rimanda, in particolare per gli ambiti di:

- Politiche per la sicurezza delle informazioni
- Analisi e gestione dei rischi
- Sicurezza delle risorse umane
- Relazioni con i fornitori
- Sicurezza delle comunicazioni
- Controllo degli accessi
- Sicurezza delle attività operative
- Acquisizione, sviluppo e manutenzione dei sistemi
- Gestione degli incidenti relativi alla sicurezza delle informazioni
- Conformità
- Monitoraggio e auditing

[Torna al sommario](#)

9.2 Verifica dell'integrità degli archivi

Al fine di garantire l'integrità e la leggibilità dei documenti sottoposti al processo di conservazione per tutto il periodo per cui è obbligatorio il loro mantenimento, è previsto un processo di verifica degli archivi. In particolare, il Conservatore in accordo con il Responsabile della Conservazione del Titolare ha il compito di pianificare le attività atte ad evitare che il deterioramento dei supporti e l'obsolescenza tecnologica dei sistemi hardware e software possa inficiare la fruibilità delle informazioni conservate. Il Conservatore, con frequenza almeno quinquennale, ha il compito di:

- verificare la leggibilità dei supporti sia dal punto di vista del deterioramento del supporto stesso sia dal punto di vista della disponibilità di hardware e software di lettura dei supporti stessi. Le attività di verifica a campione vengono riportate in apposito verbale;
- nel caso si ritenga opportuno il riversamento diretto, prevedere il controllo di integrità dei duplicati informatici prodotti;
- nel caso si ritenga opportuno il riversamento sostitutivo, prevedere l'intervento del Pubblico Ufficiale per i soli casi necessari previsti dalla normativa, previo accordo.

In tale contesto, il Conservatore ha adottato una soluzione software specifica che **impedisce l'alterazione o l'eliminazione dei file prima di una data prestabilita** che corrisponde al periodo di conservazione (funzionalità di software **WORM**), come meglio specificato nella documentazione della certificazione ISO/IEC 27001. Tale soluzione è stata adottata al fine ottenere elevate garanzie in termini di integrità delle informazioni anche nel lungo periodo.

Inoltre, il Conservatore ha adottato misure aggiuntive volte a garantire nel tempo l'integrità degli archivi:

- ogni intervento sull'architettura generale del sistema prevede una fase di analisi di impatto sul processo di conservazione e sulla leggibilità degli oggetti nel tempo degli stessi, come descritto nella procedura di Change Management, contenuta nel SGSI;
- la copia aggiornata di tutte le versioni occorrenti del software e della documentazione per la visualizzazione dei documenti è a disposizione del Conservatore;
- definizione, ove necessario, di accordi specifici concordati con i Titolari e i Produttori dei PdV sono riportati nel Disciplinare Specificità del Contratto.

[Torna al sommario](#)

9.3 Soluzioni adottate in caso di anomalie

TeamSystem Service pianifica e realizza la Gestione degli incidenti e data breach con il fine di minimizzare gli impatti sul business e raggiungere gli obiettivi di sicurezza prefissati.

All'interno del SGSI certificato ISO 27001, sono descritti tutti i controlli e le procedure adottate da TeamSystem Service per gestire le diverse tipologie di anomalie. Inoltre, al fine di gestire in maniera efficace le anomalie afferenti la sicurezza delle informazioni è stata definita una apposita procedura di gestione delle incidenti di sicurezza.

Si definisce "incidente di sicurezza" un qualsiasi evento negativo relativo alla sicurezza fisica o logica, di natura casuale, colposa o dolosa, che potrebbe compromettere il business aziendale, il corretto funzionamento dei sistemi, delle applicazioni e/o delle reti dell'organizzazione o l'integrità e/o la riservatezza delle informazioni in esse memorizzate od in transito, o che violi le politiche di sicurezza definite o le leggi in vigore.

L'Organizzazione definisce in modo chiaro i ruoli e le responsabilità nell'ambito del processo in oggetto e stabilisce un insieme di strategie e di tecniche, di natura organizzativa, procedurale e tecnologica, per individuare e rispondere, in maniera tempestiva ed efficace, ad un incidente di sicurezza reale o potenziale con impatto sui sistemi informativi.

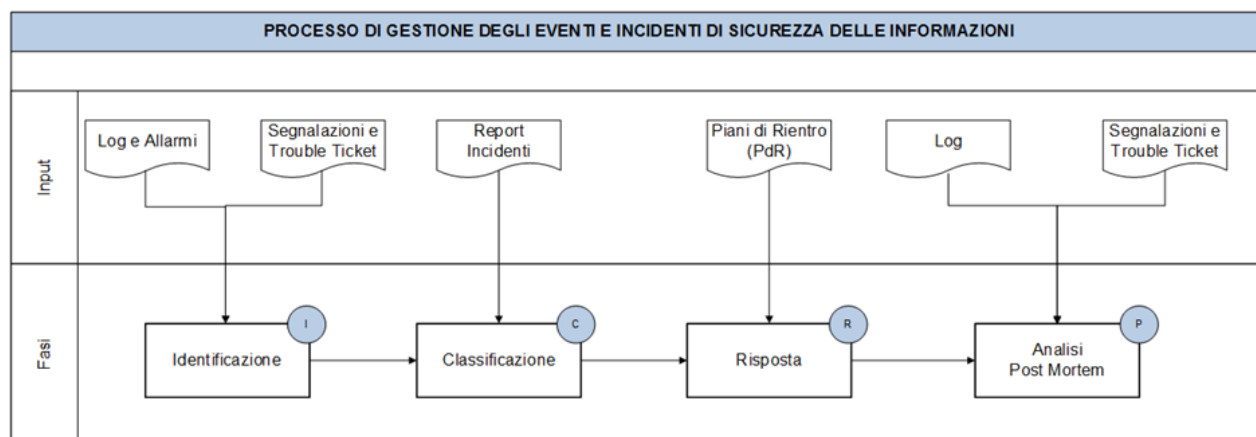


Fig. 12 – Processo di Gestione degli incidenti

A livello operativo, TeamSystem Service adotta una piattaforma di trouble ticketing per la gestione ed il tracciamento delle richieste di assistenza inerenti il sistema di conservazione, ivi comprese eventuali segnalazioni di incidenti e tracciamento delle relative operazioni di gestione.

Per una trattazione più dettagliata dell'argomento, si rimanda ai documenti aziendali specifici in ambito di Incident Management oggetto di certificazione ISO/IEC 27001

[Torna al sommario](#)

9.4 Processo di gestione dei cambiamenti hardware, software e firmware

Le fasi che caratterizzano il processo di Change Management sono finalizzate allo sviluppo o implementazione e successivo rilascio in esercizio delle modifiche da apportare in ambito:

- **Applicativo:** modifiche relative alla componente applicativa del sistema;
- **Infrastrutturale:** modifiche relative ad una o più delle seguenti componenti del sistema:
 - Hardware (es. server, apparati di sicurezza)
 - Middleware
 - DBMS
 - Sistema Operativo
 - Infrastruttura di rete.

Nella seguente tabella sono identificate le macro tipologie di change applicativi/infrastrutturali.

TIPOLOGIA DI CHANGE	DESCRIZIONE
Change Complessi	Modifiche non comuni e predefinite ma piuttosto complesse, per le quali è necessaria un'analisi preliminare volta a definire le attività da svolgere con un piano di lavoro specifico. Tali change necessitano di un flusso approvativo più articolato e richiedono l'approvazione del Cliente a seconda delle situazioni. Per tali tipi di change sono previste più fasi approvative che coinvolgono ruoli aziendali del Fornitore e del Cliente. Rientrano in questa categoria i cambiamenti che richiedono lo sviluppo evolutivo sull'Applicazione.
Change Standard	Modifiche per le quali esiste una definizione ben strutturata delle attività da effettuare. Tali tipi di change sono definibili a priori con template che contengono il flusso definito per l'implementazione che, riguardando attività predefinite, ripetibili ed a basso impatto e rischio, necessitano di un iter approvativo ridotto, relativo ad esempio agli aspetti di pianificazione della data in cui effettuare le attività necessarie.
Emergenze	Modifiche che nascono dalla necessità immediata di risolvere un incidente siano esse standard o complesse, ma che per la particolare natura di urgenza/emergenza (ad esempio risolvere una situazione di crisi) hanno la necessità di essere implementate senza una fase di approvazione formale per non bloccare il processo.

I change sono relativi allo sviluppo evolutivo e correttivo dell'applicazione o dell'infrastruttura a supporto e possono scaturire da uno o più dei seguenti input:

INPUT	TIPOLOGIA MODIFICA
• Richieste dei clienti/rivenditori (*) • Esigenze di business interne • Adeguamento normativo	Evolutiva
• Manutenzione ordinaria • Anomalie/errori non aventi potenziali impatti sulla disponibilità del servizio • Anomalie/errori con potenziale impatto sulla disponibilità del servizio	Preventiva/Correttiva

(*) si precisa che il Servizio è standardizzato, ossia è erogato con le stesse modalità e la stessa User Experience per tutti i clienti; di conseguenza non sono previsti sviluppi di personalizzazioni specifiche per cliente. Ogni richiesta di implementazione che viene ritenuta utile in ottica evolutiva e di miglioramento del Servizio viene sviluppata, industrializzata e resa disponibile a tutti.

L'input del processo innesca il cambiamento di alcune caratteristiche o funzionalità del sistema informatico interessato in ottica evolutiva (qualora si voglia arricchire il sistema con nuove

funzionalità o migliorare quelle esistenti) o nell'ambito di interventi correttivi (qualora sia necessario intervenire su alcune anomalie riscontrate). Tali circostanze avviano il processo di Change Management che sarà caratterizzato da uno specifico flusso sulla base della tipologia di change. Il legame tra input e tipologia di change è riportato nella figura successiva:

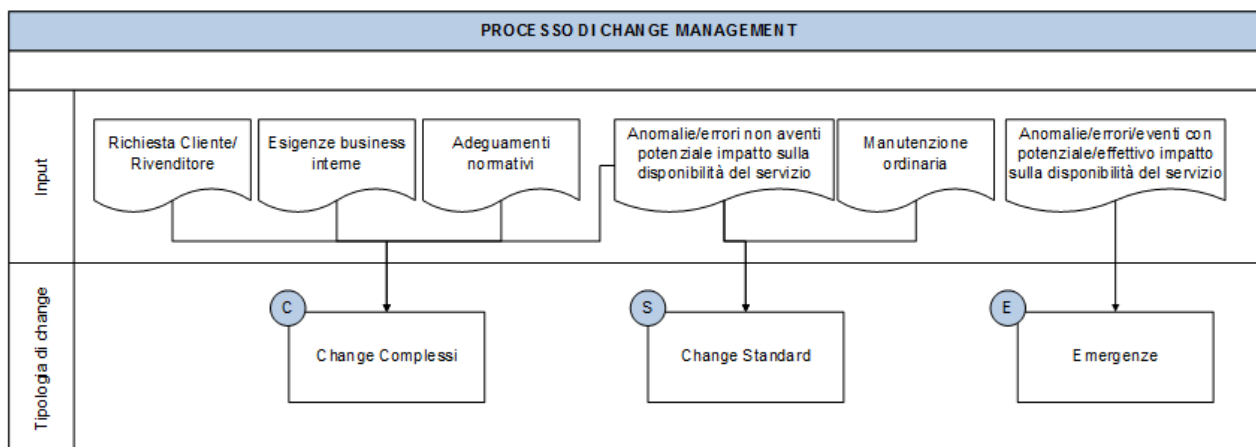


Figura 13 - Processo di gestione dei cambiamenti – macro tipologie di changes

Per una trattazione più dettagliata dell'argomento, si rimanda ai documenti aziendali specifici in ambito di Change Management oggetto di certificazione ISO/IEC 27001

[Torna al sommario](#)