MANUALE DI CONSERVAZIONE

di TEAMSYSTEM SERVICE S.R.L.

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	20/09/2018	Ilaria Bruno	Responsabile Funzione Archivistica di Conservazione
Verifica	24/09/2018	Stefano Liguori - Michele di Rienzo	Responsabile Sicurezza e Sistemi Informativi per la Conservazione - Responsabile del Servizio di Conservazione
Approvazione	28/09/2018	Michele Di Rienzo - Fulvio Talucci	Responsabile del Servizio di Conservazione Legale Rappresentante

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	

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 13
3.1 NORMATIVA DI RIFERIMENTO 13
3.2 STANDARD DI RIFERIMENTO 17
4. RUOLI E RESPONSABILITÀ 19
5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE 25
5.1 ORGANIGRAMMA 25
5.2 STRUTTURE ORGANIZZATIVE 27
6. OGGETTI SOTTOPOSTI A CONSERVAZIONE 37
6.1 OGGETTI CONSERVATI 37
6.2 METADATI E FASCICOLI 39
6.2.1 Metadati minimi del documento informatico 40
6.2.2 Metadati minimi del documento informatico amministrativo 40
6.2.3 Fascicoli informatici 41
6.2.4 Metadati minimi del fascicolo informatico o aggregazione documentale 43
6.3 FORMATI 44
6.4 PACCHETTO DI VERSAMENTO 45
6.5 RAPPORTO DI VERSAMENTO 49
6.6 PACCHETTO DI ARCHIVIAZIONE 50
6.7 PACCHETTO DI DISTRIBUZIONE 56
7. PROCESSO DI CONSERVAZIONE 57
7.1 MODALITÀ DI ACQUISIZIONE DEI PACCHETTI DI VERSAMENTO PER LA LORO PRESA IN CARICO 59
7.2 VERIFICHE EFFETTUATE SUI PACCHETTI DI VERSAMENTO E SUGLI OGGETTI IN ESSI CONTENUTI 61
7.3 ACCETTAZIONE DEI PACCHETTI DI VERSAMENTO E GENERAZIONE DEL RAPPORTO DI VERSAMENTO DI PRESA IN CARICO 62
7.4 RIFIUTO DEI PACCHETTI DI VERSAMENTO E COMUNICAZIONE DELLE ANOMALIE 62
7.5 PREPARAZIONE E GESTIONE DEL PACCHETTO DI ARCHIVIAZIONE 63
7.6 PREPARAZIONE E GESTIONE DEL PACCHETTO DI DISTRIBUZIONE AI FINI DELL'ESIBIZIONE 65
7.7 PRODUZIONE DI DUPLICATI E COPIE INFORMATICHE E DESCRIZIONE DELL'EVENTUALE INTERVENTO DEL PUBBLICO UFFICIALE NEI CASI PREVISTI 66
7.8 SCARTO DEI PACCHETTI DI ARCHIVIAZIONE 67
7.9 PREDISPOSIZIONE DI MISURE A GARANZIA DELL'INTEROPERABILITÀ E TRASFERIBILITÀ AD ALTRI CONSERVATORI 67
8. IL SISTEMA DI CONSERVAZIONE 69
8.1 COMPONENTI LOGICHE 69
8.2 COMPONENTI TECNOLOGICHE 71

8.3 COMPONENTI FISICHE 72
9. MONITORAGGIO E CONTROLLI **75**
9.1 PROCEDURE DI MONITORAGGIO 75
9.1.1 Procedure di audit interno 75
9.1.2 Procedure di audit sui fornitori 77
9.1.3 Monitoraggio dei fornitori 77
9.1.4 Monitoraggio delle operazioni nel sistema di log 77
9.1.5 Monitoraggio componenti hardware del sistema Conservazione Cloud 80
9.1.6 Controllo autenticazione ed accesso al Servizio 80
9.1.7 Procedura di verifica periodica dei permessi di accesso alla piattaforma 82
9.1.8 Procedure di sicurezza 82
9.2 VERIFICA DELL'INTEGRITÀ DEGLI ARCHIVI 86
9.3 SOLUZIONI ADOTTATE IN CASO DI ANOMALIE 87
9.4 PROCESSO DI GESTIONE DEI CAMBIAMENTI HARDWARE, SOFTWARE E FIRMWARE 88

1. SCOPO E AMBITO DEL DOCUMENTO

Il presente documento ha lo scopo di descrivere sulla base di quanto previsto dalle disposizioni di cui al D.P.C.M. del 3 dicembre 2013 (nel seguito Regole Tecniche) 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	
Denominazione	**TeamSystem Service S.r.l. con Unico Socio** Società del Gruppo TeamSystem controllata al 100% da TeamSystem S.p.A.
Rappresentante Legale	Fulvio Talucci
Sede legale ed operativa	Viale Giuseppe Ferro 86100 Campobasso (CB)
Codice Fiscale e Partita Iva	01641790702
Registro Imprese	Iscritta al Registro Imprese di Campobasso n. 01641790702
Repertorio Economico Amministrativo	Nr. R.E.A. 124222
Capitale Sociale	€ 200.000 Interamente versato
Contatti	marketing@teamsystemservice.it info@teamsystemservice.it

Più nel dettaglio, ai sensi dell'articolo 8 delle Regole Tecniche, 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 "*Conservazione Cloud*".

La redazione del Manuale di Conservazione si basa sui principi dell'aggiornamento e della trasparenza al fine di garantire al Produttore e all'Utente fruitore del Servizio di Conservazione una descrizione fedele del sistema *Conservazione Cloud* adottato e gestito da 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 Produttore dei Documenti 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 dei documenti.
Manuale Utente	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.

Torna al sommario

2. TERMINOLOGIA (GLOSSARIO, ACRONIMI)

2.1 Glossario

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

Accreditamento: riconoscimento, da parte dell'Agenzia per l'Italia Digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione;

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 11386:2010;

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;

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;

Certificato qualificato: certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciato da certificatore rispondente ai requisiti fissati dall'allegato II della medesima direttiva;

Conservatore accreditato: soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia Digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, dall'Agenzia per l'Italia Digitale;

Conservazione: insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel Manuale di Conservazione;

Copia di sicurezza: copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 delle Regole Tecniche per il sistema di conservazione;

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 del decreto attuativo D.P.C.M. 13 novembre 2014;

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

Documento informatico amministrativo: atto formato dalle Pubbliche Amministrazioni con strumenti informatici, nonché dati o documenti informatici detenuti dalle stesse;

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 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 strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella Pubblica Amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del Codice dell'Amministrazione Digitale. Secondo lo standard ISAD (G), adottato nel sistema di conservazione in oggetto, il fascicolo (unità archivistica) costituisce di solito l'unità elementare di una serie;

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

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;

Fondo: l'insieme organico dei documenti archivistici, senza distinzione di tipologia o di supporto, formati e/o accumulati e usati da un determinato ente nello svolgimento della propria attività aziendale o istituzionale (standard ISAD-G);

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 nell'allegato 5 delle Regole Tecniche, 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 in ambito tributario il D.M. 17 giugno 2014;

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

Leggibilità: insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti;

Livello di descrizione: la posizione dell'unità archivistica all'interno della struttura gerarchica del fondo;

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

Metadati: insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 delle Regole Tecniche;

Pacchetto di Archiviazione: pacchetto informativo composto dalla trasformazione di uno o più Pacchetti di Versamento secondo lo standard UNI SInCRO 11386:2010 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 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 al sistema di conservazione nella fase di pre-acquisizione e secondo le specifiche e le condizioni concordate nelle Specificità del Contratto;

Piano della sicurezza del sistema di conservazione: documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza;

Pre-acquisizione: 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 11386:2010 per poter essere così accettati dal sistema di conservazione;

Processo di conservazione: insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 10 delle Regole Tecniche del sistema di conservazione;

Produttore dei documenti: persona fisica o giuridica che produce il pacchetto di versamento 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 conformi allo standard UNI SInCRO 11386:2010 inviati dal Produttore;

Repertorio informatico: registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche con cui si formano altri atti e documenti o indici di atti e documenti secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica;

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;

Serie: documenti ordinati secondo un sistema di archiviazione o conservati insieme perché sono il risultato di un medesimo processo di sedimentazione o archiviazione o di una medesima attività; appartengono ad una specifica tipologia; o a ragione di qualche altra relazione derivante dalle modalità della loro produzione, acquisizione o uso *(secondo lo standard di descrizione archivistica ISAD-G)*;

Sub-fondo: la suddivisione di un fondo contenente un insieme di documentazione correlata, corrispondente a suddivisioni amministrative dell'istituzione o dell'organismo produttore, o altrimenti, a raggruppamenti geografici, cronologici, funzionali, o di simile natura del materiale documentario. Quando l'Ente Produttore ha una struttura gerarchica complessa, ciascuna suddivisione si articola nelle suddivisioni necessarie a dar conto dei livelli della struttura gerarchica stessa *(secondo lo standard di descrizione archivistica ISAD-G)*;

Unità documentaria: l'unità minima, concettualmente non divisibile, di cui è composto un archivio, per esempio, il documento informatico inteso come oggetto dati (file);

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;

IPdS: Indice del Pacchetto 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;

PdS: Pacchetto di Scarto;

PdV: Pacchetto di Versamento;

RdV: Rapporto di Versamento;

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.

Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013
Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71.

Decreto del Presidente del Consiglio dei Ministri 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.

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.

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.

Determinazione AGID n. 191 in vigore dal 5 giugno 2018
Adozione del Regolamento recante le modalità per l'esercizio del potere sanzionatorio ai sensi dell'art. 32-bis del decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni.

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.

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.

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.

Regolamento di esecuzione (UE) 2015/1502 della Commissione, dell'8 settembre 2015
Relativo alla definizione delle specifiche e procedure tecniche minime riguardanti i livelli di garanzia per i mezzi di identificazione elettronica ai sensi dell'articolo 8, paragrafo 3, 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.

Regolamento di esecuzione (UE) 2015/1505 della Commissione, dell'8 settembre 2015
Stabilisce le specifiche tecniche e i formati relativi agli elenchi di fiducia di cui all'articolo 22, paragrafo 5, 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.

Regolamento di esecuzione (UE) 2015/1506 della Commissione, dell'8 settembre 2015
Stabilisce le specifiche relative ai formati delle firme elettroniche avanzate e dei sigilli avanzati che gli organismi del settore pubblico devono riconoscere, di cui all'articolo 27, paragrafo 5, e all'articolo 37, paragrafo 5, 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.

Parte della normativa specifica, relativa ad esempio ad un particolare ambito come quello tributario, lavoristico, assicurativo è riportata nel seguito.

Decreto Ministero dell'Economia e Finanze 17 giugno 2014
Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005. In vigore dal 27 giugno 2014.

Decreto Ministero dell'Economia e delle Finanze del 23 gennaio 2004
Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di supporto. In vigore fino al 26 giugno 2014.

Decreto Ministero dell'Economia e delle Finanze del 7 marzo 2008
Individuazione del gestore del sistema di interscambio della fatturazione elettronica nonchè delle relative attribuzioni e competenze.

Decreto Ministeriale 3 aprile 2013, n. 55
Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'articolo 1, commi da 209 a 213, della legge 24 dicembre 2007, n. 244.

Decreto Legislativo 5 agosto 2015, n. 127
Trasmissione telematica delle operazioni IVA e di controllo delle cessioni di beni effettuate attraverso distributori automatici, in attuazione dell'articolo 9, comma 1, lettere d) e g), della legge 11 marzo 2014, n. 23.

Circolare n. 36/E dell'Agenzia delle Entrate 6 dicembre 2006
Decreto ministeriale 23 gennaio 2004 – Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici e alla loro riproduzione in diversi tipi di supporto.

D.P.R. 26 ottobre 1972, n. 633 s.m.
Decreto sulla disciplina dell'imposta sul valore aggiunto.

Circolare n. 18/E del 24 giugno 2014
IVA. Ulteriori istruzioni in tema di fatturazione.

D.P.C.M. del 19 luglio 2012 modificato dal D.P.C.M. 5 febbraio 2014
Definizione dei termini di validità delle autocertificazioni circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza di cui al DPCM 30 ottobre 2003, e dei termini per la sostituzione dei dispositivi automatici di firma.

Risoluzione n. 106/E del 2 dicembre 2014
Istituzione del codice tributo per il versamento, mediante il modello F24, dell'imposta di bollo su libri, registri ed altri documenti rilevanti ai fini tributari – articolo 6 del decreto del Ministro dell'economia e delle finanze 17 giugno 2014.

Risoluzione n. 158/E del 15 giugno 2009
Consulenza giuridica Associazione e Ordini Professionali – D.M. 23 gennaio 2004 e fatturazione elettronica – risposta a quesiti.

Risoluzione Agenzia delle Entrate n. 318/E del 7 novembre 2007
Obbligo di numerazione delle fatture di acquisto nell'affido in outsourcing dell'esecuzione delle operazioni di ricezione, protocollazione, registrazione in contabilità, ed archiviazione delle fatture passive e delle note di credito.

Risoluzione Agenzia delle Entrate n. 81/E del 25 settembre 2015
Obbligo di comunicazione del luogo di conservazione in modalità elettronica dei documenti rilevanti ai fini tributari, art. 5 D.M. 17 giugno 2014.

Risoluzione Agenzia delle Entrate n. 46/E del 10 aprile 2017
Produzione e conservazione elettronica dei documenti informatici rilevanti ai fini tributari - D.M. 17 giugno 2014.

Risoluzione Agenzia delle Entrate n. 96/E del 21 luglio 2017
Gestione documentale delle note spese e dei relativi giustificativi – D.M. 17 giugno 2014.

Risoluzione Agenzia delle Entrate n. 9/E del 29 gennaio 2018
Termine di conservazione elettronica delle dichiarazioni fiscali.

Decreto Ministeriale del 9 luglio 2008 – Tenuta e conservazione informatica del Libro Unico del Lavoro
Modalità di tenuta e conservazione del libro unico del lavoro e disciplina del relativo regime transitorio.

Vademecum sul Libro Unico del Lavoro
Vademecum del Ministero del Lavoro sul Libro Unico del Lavoro – regole sulla formazione e conservazione sostitutiva del LUL.

Circolare del Ministero del Lavoro n. 20 del 21 agosto 2008
Libro Unico del Lavoro e attività ispettiva – artt. 39 e 40 del DL n. 112 del 2008: prime istruzioni operative al personale ispettivo.

Regolamento ISVAP n. 27 del 14 ottobre 2008
Regole per la tenuta e conservazione dei registri assicurativi di cui all'art. 101 del D.Lgs. n. 209 del 7 settembre 2005 – Codice delle Assicurazioni Private.

Regolamento IVASS n. 8 del 3 marzo 2015
Regolamento concernente la definizione delle misure di semplificazione delle procedure e degli adempimenti nei rapporti contrattuali tra imprese di assicurazioni, intermediari e clientela in attuazione dell'art. 22, comma 15 bis, del decreto legge 18 ottobre 2012, n. 179, convertito nella legge 17 dicembre 2012, n. 221.

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 Produttore dei documenti.

Torna al sommario

3.2 Standard di riferimento

Di seguito sono riportati gli standard elencati nell'allegato 3 delle Regole Tecniche in materia di sistema di conservazione a cui l'attività di conservazione del Conservatore TeamSystem Service si riferisce:

ISO 14721:2012
OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;

ISO/IEC 27001:2013
Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);

ETSI TS 101 533-1 V1.3.1 (2012-04)
Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;

ETSI TR 101 533-2 V1.3.1 (2012-04)
Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;

UNI 11386:2010
Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;

ISO 15836:2009
Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core;

ISAD(G)
General International Standard Archival Description.

UNI ISO 15489-1: 2006
Informazione e documentazione - Gestione dei documenti di archivio -Principi generali sul record management.

UNI ISO 15489-2: 2007

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

Torna al sommario

4. RUOLI E RESPONSABILITÀ

Il sistema *Conservazione Cloud* descritto nel presente documento adotta ai sensi dell'Articolo 5 delle Regole Tecniche un modello organizzativo conforme al modello di riferimento Open Archival Information System (ISO 14721:2012), 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.

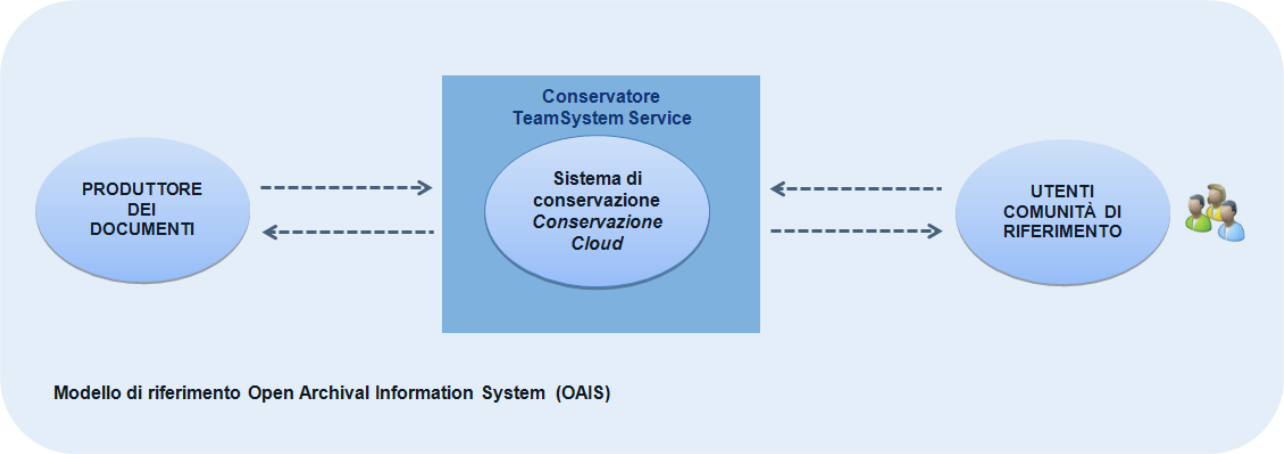

***Fig. 1** – Modello di riferimento organizzativo del sistema Conservazione Cloud*

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

- **Titolare dei documenti:** è il soggetto responsabile del contenuto dei documenti informatici oggetto del Servizio, della loro autenticità dell'origine, emissione/formazione ed è il soggetto obbligato per legge o regolamenti alla conservazione dei documenti stessi.
  Ad esempio in ambito tributario è il soggetto Titolare della contabilità.
  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 documenti:** 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.
  Può coincidere con il Titolare dei documenti ovvero può essere delegato ad un soggetto terzo.
  La corretta e certa individuazione del Produttore 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.

- **Responsabile della Conservazione:** è il soggetto responsabile dell'insieme delle attività, di cui all'articolo 7, comma 1, del D.P.C.M. 3 dicembre 2013.

Il Responsabile della Conservazione è una persona fisica che opera presso il Soggetto Produttore. Nelle Pubbliche Amministrazioni, il ruolo del Responsabile della Conservazione è svolto da un dirigente o da un funzionario formalmente designato.
Il Responsabile della Conservazione, di una Pubblica Amministrazione o anche di un Soggetto Privato, sotto la propria responsabilità ai sensi dell'art. 6, comma 6, del D.P.C.M. 3 dicembre 2013 affida il processo di conservazione al Conservatore accreditato AgID, e al suo Responsabile del Servizio di Conservazione.

- **Conservatore accreditato:** 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 all'articolo 7 delle Regole Tecniche attraverso una propria struttura organizzativa descritta nel seguito.
  Inoltre, il Conservatore esegue una normalizzazione dei Pacchetti di Input trasformandoli in Pacchetti di Versamento stardard UNI SInCRO 11386:2010 prima di sottoporli alla verifica di coerenza definitiva e quindi di generare il Rapporto di Versamento quale esito di acquisizione o rifiuto.

- **Utente:** è il soggetto autorizzato che richiede al sistema di conservazione di TeamSystem Service l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge.

- **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 Circolare AgID n. 65 del 10 aprile 2014.

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 "MANSIONARIO – FIGURE PROFESSIONALI PER LA CONSERVAZIONE" che mantiene aggiornato nel tempo e che è conforme al documento "Profili Professionali" emanato da AgID.

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 ed in particolare dai compiti previsti dall'art. 7 delle Regole Tecniche di cui al D.P.C.M. 3 dicembre 2013.

Nello specifico i ruoli e le responsabilità ricoperte nel modello organizzativo del Conservatore TeamSystem Service sono riportati nella tabella seguente:

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**	Delega per la gestione delle attività operative di configurazione, assistenza ed esercizio del processo di conservazione e per l'apposizione della firma digitale sull'indice dei Pacchetti di Archiviazione generati. I delegati con atto di nomina sono i seguenti: ▪ Rebecca Macchiagodena ▪ Rachele Cristofaro ▪ Andrea Cordeschi
Responsabile sicurezza dei sistemi per la conservazione	**Dino Del Sole - Contratto di tre anni rinnovabile** **----------** **Stefano Liguori - Contratto di tre anni rinnovabile**	▪ Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; ▪ Segnalazione delle eventuali difformità al Responsabile del Servizio di Conservazione e individuazione e pianificazione delle necessarie azioni correttive.	**Dal 02/03/2015 al 22/05/2018** **----------** **Dal 23/05/2018**	
Responsabile funzione archivistica di conservazione	**Ilaria Bruno - 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	**Dal 02/03/2015**	

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo	Eventuali deleghe
		integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; ▪ 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.		
Responsabile trattamento dati personali	**Fulvio Talucci** **Contratto di tre anni rinnovabile**	▪ Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; ▪ Garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.	**Dal 02/03/2015 fino al 04/10/2018**	
	Michele Di Rienzo **Contratto di tre anni rinnovabile**		**Dal 05/10/2018**	
Responsabile sistemi informativi per la conservazione	**Dino Del Sole** **Contratto di tre anni rinnovabile**	▪ Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione; ▪ Monitoraggio del mantenimento dei livelli di	**Dal 02/03/2015 al 22/05/2018**	

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo	Eventuali deleghe
	---------- **Stefano Liguori** **Contratto di tre anni rinnovabile**	servizio (SLA) concordati con l'Ente Produttore; ▪ Segnalazione delle eventuali difformità degli SLA al Responsabile del Servizio di Conservazione e individuazione e pianificazione delle necessarie azioni correttive; ▪ Pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione; ▪ Controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del Servizio di Conservazione	---------- **Dal 23/05/018**	
Responsabile sviluppo e manutenzione del sistema di conservazione	**Danilo Sgolastra** - **Contratto di tre anni rinnovabile** ---------- **Maurizio Corda** - **Contratto di tre anni rinnovabile**	▪ Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione; ▪ Pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione; ▪ Monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione; ▪ Interfaccia con l'Ente Produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche; ▪ Gestione dello sviluppo di siti web e portali connessi al Servizio di Conservazione.	**Dal 02/03/2015 al 30/06/2017** ---------- **Dal 01/07/2017**	

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 ed il 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.

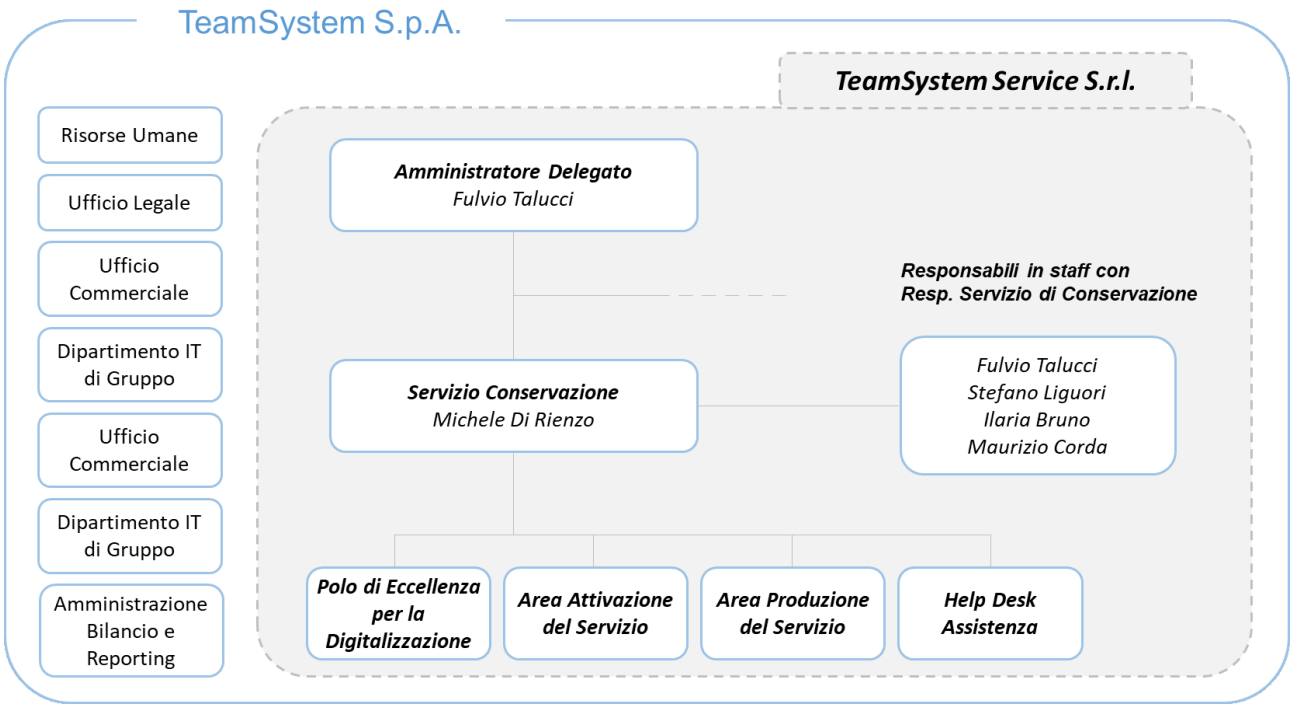

***Fig. 2** – Funzioni organizzative coinvolte nell'erogazione del Servizio*

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 e dei Responsabili della Sicurezza e del Trattamento dei dati. 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 SAL 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 o ai Partner.

- **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 (come ad esempio il censimento in anagrafica dei dati dei nuovi Clienti) e delle pratiche ad esse connesse.
  Inoltre, è l'area deputata allo svolgimento delle attività di configurazione dei profili del sistema di conservazione, delle verifiche e collaudo prima dell'avvio in produzione;

- **Area Produzione del Servizio**: costituito dagli operatori delegati che si occupano prevalentemente di esercire il processo di conservazione (produzione);

- **Area Help Desk / Assistenza**: costituito da operatori specializzati responsabili di assistere gli Utenti nell'utilizzo quotidiano del servizio. In particolare, tali operatori, oltre a svolgere le attività previste dal processo di conservazione, verificano che le operazioni automatiche utilizzate nell'ambito dell'erogazione del servizio (e.g., firma digitale, creazione Pacchetti di Archiviazione) si concludano senza anomalie. 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 – help desk agli utenti è attivo nei soli giorni lavorativi (esclusi sabato, domenica e festivi).

Le altre funzioni a supporto dell'erogazione del Servizio di Conservazione (e.g. Risorse Umane, Ufficio Legale) 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 "DC_MFP_00_Mansionario_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 intracompany di servizio per la fornitura e la gestione dei servizi ICT. Tale contratto regolamenta inoltre i livelli di servizio richiesti alla Capo Gruppo, attraverso la formalizzazione ed il monitoraggio di specifici SLA (o Service Level Agreement);

- **Software Factory:** responsabile dello sviluppo applicativo della piattaforma proprietaria *Conservazione Cloud* 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 *Conservazione Cloud*, anche in relazione agli eventuali adeguamenti normativi e tecnici e/o al miglioramento di specifiche funzionalità;

- **Qualità e Servizi Generali:** responsabile della realizzazione delle verifiche ispettive interne volte a valutare la conformità alle normative e agli standard di settore adottati a livello di Gruppo (e.g. ISO 9001, ISO 27001, normativa in materia di conservazione);

- **Amministrazione, Bilancio e Reporting:** responsabile di tutte le attività e i servizi amministrativi, contabili e finanziari dell'azienda.

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 Cliente può coincidere con il Titolare dei documenti (generalmente il caso di vendita diretta del Servizio) o può essere un Distributore del Servizio (caso della vendita indiretta) che ha l'obbligo di fornire tutti i dati relativi ai propri Clienti (Titolari e Produttori dei documenti) e ha l'obbligo di far accettare a quest'ultimi, tramite specifica modulistica, le condizioni generali di Servizio e le Specificità del Contratto (Scheda Servizio).

L'area di Attivazione del Servizio di TeamSystem Service prende in carico l'ordine di acquisto, ne verifica la correttezza ed in caso di esito positivo attiva la procedura di attivazione operativa del Servizio. Se è necessario un supporto consulenziale in merito all'esigenze espresse dal Cliente e ai contenuti della Scheda Servizio l'area Attivazione ingaggia il Polo di Eccellenza attraverso il sistema di Trouble Ticketing aziendale.

L'ordine di acquisito istanzia le attività operative di configurazione delle anagrafiche e dei profili di conservazione, delle tipologie documentali e dei metadati nel sistema di conservazione secondo quanto concordato nella Scheda Servizio e/o nell'ordine di acquisto, mentre il Cliente riceve tutti documenti contrattuali che deve ritornare debitamente sottoscritti per l'attivazione definitiva e la messa in produzione.

A supporto di tutte le attività relative all'attivazione del Servizio di Conservazione occorre produrre il contratto costituito da:

- Scheda per l'attivazione del Servizio di Conservazione (può coincidere anche con un ordine di acquisto cosiddetto coupon) condivisa ed accettata dal Conservatore e dal Produttore;
- Contratto per l'affidamento del Servizio di Conservazione al Conservatore TeamSystem Service (condizioni generali di Servizio);

- Affidamento del Responsabile della Conservazione interno al Produttore al Conservatore e al suo Responsabile del Servizio di Conservazione;

- Nomina del Conservatore in qualità di Responsabile del Trattamento Dati.

Solo se la documentazione ricevuta, verificata dall'area Attivazione, è completa viene messo in esercizio il Servizio per il determinato Produttore dei documenti. In caso di anomalie sulla contrattualistica, la comunicazione con il Cliente per la risoluzione delle anomalie è curata dall'area Assistenza / Help Desk tramite PEC.

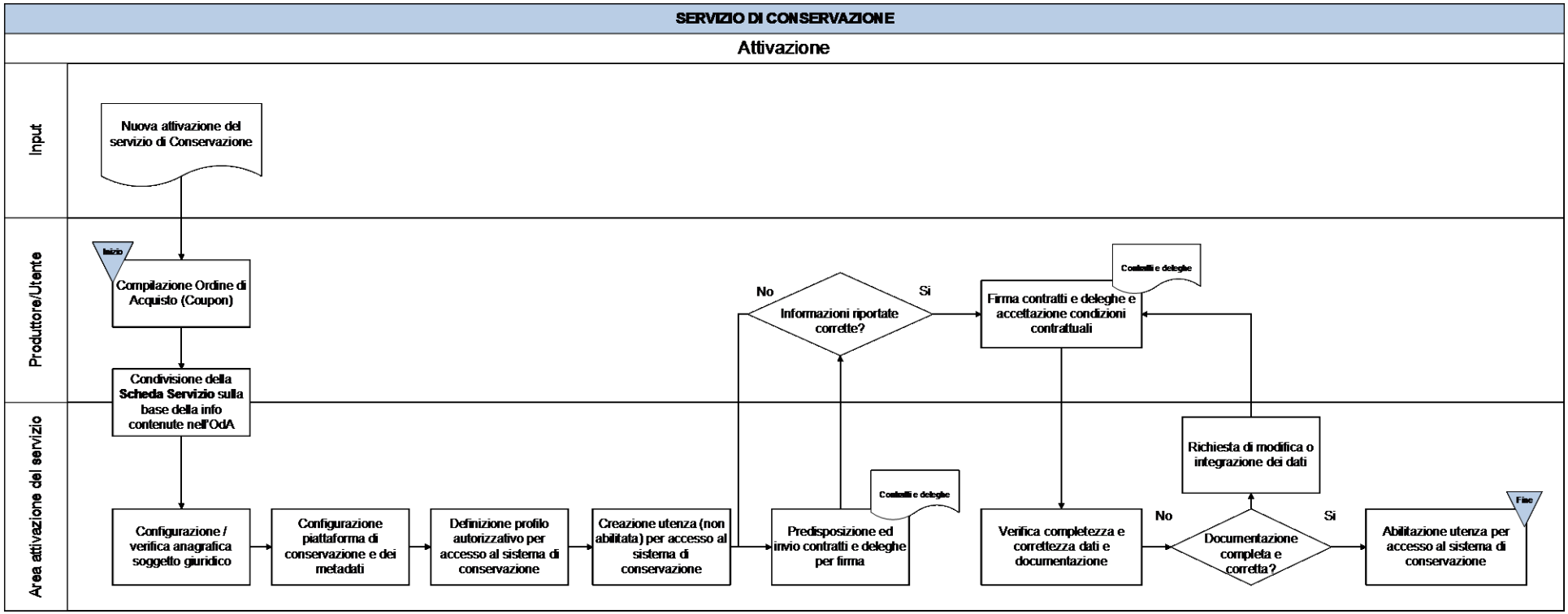

Fig. 4 *– Diagramma di flusso della fase di attivazione del Servizio*

Attraverso la predetta modulistica il Produttore dei documenti effettua la scelta della modalità di versamento con cui versare i documenti informatici al sistema di conservazione di TeamSystem Service in base alle modalità previste dal Servizio.

Inoltre, la modulistica contrattuale permette di definire tutte le tipologie documentali oggetto del processo di conservazione, corredate dei relativi metadati per la loro classificazione e la loro ricerca ed esibizione dei documenti conservati.

Tutte la fase di gestione del Cliente per l'attivazione del Servizio e la verifica della correttezza della documentazione condivisa e da quest'ultimo sottoscritta per l'adesione è in carico all'aree di Attivazione e Assistenza.

La fase di configurazione nel sistema si conclude con il collaudo del Servizio per quel determinato Produttore prima del rilascio in esercizio e prima della comunicazione attraverso il canale sicuro e riservato della PEC agli Utenti delle credenziali per l'accesso al Servizio.

Eseguito il collaudo, la messa in produzione del Servizio è sotto la supervisione interna del Responsabile del Servizio di Conservazione. Per l'esecuzione di tutte le predette attività operative Il Responsabile del Servizio si avvale di **Delegati,** operatori specialisti, con specifiche competenze professionali, a cui sono state delegate attività operative per l'esercizio del Servizio in oggetto.

La messa in produzione permette al Produttore dei Documenti di 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 all'articolo 9 delle Regole Tecniche di cui al D.P.C.M. 3 dicembre 2013 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 affidamento da parte del Responsabile della Conservazione che opera presso il Produttore. I principali compiti sono eseguiti dai delegati operativi, che attraverso gli strumenti ed i sistemi aziendali a supporto del Servizio, seguenti eseguono e presidiano le seguenti macro sotto-fasi:

- pre-verifica sui Pacchetti di Versamento di Input (PdI) ricevuti per la pre-acquisizione o scarto (generazione esito di presa in carico);
- normalizzazione dei Pacchetti di Versamento di Input (PdI) ricevuti e che hanno superato la pre-verifica al fine di trasformali in PdV standard UNI SInCRO 11386:2010;
- verifica sui PdV standard e generazione del Rapporto di Versamento (RdV) standard UNI SInCRO 11386:2010 quale esito delle verifiche di validità;
- generazione del Pacchetto di Archiviazione standard UNI SInCRO 11386:2010, firmato 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 11386:2010 su richiesta espressa dell'Utente;
- produzione di copie e duplicati su richiesta dell'Utente.

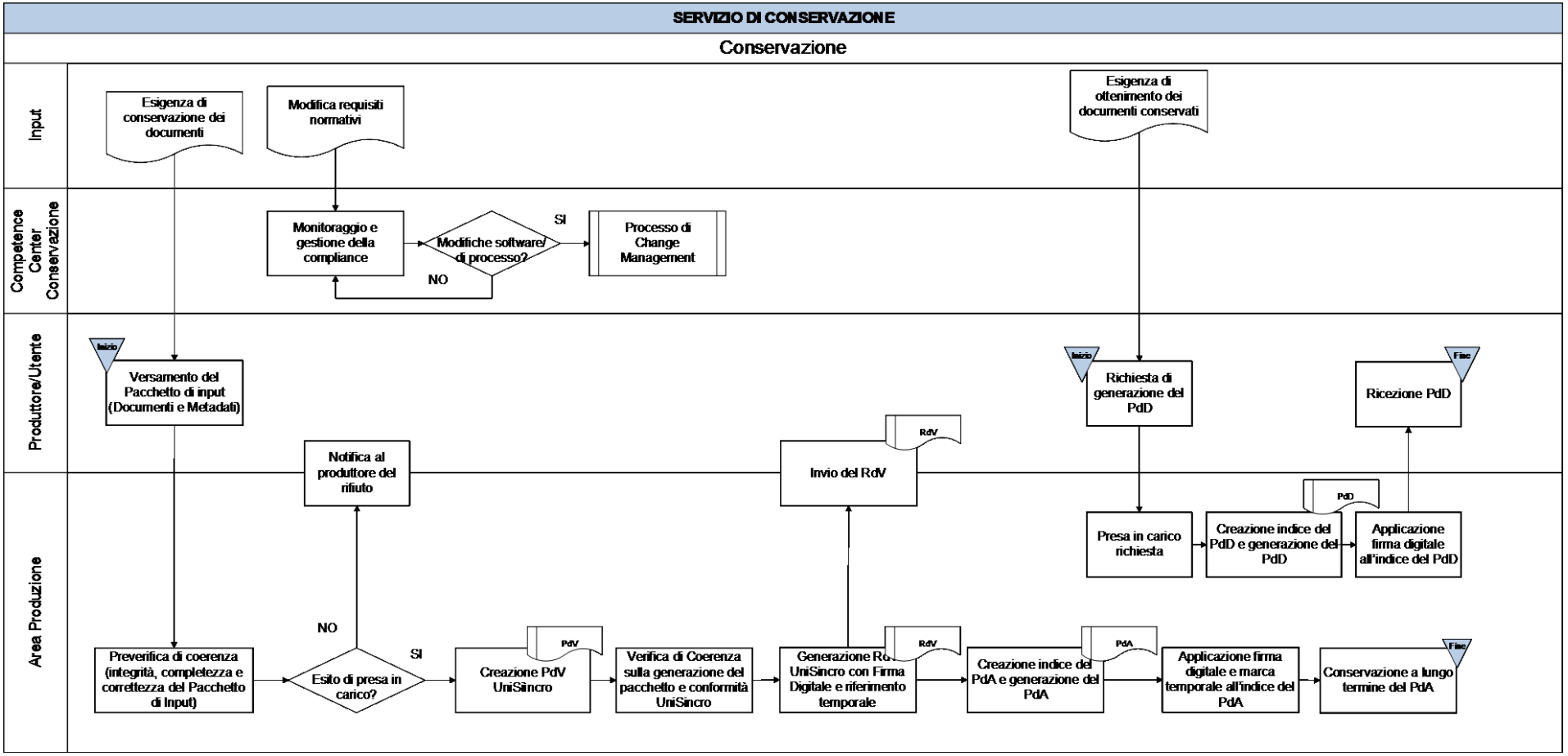

Fig. 5 *– Diagramma di flusso della fase di conservazione*

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, previsto contrattualmente con il Produttore dei documenti, dei Pacchetti di Archiviazione e degli oggetti digitali conservati a seconda dei casi (documenti informatici, documenti informatici amministrativi, fascicoli, registri e repertori informatici);
- 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.

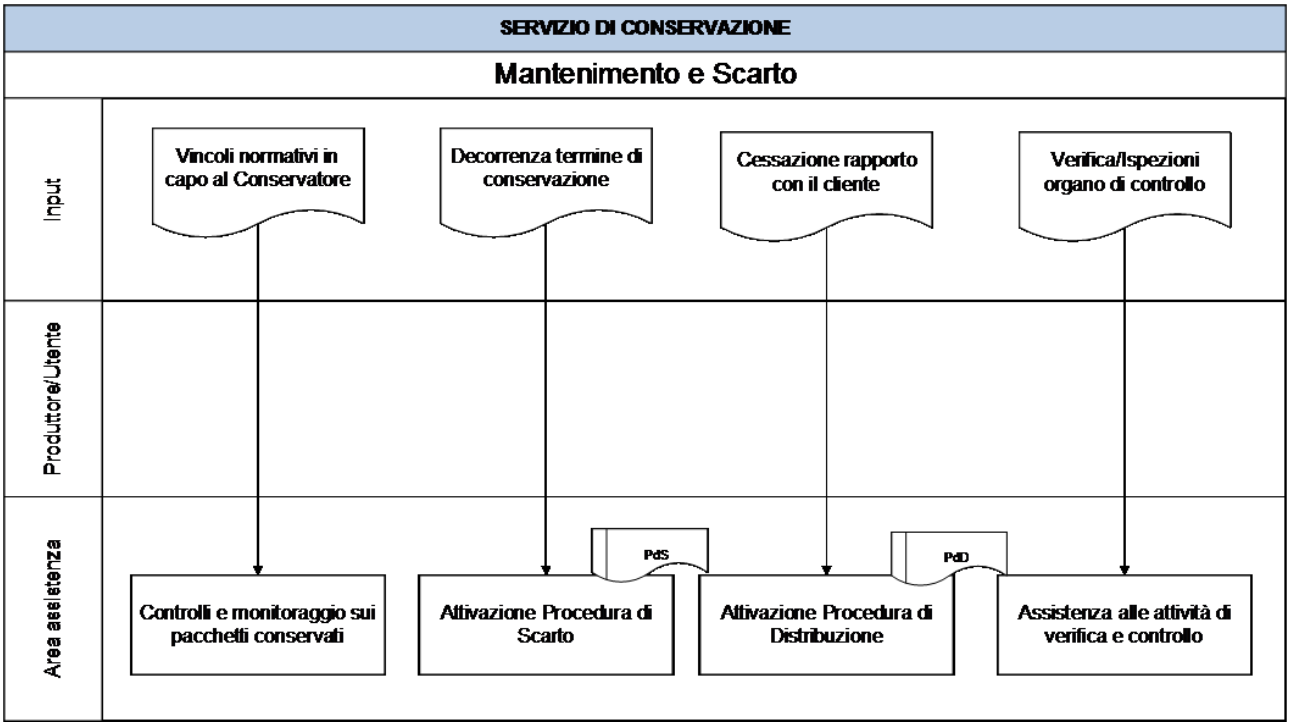

***Fig. 6** – Diagramma di flusso della fase di mantenimento e scarto*

Terminato il periodo di conservazione concordato contrattualmente, il Conservatore può provvedere allo **Scarto dei Pacchetti di Archiviazione** (tramite generazione dei Pacchetti di Scarto PdS), previa comunicazione informativa inviata al Produttore con un periodo di preavviso di **60 giorni**, per permettere a quest'ultimo eventualmente di richiedere un'estensione del Servizio di Conservazione oltre il periodo concordato.
Nel caso di archivi pubblici o privati, che rivestono interesse storico particolarmente importante, il Conservatore TeamSystem ed il Produttore dei documenti concordano preventivamente nella

Scheda Servizio che lo Scarto del Pacchetto di Archiviazione debba avvenire esclusivamente previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo rilasciata al Produttore secondo quanto previsto dalla normativa vigente in materia.

Infine, la fase di mantenimento e scarto si chiude al termine di validità del contratto o nei casi di disdetta o di recesso anticipato, con l'attivazione da parte di TeamSystem Service della **procedura di chiusura** del Servizio di Conservazione per quel determinato Produttore.

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 vari Responsabili indicati nei ruoli del Conservatore TeamSystem Service sono principalmente le seguenti:

- conduzione e manutenzione del sistema di conservazione a cura del Responsabile del Sistema Informativo;

- monitoraggio dei processi e dei sistemi dell'infrastruttura a cura del Responsabile del Sistema Informativo;

- gestione del *Change Management* a cura del Responsabile della Manutenzione e dello Sviluppo del Sistema di Conservazione secondo quanto già previsto dalla certificazione ISO IEC 27001:2013.
  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 "*PR_CHM_00_Procedura Operativa 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 i vari Responsabili e delle 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.

In ultimo, la documentazione relativa al Servizio CCT 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 *Conservazione Cloud* 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 11386:2010 per tutti gli Indici XML dei pacchetti informativi PdV, PdA, PdD ed anche per il Rapporto di Versamento (RdV) e l'Indice del Pacchetto di Scarto (IPdS) 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.);
- **documenti informatici amministrativi**;
- **fascicoli informatici o aggregazioni documentali informatiche** (che a loro volta contengono oggetti quali le unità documentarie);
- **repertori informatici** registri informatici cronologici che raccolgono i dati registrati direttamente dalle procedure informatiche con cui si formano altri atti e documenti o indici di atti e documenti.

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.

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 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.

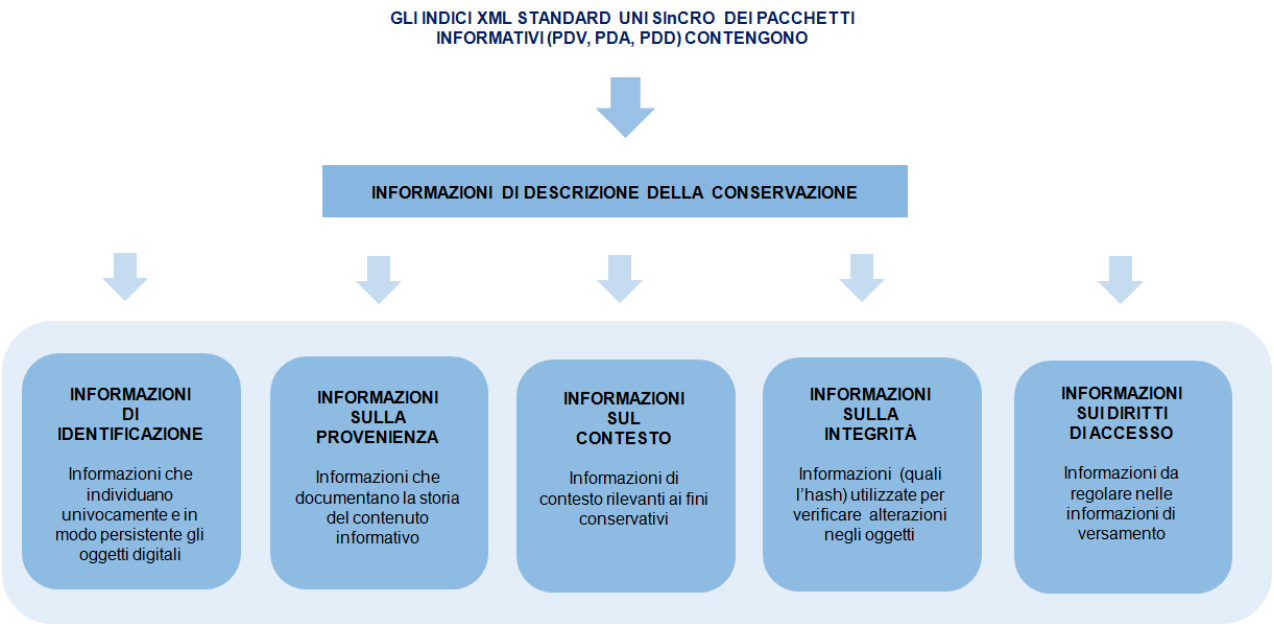

Fig. 7** – Informazioni descrittive della conservazione correlati agli oggetti sottoposti a **conservazione

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**, 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;
- definizione dei requisiti in merito alla formazione dei documenti versati ossia ad esempio se il Produttore versa documenti già firmati digitalmente e/o con firma elettronica avanzata e/o con firma elettronica, con riferimento temporale o eventualmente

marcati temporalmente; l'analisi è utile al Produttore anche per verificare la conformità alle regole tecniche in materia di documento informatico di cui al D.P.C.M. 13 novembre 2013;

- necessità del Produttore di gestire i fascicoli informatici o altre strutture di aggregazione documentale;
- periodo di conservazione concordato (valore definito in anni nell'Indice del PdV);
- metadati associati agli oggetti. Vengono definiti i metadati minimi obbligatori in conformità alle Regole tecniche di cui al D.P.C.M. 3 dicembre 2013 e quelli aggiuntivi facoltativi da valorizzare nell'IPdV in modo da associare delle chiavi ai documenti informatici ovvero ai documenti informatici amministrativi ovvero ai fascicoli informatici a seconda dei casi richiesti;
- soggetti coinvolti nel processo (titolare dei documenti, produttore dei documenti;
- Responsabile della Conservazione (RdC, delegati del RdC, ecc.) inseriti nel blocco informativo "Process" e poi nel sottonodo "Agent" dell'Indice XML dei vari pacchetti;
- 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 e fascicoli

La normativa di riferimento dispone di associare dei metadati agli oggetti sottoposti al processo di conservazione, in modo da identificarli univocamente, di classificarli e permettere la gestione di eventuali fascicoli informatici ovvero aggregazioni documentali.

Quindi il Conservatore TeamSystem Service ed il Produttore definiscono la classificazione logica delle tipologie documentali secondo uno schema articolato in campi individuati attraverso specifici metadati.

Nel presente Manuale è riportato **l'insieme minimo di metadati** del documento informatico, del documento informatico amministrativo o del fascicolo informatico ovvero un set di metadati, la cui struttura è descritta nell'Allegato 5 delle Regole Tecniche, da associare all'oggetto dati per identificarne provenienza e natura e per garantirne la tenuta.

Il Titolare ed il Produttore dei documenti devono soddisfare i requisiti legislativi in merito alla corretta valorizzazione dei metadati minimi obbligatori, riportati nel presente Manuale.

Ulteriori metadati aggiuntivi, richiesti dalla normativa in virtù della diversa natura delle tipologie documentali o richiesti dal Produttore dei documenti 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 D.M. 17 giugno 2014.

Torna al sommario

6.2.1 Metadati minimi del documento informatico

Metadato Minimo	*Descrizione del Metadato*
Identificativo (Id) del documento	Identificativo univoco e persistente del documento, è una sequenza di caratteri alfanumerici associata in modo univoco e permanente al documento informatico in modo da consentirne l'identificazione. Lo standard Dublin Core raccomanda di identificare il documento per mezzo di una sequenza di caratteri alfabetici o numerici secondo un sistema di identificazione formalmente definito
Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immodificabile. Il Conservatore valorizza questo metadato con la data in cui viene generato il Pacchetto di Archiviazione
Oggetto	Descrive o riassume brevemente il contenuto del documento o chiarendone la natura. Dublin Core prevede l'analoga proprietà "Description"
Denominazione del Soggetto Produttore	La denominazione del Soggetto che ha l'autorità e la competenza a produrre il documento informatico (Cognome e Nome ovvero Ragione Sociale)
Codice Fiscale del Soggetto Produttore	Codice Fiscale del Soggetto Produttore
Denominazione del Soggetto Destinatario	Il Soggetto che ha l'autorità e la competenza a ricevere il documento informatico
Codice Fiscale del Soggetto Destinatario	Codice Fiscale del Soggetto Destinatario

Torna al sommario

6.2.2 Metadati minimi del documento informatico amministrativo

Oltre a garantire i metadati precedenti, in caso di documento amministrativo informatico l'insieme minimo dei metadati si estende anche ai seguenti metadati:

Metadato minimo	*Descrizione del metadato*
Identificativo Amministrazione	Identificativo univoco dell'Amministrazione. Utilizzare l'identificativo dell'Amministrazione presente sul sito dell'Indice delle Pubbliche Amministrazioni (IPA)
Codice Identificativo AOO	Codice identificativo dell'Area Organizzativa Omogenea dell'amministrazione presente sull'IPA
Data Protocollo	La data di protocollo registrata in forma non modificabile automaticamente dalla procedura informatica di registrazione e segnatura di protocollo
Progressivo Protocollo	Il numero progressivo di protocollo registrato in forma non modificabile automaticamente dalla procedura informatica di registrazione e segnatura di protocollo
Mittente	Soggetto mittente del documento amministrativo informatico
Destinatario	Soggetto destinatario del documento amministrativo informatico

Torna al sommario

6.2.3 Fascicoli informatici

Ci sono casi in cui è necessario aggregare con una struttura logica ed univocamente identificata atti, documenti o dati informatici in fascicoli informatici o aggregazioni documentali informatiche, in quanto funzionali al mantenimento del legame tra gli oggetti conservati durante o dopo la chiusura di una specifica attività o di una specifica pratica o di un specifico procedimento.

In particolare, le pubbliche amministrazioni hanno l'obbligo di descrivere e mantenere le relazioni tra documenti, fascicoli e procedimenti anche nel sistema di conservazione.

Operativamente, quindi, le Pubbliche Amministrazioni titolari del procedimento raccolgono in un fascicolo informatico gli atti, i documenti e i dati del procedimento medesimo da chiunque formati.

Il sistema di conservazione di TeamSystem Service permette la gestione e l'organizzazione dei fascicoli informatici sia per Enti Pubblici che Privati, tuttavia il Servizio richiede che il Titolare e il Produttore dei documenti richiedano espressamente la gestione della fascicolazione concordando con il Conservatore l'eventuale analisi, tempi e modi di attuazione, indicati nel Disciplinare Specificità del Contratto, condiviso tra le parti.

Per organizzare l'archivio e permettere al Titolare e Produttore dei documenti di gestire il mantenimento della descrizione archivistica anche nel sistema di conservazione in coerenza con il sistema di gestione dei flussi documentali e con il Piano di Classificazione (o Titolario) della pubblica amministrazione, viene messo a disposizione dell'ente Produttore versante la possibilità di dichiarare l'apertura e la chiusura del fascicolo e poi è definito un metadato denominato "Indice di

Classificazione" in cui è possibile dichiarare il Titolo, la Classe, la Sottoclasse, la Categoria e la Sottocategoria di un determinato oggetto digitale, così come definito nel Piano di Classificazione.

Inoltre, il Conservatore TeamSystem Service adotta lo standard internazionale di descrizione archivistica **ISAD(G)** - *General International Standard Archival Description.*

Lo standard ISAD(G), essendo uno modello astratto generale, permette di mettere a disposizione nel modello-dati del Conservatore un set di elementi informativi per garantire il mantenimento della relazione dell'oggetto digitale con i livelli "alti" (**fondo, subfondo, serie, sottoserie**) attraverso l'aggiunta di specifici elementi nella struttura degli Indici dei Pacchetti per i fascicoli.

Lo standard predetto si basa sul principio che la descrizione archivistica procede **dal generale al particolare secondo un descrizione in più livelli**.

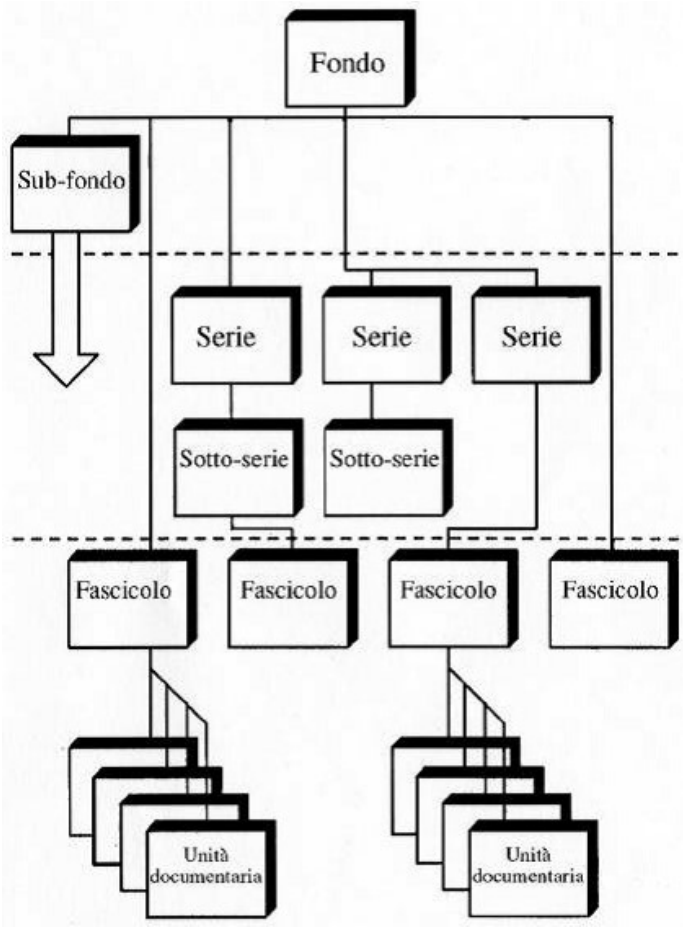

***Fig. 8** – Modello gerarchico in livelli di descrizione archivistica secondo ISAD (G)*

Il Conservatore TeamSystem Service, pertanto, mette a disposizione del Titolare e Produttore dei documenti un **modello gerarchico dei livelli** di ordinamento di un fondo e delle parti che lo compongono, partendo da una descrizione per il **livello fondo**, una per il **livello serie**, una per il

livello fascicolo e/o una per il **livello unità documentaria**. Sono, anche, prevedibili livelli intermedi di descrizione, come sub-fondi, o sub-serie.

Per i livelli "più bassi" (**unità archivistica** quale ad esempio il fascicolo, l'**unità documentaria** quale ad esempio il documento informatico) si applicano per le relazioni descrittive le Regole Tecniche di cui al D.P.C.M. 3 dicembre 2013; in particolare si adottano i metadati minimi previsti per i fascicoli informatici nell'Allegato 5 delle Regole Tecniche e si generano gli Indici del Pacchetto di Versamento, di Archiviazione e di Distribuzione con una struttura dati che contiene anche la gestione dei fascicoli e le relazioni a fondo, sub-fondo, serie, sub-serie.

Torna al sommario

6.2.4 Metadati minimi del fascicolo informatico o aggregazione documentale

Metadato minimo	*Descrizione del metadato*
Identificativo (Id) del fascicolo	Identificativo univoco e persistente del fascicolo previsto dall'articolo 41 del CAD, è una sequenza di caratteri alfanumerici associata in modo univoco e permanente al documento informatico in modo da consentirne l'identificazione. Lo standard Dublin Core raccomanda di identificare il documento per mezzo di una sequenza di caratteri alfabetici o numerici secondo un sistema di identificazione formalmente definito.
Amministrazione Titolare	Amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo. Valorizzare con Codice IPA dell'Amministrazione.
Amministrazioni partecipanti	Amministrazioni che partecipano all'iter del procedimento.
Denominazione Responsabile del procedimento	Cognome e Nome del Responsabile del procedimento.
Codice Fiscale Responsabile del procedimento	Codice Fiscale del Responsabile del procedimento.
Oggetto	Descrive o riassume brevemente il contenuto del fascicolo.
Identificativi dei documenti	Elenco degli identificativi dei documenti contenuti nel fascicolo che ne consentono la reperibilità.

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 Regole Tecniche in materia di sistema di conservazione, al fine di assicurare una corretta gestione degli oggetti conservati, indica i formati idonei che garantiscono le seguenti caratteristiche:

- apertura;
- sicurezza;
- portabilità;
- funzionalità;
- supporto allo sviluppo;
- diffusione.

Di seguito sono riportati i formati idonei alla conservazione che accetta il sistema di conservazione di TeamSystem Service e possono quindi essere utilizzati dal Produttore dei documenti per il versamento al sistema predetto.

Formato del file	*Estensione*	*Tipo Mime*	*Standard*	*Formato Aperto*	*Visualizzatore*
PDF	.pdf	application/pdf	ISO32000-1	SÌ	Adobe Reader
PDF/A	.pdf	application/pdf	ISO 19005-1:2005 (vers. PDF 1.4) ISO 19005-2:2011 (vers. PDF 1.7)	SÌ	Adobe Reader http://www.pdfa.org/doku.php
XML	.xml	application/xml text/xml		SÌ	Web Browser
TXT	.txt			SÌ	Web Browser
TIFF	.tif	image/tiff	-	SÌ	Vari visualizzatori di immagini

JPG	.jpg, .jpeg	image/jpeg	ISO/IEC 10918:1	SÌ	Vari visualizzatori di immagini
EML	.eml		RFC2822	SÌ	Client di posta elettronica supportano la visualizzazione di file eml

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

Torna al sommario

6.4 Pacchetto di Versamento

Il PdV nel formato XML standard UNI SInCRO 11386:2010 che riceve il Sistema di Conservazione di TeamSystem Service trae origine dal Pacchetto di Input (PdI), un Pacchetto che il Produttore dei Documenti 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.

Si precisa che nel caso di documenti informatici nel formato strutturato XML i metadati possono essere già contenuti nel file strutturato che il Conservatore TeamSystem Service estrae per valorizzare i relativi campi "Metadata" presenti negli Indici del Pacchetti.

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 attestato con un Esito di Presa in Carico, viene generato il **Pacchetto di Versamento standard UNI SInCRO 11386:2010**, nel seguito **PdV UNI-SInCRO**.

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

- **Oggetti Dati** (documenti informatici, documenti informatici amministrativi, fascicoli informatici, repertori informatici);

- **Indice del Pacchetto di Versamento (IPdV)** nel formato XML generato secondo un modello-dati conforme allo standard UNI SInCRO 11386:2010 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 PdV UNI-SInCRO accettato dal sistema di TeamSystem Service contiene le seguenti principali informazioni nel suo Vocabolario.

Struttura dell'Indice del Pacchetto di Versamento		
Nome Nodo	***Nome Elemento***	***Descrizione***
SelfDescription		Informazioni relative all'Indice di Versamento
	ID	Identificativo dell'Indice del Pacchetto di Versamento
SelfDescription /CreatingApplication		Informazioni sull'applicazione software che ha generato l'IPdV
	Name	Nome dell'applicazione software che ha generato l'IPdV
	Producer	Nome del Produttore dell'applicazione software che ha generato l'IPdV (soggetto che sviluppa l'applicativo)
	Version	Versione dell'applicazione che ha generato l'IPdV
VdC		Informazioni Relative al Pacchetto di Versamento
	ID	Identificativo del Pacchetto di Versamento
Vdc /VdcGroup		Informazioni applicative del Pacchetto di Versamento
	Label	Etichetta (codice) dell'oggetto PdV
	ID	Identificativo applicativo del PdV
	Description	Descrizione del PdV
FileGroup		Informazioni di uno o più raggruppamenti dei file contenuti nel Pacchetto di Versamento
	Label	Identificativo della natura del documento
FileGroup /File		Informazioni relative al file oggetto del versamento
	ID	Identificatore del documento
	Path	Nome del file oggetto del versamento
	Hash	Impronta calcolata secondo la funzione hash SHA-256

FileGroup /File /Moreinfo		Contiene Informazioni ulteriori relative al file e l'oggetto di versamento. Vedi tabella MoreInfo.DocInfo e MoreInfo.ObjectInfo
Process		Informazioni sul processo di generazione del Pacchetto di Versamento
	LawAndRegulation	Informazioni sulle norme e regolamenti che guidano il processo di generazione del PdV
Process /Agent		Informazione dei soggetti che intervengono nel processo (responsabile della conservazione, produttore dei documenti, titolare dei documenti)
	Agent_ID	Identificativo del Soggetto (PartitaIVA se organizzazione o Codice Fiscale se persona fisica)
Process /Agent /AgentName		Informazioni sul nome del Soggetto
	FormalName	Nome dell'organizzazione
Process /Agent /AgentName /NameAndSurname		Informazioni sul nome di un'eventuale persona fisica
	Name	Nome della persona fisica
	Surname	Cognome della persona fisica
Process /Agent /Moreinfo		Contiene Informazioni ulteriori relative al file di versamento. Vedi tabella MoreInfo.AgentInfo
Process /TimeReference		Informazioni relative al Riferimento Temporale
	AttachedTimeStamp	Data/ora di generazione dell'Indice di Versamento con riferimento al Tempo Universale Coordinato (UTC).

La struttura delle informazioni aggiuntive **MoreInfo**, utilizzano lo schema XML di validazione CustomMetadata.xsd.

Tutte le informazioni, sono strutturate in custom Item, sottostanti uno dei raggruppamenti "DocInfo", "ObjectInfo", "AgentInfo".

Gli attributi dei custom Item sono i seguenti:

label Nome del EmbeddedData
Type Tipo di dato
Size eventuale lunghezza massima del dato

Definizione degli Item MoreInfo			
Raggrupp.	***label***	***Type/Size***	***Descrizione***
DocInfo			Informazioni aggiuntive relative al file di versamento
	IdObject	xs:Int	Identificativo applicativo del file versato
	IdDoc	xs:Int	Progressivo del file versato
	NomeFile	xs:string 200	Nome del file
	MimeType	xs:string 200	Indica il tipo di formato del file. Vedi tabella precedente al paragrafo 6.3
	UserName dell'ente produttore	xs:string 20	Nome utente applicativo che ha versato il PdI
ObjectInfo			Informazioni aggiuntive relative all'oggetto di versamento
	Oggetto	xs:string 200	Tipo documento versato
	TitolareDocumenti_IdPaese	xs:string 2	Identificativo Paese del Titolare del Documento
	TitolareDocumenti_PartitaIVA	xs:string 11	Partita IVA del Titolare del Documento
	TitolareDocumenti_CodiceFiscale	xs:string 16	Codice Fiscale del Titolare del Documento
	TitolareDocumenti_Denominazione	xs:string 200	Denominazione del Titolare del Documento
	DestinatarioDocumenti_IdPaese	xs:string 2	Identificativo Paese del Destinatario del Documento
	DestinatarioDocumenti_PartitaIVA	xs:string 11	Partita IVA del Destinatario del Documento
	DestinatarioDocumenti_CodiceFiscale	xs:string 16	Codice Fiscale del Destinatario del Documento
	DestinatarioDocumenti_Denominazione	xs:string 200	Denominazione del Destinatario del Documento
	Esercizio	xs:int	Anno dell'esercizio di competenza del Documento (periodo di riferimento)
	DataEmissione	xs:dateTime	Data del Documento
	NumeroDocumento	xs:string 200	Sezionale/numero Documento
	DataInizio	xs:dateTime	Data iniziale del periodo di riferimento del Documento

	DataFine	xs:dateTime	Data finale del periodo di riferimento del Documento
	NumeroAnniConservazione	Xs:int	Numero anni di conservazione (periodo di conservazione concordato)
	Etichetta di altri possibili metadati		Aggiunta di altri possibili metadati legati alla natura della tipologia di documenti. Far riferimento alle Specificità del Contratto.
AgentInfo			Informazioni aggiuntive relative al soggetto che interviene nel processo di versamento
	Qualifica	xs:string 200	Qualifica del soggetto: - Produttore dei Documenti - Titolare dei Documenti - ……

La struttura-dati del IPdV UNI-SInCRO dettagliata ed ulteriori specifiche ed informazioni di dettaglio in merito al Pacchetto di Versamento per un determinato Produttore dei documenti sono riportate nel Disciplinare Specificità del Contratto, parte integrante e sostanziale del Manuale. In particolare, il blocco informativo "ObjectInfo" riportato nel presente Manuale è solo un esempio pratico in cui i metadati (indici) sono relativi ad una specifica tipologia documentale. In generale, il Produttore dei documenti, il Responsabile della Conservazione ed il Conservatore definiscono i metadati del blocco "ObjectInfo" nel Disciplinare Specificità del Contratto, a seconda della natura della tipologia documentale.

Nel caso di Pacchetto di Versamento relativo al fascicolo informatico le specifiche di dettaglio e la definizione della struttura-dati del file Indice del Pacchetto di Versamento (IPdV-F), da dichiarare nella sessione di versamento, è riportata nel Disciplinare Specificità del Contratto.

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 dall'art. 9 delle Regole Tecniche.

Nel processo TeamSystem Service viene generato un RdV in corrispondenza di un unico PdV.
In conformità con lo standard ISO 14721:2012 (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 11386:2010 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 11386:2010 con una struttura dati similare all'IPdV.

Il suo Vocabolario e gli elementi della struttura dati sono, pertanto, similari 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 ovvero dei Delegati del Conservatore TeamSystem Service prima di metterlo nella disponibilità del Produttore dei documenti. Per tal motivo nell'elemento Agent della struttura dati, tra i soggetti che prendono parte al processo di conservazione, sono stati inseriti anche i Delegati del Conservatore che hanno ricevuto una nomina a tale scopo e che possono firmare digitalmente il RdV.

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>.

In ottemperanza al D.P.C.M. 13 novembre 2014, 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 documenti in quanto se il sistema non produce un RdV con esito positivo ciò significa che gli oggetti dati contenuti nel PdI 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 per un determinato Produttore dei Documenti sono riportate nel Disciplinare Specificità del Contratto. Anche nel caso di gestione dei fascicoli informatici la struttura-dati del RdV-F è riportata 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 11386:2010, è una trasformazione di uno o più Pacchetti di Versamento.
Il suo vocabolario e gli elementi della struttura dati sono, pertanto, similari 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 ovvero dei Delegati del Conservatore ed una marca temporale (data certa elettronica o validazione temporale).

Per tal motivo nell'elemento Agent della struttura dati, tra i soggetti che prendono parte al processo di conservazione, vengono dichiarati anche i Delegati del Conservatore, soggetti persone fisiche, che hanno ricevuto una nomina a tale scopo e che possono firmare digitalmente l'IPdA.

```
<?xml version="1.0" encoding="utf-8"?>
<sincro:IdC xmlns:sincro="http://www.uni.com/U3011/sincro/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.uni.com/U3011/sincro/IdC.xsd" sincro:version="1.0"
sincro:url="http://www.uni.com/U3011/sincro/">
  <sincro:SelfDescription>
    <sincro:ID>IdC_254121</sincro:ID>
    <sincro:CreatingApplication>
      <sincro:Name>Conservazione Cloud TeamSystem Service</sincro:Name>
      <sincro:Version>1.0.0</sincro:Version>
      <sincro:Producer>TeamSystem S.p.a.</sincro:Producer>
    </sincro:CreatingApplication>
  </sincro:SelfDescription>
  <sincro:VdC>
    <sincro:ID>VdC_254121</sincro:ID>
    <sincro:VdCGroup>
      <sincro:Label>PdA</sincro:Label>
      <sincro:ID>PdA_254121</sincro:ID>
      <sincro:Description>Pacchetto di Archiviazione</sincro:Description>
    </sincro:VdCGroup>
  </sincro:VdC>
  <sincro:FileGroup>
      <sincro:Label>PdV - Pacchetto di Versamento</sincro:Label>
      <sincro:File sincro:format="application/octet-stream">
          <sincro:ID>PdI_253844</sincro:ID>
          <sincro:Path>ITXXXXXXXXXXXXXXXX_0002K.xml.p7m</sincro:Path>
          <sincro:Hash sincro:function="SHA-
256">F3EBEC7936F438BCAAF183AA78EFB030A34D5555D59C35D2E588CE7EF5781B1E</sincro:Hash>
          <sincro:MoreInfo sincro:XMLScheme="FileCustomMetadata.xsd">
          <sincro:EmbeddedMetadata>
          <CustomMetadata>
          <DocInfo>
              <Item label="IdObject" type="xs:int">253844</Item>
              <Item label="IdDoc" type="xs:int">1</Item>
              <Item label="NomeFile" type="xs:string"
size="200">ITXXXXXXXXXXXXXXXX_0002K.xml.p7m</Item>
              <Item label="Description" type="xs:string" size="200">Pacchetto di Versamento
di Input</Item>
          </DocInfo>
          <ObjectInfo>
              <Item label="Oggetto" type="xs:string" size="200">(1001) - FatturaPA
emessa</Item>
              <Item label="NumeroAnniConservazione" type="xs:int">10</Item>
              <Item label="username dell'ente produttore" type="xs:string" size="20">sqa-
010606</Item>
              <Item label="DataChiusura" type="xs:datetime">2015-07-01T09:55:26.410</Item>
              <Item label="DataEmissione" type="xs:datetime">2014-12-22T00:00:00.000</Item>
              <Item label="NumeroDocumento" type="xs:string" size="200">1E</Item>
              <Item label="Sezionale" type="xs:string" size="200"></Item>
              <Item label="Esercizio" type="xs:int">2014</Item>
              <Item label="CodiceDestinatarioIPA" type="xs:string" size="200">XXXXXX</Item>
              <Item label="IdentificativoSDI" type="xs:string"
size="200">.....</Item>
              <Item label="DestinatarioDocumenti_IdPaese" type="xs:string"
size="2">IT</Item>
              <Item label="DestinatarioDocumenti_PartitaIVA" type="xs:string"
size="11">.....</Item>
```

```
                <Item label="DestinatarioDocumenti_CodiceFiscale" type="xs:string"
size="16">............</Item>
                <Item label="DestinatarioDocumenti_Denominazione" type="xs:string"
size="200">XXXXXXXXXXXXXXXXXXXXXXXXX</Item>
                <Item label="DestinatarioDocumenti_Cognome" type="xs:string"
size="200">XXXXXXXXXXXXXXXXXXXXXXXXX</Item>
                <Item label="DestinatarioDocumenti_Nome" type="xs:string"
size="200">XXXXXXXXXXXXXXXXXXXXXXXXX</Item>
                <Item label="NomeFileOriginale" type="xs:string"
size="200">ITXXXXXXXXXXXXXXX_0002K</Item>
            </ObjectInfo>
            </CustomMetadata>
            </sincro:EmbeddedMetadata>
            </sincro:MoreInfo>
        </sincro:File>
        <sincro:File sincro:format="application/octet-stream">
            <sincro:ID>PdI_253845</sincro:ID>
            <sincro:Path>ITXXXXXXXXXXXXXXX_0002J.xml.p7m</sincro:Path>
            <sincro:Hash sincro:function="SHA-
256">06B87B05B262BC5048335F22F7AEEE42336645CE4485379D54C4E845955D1282</sincro:Hash>
            <sincro:MoreInfo sincro:XMLScheme="FileCustomMetadata.xsd">
            <sincro:EmbeddedMetadata>
            <CustomMetadata>
            <DocInfo>
                <Item label="IdObject" type="xs:int">253845</Item>
                <Item label="IdDoc" type="xs:int">1</Item>
                <Item label="NomeFile" type="xs:string"
size="200">ITXXXXXXXXXXXXXXX_0002J.xml.p7m</Item>
                <Item label="Description" type="xs:string" size="200">Pacchetto di Versamento
di Input</Item>
            </DocInfo>
            <ObjectInfo>
                <Item label="Oggetto" type="xs:string" size="200">(1001) - FatturaPA
emessa</Item>
                <Item label="NumeroAnniConservazione" type="xs:int">10</Item>
                <Item label="username dell'ente produttore" type="xs:string" size="20">sqa-
010606</Item>
                <Item label="DataChiusura" type="xs:datetime">2015-07-01T09:55:26.410</Item>
                <Item label="DataEmissione" type="xs:datetime">2014-12-22T00:00:00.000</Item>
                <Item label="NumeroDocumento" type="xs:string" size="200">2E</Item>
                <Item label="Sezionale" type="xs:string" size="200"></Item>
                <Item label="Esercizio" type="xs:int">2014</Item>
                <Item label="CodiceDestinatarioIPA" type="xs:string" size="200">XXXXXX</Item>
                <Item label="IdentificativoSDI" type="xs:string"
size="200">............</Item>
                <Item label="DestinatarioDocumenti_IdPaese" type="xs:string"
size="2">IT</Item>
                <Item label="DestinatarioDocumenti_PartitaIVA" type="xs:string"
size="11">............</Item>
                <Item label="DestinatarioDocumenti_CodiceFiscale" type="xs:string"
size="16">............</Item>
                <Item label="DestinatarioDocumenti_Denominazione" type="xs:string"
size="200">XXXXXXXXXXXXXXXXXXXXXXXXX</Item>
                <Item label="DestinatarioDocumenti_Cognome" type="xs:string"
size="200">XXXXXXXXXXXXXXXXXXXXXXXXX</Item>
                <Item label="DestinatarioDocumenti_Nome" type="xs:string"
size="200">XXXXXXXXXXXXXXXXXXXXXXXXX</Item>
```

```
            <Item label="NomeFileOriginale" type="xs:string"
size="200">ITXXXXXXXXXXXXXXX_0002J</Item>
          </ObjectInfo>
          </CustomMetadata>
          </sincro:EmbeddedMetadata>
          </sincro:MoreInfo>
      </sincro:File>
      <sincro:MoreInfo sincro:XMLScheme="FileGroupCustomMetadata.xsd">
          <sincro:EmbeddedMetadata>
          <CustomMetadata>
              <Item label="IdObject" type="xs:string" size="200">253887</Item>
              <Item label="IdDoc" type="xs:string" size="200">1</Item>
              <Item label="NomeFile" type="xs:string" size="200">IPdV.xml</Item>
              <Item label="HashType" type="xs:string" size="20">SHA-256</Item>
              <Item label="HashValue" type="xs:string"
size="200">F7BB17530D15C690AB9041BCD8A6FC0CE778963F16D98583D6CFC0A4B296461A</Item>
              <Item label="IdDocRapporto" type="xs:string" size="200">3</Item>
              <Item label="NomeFileRapporto" type="xs:string" size="200">RdV.xml.p7m</Item>
              <Item label="HashTypeRapporto" type="xs:string" size="20">SHA-256</Item>
              <Item label="HashValueRapporto" type="xs:string"
size="200">6BA59BBD65800AC1D1792303B08B7769DB5DD2C5C48038167A40D63C1659D040</Item>
              <Item label="UserName dell'ente produttore" type="xs:string" size="20">sqa-
010606</Item>
              <Item label="TitolareDocumenti_IdPaese" type="xs:string" size="2">IT</Item>
              <Item label="TitolareDocumenti_PartitaIVA" type="xs:string"
size="11">.....</Item>
              <Item label="TitolareDocumenti_CodiceFiscale" type="xs:string"
size="16">.....</Item>
              <Item label="TitolareDocumenti_Denominazione" type="xs:string"
size="200">XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX</Item>
              <Item label="TitolareDocumenti_Cognome" type="xs:string" size="200"></Item>
              <Item label="TitolareDocumenti_Nome" type="xs:string" size="200"></Item>
              <Item label="ProduttoreDocumenti_IdPaese" type="xs:string" size="2">IT</Item>
              <Item label="ProduttoreDocumenti_PartitaIVA" type="xs:string"
size="11">.....</Item>
              <Item label="ProduttoreDocumenti_CodiceFiscale" type="xs:string"
size="16">.....</Item>
              <Item label="ProduttoreDocumenti_Denominazione" type="xs:string"
size="200">XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX</Item>
              <Item label="ProduttoreDocumenti_Cognome" type="xs:string" size="200"></Item>
              <Item label="ProduttoreDocumenti_Nome" type="xs:string" size="200"></Item>
          </CustomMetadata>
          </sincro:EmbeddedMetadata>
      </sincro:MoreInfo>
  </sincro:FileGroup>
  <sincro:Process>
    <sincro:Agent sincro:role="OtherRole" sincro:type="organization">
      <sincro:AgentName>
        <sincro:FormalName>XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX</sincro:FormalName>
      </sincro:AgentName>
      <sincro:Agent_ID sincro:scheme="TaxCode">IT:.....</sincro:Agent_ID>
      <sincro:MoreInfo sincro:XMLScheme="AgentCustomMetadata.xsd">
        <sincro:EmbeddedMetadata>
          <CustomMetadata>
            <AgentInfo>
              <Item label="Qualifica" type="xs:string" size="200">Titolare dei
Documenti</Item>
            </AgentInfo>
```

```
          </CustomMetadata>
        </sincro:EmbeddedMetadata>
      </sincro:MoreInfo>
    </sincro:Agent>
    <sincro:Agent sincro:role="OtherRole" sincro:type="organization">
      <sincro:AgentName>
        <sincro:FormalName>XXXXXXXXXXXXXXXX</sincro:FormalName>
      </sincro:AgentName>
      <sincro:Agent_ID sincro:scheme="TaxCode">IT:.................</sincro:Agent_ID>
      <sincro:MoreInfo sincro:XMLScheme="AgentCustomMetadata.xsd">
        <sincro:EmbeddedMetadata>
          <CustomMetadata>
            <AgentInfo>
              <Item label="Qualifica" type="xs:string" size="200">Produttore dei
Documenti</Item>
            </AgentInfo>
          </CustomMetadata>
        </sincro:EmbeddedMetadata>
      </sincro:MoreInfo>
    </sincro:Agent>
    <sincro:Agent sincro:role="PreservationManager" sincro:type="organization">
      <sincro:AgentName>
        <sincro:FormalName>XXXXXXXXXXXXXXXX</sincro:FormalName>
      </sincro:AgentName>
      <sincro:Agent_ID sincro:scheme="TaxCode">IT:……..</sincro:Agent_ID>
    </sincro:Agent>
    <sincro:Agent sincro:role="Operator" sincro:type="organization">
      <sincro:AgentName>
        <sincro:FormalName>TeamSystem Service Srl</sincro:FormalName>
      </sincro:AgentName>
      <sincro:Agent_ID sincro:scheme="TaxCode">IT:01641790702</sincro:Agent_ID>
        <sincro:MoreInfo sincro:XMLScheme="AgentCustomMetadata.xsd">
        <sincro:EmbeddedMetadata>
          <CustomMetadata>
            <AgentInfo>
              <Item label="Qualifica" type="xs:string" size="200">Conservatore</Item>
            </AgentInfo>
          </CustomMetadata>
        </sincro:EmbeddedMetadata>
        </sincro:MoreInfo>
    </sincro:Agent>
    <sincro:Agent sincro:role="Delegate" sincro:type="person">
      <sincro:AgentName>
        <sincro:NameAndSurname>
          <sincro:FirstName>Michele</sincro:FirstName>
          <sincro:LastName>Di Rienzo</sincro:LastName>
        </sincro:NameAndSurname>
      </sincro:AgentName>
      <sincro:Agent_ID sincro:scheme="TaxCode">IT:DRNMHL66E30Z401W</sincro:Agent_ID>
        <sincro:MoreInfo sincro:XMLScheme="AgentCustomMetadata.xsd">
        <sincro:EmbeddedMetadata>
          <CustomMetadata>
            <AgentInfo>
              <Item label="Qualifica" type="xs:string" size="200">Responsabile del servizio
di conservazione</Item>
            </AgentInfo>
          </CustomMetadata>
        </sincro:EmbeddedMetadata>
```

```
        </sincro:MoreInfo>
    </sincro:Agent>
    <sincro:Agent sincro:role="Delegate" sincro:type="person">
      <sincro:AgentName>
        <sincro:NameAndSurname>
          <sincro:FirstName>Rebecca</sincro:FirstName>
          <sincro:LastName>Macchiagodena</sincro:LastName>
        </sincro:NameAndSurname>
      </sincro:AgentName>
      <sincro:Agent_ID sincro:scheme="TaxCode">IT:MCCRCC85A52E456N</sincro:Agent_ID>
        <sincro:MoreInfo sincro:XMLScheme="AgentCustomMetadata.xsd">
        <sincro:EmbeddedMetadata>
          <CustomMetadata>
            <AgentInfo>
              <Item label="Qualifica" type="xs:string" size="200">Delegato operativo del
servizio di conservazione</Item>
            </AgentInfo>
          </CustomMetadata>
        </sincro:EmbeddedMetadata>
        </sincro:MoreInfo>
    </sincro:Agent>
    <sincro:Agent sincro:role="Delegate" sincro:type="person">
      <sincro:AgentName>
        <sincro:NameAndSurname>
          <sincro:FirstName>Andrea</sincro:FirstName>
          <sincro:LastName>Cordeschi</sincro:LastName>
        </sincro:NameAndSurname>
      </sincro:AgentName>
      <sincro:Agent_ID sincro:scheme="TaxCode">IT:CRDNDR80B02H282L</sincro:Agent_ID>
        <sincro:MoreInfo sincro:XMLScheme="AgentCustomMetadata.xsd">
        <sincro:EmbeddedMetadata>
          <CustomMetadata>
            <AgentInfo>
              <Item label="Qualifica" type="xs:string" size="200">Delegato operativo del
servizio di conservazione</Item>
            </AgentInfo>
          </CustomMetadata>
        </sincro:EmbeddedMetadata>
        </sincro:MoreInfo>
    </sincro:Agent>
    <sincro:Agent sincro:role="Delegate" sincro:type="person">
      <sincro:AgentName>
        <sincro:NameAndSurname>
          <sincro:FirstName>Rachele</sincro:FirstName>
          <sincro:LastName>Cristofaro</sincro:LastName>
        </sincro:NameAndSurname>
      </sincro:AgentName>
      <sincro:Agent_ID sincro:scheme="TaxCode">IT:CRSRHL80H47B519Q</sincro:Agent_ID>
        <sincro:MoreInfo sincro:XMLScheme="AgentCustomMetadata.xsd">
        <sincro:EmbeddedMetadata>
          <CustomMetadata>
            <AgentInfo>
              <Item label="Qualifica" type="xs:string" size="200">Delegato operativo del
servizio di conservazione</Item>
            </AgentInfo>
          </CustomMetadata>
        </sincro:EmbeddedMetadata>
        </sincro:MoreInfo>
```

```
    </sincro:Agent>
    <sincro:TimeReference>
      <sincro:AttachedTimeStamp sincro:normal="2015-07-
01T09:54:04.631"></sincro:AttachedTimeStamp>
    </sincro:TimeReference>
    <sincro:LawAndRegulations sincro:language="it">D.P.C.M. 3 dicembre 2013 – UNI SInCRO
11386:2010</sincro:LawAndRegulations>
  </sincro:Process>
</sincro:IdC>
```

Si evidenzia che la struttura dati dell'Indice del Pacchetto di Archiviazione di un Fascicolo informatico (IPdA-F) è riportata nel Disciplinare Specificità del Contratto, nei casi in cui una Pubblica Amministrazione intenda versare al sistema di conservazione "*Conservazione Cloud*" dei fascicoli formati nel proprio sistema di gestione dei documenti.

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 11386:2010, è una distribuzione di uno o più Pacchetti di Archiviazione, a seconda della richiesta eseguita dall'Utente al sistema *Conservazione Cloud*.

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 carica la richiesta, la evade generando e sottoscrivendo il Pacchetto di Distribuzione con firma digitale del Responsabile del Servizio di Conservazione ovvero dei Delegati del Conservatore, prima di distribuirlo all'Utente tramite canale sicuro.

Il Pacchetto di Distribuzione nel sistema *Conservazione Cloud* 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 *Conservazione Cloud* 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 ovvero dei Delegati del Conservatore e marcati temporalmente;
- un **IPdD, Indice del Pacchetto di Distribuzione**, generato in conformità allo standard UNI SInCRO 11386:2010 e contenente le informazioni relative alla sessione di distribuzione e i riferimenti agli oggetti dati distribuiti nel contenitore compresso .zip;
- un **PdD Viewer**, denominato "*Conservazione Cloud – 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, anche nel caso della distribuzione di un fascicolo informatico (IPdD-F) ed ulteriori specifiche ed informazioni di dettaglio in merito al Pacchetto di Distribuzione per un determinato Produttore dei documenti sono riportate nel Disciplinare Specificità del Contratto.

Torna al sommario

7. PROCESSO DI CONSERVAZIONE

Il processo di conservazione è conforme a quanto disposto dall'art. 9 delle Regole Tecniche 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 *Conservazione Cloud* 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 14721:2012 di seguito schematizzato:

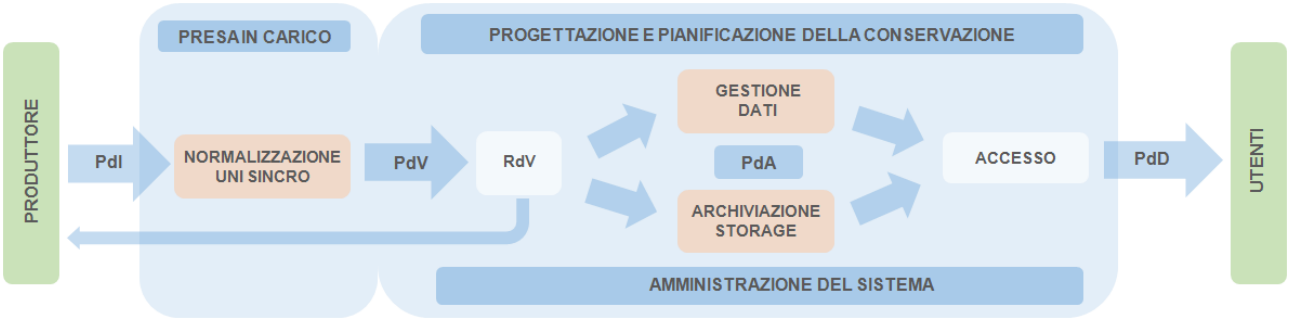

Fig. 9 *– Modello di processo di conservazione adottato dal sistema Conservazione Cloud*

Il Conservatore, affidatario dal Responsabile della Conservazione, gestisce le varie sessioni del processo, i servizi e le funzioni per la gestione complessiva del sistema *Conservazione Cloud* in osservanza a quanto previsto dall'art. 7 delle Regole Tecniche.

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

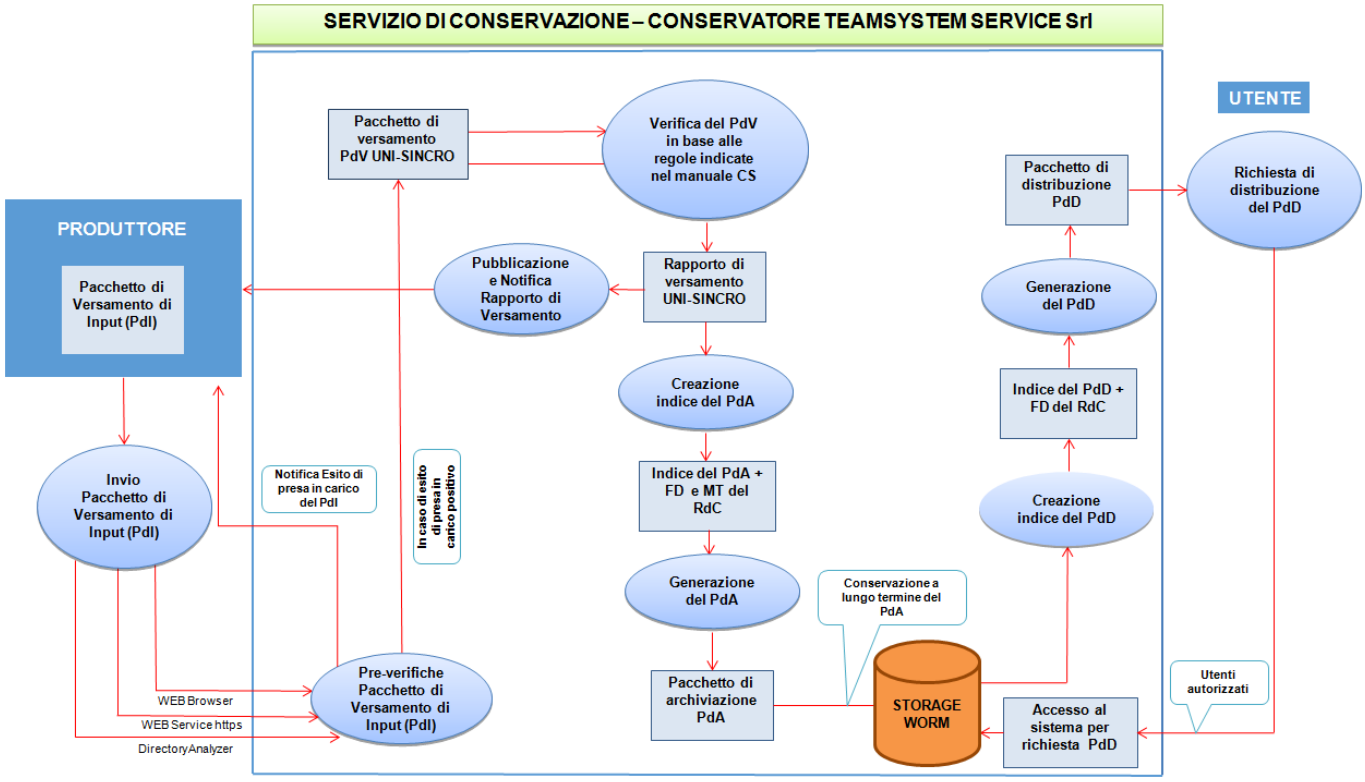

Fig. 10 *– Schema di processo del Servizio di conservazione nel sistema Conservazione Cloud*

Torna al sommario

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

Il Produttore dei documenti, preventivamente identificato dal sistema, può versare i **Pacchetti di Versamento di Input (PdI)** al sistema *Conservazione Cloud* attraverso modalità e canali trasmissivi sicuri:

- **Web service** tramite protocollo HTTPS;
- **Uploader manuale** tramite interfaccia web del sistema *Conservazione Cloud*;
- **DirectoryAnalyzer** tramite servizio Windows, modulo che permette di consegnare in modalità sicura i pacchetti PdI al sistema di conservazione depositandoli in opportune cartelle configurate.

Il Servizio *Conservazione Cloud* 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 che abbia sottoscritto il relativo contratto di servizio e quindi settato e riconosciuto nel sistema nello stato "attivo".

Le personalizzazioni e le specifiche dei Pacchetti di Versamento di Input (PdI), gestite per ogni Produttore, sono riportate nel Disciplinare Specificità del Contratto, sottoscritto dallo stesso all'atto dell'adesione (tramite coupon o ordine di acquisito) o nella fase di attivazione del Servizio di Conservazione (tramite documento condiviso tra Produttore e Conservatore).

Una volta ricevuto il PdI il sistema esegue su di esso delle verifiche descritte nel paragrafo successivo e produce un **Esito di presa in carico del PdI** che ha lo scopo di notificare al Produttore se il versamento del PdI sia andato a buon fine o meno.

In caso di **esito negativo** il Conservatore considera il caricamento nel sistema **non avvenuto** ed il Produttore riceverà un esito negativo di presa in carico del PdI, ma non riceverà mai la notifica di messa a disposizione del Rapporto di Versamento in quanto il processo si è bloccato prima della generazione del Pacchetto di Versamento standard UNI SInCRO. Pertanto, in tutti i casi in cui il Produttore non riceve la notifica di messa a disposizione del Rapporto di Versamento per quel determinato PdI, il Produttore stesso è consapevole che l'esito di versamento è negativo e gli oggetti del PdI non saranno mai posti in conservazione, in quanto scartati nella fase di pre-verifica.

Nel caso di trasmissione del PdI tramite **dialogo applicativo (Web Service)** lo stesso WS risponde in modo sincrono con un esito di presa in carico che riporta la descrizione dell'errore e quindi il motivo per cui non è stato preso in carico il PdI dal sistema. Nel caso di **upload del PdI tramite interfaccia web**¸ l'esito di risposta verrà visualizzato in real time dall'Utente alla conferma dei dati di caricamento.

Infine, in caso di utilizzo del **DirectoryAnalyzer** in modalità asincrona viene inviato dal Conservatore un file di esito di presa in carico del PdI nel formato XML che contiene la descrizione del motivo di scarto. La sicurezza, la riservatezza e la tracciabilità della trasmissione dell'esito avviene utilizzando il canale PEC indicato dal Produttore nella fase di attivazione del Servizio.

Se, al contrario, l'**esito delle verifiche sul PdI è positivo l'esito di presa in carico restituisce al Produttore**, con le medesime modalità sopra descritte, il codice univoco del PdI preso in carico dal sistema *Conservazione Cloud*.

In questo caso il sistema genera il PdV normalizzato nel formato XML conforme allo standard UNI SInCRO 11386:2010 a partire da uno o più PdI acquisiti.

I sistemi, presenti nell'infrastruttura di erogazione del Servizio, per la presa in carico dei PdI, 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 27001:2013.

Torna al sommario

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

Il sistema *Conservazione Cloud*, 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:

- **C01** - Verifica credenziali Utente e stato Utente attivo ed autorizzato;
- **C02** - Verifica dell'idoneità del formato del files contenuti nel PdI;
- **C03** - Verifica di quadratura tra il numero di files fisici ed il numero di record logici che li classificano;
- **C04** - Verifica della integrità del documento mediante il confronto tra dimensione associata al file in ingresso e la dimensione ricalcolata dal sistema di conservazione;
- **C05** - Verifica della integrità del documento mediante il confronto tra l'impronta associata al file in ingresso e l'impronta ricalcolata dal sistema di conservazione;
- **C06** - Verifica della eventuale presenza nel corrispondente archivio informatico di un documento o oggetto identico;
- **C07** - Verifica della presenza dei dati anagrafici dei soggetti Produttore, Affidante, Titolare dei documenti, Responsabile della Conservazione nel sistema di conservazione;
- **C08** - Verifica della avvenuta compilazione dei metadati obbligatori per ogni tipo di documento o in generale oggetto digitale.

Tutte le azioni di controllo eseguite e di comunicazione dell'esito sono tracciate nel log Management System del Sistema *Conservazione Cloud* con l'indicazione nei log dell'impronta dei documenti verificati, con la registrazione di un riferimento temporale, l'individuazione dell'Utente che ha versato i PdI oltre all'esito della verifica.

In caso di esito positivo, viene generato il PdV normalizzato standard UNI SInCRO.
Il sistema prende in carico il PdV normalizzato e verifica la sua coerenza e valida la conformità sintattica del XML allo schema UNI SInCRO di riferimento, eseguendo le ulteriori seguenti verifiche:

- verifica che il PdV normalizzato contenga l'indice IPdV e gli oggetti dati da esso referenziati;
- controllo di validità del file XML IPdV con il file schema XSD dell'UNI SInCRO 11386:2010;
- verifica di coerenza tra i nomi degli oggetti dati presenti nel PdV e i nomi degli oggetti dati dichiarati nell'IPdV;
- controllo della corretta valorizzazione dei campi ID e MimeType dei files dichiarati nell'IPdV.

Quale esito definitivo del versamento del PdV (e quindi del PdI) da parte del Produttore dei documenti, 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 e scarto 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 *Conservazione Cloud* accetta i PdV e quindi il Conservatore si assume la responsabilità contrattuale di erogare il Servizio della 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 ovvero dei Delegati del Conservatore e a cui è stato associato un Riferimento Temporale riferito al Tempo Universale Coordinato (UTC), che viene generato automaticamente da un job con una periodicità che può essere settata e configurata nel profilo di conservazione del sistema *Conservazione Cloud* e per quel determinato Produttore.

Il RdV è univocamente identificato come tutti gli oggetti del sistema, contiene i 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 programma di portarli in conservazione periodicamente al fine di mantenere la prova della verifica eseguita.

I Rapporti di Versamento sono messi a disposizione del Produttore e degli Utenti autorizzati attraverso l'apposita interfaccia web based del sistema *Conservazione Cloud*, che tramite un filtro di ricerca, ne consente la visualizzazione attraverso un viewer dedicato e il download del file firmato digitalmente.

Torna al sommario

7.4 Rifiuto dei Pacchetti di Versamento e comunicazione delle anomalie

Il rifiuto di un Pacchetto di Versamento di Input avviene attraverso esito di presa in carico che ha il compito di notificare le anomalie riscontrate al Produttore tramite PEC ed in caso negativo di bloccare il processo di caricamento e di successiva normalizzazione del PdI nel PdV UNI SInCRO.

L'esito, invece, delle verifiche riepilogative sul PdV UNI SInCRO sono comunicate attraverso la generazione del RdV. La comunicazione avviene attraverso la produzione di una mail di notifica trasmessa al Produttore **tramite PEC**.

Il Produttore dei documenti ha l'obbligo di verificare il buon esito del versamento attraverso la presa visione de RdV.

Inoltre, sia gli Operatori delegati del Conservatore che l'Utente autorizzato hanno a disposizione una **console di controllo** nell'interfaccia web del sistema *Conservazione Cloud* a cui possono accedere e visualizzare la situazione dei documenti conservati, suddivisa per Pacchetti di Input (PdI), Pacchetti di Versamento (PdV); Pacchetti di Archiviazione (PdA) e Pacchetti di Distribuzione (PdD).

***Fig. 11** – Console di controllo web del sistema Conservazione Cloud*

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 ovvero dei Delegati del Conservatore e la marca temporale sull'Indice del Pacchetto di Archiviazione.

Anche la cristallizzazione dell'Indice del Pacchetto di Archiviazione per il Fascicolo informatico (PdA-F) avviene con l'apposizione della firma digitale e marca temporale, con la differenza che un pacchetto PdA-F non contiene oggetti digitali, ma contiene negli indici della struttura dati i riferimenti agli oggetti digitali in esso contenuti, secondo quanto previsto dalla normativa vigente nel tempo.

Inoltre, ad ogni progressiva aggiunta di nuovi oggetti digitali appartenenti ad un determinato fascicolo avviene una nuova cristallizzazione del processo di conservazione del fascicolo, secondo le tempistiche concordate con la Pubblica Amministrazione e previste nel loro Piano di Conservazione.

La corretta generazione del Pacchetto di Archiviazione è presidiata e monitorata dai delegati operativi del Conservatore TeamSystem Service attraverso gli strumenti di console di controllo, le notifiche via mail, ecc.

La garanzia di sicurezza, immodificabilità, integrità del processo e del PdA generato ai fini di mantenimento e conservazione (long-term preservation) sono garantiti nel sistema *Conservazione Cloud* attraverso la memorizzazione degli oggetti sottoposti al processo di conservazione in un secondo sottosistema di memorizzazione SAN, impiegato per l'archiviazione a lungo termine dei documenti, che garantisce **il massimo livello di sicurezza e integrità dei dati**. Tale sistema dedicato è dotato di una soluzione software specifica (**sistema NetApp SnapLock**) che consente di creare **volumi segregati**, **impedendo 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 27001:2013.

La firma digitale 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 al momento dell'apposizione della firma. Ogni qualvolta sia eseguita un'operazione significativa ed a richiesta del delegato operatore viene controllata la validità delle firme, del certificato e l'integrità del documento informatico oggetto di sottoscrizione.

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 ovvero dei Delegati del Conservatore al fine di garantire una data opponibile a Terzi in cui la conservazione dei documenti era già avvenuta.

Il presidio operativo ed i controlli automatici del sistema *Conservazione Cloud* 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'anomalie 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 dall'articolo 10 del D.P.C.M. del 3 Dicembre 2013 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 ovvero dei Delegati del Conservatore.

***Fig. 12** – Interfaccia del sistema Conservazione Cloud in cui è presente la richiesta del Pacchetto di Distribuzione*

In maggior dettaglio, tramite apposito accesso web accreditato, 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 delle credenziali di accesso dell'utente e dei seguenti dati:

- Soggetto Titolare dei documenti;
- tipo di 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) l'impronta hash di ciascuno (per permettere di controllare che il documento non sia stato modificato)

- selezionare i documenti da scaricare per comporre 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.

Sull'Indice del Pacchetto di Distribuzione (IPdD) viene apposta la firma digitale del Responsabile del Servizio di Conservazione ovvero dei Delegati del Conservatore.

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 *Conservazione Cloud*, tramite le proprie credenziali, può scaricare duplicati informatici secondo le proprie esigenze o richiedere Pacchetti di Distribuzione (PdD) che contengono anche i duplicati informatici.
Inoltre, attraverso chiamate web service, possono essere richiesti ed ottenuti 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.

In relazione a specifici accordi definiti nel contratto o nel Disciplinare Specificità del Contratto, il Conservatore potrà produrre un contenitore in cui sono riportati i duplicati informatici richiesti (ad esempio supporto ottico).

Per la produzione di copie informatiche, previa richiesta dell'Utente secondo quanto concordato, le procedure operative del sistema *Conservazione Cloud* fanno riferimento alle disposizioni di cui al D.P.C.M. 13 novembre 2014, 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 sono mantenute nel tempo nel sistema di log.

Torna al sommario

7.8 Scarto dei Pacchetti di Archiviazione

L'articolo 9, comma 2, lettera k) del D.P.C.M. 3 dicembre 2013 stabilisce che, successivamente alla scadenza dei termini di conservazione previsti dalla norma, debba essere effettuato lo scarto dei PdA dal sistema di conservazione dandone comunicazione con preavviso al Produttore, ad eccezione dei casi in cui lo scarto può avvenire solo previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo rilasciata al produttore secondo quanto previsto dalla normativa vigente in materia, in quanto trattasi di archivi pubblici o privati, che rivestono interesse storico particolarmente importante.

Ad ogni tipo documento è associata la durata in anni dell'obbligo di conservazione, quindi un servizio provvede a valutare, per ciascun Produttore, quali documenti e relativi PdA sono in scadenza di conservazione e ad avvisare il Conservatore, in particolare i suoi Responsabili ed i suoi delegati.

Il Servizio produrrà un elenco dei Pacchetti di Archiviazione che hanno superato il periodo di conservazione previsto che sarà comunicato via PEC al Produttore.

Quest'ultimo dovrà prendere visione dell'elenco dei documenti e pacchetti e far pervenire non oltre 60 giorni al Conservatore l'eventuale richiesta di estensione del periodo di conservazione rinegoziandone le condizioni contrattuali. 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.

La funzione di scarto provvederà a generare un Pacchetto di Scarto cancellando dal file system documenti gli oggetti digital, i pacchetti PdA, se presenti i pacchetti PdA-F, ma mantenendo in conservazione un Indice del Pacchetto di Scarto (IPdS) conforme allo standard UNI SInCRO 11386:2010 che tiene evidenza dell'avvenuto scarto e traccia di tutte le informazioni ad esso associate.

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 Conservatore 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 11386:2010 proprio per garantire l'interoperabilità e la trasferibilità degli oggetti da un sistema ad un altro.

Inoltre, il Conservatore mantiene un registro cronologico dei software, quali ad esempio i viewer, per garantire nel tempo la visualizzazione dei vari oggetti.

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 dei documenti o di un altro Conservatore, secondo il principio della traspirazione e della collaborazione.

Il trasferimento dei PdA avviene sempre sottoforma di generazione dei PdD attraverso canali trasmissivi sicuri (ad esempio HTTPS o tramite supporti fisici) previo accordo e/o richiesta via PEC del Produttore.

In caso di scadenza o disdetta del contratto di affidamento del Servizio di conservazione, il Produttore verrà sollecitato tramite PEC a scaricare i Pacchetti di Distribuzione di tutti i documenti e PdA sottoposti al processo di conservazione entro un termine concordato. In tal caso il Produttore è tenuto a verificare che gli oggetti scaricati siano coerenti entro i termini stabiliti contrattualmente e a fornirne comunicazione al Conservatore in caso di riscontro di anomalie. Una volta restituiti i PdA, verrà disattivata l'utenza di accesso del Produttore e trascorsi ulteriori 60 giorni scartati i PdA se previsto dalle condizioni contrattuali.

Torna al sommario

8. IL SISTEMA DI CONSERVAZIONE

8.1 Componenti logiche

La figura seguente, descrive schematicamente, le diverse componenti logiche del sistema *Conservazione Cloud* di TeamSystem Service.

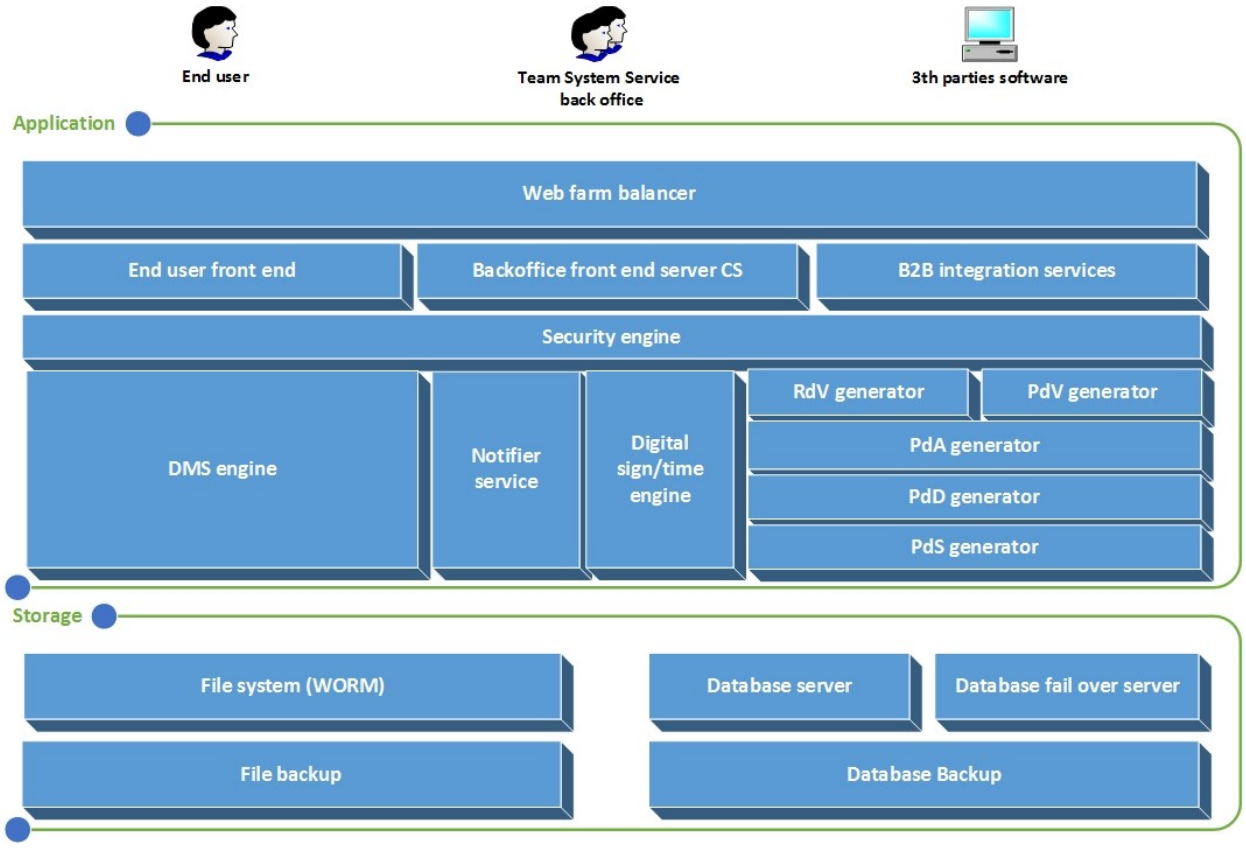

***Fig. 13**– Rappresentazione grafica delle componenti logiche del sistema Conservazione Cloud*

Web farm balancer
I server applicativi del front end per gli Utenti finali e per il back office sono ospitati presso la farm TeamSystem.
Tali server sono esposti attraverso strumenti di bilanciamento del carico e che ottimizzano le attività utente sui server applicativi.

End 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.

Backoffice front end server
Gli operatori interni del Servizio potranno accedere alla sezione riservata dove sarà possibile amministrare il servizio in funzione del proprio ruolo all'interno dell'azienda.

B2B integration services
Le applicazioni proprietarie o di terze parti potranno interfacciarsi con il sistema attraverso servizi esposti.

Security engine
L'intero sistema è sottoposto a stringenti regole di sicurezza che consentono o meno l'accesso alle funzionalità applicative in funzione dei permessi definiti.

Dms engine
Il motore di gestione documentale consente di classificare, fascicolare ed archiviare i documenti.

Notifier service
Il sistema può emettere notifiche per avvisare utenti finali e gli operatori del back office per le diversi fasi del processo di conservazione.

Digital sign/time engine
Motore e componenti dedicati all'apposizione della firma digitale di documenti e degli indici dei Pacchetti e all'apposizione della marca temporale, attraverso la connessione sicura con un certificatore accreditato.

RdV, PdV, PdA, PdD, PdS generator
Strumenti che collaborando con il resto del sistema supportano la creazione e la gestione delle sessioni di versamento, presa in carico, archiviazione, distribuzione e scarto dei diversi Pacchetti Informativi e degli oggetti dati.

File system (WORM)
I documenti conservati e archiviati verranno conservati da questo componente che garantirà la conservazione dei dati nel rispetto dei termini legali.

File system backup
Il file system primario viene periodicamente sottoposto a procedure di backup secondo le politiche di disaster recovery espresse nell'ambito della certificazione ISO IEC 27001:2013.

Database server
Le informazioni del sistema sono mantenute da un RDBMS.

Database failover server
Nel caso in cui il database server primario abbia un malfunzionamento questo componente interviene per sostenere le funzionalità del servizio

Database Backup
I database vengono periodicamente sottoposti a procedura di backup secondo le politiche di disaster recovery espresse nell'ambito della certificazione ISO IEC 27001:2013.

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 ASP con un'interfaccia HTML5, operante su protocollo HTTPS all'interno del web server Microsoft IIS. L'autenticazione è effettuata tramite un sistema di gestione di chiavi ed utenze. Dialoga con la parte di Web Services tramite chiamate HTTP;

- l'**interfaccia WCF Services** è sviluppata sulla piattaforma Microsoft .NET e dialoga secondo lo standard SOAP con un set di API di tipo open all'interno del web server IIS. L'autenticazione è effettuata tramite un sistema di gestione di chiavi ed utenze. L'interfaccia interagisce con un sistema di database relazionale MsSQL. Dialoga con la parte di interfaccia Web e con i sistemi esterni tramite chiamate HTTPS;

- i **windows service** delegati ai processi batch sono sviluppati sulla piattaforma Microsoft .NET e messi in esecuzione su server ospitati nella farm. Il monitoraggio dei servizi viene effettuato attraverso il sistema di log e delle relative interfacce di test e controllo implementate;

- l'**engine documentale** all'interno del quale sono memorizzati i documenti è sviluppato in linguaggio ASP ed in linguaggio C++ per le funzionalità di basso livello e gestione della security. Interagisce con un sistema di database relazionale Microsoft SQL e dialoga con la parte di interfaccia web e servizi attraverso chiamate a servizi interni;

- tutti i sistemi sono operanti dietro dei Load Balancer basati su tecnologia Microsoft 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.

Lo schema seguente, descrive brevemente le componenti tecnologiche del sistema *Conservazione Cloud* di TeamSystem Service.

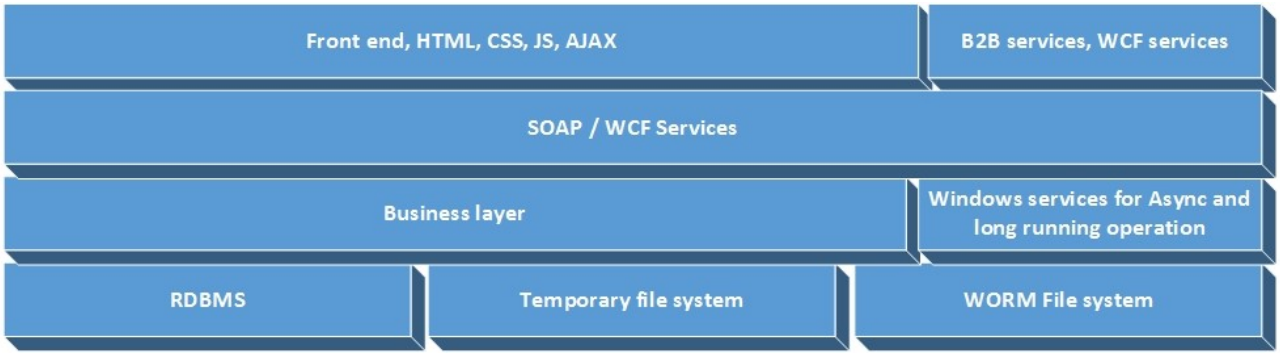

***Fig. 14** – Rappresentazione grafica delle componenti tecnologiche del sistema Conservazione Cloud*

Front end
Il front end è sviluppato con un'interfaccia HTML5 offrendo una applicazione fruibile dalle piattaforme maggiormente utilizzate.

B2B services / WCF Services
Servizi di comunicazione sviluppati in piattaforma .NET, accessibile dalle applicazioni di terze parti.

SOAP / WCF Services
Il software è stratificato e organizzato attraverso una serie di servizi interni a loro volta esposti attraverso protocollo SOAP e WCF.

Windows service for async and long running operation
Tutte le operazioni di elaborazione massive che richiedono un dispendio di risorse e una attesa da parte dell'Utente sono state spostate in servizi batch.

Temporary file system
A supporto del sistema viene utilizzato il file system non WORM per tutte le elaborazioni temporanee e non definitive

WORM file system
Per la persistenza dei dati con valore legale viene utilizzato un file system a sola lettura, così da garantire la conservazione dei file per l'intera durata richiesta.

Torna al sommario

8.3 Componenti fisiche

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

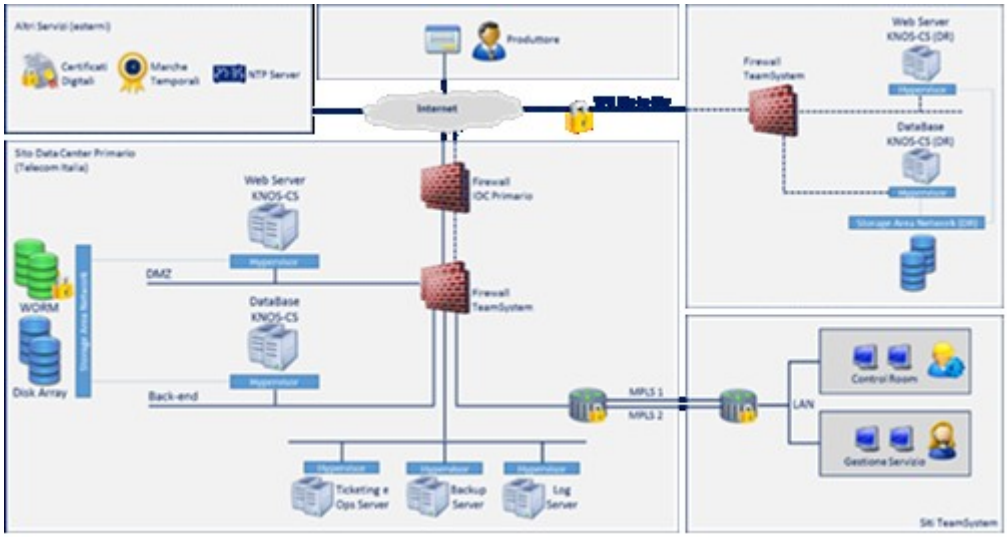

***Fig. 15** – Rappresentazione grafica delle componenti fisiche del sistema Conservazione Cloud*

In particolare, l'architettura fisica è basata su un Data Center primario e su un "virtual Data Center" utilizzato come soluzione di Disaster Recovery. Nello specifico:

- il Data Center primario presso il Provider TIM Italia sito in Bologna nel quale sono ospitati tutti i sistemi Server e gli apparati di rete, di sicurezza e di connettività della piattaforma di Conservazione. TIM fornisce le facility tecniche (elettricità, condizionamento, ecc.) e di protezione ambientale. Maggiori informazioni sulle caratteristiche tecniche del Data Center e degli impianti sono riportate nel Piano della Sicurezza;

- il "virtual Data Center" implementato nel Data Center secondario presso il Provider ARUBA sito in Arezzo, via Gobetti 96, che rende disponibili le risorse elaborative richieste da TeamSystem Service. La soluzione tecnica di disaster recovery adottata per garantire la continuità operativa del Servizio di Conservazione prevede una replica geografica realizzata mediante una soluzione di tipo "vCloud", basata su un allineamento dei dati di tipo "Asincrono on-line". In particolare, il Servizio di replica vCloud consente la replica a livello di hypervisor raggiungendo ordini di grandezza del minuto per RTO e del secondo per RPO. Maggiori informazioni relative alla soluzione di Disaster Recovery e replica geografica sono riportate nel Piano della Sicurezza;

Le altre caratteristiche architetturali e tecnologiche dell'infrastruttura di rete e sicurezza del sistema di conservazione sono di seguito elencate:

- l'architettura Server è completamente basata sull'utilizzo della soluzione di virtualizzazione VMWare applicata, per quanto concerne la piattaforma *Conservazione Cloud*, mediante duplicazione fisica e virtuale dei singoli sistemi, al fine di garantire la tolleranza ai guasti e l'eliminazione dei *single point of failure*. In particolare, in caso di failure di uno più sistemi, il software di gestione dell'ambiente virtuale è in grado di ridistribuire le attività in corso verso gli altri sistemi (high availabilty e load balancing), riducendo al minimo i disservizi e garantendo la persistenza delle connessioni esistenti;
- ciascun Server è attestato su una SAN mediante connessione Fiber Channel ad alta velocità;

- un secondo sottosistema SAN è impiegato per l'archiviazione a lungo termine dei documenti, garantendo il **massimo livello di sicurezza e integrità dei dati**. Tale sistema dedicato è dotato di una soluzione software specifica (sistema NetApp SnapLock) che consente di creare volumi segregati, impedendo l'alterazione o l'eliminazione dei file prima di una data prestabilita (funzionalità di software **WORM**);

- qualsiasi componente dell'infrastruttura, tra i quali server, apparati di rete e sicurezza, sistemi Storage ed infrastruttura SAN, ecc. è completamente ridondata per eliminare ogni *single point of failure;*

- l'architettura di rete è progettata per proteggere i sistemi di front-end da Internet e dalle reti interne mediante l'utilizzo di una DMZ protetta da due livelli di firewalling distinti (defense-in-depth): il firewall di frontiera gestito direttamente da TIM e connesso ad Internet; il secondo firewall, che integra anche funzionalità di Intrusion Prevention e antimalware, di proprietà dell'organizzazione, è messo a protezione della DMZ e dei sistemi di backend;

- in termini di connettività sono presenti i seguenti collegamenti principali:

    - connessione ad Internet su doppio circuito ridondato da parte di COLT;

    - connessione MPLS tra Data Center primario e sedi TeamSystem realizzata con doppio anello appartenenti a provider diversi (COLT e Fastweb);

    - connettività geografica per l'interconnessione tra Data Center primario e secondario (doppio link forniti da Fastweb e COLT), utilizzato per funzionalità di replica dati e gestione remota.

In aggiunta all'architettura IT ed alla descrizione delle singole componenti infrastrutturali impiegate, di seguito sono riassunte le principali tipologie hardware di sistemi adottati:

- infrastruttura LAN: apparati di rete (switch) di tipologia Layer 3 di ultima generazione, basati su tecnologia CISCO con architettura completamente ridondata (fault tolerance);

- infrastruttura WAN: router MPLS/DMVP per la gestione delle connessioni WAN esistenti, in configurazione completamente ridondata (fault tolerance);

- infrastruttura Server: sistemi IBM di fascia alta, per applicazioni business critical, dotati delle le funzioni Predictive Failure Analysis (PFA) e Light Path Diagnostics che provvedono al monitoraggio dei sottocomponenti di sistema e alla segnalazione anticipata di eventuali problemi a carico di alimentatori, ventole, regolatori di tensione, dischi, processori e memoria. I componenti ridondati hot-swap facilitano la sostituzione delle parti malfunzionanti senza alcun fermo del sistema. Light Path Diagnostics inoltre mostra un indicatore visibile sui componenti malfunzionanti e consente di avere il tempo di sostituire i componenti prima del malfunzionamento, offrendo quindi fattori di elevata disponibilità.

Ulteriori dettagli relativi all'infrastruttura hardware e di rete adottata per il sistema *Conservazione Cloud* sono riportati nel Piano della Sicurezza.

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 9001:2008.

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 i responsabili devono 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 27001:2013, 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 di 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 della 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.

Nello specifico, si distinguono due procedure di verifica:

- verifica dell'integrità e della consistenza dei pacchetti di documenti generati dal Processo di Conservazione, eseguita mensilmente in modo automatico da un processo batch su un adeguato campione pseudo casuale
- verifica dell'effettiva leggibilità dei documenti inseriti all'interno dei pacchetti. Per questa seconda procedura, il Conservatore, sotto la supervisione del Responsabile della Conservazione, con cadenza annuale verificherà che, per i formati dei file utilizzati per la conservazione dei documenti, sia disponibile un visualizzatore aggiornato e conforme al fine di garantire accesso e leggibilità.

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 dai 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 ISO27001:2013, 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 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 *Conservazione Cloud* 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.

Una volta prodotti i file di log sono raccolti e conservati mediante l'utilizzo di una piattaforma di raccolta centralizzata dei log (log collecting), posizionata nel Data Center primario.

La piattaforma centralizzata garantisce una serie di requisiti tecnici per la gestione sicura dei log, tra i quali:

- completezza, inalterabilità e possibilità di verifica dell'integrità dei log;
- completa 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, per almeno 6 mesi, dei Log di Accesso (log di sicurezza) delle utenze con privilegi di amministrazione.

Per il Servizio di Conservazione sono state introdotte ulteriori funzionalità di logging direttamente all'interno dell'applicazione *Conservazione Cloud*, al fine di prevedere le seguenti attività aggiuntive:

- estrazione dei log (applicativi, di sicurezza e di servizi) con frequenza settimanale;
- applicazione della firma digitale ai log estratti;
- conservazione digitale dei log nel lungo periodo mediante la piattaforma *Conservazione Cloud*, con cui viene erogato il servizio di conservazione in cui solo gli utenti abilitati avranno accesso ai in sola lettura per consultazioni e verifiche.

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

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

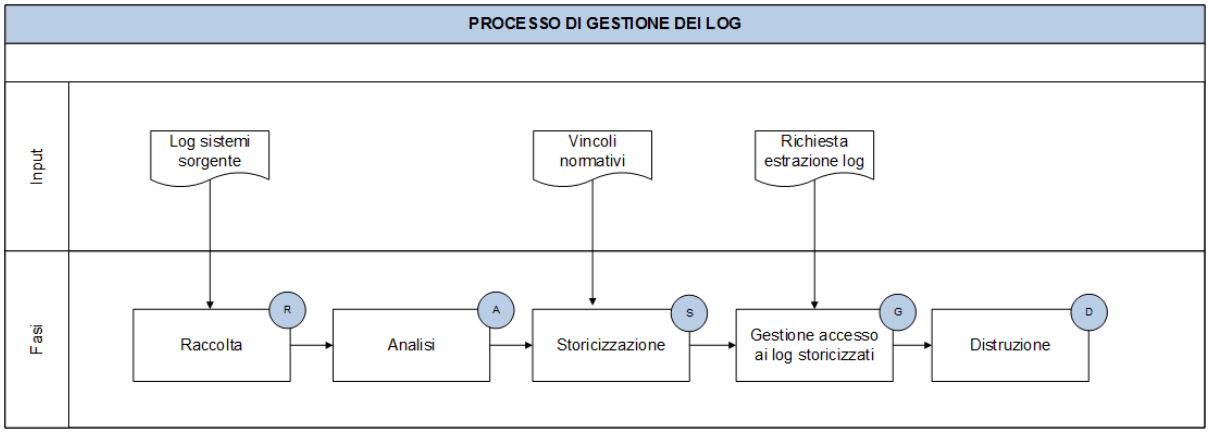

***Fig. 16** – Processo di gestione dei log*

***Fig. 17** – Interfaccia web del sistema di log*

Le modalità di ricerca e visualizzazione dei Log sono dettagliate nel Manuale Tecnico del Servizio, al capitolo “Ricerca e visualizzazione dei Log”.

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.

All'interno del Piano della Sicurezza di TeamSystem Service sono indicati puntualmente gli attributi dei file di log generati e relativi alla piattaforma con cui viene erogato il Servizio di Conservazione.

Torna al sommario

9.1.5 Monitoraggio componenti hardware del sistema Conservazione Cloud

Le procedure di monitoraggio, così come documentato all'interno del Piano della Sicurezza, 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 Piano della Sicurezza, 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. Ulteriori dettagli sono riportati nel Piano della Sicurezza.

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 Conservazione Cloud) 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 dal Codice in materia di protezione dei dati personali (D. Lgs. 196/03);

- 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;

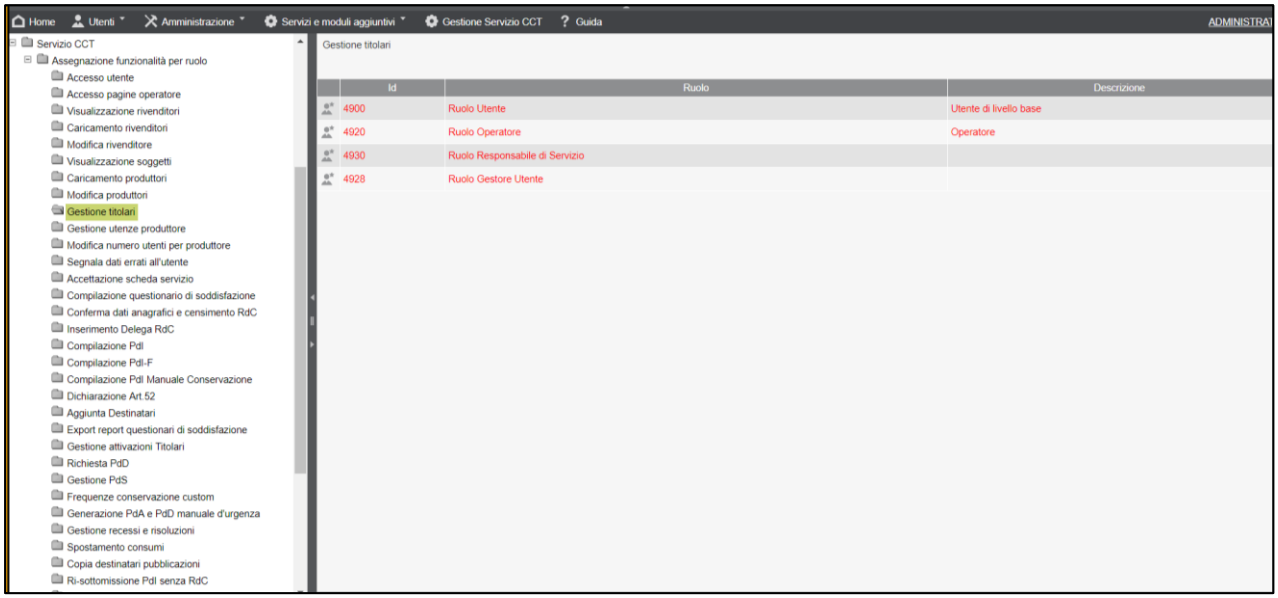

***Fig. 18** – Assegnazione funzionalità per ruolo*

- 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 Piano della Sicurezza;

- i sistemi anti-intrusione, quali Firewall e IDS/IPS, sono posizionati all'interno del segmento di rete che collega la piattaforma Conservazione Cloud 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 Piano della Sicurezza;

    - 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 tramite PEC, 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 *Conservazione Cloud* si rimanda alla specifica procedura referenziata all'interno del Piano della Sicurezza.

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 PR_GSU_00_Gestione accessi logici.

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 27001:2013 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 architetturali associati, quando ne fanno richiesta.

Le tematiche specifiche che contribuiscono a vario titolo al fine comune di salvaguardia delle informazioni sono delineate all'interno di documentazione di dettaglio riportata all'interno della seguente tabella.

Nome documento	Descrizione	Ambito
PO_SEC_00_Information Security Policy	Politica che definisce l'indirizzo strategico che l'Organizzazione deve perseguire per garantire la sicurezza del proprio patrimonio informativo e di quello dei propri Clienti.	**Politiche per la Sicurezza delle Informazioni**
DC_OBJ_00_Obiettivi di Sicurezza delle Informazioni	Documento che descrivere gli obiettivi in materia di Sicurezza delle Informazioni.	
ANNEX B (DC_OBJ_00) - Misure relative agli obiettivi	Documento utilizzato per valutare il raggiungimento degli obiettivi di sicurezza in funzione di parametri e soglie definiti.	
DC_CNT_00_Contesto dell'Organizzazione	Documento che definisce il contesto, sia esterno sia interno, in cui l'Organizzazione eroga i propri servizi.	
PR_RSK_00_Analisi e trattamento rischi	Procedura che definisce i processi di analisi e trattamento dei rischi legati alla sicurezza delle informazioni.	**Analisi e Gestione dei Rischi della Sicurezza delle Informazioni**
DC_RSK_01_Metodologia di Gestione dei Rischi	Documento che definisce la metodologia di valutazione e gestione dei rischi legati alla sicurezza delle informazioni.	

Nome documento	Descrizione	Ambito
ANNEX A - Criteri di Accettazione dei Rischi	Documento che definisce i criteri utilizzati dall'Organizzazione per individuare le soglie di accettazione dei rischi in funzione della tipologia di impatto sul business.	
DC_RSK_02_Risk Assessment Report	Documento che illustra i risultati dell'attività di Analisi dei Rischi svolta sul processo di erogazione del servizio di Conservazione Sostitutiva.	
DC_RSK_03 - Piano di Trattamento dei Rischi	Documento che riporta l'elenco dei rischi e delle relative azioni di trattamento.	
DC_SOA_00_Statement Of Applicability	Lista di tutti i controlli di sicurezza, nell'ambito dello standard ISO/IEC 27001-2013, applicabili dall'Organizzazione.	
DC_AST_00_Asset Register	Elenco degli asset, tangibili e intangibili, relativi al servizio di Conservazione Sostitutiva.	
DC_MAN_00_Mansionario Figure_Sicurezza	Documento che definisce i compiti, le funzioni ed i requisiti richiesti per le figure professionali rilevanti ai fini della sicurezza delle informazioni.	
DC_MFP_00_Mansionario_ Figure_Professionali	Documento che definisce i compiti, le funzioni ed i requisiti richiesti per le figure professionali rilevanti ai fini dell'erogazione del Servizio di Conservazione.	
Procedura HR	Procedura che regolamenta i processi di selezione, assunzione e gestione del personale.	**Sicurezza delle Risorse Umane**
PO_AUP_00_Acceptable Use Policy	Policy che descrive le misure di sicurezza atte a garantire l'utilizzo corretto e sicuro degli strumenti informatici e la protezione dell'intero patrimonio informatico societario.	
DC_PDT_00_Piano di Training	Documento nel quale è formalizzato il piano di formazione per il personale dell'Organizzazione.	
PR_GTP_Gestione delle Terze Parti	Procedura che definisce i principi generali che devono essere rispettati in fase di contrattualizzazione, gestione e monitoraggio periodico delle Terze Parti.	**Relazioni con i fornitori**
DC_MSA_01_Allegato tecnico	Allegato tecnico contrattuale che regolamenta i servizi di natura ICT e Information Security forniti dalla società Capogruppo verso TeamSystem Service S.r.l.	
PR_COM_00_Gestione delle Comunicazioni	Procedura che definisce le modalità di gestione delle comunicazioni all'interno e all'esterno dell'Organizzazione sulla base delle esigenze comunicative e che definisce priorità, canali comunicativi, ruoli e responsabilità.	**Sicurezza delle comunicazioni**
PO_DCI_00_Data Classification	Policy aziendale che definisce i criteri che devono essere seguiti per la corretta classificazione delle informazioni garantendone la Riservatezza, l'Integrità e Disponibilità.	

Nome documento	Descrizione	Ambito
ANNEX A - Gestione sicura della documentazione	Allegato delle Policy "PO_DCI_00" che definisce i criteri di classificazione e di gestione dei documenti.	
PR_GSU_00_Gestione accessi logici	Procedura che definisce le modalità di gestione degli accessi logici ai sistemi informatici in cui risiedono dati aziendali.	**Controllo degli accessi**
DC_PWD_00 Policy per la gestione della password	Standard di sicurezza delle informazioni che definisce le regole per la scelta, l'utilizzo e la custodia delle password di accesso ai sistemi aziendali da parte degli utenti dell'Organizzazione.	
PR_CHM_00_ Procedura Operativa Change Management	Procedura operativa per un corretto controllo del processo di gestione delle modifiche da apportare ai sistemi informatici aziendale.	**Sicurezza delle attività operative**
PR_CMN_00_Capacity Management	Procedura che descrive il processo di Capacity Management, i ruoli e le responsabilità al fine di gestire ed ottimizzare le risorse IT a supporto del business.	
PR_BCP_00_Business Continuity Plan_Spa	Procedura che descrive l'insieme delle attività pianificate e realizzate volte ad assicurare la continuità del servizio di conservazione e a ridurre gli impatti causati da disastri o incidenti di sicurezza a livelli accettabili.	
DC_DRO_00_Disaster Recovery Plan	Documento che identifica e descrive la soluzione di Disaster Recovery individuata e contrattualizzata a livello di Gruppo.	
PR_GVM_00_Gestione di Virus e Malware	Procedura che descrive le politiche di sicurezza adottate per la configurazione e la corretta gestione dei sistemi di protezione dai codici malevoli, al fine di proteggere il patrimonio informativo aziendale dall'azione di questi ultimi.	
PR_BKP_00_Salvataggio e Ripristino dei dati	Procedura che descrivere le fasi, le attività, i ruoli, le responsabilità ed i controlli per gestire in modo organico ed efficace il processo di backup e di restore dei dati.	
PR_LOG_00_Procedura Log Management	Procedura che definisce i criteri e le modalità, tecnologiche ed organizzative, necessarie a garantire un'efficace e sicura gestione dei file di log.	
PR_GVA_00_ Gestione delle vulnerabilità e debolezze di sicurezza	Procedura che definisce il processo da seguire per l'esecuzione delle attività di analisi delle vulnerabilità di sicurezza dei sistemi.	
PO_SSS_00_ Policy Per lo Sviluppo Sicuro del Software	Policy che fornisce i requisiti di sicurezza da adottare durante le fasi di sviluppo del software applicativo al fine di prevenire compromissioni del patrimonio informativo aziendale.	**Acquisizione, sviluppo e manutenzione dei sistemi**

Nome documento	Descrizione	Ambito
PR_GIV_00_ Gestione degli eventi e degli incidenti di sicurezza delle informazioni	Procedura che descrivere le attività relative al processo di Gestione degli Eventi e degli Incidenti di Sicurezza delle Informazioni, definendo i ruoli e le responsabilità nell'ambito dell'intero processo.	**Gestione degli incidenti relativi alla sicurezza delle informazioni**
PR_PGC_00_Procedura di Gestione della Conformità	Procedura che descrive la metodologia di conduzione delle verifiche di conformità volte a valutare e gestire nel tempo il livello di aderenza ai requisiti normativi esterni, nonché agli standard ed ai requisiti di sicurezza informatica.	**Conformità**
20140331_DPSS_Teamsystem	Documento Programmatico sulla Sicurezza.	
Manuale della Qualità	Documento che descrive le attività relative al sistema di gestione della Qualità, conformemente alla norma ISO9001:2008.	
DC_VII_00_Programma delle Verifiche Ispettive Interne	Documento nel quale è formalizzato il piano delle verifiche ispettive interne.	**Monitoraggio e auditing**
DC_GAC_00_Piano di Gestione azioni correttive	Documento nel quale è formalizzato il piano di gestione delle azioni correttive derivanti dalle verifiche ispettive interne.	
DC_KPI_00_Key Performance Indicator	Documento che definisce i Key Performance Indicator del SGSI	
Manuale Utente	Manuale che descrive le funzionalità operative lato Utente	**Servizio di Conservazione**
Manuale Operatore	Manuale che descrive le funzionalità riservate agli Operatori del Servizio Assistenza	
Manuale Amministratore	Manuale che descrive le funzionalità riservate all'Amministratore del Servizio	
Manuale Tecnico	Manuale che descrive i processi ed il monitoraggio del sistema di conservazione	

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 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 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 casi previsti dalla normativa.

In tale contesto, il Conservatore ha adottato uno specifico sistema di memorizzazione "NetApp SnapLock" che consente di creare volumi segregati, **impedendo l'alterazione o l'eliminazione dei file prima di una data prestabilita** che corrisponde la data di fine periodo di conservazione (funzionalità di software WORM). 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 all'interno del Piano della Sicurezza e nello specifico nella procedura di Change Management;

- 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 il Soggetto Produttore sono riportati nel Disciplinare Specificità del Contratto.

Torna al sommario

9.3 Soluzioni adottate in caso di anomalie

Le soluzioni adottate nel caso di anomalie sono selezionate in funzione della gravità dell'anomalia riscontrata. All'interno del Piano della Sicurezza 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 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.

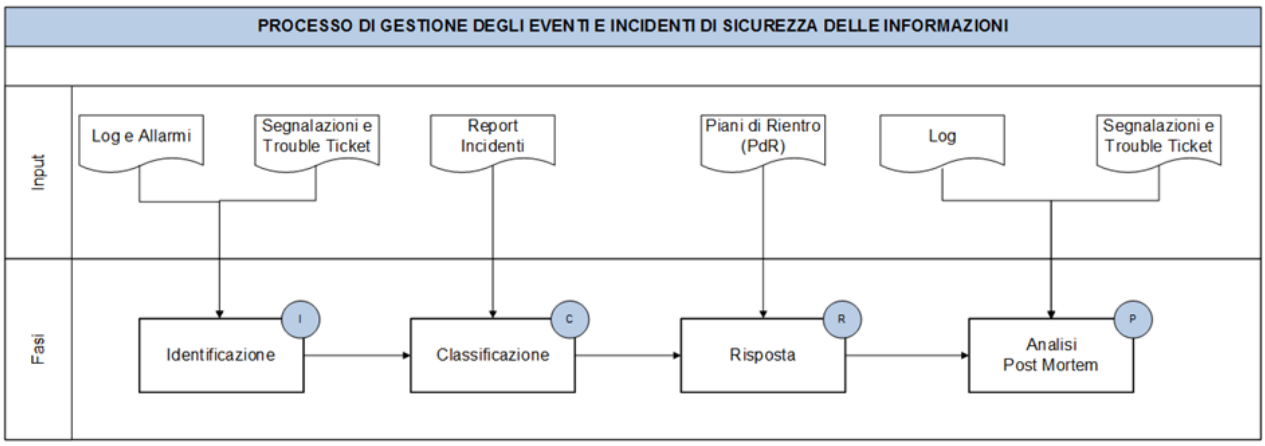

***Fig. 19** – Processo di Gestione degli incidenti*

A livello operativo, TeamSystem Service adotta una piattaforma di trouble ticketing basata su una soluzione proprietaria (i.e. WebRecall) 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.

Ulteriori dettagli relativi alla procedura di gestione degli eventi e incidenti di sicurezza sono riportati nel Piano della Sicurezza.

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 richiedere 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
• Richiesta del cliente/rivenditore • 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

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:

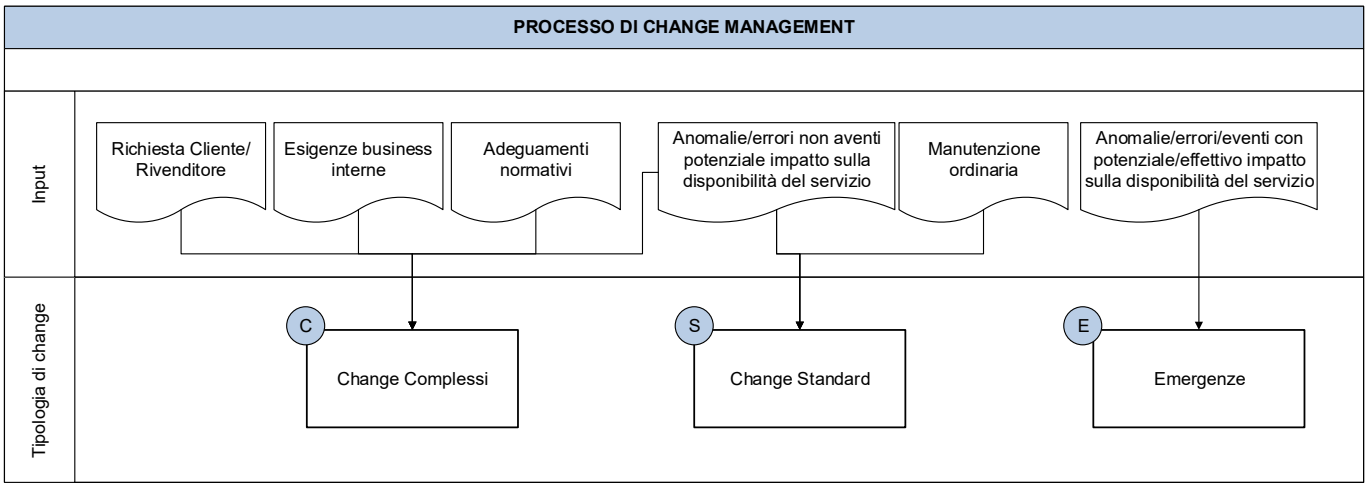

Figura 20 - *Processo di gestione dei cambiamenti – macro tipologie di changes*

I change di tipo applicativo e infrastrutturale sono approfonditi all'interno del documento descrivente le procedure di change management "*PR_CHM_00_Procedura Operativa Change Management*" e tutte le tipologie di change implementate sono censite all'interno del documento "*MD_CHM_05_Censimento CR*" fornendo il dettaglio di:

- ID progressivo della change;
- Natura (applicativa/infrastrutturale);
- Tipologia (Standard/Complesso/Emergenza);
- Descrizione;
- Stato attività;
- Percentuale Avanzamento;
- Note
- Data esecuzione UAT;
- Esito UAT;
- Data rilascio in esercizio;
- Esito rilascio in esercizio.

Torna al sommario