Manuale della Conservazione

Versione 1.0

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	09/02/2015	Antonio Campanile	*Responsabile divisione IT Engineering*
Verifica	18/02/2015	Antonio Nacca	Responsabile della Conservazione
Approvazione	18/02/2015	Antonio Nacca	Responsabile della Conservazione

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
1.0	18/02/2015	Prima stesura	-

Sommario

Indice delle Figure

1 SCOPO E AMBITO DEL DOCUMENTO

Il presente Manuale della Conservazione ha lo scopo di illustrare le caratteristiche del servizio di conservazione a norma erogato da CSA S.c. a r.l.

Come previsto dall'art 8 del D.P.C.M. del 3 Dicembre 2013 esso descrive sia aspetti tecnologici che organizzativi del processo di conservazione ed in particolare:

- i soggetti coinvolti nel processo ed i ruoli svolti dagli stessi. (Capitolo 5)
- la struttura organizzativa che interviene nel processo di conservazione (Capitolo 6)
- la descrizione del processo (Capitolo 8)
- la descrizione delle architetture e delle infrastrutture utilizzate (Capitolo 9)
- le misure di sicurezza adottate ed ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione. (Capitoli 9 e 10)

2 TERMINI E DEFINIZIONI

TERMINE	DEFINIZIONE
Accesso	Operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici
Accreditamento	Riconoscimento, da parte dell'Agenzia per l'Italia digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione
Affidabilità	Caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico
Aggregazione documentale informatica	Aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente
Archiviazione	Operazione con la quale documenti, fascicoli, registri, scritture in genere, vengono ordinatamente conservati. Risponde al bisogno di conservare il materiale documentario in modo razionale e uniforme per renderlo recuperabile alla ricerca. È passo propedeutico alla conservazione, per il quale non sono previsti particolari obblighi di legge
Archivio	Complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività
Archivio informatico	Archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico
Area organizzativa omogenea	Un insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445
Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico
Autenticità	Caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico

Base di dati	Collezione di dati registrati e correlati tra loro
Certificatore accreditato	Soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
Ciclo di gestione	Arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo
Classificazione	Attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati
Codice	Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni
Codice eseguibile	Insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici
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
Conservazione sostitutiva	Vedi conservazione a norma
Conservazione a norma	Processo che consente di conservare documenti e fascicoli in modalità informatica in attuazione secondo quanto previsto dall'art.44 del Decreto Legislativo del 7 marzo 2005 n. 82 ovvero garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità
Coordinatore della gestione documentale	Responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le **AOO** ai sensi di quanto disposto dall'articolo 50 comma 4 del D.P.R. 445/2000 nei casi di amministrazioni che abbiano istituito più Aree Organizzative Omogenee
Copia analogica del documento informatico	Documento analogico avente contenuto identico a quello del documento informatico da cui è tratto
Copia di sicurezza	Copia di *backup* degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 delle presenti regole tecniche per il sistema di conservazione

Destinatario	Identifica il soggetto/sistema al quale il documento informatico è indirizzato
Documento originale "non unico"	Documento originale il cui contenuto può essere ricavato attraverso altre scritture o documenti di cui siano obbligatorie la tenuta e la conservazione, anche se da parte di terzi. Sono inclusi tra questi, ad esempio, quelli considerati originali dallo stesso art. 2214 del codice civile già citato, come la fattura ricevuta da un imprenditore che, generata da un atto negoziale, assume il valore di dichiarazione di scienza. Essa viene emessa dal venditore del bene oggetto di transazione, che ne conserva copia; per la stessa è prescritta in forma obbligatoria la registrazione, a fini sia fiscali sia civilistici e contabili, adempimento che ne consente l'eventuale riscontro, anche se attraverso un processo di cognizione
Duplicazione dei documenti informatici	Produzione di duplicati informatici
Estratto per riassunto	Documento nel quale si attestano in maniera sintetica ma esaustiva fatti, stati o qualità desunti da dati o documenti in possesso di soggetti pubblici
Evidenza informatica	Una sequenza di simboli binari (*bit*) che può essere elaborata da una procedura informatica
Fascicolo informatico	Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del Decreto Legislativo del 7 marzo 2005 n. 82
Firma elettronica avanzata	Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati (art. 1 comma 1 lettera q-bis) Decreto Legislativo del 7 marzo 2005 n. 82)
Firma digitale	È un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici (art. 1 comma 1 lettera s) Decreto Legislativo del 7 marzo 2005 n. 82)
Formato	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione

	del file.
Funzionalità aggiuntive	Le ulteriori componenti del sistema di protocollo informatico necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni
Funzionalità interoperative	Le componenti del sistema di protocollo informatico finalizzate a rispondere almeno ai requisiti di interconnessione di cui all'articolo 60 del D.P.R. 28 dicembre 2000, n. 445
Funzionalità minima	La componente del sistema di protocollo informatico che rispetta i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445
Funzione di *hash*	Una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
Generazione automatica di documento informatico	Formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni
Identificativo univoco	Sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione
Immodificabilità	Caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso
Impronta	La sequenza di simboli binari (*bit*) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di *hash*
Insieme minimo di metadati del documento informatico	Complesso dei metadati, la cui struttura è descritta nell'allegato 5 del presente decreto, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta
Integrità	Insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato
Interoperabilità	Capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi
Leggibilità	Insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti
Log di sistema	Registrazione cronologica delle operazioni eseguite su di un sistema

	informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati
Manuale di conservazione	Strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 delle regole tecniche del sistema di conservazione
Manuale di gestione	Strumento che descrive il sistema di gestione informatica dei documenti di cui all'articolo 5 delle regole tecniche del protocollo informatico ai sensi delle regole tecniche per il protocollo informatico D.P.C.M. 31 ottobre 2000 e successive modificazioni e integrazioni
Marca temporale	Riferimento temporale che consente la validazione temporale, così come definita all'art. 1 comma 1 lettera i) D.P.C.M. del 30 marzo 2009. La marca temporale è opponibile a terzi
Memorizzazione	Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici
Metadati	Insiemi di dati associati ad un documento, ad un fascicolo o ad un'aggregazione documentale al fine di descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo
Pacchetto di archiviazione	Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del D.P.C.M. del 3 Dicembre 2013 e secondo le modalità riportate nel manuale di conservazione
Pacchetto di distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta
Pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione
Pacchetto informativo	Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare
Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza
Piano della sicurezza del sistema di gestione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei

informatica dei documenti	documenti da possibili rischi nell'ambito dell'organizzazione di appartenenza
Piano di conservazione	Strumento integrato con il sistema di classificazione per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445
Piano generale della sicurezza	Documento per la pianificazione delle attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza
Presa in carico	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione
Processo di conservazione	Insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 10 delle regole tecniche del sistema di conservazione
Produttore	Persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con il responsabile della gestione documentale
Protocollo TLS 1.0	È un protocollo di comunicazione che garantisce connessioni sicure attraverso la crittografia dei messaggi fra client e server. Esso consente alle applicazioni client/server di comunicare attraverso una rete in modo tale da prevenire il '*tampering*' (manomissione) dei dati, la falsificazione e l'intercettazione. È un protocollo standard IETF che, nella sua ultima versione, è definito nella RFC 5246, sviluppata sulla base del precedente protocollo SSL da *Netscape Communications*
Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore
Registrazione informatica	Insieme delle informazioni risultanti da transazioni informatiche o dalla presentazione in via telematica di dati attraverso moduli o formulari resi disponibili in vario modo all'utente
Registro particolare	Registro informatico di particolari tipologie di atti o documenti; nell'ambito della pubblica amministrazione è previsto ai sensi dell'articolo 53, comma 5 del D.P.R. 28 dicembre 2000, n. 445
Registro di protocollo	Registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti

Repertorio informatico	Registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche con cui si formano 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
Responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi	Dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione
Responsabile della conservazione	Soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 delle regole tecniche del sistema di conservazione
Responsabile del trattamento dei dati	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali
Responsabile della sicurezza	Soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza
Riferimento temporale	Informazione contenente la data e l'ora che viene associata ad uno o più documenti informatici
Scarto	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale
Sistema di classificazione	Strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni ed alle attività dell'amministrazione interessata
Sistema di conservazione a norma	Insieme di regole, procedure e tecnologie che assicura, dalla presa in carico dal produttore fino all'eventuale scarto, la conservazione a norma dei documenti e dei fascicoli in esso contenuti secondo le modalità previste dalla deliberazione CNIPA 11 del 19 febbraio 2004 e dalle regole tecniche di cui al D.P.C.M. 3 Dicembre 2013
Sistema di gestione informatica dei documenti	Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445; per i privati è il sistema che consente la tenuta di un documento informatico
Staticità	Caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri

	e gestite dal prodotto software utilizzato per la redazione
Transazione informatica	Particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche della base di dati
Testo unico	Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni
Ufficio utente	Riferito ad un'Area Organizzativa Omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico
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
Versamento agli archivi di Stato	Operazione con cui il responsabile della conservazione di un organo giudiziario o amministrativo dello Stato effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali

3 ACRONIMI ED ABBREVIAZIONI

- **AOO**: Area Organizzativa Omogenea
- **IPdA:** Indice del Pacchetto di Archiviazione
- **RdC**: Responsabile della Conservazione
- **Rdv**: Rapporto di Versamento
- **PdV**: Pacchetto di Versamento
- **PdA**: Pacchetto di Archiviazione
- **PdD**: Pacchetto di Distribuzione
- **SCN**: Sistema di Conservazione a Norma
- **SO**: Sistema Operativo
- **UTC**: Coordinated Universal Time
- **DBMS**: Database management system

4 NORMATIVA E STANDARD DI RIFERIMENTO

4.1 Normativa di riferimento

– Risoluzione Agenzia delle Entrate n.4/E del 19 Gennaio 2015 - Consulenza giuridica – Conservazione sostitutiva dei documenti informatici rilevanti ai fini tributari – Obbligo di invio dell'impronta dell'archivio informatico di cui all'art. 5 del D.M. 23 gennaio 2004 – Non sussiste.

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

– Decreto Ministero Economia e Finanze del 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.

– 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.

– D.P.C.M. 3 Dicembre 2013 pubblicato in GU il 12/03/2014 - 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 CAD di cui al decreto legislativo n. 82 del 2005.

- D.P.C.M. 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.
- D.P.C.M. 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.
- D.LGS 30 dicembre 2010, n. 235 - Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69.
- LEGGE 18 giugno 2009, n. 69 - Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile.
- Decreto Legge 29 novembre 2008, n. 185 (Decreto anticrisi) - Misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale. (GU n.280 del 29-11-2008 - Suppl. Ordinario n. 263).
- LEGGE 24 dicembre 2007, n. 244 - Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (legge finanziaria 2008).
- Circolare Agenzia delle Entrate 6 dicembre 2006, n. 36/E - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici e alla loro riproduzione in diversi tipi di supporto.
- Decreto Legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale.
- Decreto Legislativo 22 Gennaio 2004, n.42 - Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137.
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- D.P.R. 28 Dicembre 2000, n.445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.
- D.P.R. 22 luglio 1998, n. 322 - Regolamento recante modalità per la presentazione delle dichiarazioni relative alle imposte sui redditi, all'imposta regionale sulle attività produttive e all'imposta sul valore aggiunto, ai sensi dell'articolo 3, comma 136, della legge 23 dicembre 1996, n. 662.

- LEGGE 8 Agosto 1994, n. 489 - Conversione in legge, con modificazioni, del decreto-legge 10 giugno 1994, n. 357, recante disposizioni tributarie urgenti per accelerare la ripresa dell'economia e dell'occupazione, nonché per ridurre gli adempimenti a carico del contribuente.
- Decreto Legge del 10 giugno 1994 n. 357 - Disposizioni tributarie urgenti per accelerare la ripresa dell'economia e dell'occupazione, nonché per ridurre gli adempimenti a carico del contribuente.
- 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.

4.2 Standard di riferimento

- 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.

5 RUOLI E RESPONSABILITÀ

Nella tabella seguente sono riportati i nominativi delle persone che nell'ambito dell'organizzazione di CSA S.c. a r.l. ricoprono i ruoli principali previsti dal processo di conservazione. Per ogni ruolo sono indicati le attività di competenza, il periodo di copertura del ruolo e le eventuali deleghe.

Ruolo	Nominativo	Attività di competenza	Periodo nel ruolo	Eventuali deleghe
Responsabile del servizio di conservazione	Antonio Nacca	– Definizione e 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 14/10/2013 ad oggi	nessuna
Responsabile sicurezza dei sistemi per la conservazione	Antonio Campanile	– 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 ed individuazione e pianificazione delle necessarie azioni correttive	dal 14/10/2013 ad oggi	nessuna

Responsabile funzione archivistica di conservazione	Simona Marini	– Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato – Definizione 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 e del turismo per quanto di competenza	dal 14/10/2013 ad oggi	nessuna
Responsabile trattamento dati personali	Antonio Nacca	– 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 14/10/2013 ad oggi	nessuna
Responsabile sistemi informativi per la conservazione	Umberto Adamo	– Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione – Monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore	dal 14/10/2013 ad oggi	nessuna

		– 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		
Responsabile sviluppo e manutenzione del sistema di conservazione	Antonio Campanile	– 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 14/10/2013 ad oggi	nessuna

6 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

6.1 Organigramma di CSA S.c. a r.l.

Le strutture organizzative coinvolte nel servizio di conservazione sono riportate in Figura 1

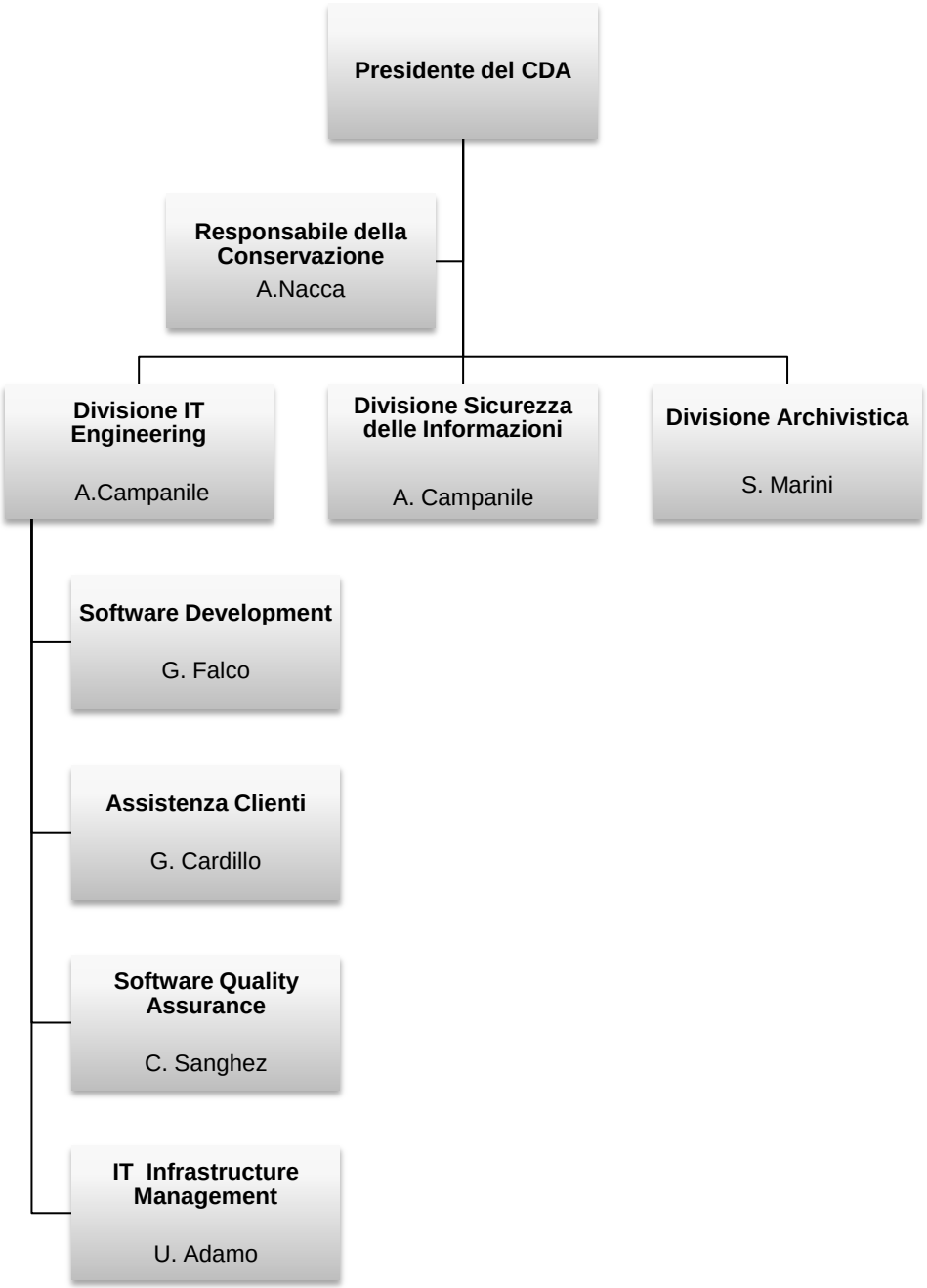

Figura 1 - Strutture di CSA S.C. A R.L. coinvolte nel servizio di conservazione

6.2 Strutture organizzative

Nel presente paragrafo si descrivono le principali attività/responsabilità delle strutture organizzative che a vario titolo intervengono nelle principali fasi del servizio di conservazione.

1. **IT Engineering**: È la divisione di CSA S.c. a r.l. che si occupa della progettazione, implementazione e manutenzione delle componenti software ed infrastrutturali attraverso le quali CSA S.c. a r.l. eroga i propri servizi. Le sotto-divisioni dell'IT Engineering coinvolte nel processo di conservazione sono:

   1.1. **Software Development**: si occupa della manutenzione correttiva, evolutiva ed adeguativa della componente software del sistema di conservazione finalizzate a garantire la correttezza delle elaborazioni, il continuo e regolare funzionamento dell'ambiente applicativo e la sua evoluzione ed adeguamento alle esigenze dei soggetti produttori.

   1.2. **Assistenza Clienti**: Si occupa dei servizi di assistenza, manutenzione che riguardano l'insieme degli interventi a supporto dell'operatività degli utenti del sistema di conservazione. Il servizio erogato dalla struttura è organizzato secondo due livelli.

   - **HelpDesk di I Livello**: fornisce supporto all'utente evadendo le richieste d'intervento pervenute attraverso i canali sincroni (es. telefono) ed asincroni (es. *trouble ticketing*).
   - **HelpDesk di II Livello**: rappresenta il livello di *escalation* delle richieste di assistenza tecnica-funzionale degli utenti per far fronte alle richieste che il primo livello non riesce ad evadere: composto da personale dotato di competenze funzionali e tecniche che pur mantenendo un alto livello di interscambiabilità è in grado di analizzare in dettaglio le segnalazioni pervenute individuando di volta in volta la causa del problema (sia esso funzionale o tecnico), attivando, dove necessario, il servizio di manutenzione correttiva e/o il servizio di Conduzione Sistemistica e le corrette procedure di escalation. La natura delle problematiche analizzate dall'HD di II livello possono essere di due tipi:
     - **applicative**: per tutte quelle chiamate ricevute dal primo livello e per le quali è richiesto un suo intervento in relazione ad analisi di problematiche complesse che comportano l'investigazione su basi dati, *log* di applicazioni o per richieste di intervento che comportano una "*problem determination"* e l'eventuale attivazione del servizio di Manutenzione Correttiva ed Adeguativa o anche Evolutiva;
     - **sistemistiche**: nel caso in cui le segnalazioni pervenute riguardino problematiche di natura tecnico/sistemistica il servizio ha il compito di attivare gli altri gruppi/fornitori, ciascuno responsabile per la propria area di competenza.

   1.3. **Software Quality Assurance**: controlla il processo di sviluppo ed applica le procedure di test per prevenire non conformità applicative. Si occupa del qualità della documentazione utente e tecnica, evita problemi e concorre a ridurre i *bug*. La divisione applica le *best practice* di

riferimento, utilizza metodologie, risorse e strumenti per garantire la qualità del software prodotto. In particolare, ad ogni avanzamento di versione e prima di ogni rilascio, la Divisione definisce un piano delle attività. Tale piano include: il perimetro funzionale dell'intervento (ovvero le funzionalità da testare) con le configurazioni HW e SW richieste per il test; la matrice di copertura con le indicazioni delle tipologie di test da fare (*black box*, *load test*, *stress test*, *security test*, etc.) e quelle da evitare; le risorse necessarie al test (persone e profili); i software e gli strumenti per i controlli automatici; la programmazione e la durata.

1.4. **IT Infrastructure Management**: si occupa della gestione operativa dell'infrastruttura hardware e software di base per l'erogazione dei servizi coinvolti nel processo di conservazione. Per la verifica del corretto funzionamento delle componenti infrastrutturali, la divisione utilizza un sistema distribuito di monitoraggio che misura lo stato di *salute* di tutti gli *asset* di interesse (server, servizi, applicativi, allarmi, hardware, dischi, ram, storage di backup, connessione dati e voce, ecc.) e segnala errori ed anomalie. Oltre al monitoraggio il sistema è in grado di eseguire azioni correttive mirate al ripristino, senza intervento umano, delle condizioni normali di funzionamento degli *asset* per cui sia stato rilevato uno stato critico. Il monitoraggio non si limita alla misurazione dei soli dati qualitativi, ma misura nel dettaglio l'operatività di ogni singolo *asset* fornendo una misurazione dettagliata dello stato di salute dell'intera infrastruttura.

2. **Divisione Sicurezza delle Informazioni**: coordina il *team* responsabile della corretta applicazione delle procedure interne a garanzia della disponibilità, riservatezza ed integrità dei dati in accordo alla certificazione ISO27001. Il team è coordinato dal **Chief Security Officer** che valuta i rischi, stabilisce le linee di intervento ed approva la politica sulla sicurezza. Il team è responsabile di applicare le revisioni alla politica della sicurezza stabilite dal **Chief Security Officer**. La **Divisione Sicurezza delle Informazioni** garantisce, inoltre, che i cambiamenti significativi alle infrastrutture per l'elaborazione e la sicurezza delle informazioni siano soggette al **Change Management**. I proprietari, i responsabili ed i gestori degli *asset* interessati al *cambiamento* sottomettono le richieste di aggiornamento alla **Direzione Software Development** della Divisione. Se le verifiche di qualità superano i test, allora il **Chief Security Officer** può autorizzare il passaggio dall'ambiente di test a quello di produzione. I seguenti cambiamenti sono considerati non significativi, in quanto di routine: aggiornamenti antivirus, aggiornamento **SO**, aggiornamenti software. Chi fa la richiesta per il cambiamento deve ottenere l'approvazione e deve indicare i costi di esercizio ed i potenziali benefici. La richiesta avviene tramite lo strumento di *tracking* delle attività della Divisione, sul progetto a cui l'*asset* appartiene. Affinché i cambiamenti proseguano e per garantire la continuità del servizio, vengono creati "punti di ripristino" e procedure di *roll back*.

2. **Divisione Archivistica:** La divisione si occupa della definizione e gestione del processo di conservazione definendo le aggregazioni documentarie e l'insieme dei metadati di conservazione dei documenti e dei fascicoli informatici. In accordo con il Responsabile della conservazione ed il

Responsabile dell'IT Engineering effettua analisi di tipo archivistico allo scopo di individuare nuove funzionalità del sistema di conservazione e/o miglioramenti delle quelle esistenti. La divisione si occupa, inoltre, della gestione dei rapporti con il Ministero dei beni e delle attività culturali e del turismo per quanto di competenza.

Il livello di coinvolgimento delle strutture su indicate nelle fasi del processo di conservazione è sintetizzato nella matrice RACI (*Responsible*, *Accountable*, *Consulted*, and *Informed*) riportata in Tabella 1 dove:

- R (Responsible): Indica il Responsabile dell'esecuzione dell'attività ovvero colui che la esegue materialmente.
- A (Accountable): Indica colui che la responsabilità finale di una certa attività. È la persona che prende le decisioni ed ha il potere di veto. Per ogni attività/fase è possibile assegnare una sola A.
- C (Consulted): Indica la persona/struttura che deve essere consultata prima di eseguire l'attività o prima di prendere decisioni esecutive.
- I (Informed): Indica la persona/struttura che deve essere informata dopo che una decisione o azione è stata intrapresa.

Attività/Responsabilità	Resp. Conservazione	Resp. IT Engineering	Resp. Archivista	Resp. sicurezza delle informazioni	Resp. Trattamento dei dati personali
Attivazione del Servizio	A	R	C	C	C
Presa in carico dei PdV	A-R	I	I		I
Preparazione e gestione dei PdA	A-R	I	C		
Preparazione e gestione dei PdD	A-R	I			
Scarto dei PdA	A	I	R		I
Chiusura servizio di conservazione al termine di un contratto	A	R	C	C	I
Manutenzione Correttiva del SCN	I	A-R		I	
Manutenzione Evolutiva del SCN	A	C-R	C	C	I
Manutenzione Adeguativa del sistema di conservazione	A	C-R	C	I	I
Change Management	C	R		A	I

Tabella 1 - Matrice RACI per il servizio di conservazione

7 OGGETTI SOTTOPOSTI A CONSERVAZIONE

7.1 Formati accettati per la conservazione

Ai fini della conservazione dei documenti è necessario scegliere formati che possano garantirne la leggibilità e la reperibilità durante tutto il loro ciclo di vita. Le caratteristiche di cui bisogna tener conto nella scelta sono:

1. apertura
2. sicurezza
3. portabilità
4. funzionalità
5. supporto allo sviluppo
6. diffusione

Un formato si dice "aperto" quando è conforme a specifiche pubbliche, cioè disponibili a chiunque abbia interesse ad utilizzare quel formato. La disponibilità delle specifiche del formato rende sempre possibile la decodifica dei documenti rappresentati in conformità con dette specifiche, anche in assenza di prodotti che effettuino tale operazione automaticamente. Questa condizione si verifica sia quando il formato è documentato e pubblicato da un produttore che per i formati definiti da organismi di standardizzazione riconosciuti (quali ISO e ETSI).

La sicurezza di un formato dipende dal grado di modificabilità del contenuto del file e dalla capacità di essere immune dall'inserimento di macroistruzioni o codice eseguibile.

Per portabilità si intende la facilità con cui i formati possano essere usati su piattaforme diverse, sia dal punto di vista dell'hardware che del software, inteso come sistema operativo.

Per funzionalità si intende la possibilità da parte di un formato di essere gestito da prodotti informatici, che prevedono una varietà di funzioni messe a disposizione dell'utente per la formazione e gestione del documento informatico.

Il supporto allo sviluppo rappresenta la modalità con cui si mettono a disposizione le risorse necessarie alla manutenzione e sviluppo del formato e i prodotti informatici che lo gestiscono (organismi preposti alla definizione di specifiche tecniche e standard, società, comunità di sviluppatori, ecc.).

Per diffusione si intende l'estensione dell'impiego di uno specifico formato per la formazione e la gestione dei documenti informatici. Questo elemento influisce sulla probabilità che esso venga supportato nel tempo, attraverso la disponibilità di più prodotti informatici idonei alla sua gestione e visualizzazione.

La scelta dei formati idonei alla conservazione, oltre al soddisfacimento delle caratteristiche suddette, deve essere tale da favorire le caratteristiche di immodificabilità e di staticità dei documenti così come previste

dalle regole tecniche. Per tale motivo sono adottati formati standard internazionali (*de jure* e *de facto*) o formati proprietari le cui specifiche tecniche siano pubbliche.

Di seguito l'elenco dei formati accettati dal sistema di conservazione:

- Portable Document Format (PDF/A)
- TIFF
- JPEG
- Office Open XML (OOXML)
- Open Document Format (ODF)
- Extensible Markup Language (XML)
- TXT
- Formati Messaggi di posta elettronica: RFC 2822/MIME (estensione .eml)

È possibile che un Produttore per esigenze specifiche richieda la conservazione di formati non compresi nell'elenco di cui sopra. In tal caso gli ulteriori formati sono concordati con il Responsabile della conservazione e inseriti nell'allegato "Specifica del contratto" dove sono riportati anche i riferimenti ai rispettivi *viewer*. Tutti i formati ammessi sono registrati e gestiti attraverso l'utilizzo di una struttura dati del Sistema di Conservazione a Norma denominata "registro dei formati".

7.2 Pacchetto di versamento

Il **pacchetto di versamento** è un pacchetto informativo inviato dal Produttore al sistema di conservazione secondo un formato predefinito e concordato con il Responsabile della conservazione. Il pacchetto di versamento si compone di:

- **Oggetto del versamento**: documento/i da conservare
- **File indice** contenente sia metadati descrittivi dell'Oggetto di versamento che le informazioni per la conservazione (Indice del Pacchetto di Versamento - **IPdV**)

Per quanto riguarda i metadati descrittivi il sistema di conservazione consente di associare ad ogni soggetto produttore una molteplicità di tipologie documentali ad ognuna delle quali è associato un insieme di informazioni minime in conformità con l'Allegato 5 del D.P.C.M. del 3 Dicembre 2013. Oltre ai metadati minimi il Produttore, in accordo con il Responsabile della Conservazione, può decidere di aggiungere ulteriori metadati di specializzazione del documento utilizzando la struttura "ExtraInfo" [Standard UNI-SINCRO 2010]. Per ogni tipologia documentale i metadati di base e quelli "ExtraInfo" dovranno essere esplicitati nell'allegato "Specifica del contratto".

Sia i metadati minimi che quelli "extra" sono oggetto di indicizzazione e quindi utilizzabili ai fini della ricerca dei documenti all'interno del sistema di Conservazione.

Si riportano di seguito i metadati minimi previsti dal Sistema di Conservazione.

7.2.1 Metadati minimi documento generico

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">

	<xs:complexType name="PersonaFisica">
		<xs:sequence>
			<xs:element name="Nome" type="xs:string" />
			<xs:element name="Cognome" type="xs:string" />
			<xs:element name="CodiceFiscale" type="xs:string" />
		</xs:sequence>
	</xs:complexType>

	<xs:complexType name="PersonaGiuridica">
		<xs:sequence>
			<xs:element name="DenominazioneImpresa" type="xs:string" />
			<xs:element name="PartitaIva" type="xs:string" />
			<xs:element name="Nome" type="xs:string" minOccurs="0" />
			<xs:element name="Cognome" type="xs:string" minOccurs="0" />
			<xs:element name="CodiceFiscale" type="xs:string" minOccurs="0" />
			<xs:element name="Ruolo" type="xs:string" minOccurs="0" />
		</xs:sequence>
	</xs:complexType>

	<xs:complexType name="Persona">
		<xs:choice>
			<xs:element name="PersonaFisica" type="PersonaFisica" />
			<xs:element name="PersonaGiuridica" type="PersonaGiuridica" />
		</xs:choice>
	</xs:complexType>

	<xs:complexType name="DocumentoGenerico">
		<xs:sequence>
			<xs:element name="DataChiusuraDocumento" type="xs:date" />
			<xs:element name="OggettoDocumento" type="xs:string" />
			<xs:element name="SoggettoProduttore" type="Persona" />
			<xs:element name="Destinatario" type="Persona" />
		</xs:sequence>
		<xs:attribute name="IDDocumento" type="xs:string" use="required" />
	</xs:complexType>

	<xs:element name="DocumentoGenerico" type="DocumentoGenerico" />

</xs:schema>
```

7.2.1.1 Descrizione struttura "Persona"

La struttura "Persona" generalizza in modo mutuamente esclusivo le strutture "PersonaFisica" (descritta in 7.2.1.2) e "PersonaGiuridica" (descritta in 7.2.1.3).

7.2.1.2 *Descrizione struttura "PersonaFisica"*

Informazione	Valori Ammessi	Tipo dato	Definizione
Nome	Testo libero	Alfanumerico 40 caratteri	Nome del soggetto
Cognome	Testo libero	Alfanumerico 40 caratteri	Cognome del soggetto
CodiceFiscale	Codice fiscale	Alfanumerico 16 caratteri	Codice Fiscale del soggetto

7.2.1.3 *Descrizione struttura "PersonaGiuridica"*

Informazione	Valori Ammessi	Tipo dato	Definizione
DenominazioneImpresa	Testo libero	Alfanumerico 40 caratteri	Ragione sociale del soggetto
PartitaIva	Partita IVA	Alfanumerico 11 caratteri	Partita Iva del soggetto
Nome	Testo libero	Alfanumerico 40 caratteri	Nome del soggetto
Cognome	Testo libero	Alfanumerico 40 caratteri	Cognome del soggetto
CodiceFiscale	Codice fiscale	Alfanumerico 16 caratteri	Codice Fiscale del soggetto
Ruolo	Testo libero	Alfanumerico 40 caratteri	Ruolo del soggetto

7.2.1.4 *Descrizione struttura "DocumentoGenerico"*

Informazione	Valori Ammessi	Tipo dato	Definizione
IDDocumento	Come da sistema di identificazione formalmente definito.	Alfanumerico 24 caratteri	Identificativo univoco e persistente è una sequenza di caratteri alfanumerici associata in modo univoco e permanente al documento informatico in modo da consentirne l'identificazione all'interno del SCN

DataChiusuraDocumento	Data	Data formato gg-mm-aaaa	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immodificabile
OggettoDocumento	Testo libero	Alfanumerico 250 caratteri	Metadato funzionale a riassumere brevemente il contenuto del documento o comunque a chiarirne la natura
SoggettoProduttore	Tipo complesso	Persona	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico
Destinatario	Tipo complesso	Persona	Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico

7.2.2 Metadati minimi documento amministrativo

L'insieme minimo dei metadati del documento amministrativo informatico è quello riportato agli articoli 9 e 21 del D.P.C.M. 3 dicembre 2013 e descritti nella Circolare N.60 del 23 gennaio 2013 dell'Agenzia per l'Italia Digitale. Detti metadati sono riportati di seguito:

- codice identificativo dell'amministrazione
- codice identificativo dell'area organizzativa omogenea
- codice identificativo del registro
- data di protocollo
- progressivo di protocollo
- impronta del documento
- oggetto
- mittente
- destinatario o i destinatari

Integrando i metadati di cui sopra con quelli previsti per il documento generico previsti dall'Allegato 5 del D.P.C.M. 3 dicembre del 2013 si ottiene la struttura seguente:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
	<xs:complexType name="Identificatore">
		<xs:sequence>
			<xs:element name="CodiceAmministrazione" type="xs:string" />
			<xs:element name="CodiceAoo" type="xs:string" />
			<xs:element name="CodiceRegistro" type="xs:string" />
			<xs:element name="NumeroRegistrazione" type="xs:integer" />
			<xs:element name="DataRegistrazione" type="xs:date" />
			<xs:element name="ImprontaDocumento" type="xs:string" />
		</xs:sequence>
	</xs:complexType>
	<xs:complexType name="DocumentoAmministrativo">
		<xs:complexContent>
			<xs:extension base="DocumentoGenerico">
				<xs:sequence>
					<xs:element name="Identificatore" type="Identificatore" />
				</xs:sequence>
			</xs:extension>
		</xs:complexContent>
	</xs:complexType>

</xs:schema>
```

7.2.2.1 *Descrizione struttura "Identificatore"*

Informazione	Valori Ammessi	Tipo dato	Definizione
CodiceAmministrazione	Codice Amministrazione	Alfanumerico 8 caratteri	Valore del codice dell'Amministrazione mittente o destinataria
CodiceAoo	Codice Aoo	Alfanumerico 8 caratteri	Valore del codice dell'Area Organizzativa Omogenea
CodiceRegistro	Testo	Alfanumerico 16 caratteri	Valore del codice identificativo del registro di protocollo
NumeroRegistrazione	Numero Registrazione	Intero	Numero del protocollo
DataRegistrazione	Data	Data formato ISO 8601 esteso aaaa-mm-gg	Data del protocollo
ImprontaDocumento	Testo	SHA-256	Impronta SHA-256 del documento

7.2.2.2 Descrizione struttura "DocumentoAmministrativo"

La struttura "DocumentoAmministrativo" estende la struttura "DocumentoGenerico" (descritta in 7.2.1.4) con le seguenti informazioni:

Informazione	Valori Ammessi	Tipo dato	Definizione
Identificatore	Tipo complesso	Identificatore	Contiene le informazioni identificative riferite alla segnatura di protocollo

7.2.3 Metadati minimi documento rilevante ai fini tributari

Il Decreto Ministero Economia e Finanze del 17 giugno 2014 (art.3 comma b) definisce, per i documenti rilevanti ai fini tributari (di cui all'Allegato 1 del Provvedimento Attuativo Agenzia delle Entrate del 25 ottobre 2010, n. 2010/143663) l'insieme minimo dei metadati di seguito riportato:

- cognome
- nome
- denominazione
- codice fiscale
- partita Iva
- data documento
- periodo d'imposta
- tipo documento (vedi Allegato 1 del Provvedimento Agenzia delle Entrate n.20107143663)

Questi metadati vanno ad integrarsi a quelli previsti per il documento generico previsti dall'Allegato 5 del D.P.C.M. 3 dicembre del 2013 ottenendo la seguente struttura:

```
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">

	<xs:complexType name="PeriodoImposta">
		<xs:sequence>
			<xs:element name="DataInizio" type="xs:date" />
			<xs:element name="DataFine" type="xs:date" />
		</xs:sequence>
	</xs:complexType>

	<xs:simpleType name="TipoDoc">
		<xs:restriction base="xs:integer">
			<xs:minInclusive value="1" />
			<xs:maxInclusive value="999999" />
		</xs:restriction>
	</xs:simpleType>

	<xs:complexType name="DocumentoTributario">
		<xs:complexContent>
			<xs:extension base="DocumentoGenerico">
				<xs:sequence>
				   <xs:element name="PeriodoImposta" type=" PeriodoImposta"/>
				   <xs:element name="TipoDoc" type="TipoDoc"/>
				</xs:sequence>
			</xs:extension>
		</xs:complexContent>

	</xs:complexType>

	<xs:element name="DocumentoTributario" type="DocumentoTributario" />
</xs:schema>
```

7.2.3.1 *Descrizione struttura "PeriodoImposta"*

Informazione	Valori Ammessi	Tipo dato	Definizione
DataInizio	Data	Data formato gg-mm-aaaa	Data iniziale del periodo di riferimento dell'imposta
DataFine	Data	Data formato gg-mm-aaaa	Data finale del periodo di riferimento dell'imposta

7.2.3.2 *Descrizione struttura "DocumentoTributario"*

La struttura "DocumentoTributario" estende la struttura "DocumentoGenerico" (descritta in 7.2.1.4) con le seguenti informazioni:

Informazione	Valori Ammessi	Tipo dato	Definizione
PeriodoImposta	Tipo complesso	PeriodoImposta	L'anno fiscale e quello solare potrebbero non coincidere è necessario, quindi, esplicitare le date di inizio e fine dell'anno fiscale a cui il documento fa riferimento
TipoDoc	da 1 a 999999	Intero	Identificativo univoco del tipo di documento di appartenenza

7.3 Pacchetto di archiviazione

Il **pacchetto di archiviazione** è un pacchetto informativo composto dalla trasformazione di uno o più PdV a scopo di conservazione. Ogni PdA prevede un file indice chiamato "Indice del Pacchetto di Archiviazione" (**IPdA**). La struttura dell'IPdA è riportata nell'allegato 4 del D.P.C.M. del 3 Dicembre 2013. Essa fa riferimento allo standard UNI SInCRO 2010 - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010), che è lo standard nazionale riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione.

Di seguito si riportano le differenze di nomenclatura fra lo standard e la struttura riportata nel D.P.C.M.:

Allegato 4 del D.P.C.M. 3/12/2013	UNI SINCRO 2010
IPdA – Indice del Pacchetto di Archiviazione	**IdC** – Indice di Conservazione
PdA – Pacchetto di Archiviazione	**VdC** – Volume di Conservazione
DescGenerale	**SelfDescription**
ExtraInfo	**MoreInfo**
Soggetto	**Agent**

Tabella 2 - Differenze nomenclatura fra D.P.C.M. 3/12/2013 e UNI SINCRO 2010

L'IPdA è corredato da un riferimento temporale e dalla firma digitale del Responsabile della Conservazione; rappresenta l'evidenza informatica associata ad ogni PdA e contiene le seguenti informazioni:

- **informazioni inerenti il Pacchetto di Archiviazione**, in particolare: un identificatore del PdA, eventuali riferimenti ad altri PdA da cui deriva il presente, informazioni relative ad una eventuale tipologia/aggregazione (di natura logica o fisica) cui il PdA appartiene ed infine un eventuale elemento "ExtraInfo" che consente di introdurre metadati soggettivi relativi al PdA;

- **indicazione di uno o più raggruppamenti di uno o più file che sono contenuti nel PdA**. È possibile raggruppare file sulla base di criteri di ordine logico o tipologico ed assegnare ad ogni raggruppamento/singolo file le informazioni di base ed un eventuale elemento "ExtraInfo" che consente di introdurre metadati definiti del Produttore. Ogni elemento "file" contiene l'impronta attuale dello stesso, ottenuta con l'applicazione di un algoritmo di *hash* e un'eventuale impronta precedentemente associata ad esso: in questo modo è possibile ad esempio gestire il passaggio da un algoritmo di *hash* diventato non più sicuro ad uno più robusto;
- **informazioni relative al processo di produzione del PdA,** come: l'indicazione del nome e del ruolo dei soggetti che intervengono nel processo di produzione del PdA (es. responsabile della conservazione, delegato, pubblico ufficiale ecc.), il riferimento temporale adottato (generico riferimento temporale o marca temporale), l'indicazione delle norme tecniche e giuridiche applicate per l'implementazione del processo di produzione del PdA ed, infine, anche per il processo, un elemento "*ExtraInfo*" che consente di aggiungere dati soggettivi relativi al processo.

La flessibilità della struttura consente di gestire situazioni in cui è necessario ordinare in modo diverso gli indici creandone di nuovi, accorpando o frammentando le informazioni contenute negli IPdA precedenti, oppure generare uno nuovo IPdA facendo riferimento ad una precedente versione dello stesso: questo è il caso in cui si desidera effettuare migrazioni a causa di evoluzioni tecnologiche (migrazione dei formati).

L'elemento "*ExtraInfo*" è utilizzato per la specializzazione dei metadati che può essere relativa al dominio applicativo (sanità, banche, etc.) o alla tipologia documentaria (fatture, circolari, rapporti diagnostici, etc.).

7.4 Pacchetto di distribuzione

Il **pacchetto di distribuzione** è un pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta. È derivato da uno o più PdA, o da una parte di un singolo PdA. Ogni PdD prevede un file indice chiamato "Indice del Pacchetto di Distribuzione" (**IPdD**) che contiene informazioni riguardanti i PdA di cui si compone. La struttura dell'IPdD è anch'essa conforme allo standard UNI SInCRO 2010. Nell'ipotesi di coincidenza fra PdA e PdD l'IPdD coincide con l'IPdA.

8 IL PROCESSO DI CONSERVAZIONE

Il sistema di conservazione prevede due tipi di interfaccia: un'interfaccia utente web-based ed un'interfaccia applicativa (web-services); quest'ultima consente l'integrazione del servizio di conservazione con sistemi informatici terzi (ad esempio il sistema di gestione documentale del produttore). Le specifiche di dettaglio di entrambe le interfacce sono allegate al contratto di servizio stipulato con il produttore.

Tutte le fasi del processo di conservazione e le operazioni effettuate dagli utenti del sistema, sono tracciate attraverso scrittura sui opportuni file di log le cui modalità di gestione e conservazione sono descritte nel paragrafo 9.4.2.

Nei paragrafi seguenti si procederà ad una descrizione dettagliata delle macrofasi di cui è composto il processo di conservazione.

8.1 Presa in carico dei Pacchetti di Versamento

La fase "Presa in carico" dei PdV (**PIC**) consente ai soggetti produttori di trasferire i PdV al Sistema di Conservazione. La PIC rappresenta un trasferimento legalmente valido della custodia del contenuto del PdV dal Produttore al SCN a conclusione della quale il sistema genera il "Rapporto di Versamento" (**RdV**). Il RdV è relativo ad uno o più PdV ed è un documento informatico che attesta l'avvenuta presa in carico da parte del SCN dei PdV inviati dal Produttore. Il RdV, a cui è associato un identificativo univoco (UID) all'interno del SCN, contiene un "riferimento temporale" specificato con riferimento alla UTC, le impronte associate ai PdV versati e per ognuno di essi l'esito del versamento. Il RdV viene firmato digitalmente dal Responsabile della Conservazione ed inviato al Produttore.

La fase di "Presa in carico" si articola nei seguenti passi:

1. Il Produttore invia uno o più PdV al SCN attraverso web services SOAP su canale Https/TLS 1.0
2. Il SCN effettua una prima verifica formale (ad esempio verifica dei metadati minimi associati alla tipologia documentale, verifica dei valori ammessi per i singoli metadati, etc.)
3. Se l'esito della Verifica Formale è "KO" il PdV è rifiutato dal SCN e la fase si conclude. Se, invece, la verifica è "OK" il SCN prende in carico il PdV fornendo come risposta un identificativo univoco dello stesso.
4. Il PdV è sottoposto ad una verifica di qualità da parte del SCN. In questa fase il sistema valuta aspetti di dettaglio del PdV quali ad esempio: verifica dell'impronta dei file, verifica delle firme digitali, verifica dei formati, etc.
5. Se la verifica è "KO" il PdV viene posto in uno stato "Scartato" ed al Produttore viene inviata una "notifica di scarto". Viceversa, se la verifica è "OK" il PdV viene posto in uno stato "Valido - In attesa di archiviazione".
6. Il SCN genera il RdV
7. Il RdC firma il Rapporto di Versamento

8. Il SCN invia il RdV al Produttore

Il flusso della fase di "presa in carico" è mostrata sinteticamente in Figura 2

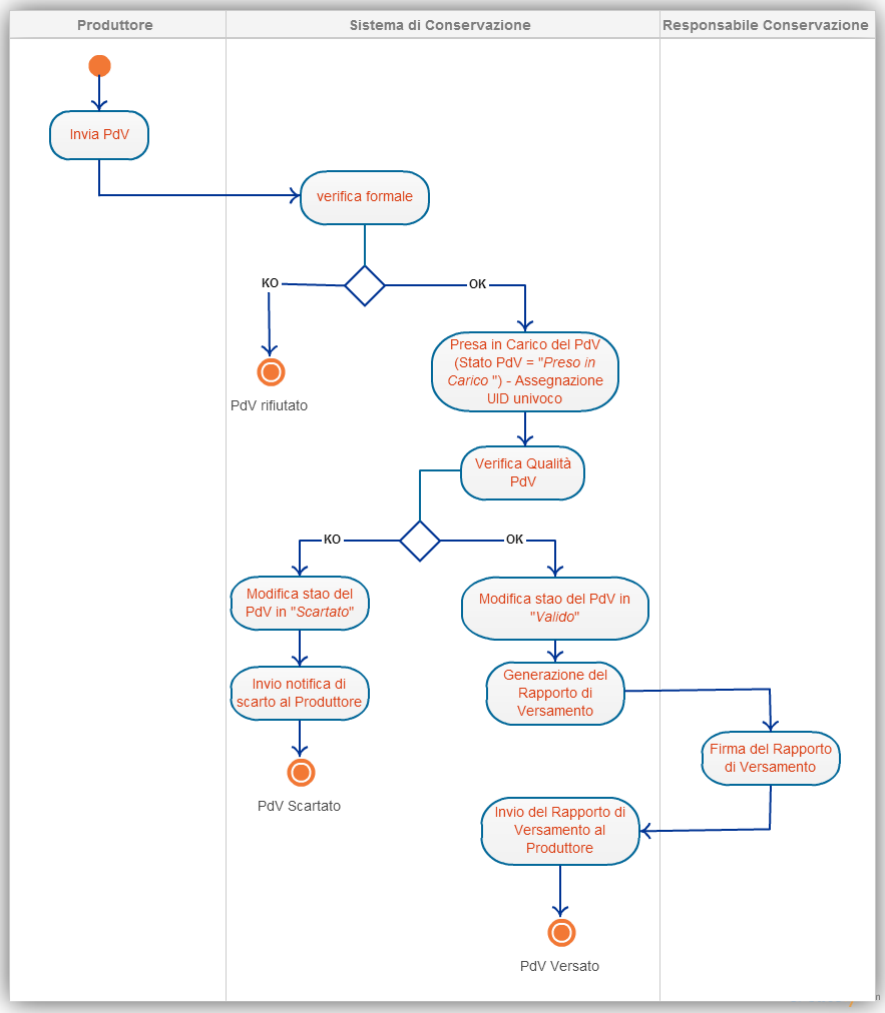

Figura 2 - Fase di Presa in carico dei PdV

8.2 Preparazione ed archiviazione dei PdA

La fase di archiviazione consente di trasformare/aggregare i PdV in PdA ai fini dell'archiviazione a norma. Essa si articola nei seguenti passi:

1. Preparazione dei PdA: in questa fase il SCN crea uno o più PdA a partire dai PdV che si trovano nello stato "Valido". Ogni PdA si compone di uno o più PdV. Per ogni PdA viene creato l'Indice del Pacchetto di Archiviazione (IPdA) la cui struttura è conforme allo Standard UNI 11386:2010 – SInCRO. La creazione dei PdA può avvenire in modalità automatica e periodica secondo quanto previsto nell'Allegato "specifica del contratto" oppure su esplicita richiesta da parte del RdC. Alla fine di questa fase i PdA sono posti nello stato "nuovo – in attesa di firma del RdC".
2. Il Responsabile della Conservazione (RdC) appone la firma digitale ai PdA attraverso procedura manuale o automatica. Di conseguenza il SCN pone i PdA firmati in stato "In attesa di Marcatura"

3. Il SCN appone la marca temporale ai PdA firmati dal RdC e trasferisce gli stessi nello storage definitivo ponendoli nello stato “archiviati”.

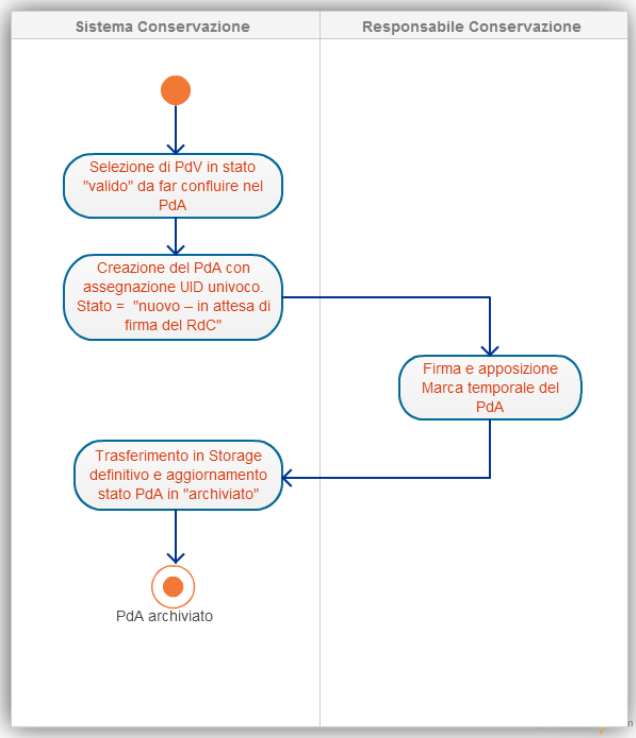

Figura 3 - Preparazione ed archiviazione dei PdA

Il sistema di conservazione può, opzionalmente, aggregare più PdA in un ulteriore PdA di secondo livello anch’esso firmato dal RdC e marcato temporalmente. L’aggregazione può essere fatta riferendosi ad un certo periodo temporale. Ad esempio, per i documenti a rilevanza tributaria l’aggregazione è effettuabile per Produttore e per periodo d’imposta. In caso di aggregazione il mantenimento della validità legale dei PdA di primo livello avverrà attraverso aggiornamento della marca temporale del PdA di secondo livello.

8.3 Preparazione e gestione del pacchetto di distribuzione ai fini dell’esibizione

Il sistema di conservazione consente ai soggetti autorizzati l’accesso diretto ai documenti in esso conservati attraverso l’utilizzo di *web services* oppure di una opportuna interfaccia applicativa *web based*. Entrambe le modalità di accesso utilizzano canali sicuri Https su protocollo TLS 1.0. La profilatura degli utenti e delle relative regole di accesso ai documenti è definita sulla base delle specifiche fornite dal Produttore.

La selezione dei documenti di interesse avviene attraverso un’operazione di ricerca esplicitando i metadati del documento e/o la tipologia documentale e/o l’identificativo del Pacchetto di Versamento e/o l’identificativo del Pacchetto di Archiviazione.

Individuati i documenti di interesse, l’utente abilitato può richiedere al SCN un’esibizione a norma dei documenti indicando alcune opzioni che riguardano l’inclusione o meno nel PdD dei seguenti oggetti: file

Indice dei Pacchetti di Archiviazione in cui sono contenuti i documenti, file Indice dei Pacchetti di Versamento con cui i documenti sono stati trasferiti nel sistema di conservazione, i Rapporti di Versamento relativi ai Pacchetti di Versamento.

Il Pacchetto di Distribuzione si compone quindi dei seguenti oggetti:

- Indice del Pacchetto di distribuzione (IPdD): Costruito in conformità con lo standard UNI 11386:2010 – SInCRO
- I documenti di interesse
- L'IPdA dei PdA in cui i documenti sono contenuti (opzionale)
- L'IPdV dei PdV con cui i documenti sono stati trasferiti al SCN (opzionale)
- I Rapporti di versamento dei PdV (opzionale)

Indipendentemente dai contenuti opzionali selezionati dall'utente, nell'IPdD sono sempre indicati, oltre ai metadati dei documenti di cui si compone il Pacchetto di Distribuzione, anche quelli dei PdA e PdV di riferimento dei documenti stessi.

Prima dell'invio, l'utente può decidere se l'IPdD deve essere firmato digitalmente dal Responsabile della Conservazione.

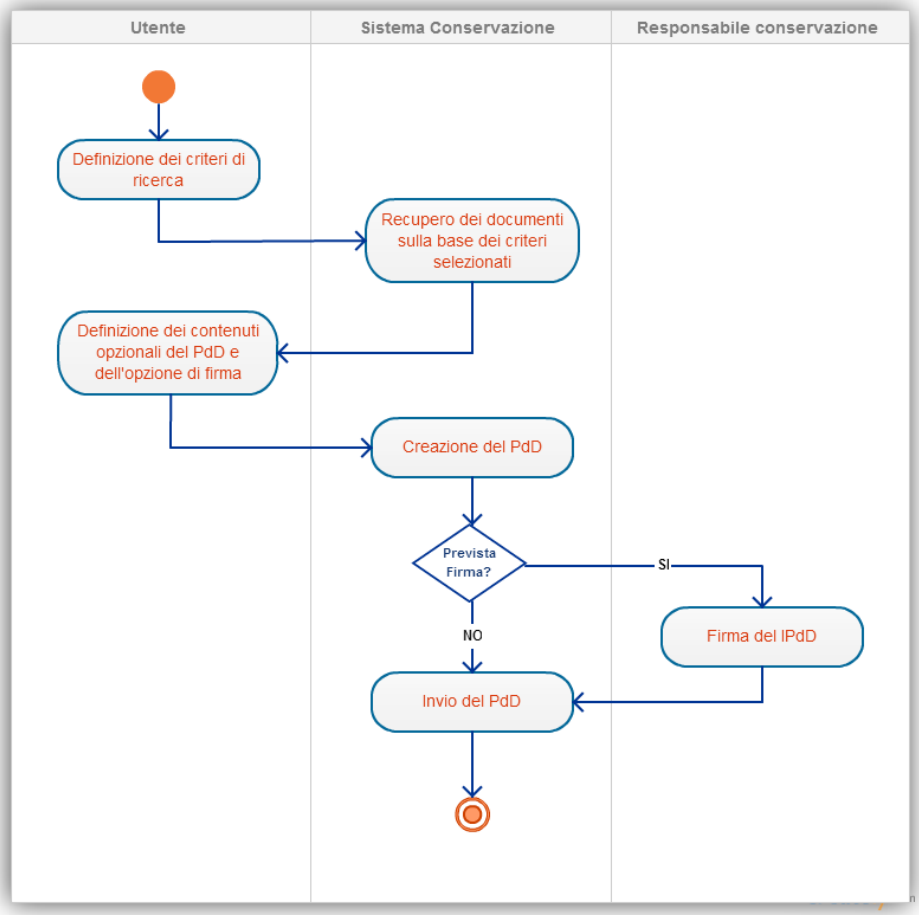

Figura 4 - Preparazione e gestione dei PdD

8.4 Produzione di duplicati e copie informatiche

La creazione di duplicati di documenti informatici può essere effettuata secondo le modalità di cui al paragrafo 8.3. Nei casi di copie cartacee di documenti informatici l'art. 23 del Codice dell'amministrazione digitale prevede l'intervento di un Pubblico Ufficiale che attesti la conformità della copia cartacea all'originale digitale. In tale evenienza CSA S.c. a r.l. garantisce al Pubblico Ufficiale l'assistenza e le risorse necessarie per l'espletamento delle attività necessarie.

L'operazione di **duplicazione** ovvero la copia di uno o più documenti da un supporto di memorizzazione ad un altro, senza alterarne la rappresentazione informatica, avviene per copie di *backup* e per la replicazione automatica dei documenti su più nodi di memorizzazione ai fini della *Business Continuity*. Per tale processo non è previsto l'intervento di un Pubblico Ufficiale.

L'operazione di **copia** di uno o più documenti con alterazione della loro rappresentazione informatica può rendersi necessaria in alcuni casi come ad esempio per obsolescenza dei formati. Tale tipo di copia si conclude con l'apposizione, sull'insieme dei documenti o su una evidenza informatica contenente una o più impronte dei documenti, del riferimento temporale e della firma digitale da parte del Responsabile della Conservazione e nel caso di documenti originali unici, con l'ulteriore apposizione del riferimento temporale e della firma digitale da parte di un Pubblico Ufficiale.

8.5 Scarto dei pacchetti di archiviazione

Per ogni tipologia documentale gestita dal SCN, il Produttore ed il Responsabile della Conservazione ne definiscono i tempi di conservazione esplicitandoli nell'allegato "specifica di contratto". Sulla base di questa associazione tipologia documentale – tempi di conservazione il SCN consente la gestione dello "scarto d'archivio" ovvero l'eliminazione controllata dei documenti i cui termini di conservazione risultano esauriti.

Periodicamente, dunque, il SCN propone al Produttore l'elenco dei documenti da scartare. Quest'ultimo può, per ognuno dei documenti dell'elenco, confermarne lo scarto oppure decidere di prorogarne i termini di conservazione. Conclusa tale operazione il sistema genera un documento "proposta di scarto".

Se il Produttore è una organizzazione privata, per poter procedere allo scarto effettivo dei documenti, la "proposta di scarto" deve essere firmata digitalmente da un suo Responsabile designato a tale funzione ed individuato all'atto della definizione del contratto di servizio.

In caso di Ente Pubblico, invece, sarà necessario fornire al Responsabile della Conservazione di CSA S.c. a r.l. oltre alla proposta di scarto firmata digitalmente anche il "nulla osta allo scarto" rilasciato dall'autorità vigilante.

Per gli Enti Pubblici, infatti, la procedura da rispettare è quella prescritta dall'art. 35 del D.P.R. n. 1409/63 come modificato e sostituito dall'art. 21, comma 1 lettera d del D. Lgs 42/2004. L'iter del procedimento amministrativo a norma di legge può essere sintetizzato come segue:

- Definizione della proposta di scarto
- Redazione e approvazione della determina di scarto da parte del Dirigente responsabile dell'Ente
- Richiesta di nulla osta alla Soprintendenza Archivistica competente per territorio

Superata la fase formale di approvazione della proposta, il Responsabile della Conservazione o suo delegato procede a rendere operativo lo scarto attraverso apposita funzione del SCN.

In risposata ad una richiesta di scarto, il SCN, come primo passo, effettua un raggruppamento dei documenti per PdA di appartenenza. Per ognuno dei PdA interessati dallo scarto è possibile che si presenti uno dei due seguenti scenari:

1. tutti i documenti del PdA devono essere scartati
2. solo alcuni documenti del PdA devono essere scartati

Nel primo caso il SCN elimina fisicamente i file di tutti i documenti del PdA, aggiorna i metadati dell'IPdA ponendone lo stato a "scartato". Il file relativo all'IPdA viene comunque conservato dal sistema.

Nel secondo caso, invece, il sistema effettua le seguenti operazioni:

- Eliminazione fisica dei file relativi ai documenti da scartare dal PdA di appartenenza
- Aggiornamento del metadato "stato" del documento scartato ponendolo a "scartato"
- Creazione di un nuovo Pacchetto di Archiviazione con relativo indice contenente i documenti non scartati e l'indice del Pacchetto di archiviazione originario
- Firma e marcatura da parte del Responsabile della Conservazione del nuovo PdA

Nel caso 1 pur conservando l'IPdA, non sarà necessario gestirne la validità legale nel tempo in quanto esso fa riferimento a documenti che sono stati eliminati dal sistema. Nel caso 2, invece, è possibile che per motivi di ottimizzazione, i documenti non scartati inizialmente appartenenti a PdA diversi siano aggregati in un unico nuovo PdA.

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

Il Sistema di Conservazione è in grado di garantire l'interoperabilità con altri sistemi in quanto esso produce ed accetta rispettivamente Pacchetti di distribuzione e di versamento conformi allo standard UNI 11386:2010 – SInCRO.

In caso di trasferimento dei documenti verso altri sistemi di conservazione i PdA sotto forma di PdD sono resi disponibili secondo le modalità di cui al paragrafo 8.3., ovvero attraverso *download* da interfaccia applicativa web oppure attraverso invocazione di *web services*.

Ulteriori modalità di riconsegna dei documenti al Produttore possono essere concordate fra quest'ultimo e il Responsabile della Conservazione. In particolare, nel caso in cui la riconsegna preveda l'utilizzo di supporti

di memorizzazione esterni su questi verranno applicate le procedure previste dalla certificazione ISO:IEC 27001:2013 e descritte nel manuale per la sicurezza delle informazioni nei seguenti documenti:

- Risk management - doc 4.4
- External parties: information security procedure doc 6.8
- Removal off-site of information assets - doc 9.12
- Information security classification guidelines - doc 7.6
- Secure disposal of storage media - doc 9.11
- Schedule of required cryptographic controls - doc 12.1
- Data protection and privacy policy statement - doc 15.6

Le attività previste a fine contratto, compresi termini e modalità di riconsegna dei documenti, sono dettagliatamente descritte nel contratto di servizio.

9 IL SISTEMA DI CONSERVAZIONE

Il sistema di conservazione di CSA S.c. a r.l. è stato realizzato ponendo particolare attenzione ad aspetti quali la sicurezza delle informazioni e degli accessi, la disponibilità dei servizi offerti, la scalabilità, gli standard di settore e l'indipendenza da tecnologie proprietarie. Nei paragrafi seguenti si descrivono i moduli che compongono il sistema di conservazione.

9.1 Componenti Logiche

In Figura 5 è schematizzata l'architettura logica del sistema che si compone di un insieme di livelli e moduli descritti di seguito.

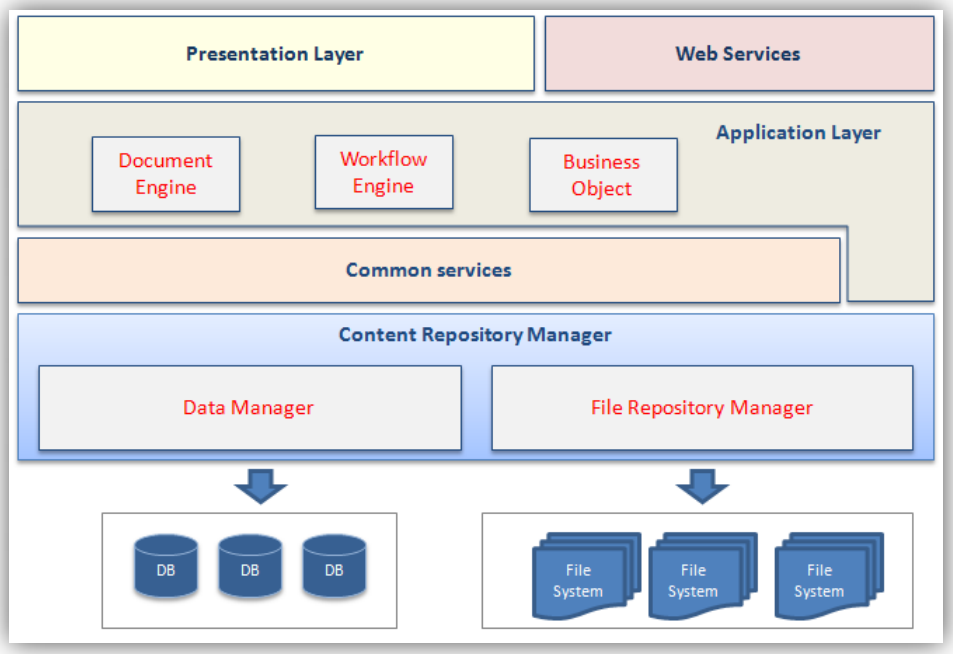

Figura 5 - Architettura logica del sistema di conservazione

9.1.1 Presentation Layer

È lo strato responsabile della visualizzazione della *Graphical User Interface* (GUI) con la quale l'Utente può effettuare le sue richieste e ricevere il risultato delle stesse. La modalità di interazione attualmente disponibile è quella *web based*. L'utente, dunque, può interagire con il sistema attraverso l'utilizzo di un qualsiasi *browser web*.

9.1.2 Web Services

Per consentire l'interoperabilità con sistemi esterni, il SCN dispone di un set di servizi web. I servizi sono sia di tipo **REST** che **SOAP**.

9.1.3 Application Layer

Lo strato applicativo si compone dei moduli che consentono l'esecuzione delle funzionalità *core* del sistema. Esso comprende: il "Document Engine" che è il modulo di gestione delle funzionalità documentali del SCN quali ad esempio: gestione tipologie documentali, definizione e gestione schemi di metadati, ricerca, fascicolazione, etc; il modulo "Workflow Engine" che consente la definizione, l'esecuzione e la gestione dei processi di business in esso codificati; i "Business Object" ovvero i componenti software di back-end che implementano la logica di funzionamento del sistema.

9.1.4 Common Services

È lo strato che racchiude un insieme di servizi, sincroni ed asincroni, di supporto alle componenti dell'"*Application Layer*". In particolare: l'"*Indexer*" che consente, nei casi previsti, l'indicizzazione del contenuto dei documenti presenti all'interno del sistema ai fini di una ricerca *full-text*; il "Mailer/PEC Manager" a cui è delegato l'invio/ricezione dei messaggi di posta elettronica ordinaria e certificata. Il "*Signer*" che si occupa, nel caso di utilizzo di firma automatica, di firmare digitalmente ed apporre la marca temporale ai documenti, interfacciandosi con i dispositivi remoti di firma (ad esempio HSM) e con i servizi esterni di marca temporale.

9.1.5 Content Repository Layer

È l'insieme di moduli e sottosistemi che garantiscono la persistenza delle informazioni in tutte le loro forme. Si compone essenzialmente di due moduli: il "*Data Manager*" ed il "*File Repository Manager*".

Il Data Manager (DM) consente la persistenza, la ricerca ed il recupero, su database relazionali, dei dati descrittivi degli oggetti archiviati e di tutte le informazioni utili al funzionamento del sistema di conservazione. Esso utilizza un **ORM** (Object Relational Mapping) ed è dunque indipendente dal particolare DBMS utilizzato. Il **File Repository Manager (FRM)** è il modulo che espone servizi specifici per la memorizzazione e la gestione dei file. Esso ha lo scopo di rendere trasparente allo strato applicativo problematiche riguardanti la gestione di copie di sicurezza dei file e di fornire uno risorsa di *storage* affidabile e scalabile. Il FRM gestisce, dunque, le problematiche riguardanti la replica di sicurezza dei file su più nodi (SAN e/o NAS) di memorizzazione geograficamente distribuiti, la scalabilità attraverso l'utilizzo di tecniche di "*sharding*" dei file su più *cluster*, il *failover* automatico dei nodi, etc.

9.2 Componenti Tecnologiche

Il sistema di conservazione a norma è completamente scritto in tecnologia *J2EE* ed utilizza per il suo funzionamento *middleware* standard ed *open source*. L'affidabilità dei servizi erogati dai livelli logici individuati nel paragrafo precedente è garantita da configurazioni "clusterizzate" ad ogni livello dell'architettura.

In particolare, il "*Presentation Layer*" utilizza un cluster di *Apache web server* che funge anche da *load balancer* verso il *middleware* dell'"*Application Layer*" a sua volta costituito da un *cluster* di *Apache Tomcat*. Nel livello applicativo si utilizzano *framework* quali *Spring* e *JSF2.0*

I *Web services* si basano sul *framework Apache CXF*, mentre il *layer* "*Common Services*" utilizza il motore *Apache Solr*, le librerie *Apache Tika* e il *Message Oriented Middleware Apache ActiveMQ*.

Il "*Content Repository Manager*" fa uso del *framework* di *Hibernate ORM* che, come detto nel paragrafo precedente, consente l'indipendenza del sistema dal DBMS. È possibile, quindi, utilizzare i DBMS più diffusi tra cui, *MySQL*, *Oracle*, *Microsoft SQL Server*, *PostgreSQL*, etc. Allo stato attuale si utilizza un cluster di *Oracle MySQL Server*. Infine, poiché il sistema è scritto completamente in *Java* esso è portabile su più piattaforme ed installabile, dunque, sui sistemi operativi più diffusi. Attualmente, tutti i server, utilizzano il sistema operativo *Linux CentOS*.

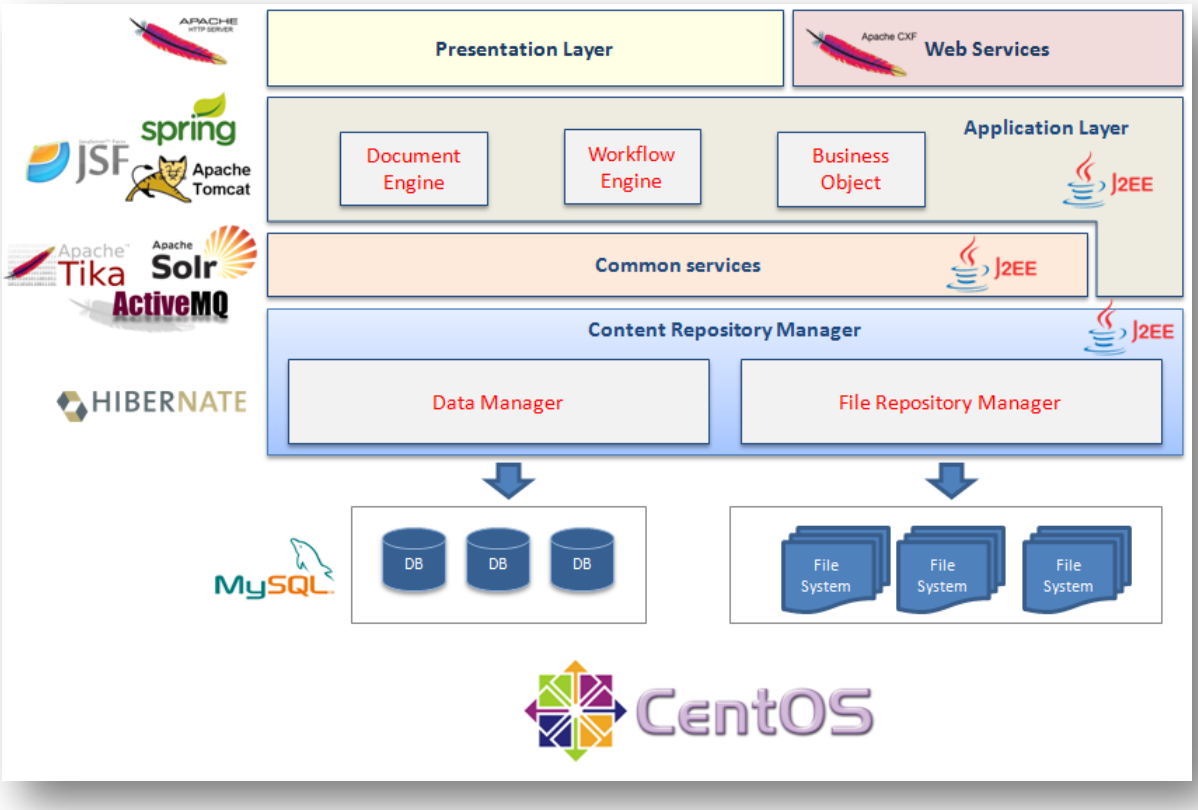

Figura 6 - Componenti tecnologiche del sistema

9.3 Componenti Fisiche

Il sistema di conservazione è ospitato presso i data center di CSA S.c. a r.l.. Tali siti sono attrezzati con tecnologie innovative in termini di affidabilità, sicurezza, scalabilità e ridondanza e sono certificati secondo lo Standard **UNI CEI ISO/IEC 27001:2006**. La strategia per la continuità del servizio (*Business continuity plan - DOC 14.3*) che ha portato allo sviluppo del piano di continuità, prevede la disponibilità di un sito

alternativo per il *disaster recovery*. CSA S.c. a r.l. dispone, infatti, di due siti: il "**Sito primario**", che rappresenta il sito operativo normalmente utilizzato per l'esposizione e la fruizione dei servizi ed il "**Disaster Recovery**", che è speculare al primo in termini di risorse e di servizi, ma che diventa "operativo" solo in caso di disastro del sito primario. La distanza di **oltre 400km** tra il sito primario ed il sito disaster recovery è tale da garantire la continuità del servizio anche a fronte di eventi catastrofici.

Figura 7 - Distanza fra Sito Primario e Secondario

Entrambi i siti dispongono di connessioni ridondate ad alte prestazioni che garantiscono **servizi di replica sincrona**, **maggiore resilienza** ed **alta affidabilità.** Sia i locali che ospitano i siti, sia le macchine e gli apparati che compongono l'infrastruttura sono controllati H 24x7x365 da un sistema distribuito per il **monitoraggio ed il controllo** (si veda paragrafo 10.1). L'infrastruttura tecnologica dei data center è caratterizzata da:

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

In riferimento alla salvaguardia dei dati ed alla *business continuity* sono presenti i seguenti accorgimenti:

- Replica di tutti i dati e di tutte le applicazioni

- Installazione sul sito primario di dispositivi hardware e software per il *backup* automatico dei dati su cassette a nastro
- Utilizzo di configurazioni *cluster*
- Ampio utilizzo di ridondanza a livello hardware
- Sistemi avanzati per la protezione fisica dei siti

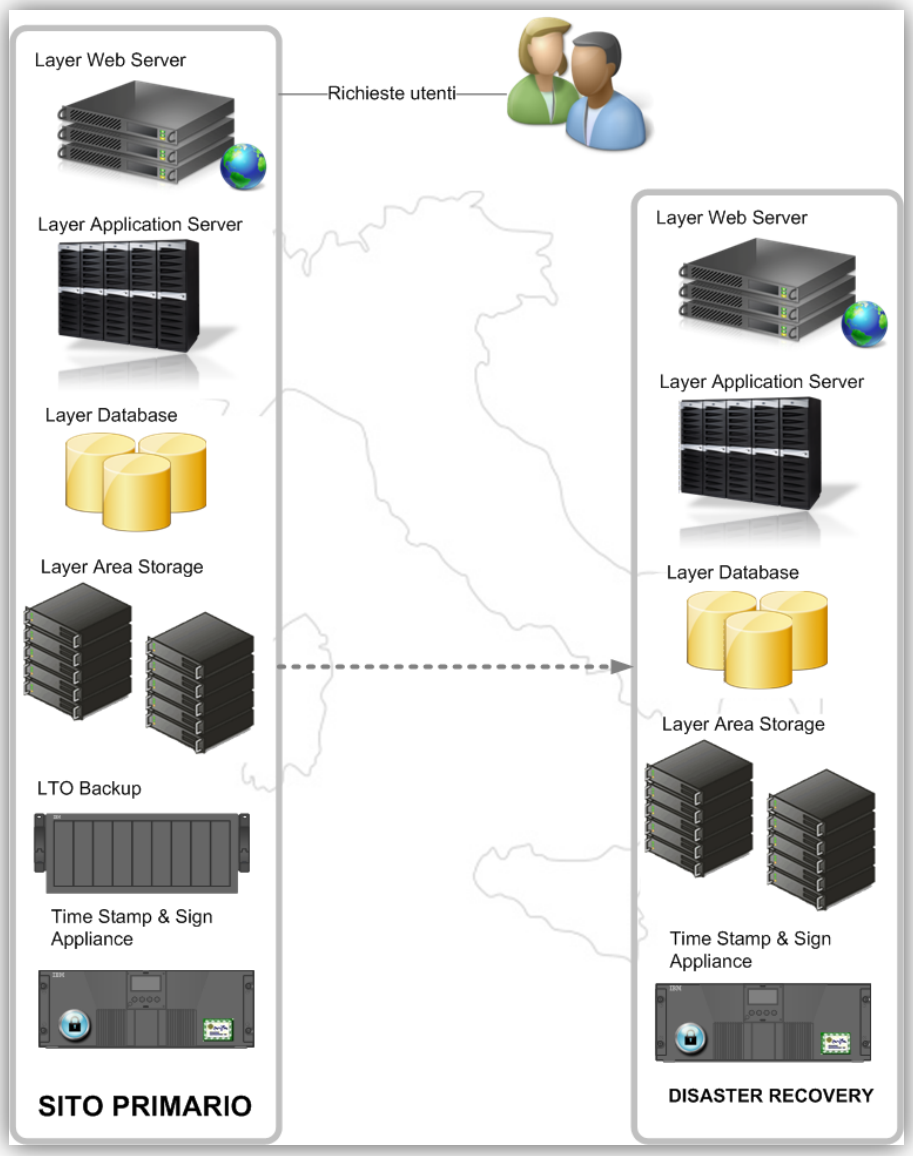

Figura 8 - Architettura dell'impianto tecnologico per l'erogazione dei servizi

L'architettura dell'infrastruttura è suddivisa in livelli logici (*layer*) in configurazione cluster in modalità attiva-attiva. In particolare sono previsti i seguenti layer:

LAYER WEB SERVER: distribuisce il carico sui vari *application server* e funge da **livello di presentazione** per le informazioni statiche, lasciando quelle dinamiche all'"*Application Layer*". I server che

compongono il cluster sono attestati sulla rete DMZ conferendo, quindi, al sistema un elevato grado di sicurezza.

LAYER APPLICATION SERVER: è la *farm* di *application server* configurati in *load balancing*. La distribuzione del carico viene gestita dal *cluster* di *web server*.

LAYER DATABASE: il *cluster* di database server *Mysql* contiene tutte le descrizioni e le relazioni dei documenti contenuti nello *storage*.

LAYER AREA STORAGE: lo *storage* è rappresentato da un *file system* distribuito su scala geografica dove fisicamente sono immagazzinati i dati. Lo *storage* ha caratteristiche di alta disponibilità, scalabilità orizzontale illimitata e *fault tolerance*.

FIREWALL: i componenti del cluster sono in configurazione di alta affidabilità attivo-standby. Il *cluster* ha la funzione sia di regolare il traffico tra le varie sottoreti che compongono il sistema attraverso opportune politiche di sicurezza sia quella di bilanciare il traffico sui server che compongono il sottosistema di *front-end*.

UNITÀ DI BACKUP: per la gestione dei backup periodici è utilizzata la tecnologia LTO (*Linear Tape-Open*) che si basa su una libreria nastro. Per garantire protezione dei dati da eventi straordinari, la conservazione dei nastri è in un armadio ignifugo.

TIME STAMP & SIGN APPLIANCE: *cluster* applicativo dedicato alla firma automatica ed alla marcatura temporale.

9.4 Procedure di gestione ed evoluzione del sistema

I processi di gestione coprono tutto il ciclo di vita del servizio di conservazione e consentono di monitorarne e controllarne tutti gli aspetti. Le procedure di gestione operative del servizio e dei relativi sistemi a supporto del sistema di conservazione sono gestite secondo il M**anuale per la sicurezza delle informazioni** di CSA S.c. a r.l. che include riferimenti a:

- Conduzione e manutenzione del sistema di conservazione
- Gestione e conservazione dei *log*
- Monitoraggio del sistema di conservazione
- *Change management*
- Verifica periodica di conformità a normativa e standard di riferimento
- Soluzioni adottate in caso di anomalie

La documentazione relativa al Sistema di Gestione della Sicurezza delle Informazioni sarà resa disponibile solo su esplicita richiesta del Cliente previa compilazione ed accettazione di apposito accordo di confidenzialità.

9.4.1 Conduzione e manutenzione del sistema di conservazione

Le procedure di conduzione e manutenzione del sistema di conservazione rientrano nel perimetro della certificazione ISO/IEC 27001:2006. Le attività di sviluppo per adeguamento software rientrano, invece, nel perimetro della ISO 9001:2008 cat. EA 35 EA 33.

Rientrano nella **Gestione degli incidenti** le seguenti procedure e schede di registrazione operative:

- *Gestione degli incidenti di sicurezza delle informazioni (Capitolo 13 del Manuale per la Sicurezza delle Informazioni);*
- *Reporting information security weaknesses and events - DOC 13.1;*
- *Responding to information security reports - DOC 13.2;*
- *Collection of evidence - DOC 13.4;*
- *Info security weaknesses and events checklist - REC 13.1a;*
- *Schedule of information security event reports - REC 13.5;*

Rientrano nella **Business Continuity Management** le seguenti procedure e schede di registrazione operative:

- *Business continuity managment (Capitolo 14 del Manuale per la Sicurezza delle Informazioni);*
- *Risk assessment procedure - DOC 14.4;*
- *Business continuity planning - DOC 14.1;*
- *Business continuity risk assessments - DOC 14.2;*
- *Business continuity plan - DOC 14.3,*
- *Testing, maintaining and re-assessing business continuity plans - DOC 14.4;*

Rientrano nella **Conformità ai requisiti legali e con gli standard per la sicurezza** le seguenti procedure e schede di registrazione operative:

- *Conformità con i requisiti legali (Capitolo 15 del Manuale per la Sicurezza delle Informazioni);*
- *Data protection and privacy policy statement - DOC 15.6;*
- *Information security monitoring procedure - DOC 10.18;*
- *Internal independent review procedure - DOC 6.7;*
- *Compliance and compliance checking procedure - DOC 15.4*

Per la manutenzione software, CSA S.c. a r.l. ha formalizzato, all'interno del Sistema di Gestione per la Qualità, la procedura *PR10 Sviluppo applicativi sw*.

9.4.2 Gestione e conservazione dei log

Il sistema di conservazione genera i seguenti *log*:

- accessi utente: registra le connessioni al sistema per i vari utenti

- registrazione delle operazioni applicative: data, ora, operazione, dati identificativi ed esito per ogni evento occorso

Ciascun *log* è registrato in tempo reale sul *Log Server* di CSA S.c. a r.l. per una gestione applicativa del monitoraggio di tutti gli eventi significativi occorsi ai singoli oggetti trattati dal sistema (documenti, PdV, PdA, PdD, etc.). In particolare, tutte le macchine facenti parte del perimetro applicativo del sistema di conservazione sono configurate affinché inviino i *log* verso il *Log Server*. Le informazioni registrate nei *log* sono:

- l'operazione
- l'autore
- l'identificativo del documento / lotto inviato a conservazione
- la data e l'ora

Sul *Log Server* è pianificata un'attività che procede ad effettuare una compressione dei *log* più vecchi di due giorni per la periodica conservazione. I dati, i *log* e gli *asset* intangibili afferenti al *log server* sono protetti da adeguate procedure di *backup* e ripristino.

9.4.3 Change Management

Tutte le modifiche che interessano gli *asset* vengono gestite nell'ambito del sistema di qualità aziendale secondo quanto definito nel processo di **Change Management** (*Change control procedure DOC 10.7* del *Manuale per la sicurezza delle informazioni*). In particolare, tutti i cambiamenti significativi (non di routine) alle infrastrutture per l'elaborazione delle informazioni sono soggette al controllo del cambiamento. Il processo di **Change Management** specifica le modalità da seguire per le richieste dei cambiamenti, per la verifica degli aggiornamenti dovuti alle nuove *release*, per il passaggio dall'ambiente di test a quello di produzione e per l'installazione della nuova *release*.

La procedura prevede i seguenti passi:

1. ogni richiesta di cambiamento deve indicare i costi di esercizio ed i potenziali benefici
2. il cambiamento è soggetto alla valutazione del rischio
3. vengono creati opportuni "punti di ripristino" e procedure di *roll back*
4. viene prodotto un piano di test completo
5. il test avviene nell'ambiente di test
6. i cambiamenti vengono trasferiti all'ambiente reale

Gli aggiornamenti software sono versionati secondo una rigorosa politica di *versioning*: ogni etichetta, utilizzata per il versionamento del software è composta di tre numeri: *Major* . *Minor* . *Build*

dove

- Major: è la parte della versione relativa all'architettura del software etichettato, viene aggiornato qualora questa cambi da una versione ad un'altra
- Minor: è la parte della versione relativa alle funzionalità del software etichettato, viene aggiornato qualora siano aggiunte nuove funzionalità da una versione ad un'altra
- Build: è la parte della versione relativa alla gestione dei bug segnalati al software etichettato, viene aggiornato qualora siano stati risolti dei bug segnalati

Per far riferimento a nuove funzionalità o bug, CSA S.c. a r.l. utilizza uno strumento per il tracciamento automatico delle segnalazioni. Tale strumento, infatti, oltre ad associare un identificativo univoco ad ogni segnalazione, permette di indicare la versione di riferimento, *l'environment* in cui si è verificato, un eventuale *screenshot* e l'associazione di una descrizione.

9.4.4 Verifica periodica di conformità a normativa e standard di riferimento.

La verifiche periodiche di conformità a normativa e standard di riferimento sono effettuate in conformità alla procedura *Internal independent review procedure* DOC 6.7 del M*anuale per la sicurezza delle informazioni* ed al Sistema di gestione della Qualità di CSA S.c. a r.l.

In conformità ai requisiti della normativa sulla Privacy, nonché ai requisiti specifici del Servizio di Conservazione dei documenti informatici, il sistema di gestione della sicurezza delle informazioni prevede specifici controlli quali *audit* normativi interni, *check list*, ecc.

Il processo di verifica di conformità prevede un piano annuale di revisioni interne. Tutte le aree di rischio per le attività del sistema di conservazione sono revisionate periodicamente da revisori indipendenti.

10 MONITORAGGIO E CONTROLLI

10.1 Monitoraggio del sistema di conservazione

Sia i locali che ospitano i siti, sia le macchine e gli apparati che compongono l'infrastruttura sono controllati H 24x7x 365 dal sistema **SmartCo**.

SmartCo sviluppato dalla divisione IT Engineering di CSA S.c. a r.l., è una robusta applicazione per il monitoraggio ed il controllo integrato dell'ambiente, degli *host*, della rete e dei servizi di un'infrastruttura tecnologica. La sua progettazione è stata realizzata tenendo conto dei seguenti aspetti chiave: flessibilità, facilità di utilizzo, affidabilità, efficacia, scalabilità e modularità.

Figura 9 - SmartCo

Il sistema, basato sulla piattaforma Nagios[1], consente il monitoraggio di tutti gli elementi ritenuti critici per la continuità dei servizi erogati attraverso il data center. Oltre al monitoraggio, esso è in grado di eseguire azioni correttive mirate al ripristino, senza intervento umano, delle condizioni normali di funzionamento degli *asset* per cui sia stato rilevato uno stato critico, dove con tale termine si intende una condizione di funzionamento che porta o potrebbe portare ad una indisponibilità o inefficienza del servizio che quel particolare *asset* concorre ad erogare. **SmartCo** controlla lo stato di tutti gli attori coinvolti nella fornitura di

[1] **NAGIOS** è la più diffusa soluzione open source per il monitoraggio remoto di sistemi e servizi.

un servizio, fornendo una misura innanzitutto della salute dell'intero sistema. In particolare, il monitoraggio è effettuato su:

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

Ricadono nel "monitoraggio e controllo" l'hardware, il software e l'insieme delle attività e delle procedure che gli operatori sono tenuti ad eseguire per il corretto funzionamento dei data center.

Il controllo è finalizzato alla produzione di allarmi in caso di anomalie ed eventi che non solo possono compromettere il corretto funzionamento delle macchine, ma anche eventuali guasti o malfunzionamenti delle macchine stesse.

Il sistema è concepito in maniera completamente indipendente dal data center e, quindi, è in grado di continuare il suo funzionamento anche in caso di:

- black-out della rete elettrica
- guasto o malfunzionamento del gruppo di continuità
- black-out della rete pubblica (dovuto a problemi dell'ISP)
- guasto o malfunzionamento degli apparati di rete privata
- guasto o malfunzionamento della linea telefonica

Il sistema di monitoraggio e controllo utilizza i seguenti **sensori**:

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

disponibilità o meno della corrente elettrica a livello di distribuzione e a livello di uscita di ogni singolo gruppo.

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

La mancanza dell'energia elettrica è sopperita attraverso la predisposizione dell'intero sistema a funzionare con un impianto a 12V al fine di poter essere alimentato a batteria.

L'indisponibilità dell'accesso alla rete pubblica, può essere ovviata attraverso la possibilità di instaurare una connessione UMTS/HSDPA.

10.2 Gestione della disponibilità dei servizi

Per la gestione della disponibilità dei servizi, CSA S.c. a r.l. ha prodotto un piano, indicato nel *Business continuity plan - DOC 14.3* dove vengono definiti gli intervalli temporali di intervento in caso di disastro. Il piano di continuità del servizio è oggetto di test e verifica periodicamente durante l'anno, secondo quando indicato nella procedura *Testing, maintaining and re-assessing bc plans - DOC 14.4.* La documentazione afferente al sistema di gestione della sicurezza delle informazioni include tutti manuali e le procedure operative per la gestione ed il ripristino dei data center.

10.3 Sicurezza fisica

Gli accessi e l'utilizzo delle aree sicure sono soggette a controllo da parte del personale di CSA S.c. a r.l.:

- Le aree sicure sono interdette e bloccate in ogni momento. Periodicamente si verifica che le aree siano sicure e protette
- L'accesso alle aree sicure segue la procedura indicata nel *Reception area monitoring work instruction DOC 9.6* dove è specificato chi, in quale modalità ed in quale occasione autorizza le visite
- L'accesso alle aree sicure è consentito solo a persone formalmente riconosciute ed autorizzate che sono fornite degli strumenti per accedere
- Il sistema di autenticazione mantiene una traccia degli accessi
- Non è consentito scattare foto, fare filmati, manomettere o prendere materiale dall'area riservata

La sicurezza perimetrale dei siti è formalizzata nella procedura *Physical perimeter security checklist - doc 9.7* dove, sinteticamente, si evidenzia che:

- I siti sono nascosti al pubblico
- Non è possibile accedere da muri esterni o dal piano terra
- Le porte esterne sono allarmate, dotate di meccanismi di chiusura automatica e gli ingressi protetti da videocamere di sicurezza

- Le finestre esterne sono chiuse
- Gli allarmi anti incendio e gli estintori sono controllati periodicamente
- Gli allarmi anti intrusione sono funzionanti 24h su 24h e coprono tutti i punti di accesso esterni. Le aree non occupate sono allarmate costantemente e l'area di ricezione è controllata

10.3.1 Protezione esterna

Il Data Center è protetto lungo tutto il perimetro da muri, recinzioni metalliche ed infissi esterni blindati. L'altezza delle recinzioni è sempre superiore ai 2 metri nel punto più basso lato esterno, i cancelli di accesso sono videosorvegliati e comandati elettricamente. La protezione da intrusioni esterne è affidata ad un sistema antintrusione a marchio IMQ con centrale a microprocessore, barriere a 4 raggi IR esterne, rivelatori a doppia tecnologia e sirene interne ed esterne. I rilevatori ad ultrasuoni formano una barriera ad incrocio che rilevano l'attraversamento mediante la temporanea interruzione del segnale.

10.3.2 Sistema antiscasso e antifurto interno

Il sistema è costituito da una serie di dispositivi di rilevazione, come contatti magnetici, rivelatori di rottura vetri, rivelatori di fumo, rivelatori volumetrici. Tali dispositivi identificano le condizioni di allarme. Ciascuna area sorvegliata da un sensore attiva un segnale d'allarme quando il sistema è inserito, il segnale viene inviato alla centrale operativa della vigilanza ed al sistema interno di registrazione eventi. Il sistema interno di antiscasso ed antifurto è costituito da una centrale d'allarme collegata con i sensori esterni (barriere antintrusione) ed i sensori interni, questi consentono di rilevare i movimenti all'interno della strutture e sono posizionati in maniera da coprire l'intera area sicura, inoltre la centralina è collegata con sensori di prossimità posizionati presso tutte le aperture verso l'esterno, porte e finestre. Tutti gli eventi registrati dalla centralina d'allarme, compreso l'attraversamento delle barriere esterne, vengono riportati in apposito registro elettronico e tenuti a disposizione per controlli successivi. La centrale d'allarme è configurabile e controllabile da postazione remota, essa è programmata per l'attivazione e la disattivazione automatica ed è dotata di sistema di riconoscimento del calendario con la programmazione degli eventi festivi. I rilevatori volumetrici, gestiti dalla centrale per controllare le intrusioni all'interno sono direttamente collegati ad un istituto di vigilanza di primaria affidabilità.

10.3.3 Sorveglianza

Oltre agli impianti di allarme, nelle ore notturne le aree sicure sono presidiate da guardiani all'ingresso che si preoccupano di verificare nell'immediato intrusioni e falsi allarmi degli impianti di sicurezza. E' presente, inoltre, un sistema di radio-allarme collegato 24 ore su 24 a primario Istituto di Vigilanza. In caso di allarme è previsto l'immediato intervento di un'autopattuglia per ispezionare i locali da cui l'allarme è partito.

10.4 Verifica dell'integrità degli archivi

Così come previsto dall'art. 7 del D.P.C.M. del 3/12/2013 il Responsabile della conservazione "assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi".

I controlli di integrità sono completamente automatizzati ed effettuati con una cadenza definibile dal responsabile della Conservazione (tipicamente settimanale).

Ogni sessione di controllo è composta da un insieme di PdA selezionati in base alla data di ultimo controllo associata al pacchetto. Per ogni documento contenuto in ognuno di questi pacchetti il sistema calcola l'hash confrontandolo con quello presente nell'IPdA. Nel caso in cui il pacchetto sia completamente integro lo stato e la data di controllo ad esso associati vengono aggiornati. Nel caso in cui anche un solo file non sia risultato integro, il PdA viene posto in uno stato "corrotto". Alla fine dell'operazione di controllo il sistema genera un report che viene storicizzato nel sistema di conservazione ed inviato al responsabile della conservazione, il quale provvederà ad intraprendere le azioni correttive previste (ad esempio ripristino delle copie di backup) per i pacchetti il cui contenuto è risultato essere corrotto.

10.5 Soluzioni adottate in caso di anomalie

I servizi del sistema di conservazione sono continuamente monitorati e controllati al fine di verificarne la conformità agli SLA definiti ed il mantenimento dei livelli di riservatezza, integrità e disponibilità dei dati. Gli incidenti eventualmente occorsi e le debolezze preventivamente individuate vengono classificate per stabilirne la priorità. In base alla classificazione ed alla tipologia di evento, vengono invocate le azioni correttive previste dalle istruzioni operative e ripristinati i sistemi. Dopo che l'incidente è stato contenuto e le correzioni richieste completate, si individuano le cause per garantire una adeguata azione correttiva.