

# COMDATA S.P.A.

## Manuale della Conservazione

### EMISSIONE DEL DOCUMENTO

<b>Azione</b>	<b>Data</b>	<b>Nominativo</b>	<b>Funzione</b>
<i>Redazione</i>	02.03.2018	Gianfranco Onnis	<i>Delegato Responsabile Compliance Normativa</i>
<i>Verifica</i>	06.03.2018	Antonio Spada	<i>Responsabile Archivistica di Conservazione (Resp. Funzione AM)</i>
<i>Verifica</i>	06.03.2018	Daniele Medone	<i>Delegato Sviluppo e Manutenzione Sistema di Conservazione</i>
<i>Approvazione</i>	09.03.2018	Andrea Armani	<i>Responsabile Servizio di Conservazione</i>

### REGISTRO DELLE VERSIONI

<b>N° Ver/Rev/Bozza</b>	<b>Data emissione</b>	<b>Modifiche apportate</b>	<b>Osservazioni</b>
Versione Beta	05.04.2016		
Versione 1.0	10.06.2016	Prima emissione	
Versione 1.1	28.10.2016	Revisione per Comdata SPA e organigramma consolidato	
Versione 2.0	26.04.2017	Revisione per inserimento processo di scarto pacchetti di archiviazione	
Versione 3.0	28.11.2017	Revisione terminologie abrogate	
Versione 3.1	08.02.2018	Revisione compliance EIDAS	

Versione 3.2	02.03.2018	Dettagliato processo gestione obsolescenza cap 9.2.1	
--------------	------------	---	--

## INDICE DEL DOCUMENTO

<b>1</b>	<b>SCOPO E AMBITO DEL DOCUMENTO .....</b>	<b>4</b>
<b>2</b>	<b>TERMINOLOGIA (GLOSSARIO, ACRONIMI) .....</b>	<b>5</b>
<b>3</b>	<b>NORMATIVA E STANDARD DI RIFERIMENTO .....</b>	<b>11</b>
3.1	NORMATIVA DI RIFERIMENTO.....	11
3.2	STANDARD DI RIFERIMENTO.....	12
<b>4</b>	<b>RUOLI E RESPONSABILITÀ .....</b>	<b>13</b>
4.1	STORIA DEI RUOLI.....	17
<b>5</b>	<b>STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE .....</b>	<b>17</b>
5.1	ORGANIGRAMMA DELL'AZIENDA COMDATA S.P.A.....	18
5.1.1	<i>Direzioni Commerciali</i> .....	19
5.1.2	<i>Direzione IT</i> .....	19
5.1.3	<i>Business Unit ICT</i> .....	20
5.2	STRUTTURE ORGANIZZATIVE .....	22
<b>6</b>	<b>OGGETTI SOTTOPOSTI A CONSERVAZIONE.....</b>	<b>24</b>
6.1	OGGETTI CONSERVATI .....	24
6.2	TIPOLOGIE DI DOCUMENTI CONSERVATI .....	24
6.2.1	<i>Metadati</i> .....	25
6.2.2	<i>Formati</i> .....	26
6.2.3	<i>Formati di documenti firmati digitalmente</i> .....	27
6.3	PACCHETTO DI VERSAMENTO .....	27
6.3.1	<i>Struttura del file XML</i> .....	27
6.3.2	<i>Informazioni di Testata del Pacchetto: NODO &lt;INFO&gt;</i> .....	28
6.3.3	<i>Definizione della chiave univoca dei documenti: NODO &lt;LIST_KEYS&gt;</i> .....	29
6.3.4	<i>Lista dei documenti del pacchetto: NODO &lt;DOCUMENTS&gt;</i> .....	29
6.3.5	<i>Informazioni di dettaglio dei documenti: NODO &lt;DOCUMENT&gt;</i> .....	29
6.3.6	<i>Associazioni tra documenti: NODO &lt;LINK&gt;</i> .....	30
6.3.7	<i>Esempio di tracciato XML valorizzato</i> .....	31
6.4	PACCHETTO DI ARCHIVIAZIONE.....	32
6.5	PACCHETTO DI DISTRIBUZIONE.....	33
<b>7</b>	<b>IL PROCESSO DI CONSERVAZIONE .....</b>	<b>34</b>
7.1	MODALITÀ DI TRASFERIMENTO DEI PACCHETTI DI VERSAMENTO. ....	35
7.2	VERIFICA DEL PACCHETTI DI VERSAMENTO E GENERAZIONE DEL RAPPORTO DI VERSAMENTO.....	35

7.2.1	<i>Controlli sul pacchetto di versamento</i> .....	35
7.2.2	<i>Pacchetti di versamento conformi</i> .....	39
7.2.3	<i>Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie</i> .....	40
7.3	CARICAMENTO DEL PACCHETTO DI VERSAMENTO SUL SISTEMA C.SOST .....	40
7.4	PREPARAZIONE E GESTIONE DEL PACCHETTO DI ARCHIVIAZIONE .....	41
7.5	PREPARAZIONE E GESTIONE DEL PACCHETTO DI DISTRIBUZIONE AI FINI DELL'ESIBIZIONE .....	41
7.6	PRODUZIONE DI DUPLICATI E COPIE INFORMATICHE .....	42
7.7	SCARTO DEI PACCHETTI DI ARCHIVIAZIONE.....	43
7.8	PREDISPOSIZIONE DI MISURE A GARANZIA DELL'INTEROPERABILITÀ E TRASFERIBILITÀ AD ALTRI CONSERVATORI .....	44
7.9	MAPPE DI CONSERVAZIONE.....	45
<b>8</b>	<b>IL SISTEMA DI CONSERVAZIONE .....</b>	<b>46</b>
8.1	COMPONENTI LOGICHE .....	46
8.2	ARCHITETTURA TECNOLOGICA.....	47
8.3	ARCHITETTURA FISICA .....	48
8.4	INFRASTRUTTURA DI EROGAZIONE.....	49
8.4.1	<i>Sistemi di Elaborazione e Archiviazione</i> .....	50
8.4.2	<i>Caratteristiche Hardware e Software dei Sistemi</i> .....	51
8.4.3	<i>Sistemi di Firma Digitale e Marca Temporale</i> .....	52
8.4.4	<i>Connettività</i> .....	53
8.5	LUOGO DI CONSERVAZIONE DEI DOCUMENTI.....	53
8.6	SICUREZZA DEL SISTEMA DI CONSERVAZIONE .....	54
8.6.1	<i>Gestione della Privacy</i> .....	54
<b>9</b>	<b>PROCEDURE DI GESTIONE E DI MONITORAGGIO .....</b>	<b>55</b>
9.1	CONTROLLO DEL SERVIZIO .....	55
9.2	VERIFICA DELL'INTEGRITÀ DEGLI ARCHIVI.....	56
9.2.1	<i>Processo di gestione dell'obsolescenza</i> .....	57
9.3	GESTIONE DELLE SEGNALAZIONI .....	57
9.3.1	<i>Pacchetti di versamento</i> .....	57
9.3.2	<i>Anomalie di funzionamento del sistema C.Sost</i> .....	57
9.4	MONITORAGGIO DEGLI SLA.....	59
9.5	ELABORAZIONE DELLA REPORTISTICA .....	59
9.6	ARCHIVIAZIONE DEI DOCUMENTI RILEVANTI AI FINI DEL SERVIZIO.....	60

## INDICE DELLE FIGURE

Figura 1 – Struttura Aziendale	18
Figura 2 - Strutture XML SInCRO	33
Figura 1 – Schema del Processo di Conservazione	34
Figura 4 – Architettura logica del Sistema di Conservazione C.Sost	46
Figura 5 – Infrastruttura tecnica di erogazione del Sistema di Conservazione	49
Figura 6 – Dislocazione geografica dei datacenter di erogazione Sistema di Conservazione	50
Figura 7 – Schema di infrastruttura tecnica di erogazione del Sistema di Conservazione	51

## 1 SCOPO E AMBITO DEL DOCUMENTO

COMDATA S.p.A. eroga ai propri Clienti una soluzione di gestione completa del ciclo di vita dei documenti informatici. Uno dei servizi erogati nell'ambito di questa soluzione è il SISTEMA DI CONSERVAZIONE dei Documenti Informatici – C.SOST.

Il presente documento costituisce il MANUALE DELLA CONSERVAZIONE della soluzione C.SOST di COMDATA S.p.A., nel seguito COMDATA ai sensi delle regole tecniche sui sistemi di conservazione dettate dal D.P.C.M. 3 dicembre 2013.

Il sistema C.SOST assicura la conservazione degli oggetti in esso conservati, attraverso il mantenimento delle caratteristiche di:

- Autenticità
- Integrità
- Affidabilità
- Leggibilità
- Reperibilità

Il Manuale fornisce le istruzioni operative relative alle procedure di conservazione elettronica che il Responsabile della medesima procedura deve osservare nell'effettuazione del servizio.

Il Manuale, in particolare:

- a) individua il modello organizzativo definito da COMDATA per il sistema di conservazione;
- b) definisce competenze, ruoli e responsabilità dei soggetti coinvolti nel processo di conservazione;
- c) elenca le tipologie degli oggetti sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di documenti e delle eventuali eccezioni;

- d) illustra il modello di funzionamento indicando le procedure realizzate al fine di assicurare la conservazione dei documenti informatici garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità;
- e) delinea l'intero ciclo di gestione degli oggetti del processo di conservazione dal momento della presa in carico del pacchetto di versamento a quello della generazione del pacchetto di archiviazione;
- f) rappresenta sia le modalità di accesso ai documenti conservati, per il periodo prescritto dalla norma, a prescindere dall'evolversi del contesto tecnologico, sia le modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;
- g) descrive le procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie;
- h) descrive le architetture e le infrastrutture utilizzate oltre alle misure di sicurezza adottate;
- i) precisa le procedure per la produzione di duplicati o copie;
- j) indica i tempi entro i quali le diverse tipologie di documenti devono essere scartate ovvero trasferite in conservazione.

Il manuale della Conservazione è presente nel repository dei documenti aziendali denominato WEFILE (<http://wefile.comdata.it/alfresco/faces/jsp/login.jsp>) nella cartella del referente normativo, dove sono archiviate le diverse versioni e i relativi verbali di aggiornamento.

[Torna al sommario](#)

## 2 TERMINOLOGIA (GLOSSARIO, ACRONIMI)

Glossario dei termini e Acronimi	
<b>AGID</b>	Agenzia per l'Italia Digitale (sostituisce CNIPA/AIPA)
<b>Autenticità</b>	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.
<b>Base di dati</b>	Collezione di dati registrati e correlati tra loro.
<b>CA</b>	Certification Authority
<b>Cache</b>	Unità Logica di Archiviazione Documenti il cui contenuto è omogeneo

	per Soggetto Titolare del Documento, Classe Documentale e Anno di Riferimento dei Documenti.
<b>CacheID</b>	Identificativo univo nei Sistemi di COMDATA dell'unità Logica di Archiviazione
<b>CAD</b>	Codice dell'Amministrazione Digitale (D.L 82/2005).
<b>Certificatore accreditato</b>	Soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, da AGID, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza.
<b>Ciclo di gestione</b>	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.
<b>Classificazione</b>	Attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati.
<b>Codice</b>	Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni.
<b>Codice eseguibile</b>	Insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici.
<b>Conservatore accreditato</b>	Soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, da AgID, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, da AgID.
<b>Conservazione</b>	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.
<b>Contrassegno stampa</b>	Contrassegno generato elettronicamente, apposto a stampa sulla copia analogica di un documento amministrativo informatico per verificarne provenienza e conformità all'originale.
<b>Coordinatore della gestione documentale</b>	Responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 nei casi di amministrazioni che abbiano istituito più Aree Organizzative Omogenee.
<b>Copia analogica del documento informatico</b>	Documento analogico avente contenuto identico a quello del documento informatico da cui è tratto.
<b>Copia di sicurezza</b>	copia di <i>backup</i> degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 delle presenti regole tecniche per il sistema di conservazione
<b>Destinatario</b>	Identifica il soggetto/sistema al quale il documento informatico è indirizzato
<b>DL</b>	Decreto Legge.
<b>DLGS</b>	Decreto Legislativo.
<b>DPCM</b>	Decreto Presidente del Consiglio dei Ministri.
<b>DPR</b>	Decreto Presidente della Repubblica.

<b>Duplicazione dei documenti informatici</b>	Produzione di duplicati informatici.
<b>Esibizione</b>	Operazione che consente di visualizzare un documento conservato e di ottenerne copia.
<b>Estratto per riassunto</b>	Documento nel quale si attestano in maniera sintetica ma esaustiva fatti, stati o qualità desunti da dati o documenti in possesso di soggetti pubblici
<b>Evidenza informatica</b>	Una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.
<b>Fascicolo informatico</b>	Raccolta, individuata con identificativo univoco, di atti, documenti e dati informatici, da chiunque formati, del procedimento amministrativo, nell'ambito della pubblica amministrazione. Per i soggetti privati è da considerarsi fascicolo informatico ogni aggregazione documentale, comunque formata, funzionale all'erogazione di uno specifico servizio o prestazione.
<b>Formato</b>	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
<b>FTP server</b>	programma che permette di accettare connessioni in entrata e di comunicare con un Client attraverso il protocollo FTP
<b>Funzionalità aggiuntive</b>	Le ulteriori componenti del sistema di protocollo informatico necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni.
<b>Funzionalità interoperative</b>	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.
<b>Funzionalità minima</b>	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.
<b>Funzione di hash</b>	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.
<b>Generazione automatica di documento informatico</b>	Formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni.
<b>HTTP</b>	Hyper Text Transfer Protocol (identificativo convenzionale per un sito).
<b>HTTPS</b>	Secure Hyper Text Transmission Protocol. Protocollo sviluppato allo scopo di cifrare e decifrare le pagine Web che vengono inviate dal server ai client.
<b>Identificativo univoco</b>	Sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentire l'individuazione.

<b>IdP</b>	strumento per rilasciare le informazioni di identificazione di tutti i soggetti che cercano di interagire con un Sistema; ciò si ottiene tramite un modulo di autenticazione che verifica un token di sicurezza come alternativa all'autenticazione esplicita di un utente all'interno di un ambito di sicurezza.
<b>Immodificabilità</b>	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.
<b>Impronta</b>	La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di <i>hash</i> .
<b>Insieme minimo di metadati del documento informatico</b>	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.
<b>Integrità</b>	Insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato.
<b>Interoperabilità</b>	capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi.
<b>L</b>	Legge
<b>Leggibilità</b>	Insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti.
<b>Log di sistema</b>	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.
<b>Manuale di conservazione</b>	Strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 delle regole tecniche del sistema di conservazione
<b>Manuale di gestione</b>	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.
<b>Memorizzazione</b>	Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici
<b>Metadati</b>	Insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 del presente decreto.
<b>OAIS</b>	ISO 14721:2012; Space Data information transfer system
<b>Pacchetto di archiviazione</b>	Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del presente decreto e secondo le modalità riportate nel manuale di conservazione.



<b>Pacchetto distribuzione</b>	<b>di</b>	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta.
<b>Pacchetto versamento</b>	<b>di</b>	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione.
<b>Pacchetto informativo</b>		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.
<b>PDF</b>		Portable Document Format.
<b>Piano della sicurezza del sistema di conservazione</b>		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.
<b>Piano della sicurezza del sistema di gestione informatica dei documenti</b>		Documento, che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi nell'ambito dell'organizzazione di appartenenza.
<b>Piano di conservazione</b>	<b>di</b>	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.
<b>Piano generale della sicurezza</b>		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.
<b>PKI</b>		Public Key Infrastructure (infrastruttura necessaria per creare, gestire, conservare e revocare i certificati delle firme elettroniche basati su crittografia a chiave pubblica).
<b>Presa in carico</b>		Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione.
<b>Processo di conservazione</b>	<b>di</b>	Insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 10 delle regole tecniche del sistema di conservazione.
<b>Produttore</b>		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 responsabile della gestione documentale.
<b>Rapporto versamento</b>	<b>di</b>	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore
<b>Registrazione informatica</b>		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.
<b>Registro di protocollo</b>		Registro informatico della corrispondenza 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.
<b>Registro particolare</b>	Registro informatico specializzato per tipologia o per oggetto; nell'ambito della pubblica amministrazione è previsto ai sensi dell'articolo 53, comma 5 del D.P.R. 28 dicembre 2000, n. 445.
<b>Repertorio informatico</b>	Registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche che trattano il procedimento, ordinati secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica.
<b>Responsabile del trattamento dei dati</b>	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.
<b>Responsabile della conservazione</b>	Soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 delle regole tecniche del sistema di conservazione.
<b>Responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi</b>	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.
<b>Responsabile della sicurezza</b>	Soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza.
<b>Riferimento temporale</b>	Informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento.
<b>Scarto</b>	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse culturale.
<b>Sistema di classificazione</b>	Strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata.
<b>Sistema di conservazione</b>	Sistema di cui all'art. 4 delle regole tecniche del sistema di conservazione.
<b>Sistema di gestione informatica dei documenti</b>	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.
<b>SSL</b>	Secure Socket Layer. Protocollo che consente, grazie a tecniche di crittografia, il trasferimento di dati tramite la rete Internet in modo sicuro.
<b>Staticità</b>	Caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni,

	segnalibri, gestite dal prodotto software utilizzato per la redazione.
<i>Testo unico</i>	Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni.
<i>Transazione informatica</i>	Particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche della base di dati.
<i>TSA</i>	Time Stamping Authority.
<i>Ufficio utente</i>	Riferito ad un'area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico.
<i>URL</i>	Uniform Resource Locator (indica la modalità per individuare univocamente un sito Internet).
<i>UTC</i>	Universal Time Coordinated (Misura del tempo così come stabilito dall'International Radio Consultative Committee – CCIR).
<i>Utente</i>	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.
<i>Versamento agli Archivi di Stato</i>	Operazione con cui il responsabile della conservazione di un'amministrazione statale 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.

[Torna al sommario](#)

### 3 NORMATIVA E STANDARD DI RIFERIMENTO

#### 3.1 Normativa di riferimento

Nella tabella che segue viene elencata la principale normativa di riferimento per le attività di conservazione e quella specifica relativa alle diverse tipologie di documenti, e nella specie quelli a rilevanza fiscale, riguardanti il contratto di erogazione del servizio di conservazione.

Normativa di riferimento	
<i>Codice Civile</i>	articolo 2215 bis - Documentazione informatica
<i>L. 7 agosto 1990, n. 241 e s.m.i.</i>	Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi
<i>DPR 28 dicembre 2000, n. 445 e s.m.i.</i>	Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
<i>DLGS 30 giugno 2003, n. 196 e s.m.i.</i>	Codice in materia di protezione dei dati personali

<b>DLGS 22 gennaio 2004, n. 42 e s.m.i.</b>	Codice dei Beni Culturali e del Paesaggio
<b>DLGS 7 marzo 2005 n. 82 e s.m.i.</b>	Codice dell'amministrazione digitale (CAD)
<b>DPCM 22 febbraio 2013</b>	Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71
<b>DPCM 3 dicembre 2013</b>	Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005
<b>DPCM 3 dicembre 2013</b>	Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005
<b>Circolare AGID 10 aprile 2014, n. 65</b>	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
<b>DPCM 13 novembre 2014</b>	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
<b>DM 17 giugno 2014</b>	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.
<b>GDPR 5/2016 (*)</b>	General Data Protection Regulation- Regolamento con il quale la Commissione europea intende rafforzare e rendere più omogenea la protezione dei dati personali di cittadini dell'Unione Europea e dei residenti nell'Unione Europea, sia all'interno che all'esterno dei confini dell'Unione europea (UE).

(\*) nel presente documento i riferimenti a questo GDPR saranno introdotti a partire dalla data ultima di adesione fissata dalla legge nel 28 Maggio 2018, con l'emissione di una nuova versione.

[Torna al sommario](#)

### 3.2 Standard di riferimento

Nella tabella che segue si riportano gli standard a cui si riferisce l'attività di conservazione. Si tratta degli standard elencati nell'allegato 3 delle Regole Tecniche in materia di Sistema di conservazione, con indicazione delle versioni aggiornate al 1° ottobre 2014.

Torna al

Standard di riferimento	
<i>ISO 14721:2012</i>	OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione
<i>ISO/IEC 27001:2013</i>	Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System)
<i>ETSI TS 101 533-1 V1.3.1 (2012-04)</i>	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
<i>ETSI TR 101 533-2 V1.3.1 (2012-04)</i>	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
<i>UNI 11386:2010</i>	Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali
<i>ISO 15836:2009</i>	Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core

sommario

## 4 RUOLI E RESPONSABILITÀ

Nel presente paragrafo vengono indicati attività svolte e nominativi delle persone in carica, che ricoprono i ruoli elencati nella tabella seguente, così come individuati nel documento “Profili professionali” di cui alla Circolare AgID n. 65 del 2014.

Nel caso di deleghe, per ciascuna delega sono indicate attività delegate, dati identificativi del soggetto delegato e periodo di validità della delega.

La tabella mantiene traccia dei dati delle persone che nel tempo hanno ricoperto i suddetti ruoli. I curricula dei responsabili indicati in tabella sono oggetto dell'Allegato A – Profili professionali conservazione COMDATA.

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo	Eventuali deleghe
<i>Responsabile del servizio di conservazione</i>	Andrea Armani	Il processo di conservazione vede coinvolte, a vario titolo, differenti figure e differenti professionalità. Tutte le figure coinvolte sono coordinate dal responsabile del servizio di conservazione che è il	Dal 07.01.2013	Delega della funzione di compliance normativa per il sistema di conservazione

		<p>punto di riferimento per le attività del conservatore.</p> <ul style="list-style-type: none"> <li>Il responsabile del servizio di conservazione è colui che si occupa di definire e attuare le politiche complessive del sistema di conservazione, nonché di governare la gestione del sistema di conservazione; inoltre a lui spetta la definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente.</li> </ul>		(G.Omnis)
<b>Responsabile funzione archivistica di conservazione</b>	Antonio Spada	<p>Il Responsabile della funzione archivistica di conservazione si occupa di attività di configurazione del processo di conservazione, in collaborazione con il responsabile dello sviluppo e della manutenzione. E' la figura che svolge, attraverso la struttura aziendale preposta, i seguenti compiti:</p> <ul style="list-style-type: none"> <li>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 trasferite, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato;</li> <li>monitoraggio del processo di conservazione e analisi archivistica per garantire la congruità del servizio.</li> <li>Avvalendosi di una struttura aziendale preposta alle specifiche attività, effettua il monitoraggio end to end dei livelli di servizio (SLA) concordati con il Cliente e segnala eventuali difformità degli SLA al Responsabile del</li> </ul>	Dal 01.01.2018	

		<p>servizio di conservazione individuando e pianificando le necessarie azioni correttive.</p> <ul style="list-style-type: none"> <li>• Controllo e verifica anche dei livelli di servizio erogati da terzi segnalando le eventuali difformità al Responsabile del servizio di conservazione.</li> <li>• collaborazione con l'ente produttore ai fini del trasferimento in conservazione.</li> </ul>		
<b>Responsabile trattamento dati personali</b>	Daniela Granata	<ul style="list-style-type: none"> <li>• garantisce il rispetto delle vigenti disposizioni in materia di trattamento dei dati personali;</li> <li>• garantisce 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;</li> </ul>	Dal 08.04.2015	
<b>Responsabile Sicurezza dei sistemi per la conservazione</b>	Marco Azzarini	<ul style="list-style-type: none"> <li>• garantisce il rispetto dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza, mediante il monitoraggio e l'audit del processo.</li> <li>• segnala eventuali difformità al Responsabile del servizio di conservazione e individua e propone le necessarie azioni correttive.</li> </ul>	Dal 01.01.2010	
<b>Responsabile sistemi informativi per la conservazione</b>	Alberto Tonello	<p>Il responsabile dei sistemi informativi per la conservazione gestisce il corretto funzionamento di tutte le componenti hardware e software di base del sistema di conservazione.</p> <ul style="list-style-type: none"> <li>• Avvalendosi di una struttura aziendale preposta alle specifiche attività, tiene monitorati i livelli di servizio infrastrutturali (SLA) concordati</li> </ul>	Dal 01.01.2018	

		<p>con il Responsabile del servizio di conservazione e gli segnala eventuali difformità; inoltre individua e propone le necessarie azioni correttive.</p> <ul style="list-style-type: none"> <li>• Controlla e verifica anche i livelli di servizio infrastrutturali erogati da terzi segnalando le eventuali difformità al Responsabile del servizio di conservazione.</li> <li>• Infine pianifica lo sviluppo delle infrastrutture tecnologiche del sistema di conservazione definite dal Responsabile dello sviluppo e della manutenzione.</li> </ul>		
<b>Responsabile sviluppo e manutenzione del sistema di conservazione</b>	Andrea Armani	<p>A tale responsabile compete il coordinamento dello sviluppo e della manutenzione delle componenti hardware e software del sistema di conservazione avvalendosi di una struttura aziendale preposta.</p> <ul style="list-style-type: none"> <li>• Pianifica e tiene monitorati i progetti di sviluppo del sistema di conservazione oltre agli SLA relativi alla manutenzione del sistema di conservazione.</li> <li>• Si interfaccia con il Cliente relativamente alla definizione delle 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.</li> <li>• A lui compete la gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.</li> <li>• E' colui che definisce il processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità</li> </ul>	Dal 01.01.2005	Delega operativa per lo sviluppo e manutenzione del sistema di conservazione (D. Medone)



		<p>dei documenti e delle aggregazioni documentali trasferite, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato;</p> <ul style="list-style-type: none"> <li>• Al responsabile dello sviluppo compete, in collaborazione con il responsabile della funzione archivistica di conservazione anche: <ul style="list-style-type: none"> <li>○ la definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici;</li> <li>○ l'analisi dell'andamento del servizio di conservazione per il continuous improvement e lo sviluppo di nuove funzionalità del sistema di conservazione.</li> </ul> </li> </ul>	
--	--	---	--

#### 4.1 Storia dei ruoli

Ruoli	Nominativo	Periodo nel ruolo	Eventuali deleghe
<i>Responsabile del servizio di conservazione</i>	Giancarlo Almondo	Dal 01.07.2009 al 31.12.2012	

[Torna al sommario](#)

## 5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

Comdata eroga il servizio di conservazione a norma per conto dei propri clienti, senza avvalersi di terze parti. Tutte le apparecchiature ed i sistemi di elaborazione sono di proprietà di Comdata, come pure il personale

preposto allo svolgimento del processo di conservazione è in forma a Comdata.

Il seguente schema rappresenta l'organizzazione aziendale e all'interno di questa, le strutture coinvolte a vario titolo nel processo di Conservazione.

## 5.1 Organigramma dell'Azienda Comdata S.p.A.

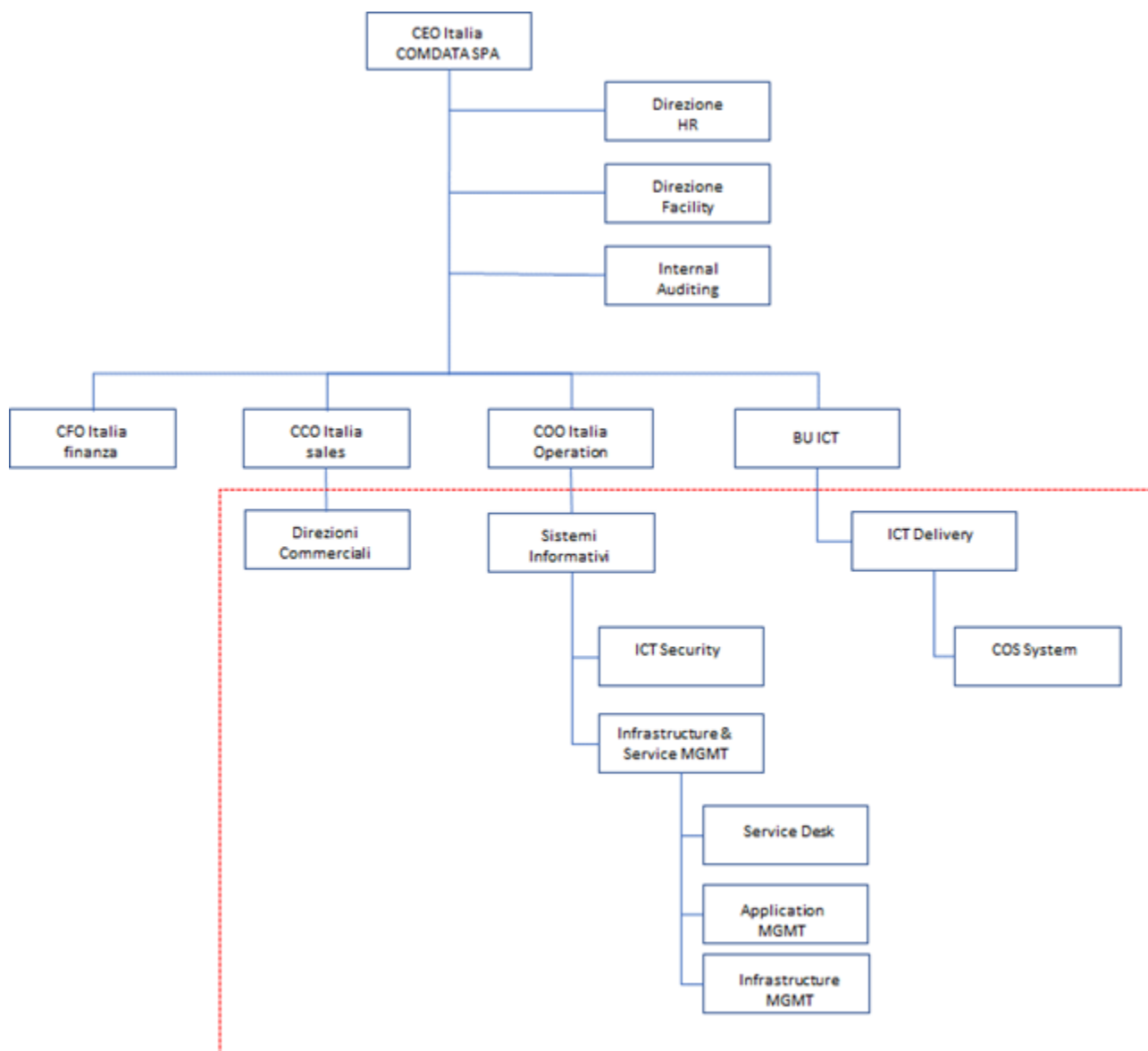


Figura 1 – Struttura Aziendale

Racchiuse nella linea rossa tratteggiata sono indicate le strutture organizzative coinvolte nel sistema di conservazione.

### 5.1.1 Direzioni Commerciali

I clienti del servizio di Conservazione, individuati dalle Direzioni Commerciali affidano in outsourcing il servizio di conservazione a COMDATA, che assume le responsabilità della conservazione in accordo con quanto previsto dal contratto, dagli allegati contrattuali.

### 5.1.2 Direzione IT

La Direzione IT ha il compito di erogare il servizio con lo scopo di:

- Assicurare che il servizio rimanga consistente ed integrato con tutti i processi, le architetture, le tecnologie ed i sistemi di gestione utilizzati;
- Assicurare che i requisiti di capacità siano effettivamente definiti e consistenti;
- Assicurare che siano rispettati i corretti requisiti (livelli) operativi dei servizi erogati;
- Gestire i rischi per rendere più affidabile lo startup del servizio;
- Disegnare le infrastrutture tecnologiche per assicurarsi che sia supportabile e cost-effective.

La struttura di Infrastructure e Service Management ha il compito di erogare il servizio operativo per la Conservazione:

- Attraverso la struttura di Application Management
  - attivare il servizio di conservazione acquisire, verificare e gestire i pacchetti di versamento presi in carico e generare il rapporto di versamento;
  - preparare e gestire il pacchetto di archiviazione;
  - preparare e gestione il pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta;
  - scartare i pacchetti di archiviazione;
  - chiudere il servizio di conservazione (al termine di un contratto).
  - garantire il monitoraggio proattivo ed il controllo degli SLA
  - attivare i processi di escalation
- Attraverso la struttura di Data center e Sistemi,
  - assicurare la conduzione e manutenzione delle infrastrutture del sistema di conservazione
  - garantire il monitoraggio proattivo delle infrastrutture che ospitano il sistema
  - gestire il capacity planning delle infrastrutture e proporre le estensioni ed i miglioramenti necessari
  - pianificare e gestire le evoluzioni infrastrutturali richieste
  - attivare i processi di escalation in caso di criticità sulle infrastrutture
- Attraverso la struttura Service Desk:
  - Assicura il punto unico di contatto per la gestione dei Trouble Ticket (TT) relativi a segnalazioni di problemi e alla richiesta di informazioni e supporto da parte dei Clienti e dei riferimenti interni;
  - Gestire il corretto instradamento dei TT alle opportune funzioni aziendali
  - Controlla il rispetto degli SLA concordati per la presa in carico e la risoluzione delle richieste Cliente e produce i report dell'andamento del servizio;

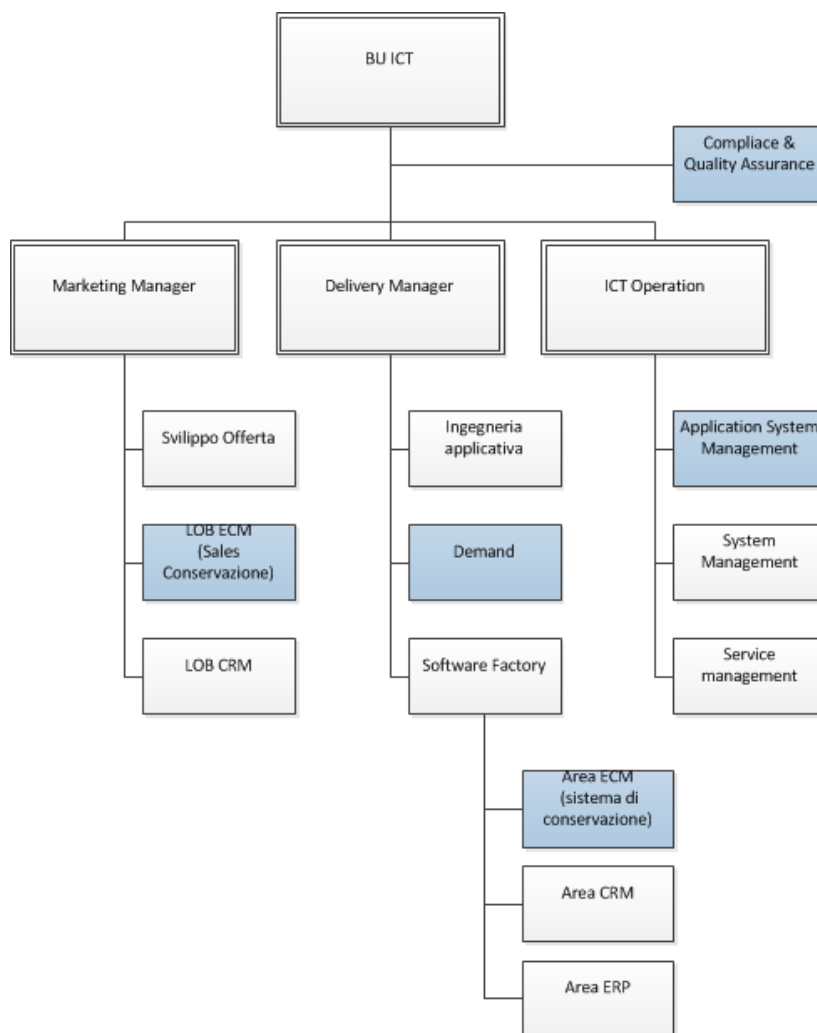
- Garantire il presidio H24 alla console di monitoraggio e alla ricezione dei TT.

La struttura Information Security ha il compito di garantire la sicurezza informatica dei Sistemi della Conservazione; più in dettaglio ha le seguenti responsabilità:

- Definire ed emettere le policy di sicurezza secondo lo standard ISO27001
- Realizzare il piano generale di sicurezza e Business Continuity
- Garantire il rispetto dei requisiti di sicurezza
- Effettuare gli audit periodici di sicurezza e gestire i piani di rientro
- • Attivare i vulnerability assessment interni gestiti direttamente dalle strutture preposte;

### 5.1.3 Business Unit ICT

La BU ICT è organizzata secondo il seguente schema



e, per il tramite della struttura di Delivery ha il compito di sviluppare e mantenere costantemente funzionanti le applicazioni software che supportano l'erogazione del servizio. In particolare all'interno della Direzione Delivery è allocata la linea di sviluppo e gestione delle soluzioni DMS & COS che sono utilizzate per l'erogazione del servizio di conservazione .

La Direzione Delivery è responsabile della gestione delle attività di delivery, coordinando ed indirizzando l'attività dei Demand Manager e delle risorse loro assegnate. Le attività della Direzione Delivery riguardano sia i progetti esterni, acquisiti dalle Divisioni Commerciali di Comdata, sia i progetti di evoluzione delle piattaforme e delle applicazioni aziendali definiti dalla struttura di Ingegneria Applicativa.

La Direzione Delivery ha la responsabilità di:

- Identificare l'architettura della soluzione per i progetti per i quali è disponibile una soluzione di

riferimento;

- Effettuare l'analisi funzionale e tecnica;
- Sviluppare il software ed effettuare lo unit test (paragrafo 7.3);
- Effettuare l'integration test ed il collaudo interno;
- Curare le attività di installazione, avviamento e collaudo con il cliente (nel caso di soluzioni installate presso i clienti);
- Curare la manutenzione delle soluzioni rilasciate e svolgere i servizi di assistenza tecnica, manutenzione correttiva ed evolutiva secondo quanto previsto dai contratti di fornitura;
- Curare il passaggio in produzione attivando ICT Operations, nel caso di soluzioni fornite in service;
- Supportare ICT Operations nella identificazione di work around e della soluzione finale di anomalie riscontrate in esercizio.

Le responsabilità all'interno della Direzione Delivery sono così assegnate:

- Il Delivery Manager o Project Manager è comunque sempre il responsabile di tutte le attività di progetto
- Il Responsabile del gruppo di lavoro (Team Leader), se nominato dal Project Manager, è responsabile di tutto il processo di sviluppo sw;
- L'Analista Funzionale, se previsto da progetto, è responsabile delle analisi concettuali del progetto; il Team Leader è responsabile dell'analisi di dettaglio. Se la figura dell'analista funzionale non è prevista nel progetto, è il Team Leader che si occupa di tutte le analisi;
- Il Team Leader è il responsabile di tutti i deliverable richiesti per il processo di realizzazione del software e responsabile della loro archiviazione sull'archivio aziendale.

La fase di verifica interna sul Progetto è un evento opzionale su progetto e riguarda la Funzione Quality Assurance ed è costituito dal controllo interno di qualità. Le attività del QA sono trasversali alle fasi del progetto e comunque pianificabili dal PM come un momento di ispezione del sw.

All'interno della BU ICT la funzione di Compliance & Quality Assurance, garantisce il monitoraggio della normativa e definisce gli interventi di adeguamento dell'applicazione C.Sost.

[Torna al sommario](#)

## 5.2 Strutture organizzative

Nel presente paragrafo vengono descritte le strutture organizzative, comprese le responsabilità, che intervengono nelle principali funzioni che riguardano il servizio di conservazione.

All'interno del sistema di conservazione C.SOST è stata prevista una struttura organizzativa comprensiva di funzioni, responsabilità e obblighi in capo ai diversi soggetti che intervengono nel processo di conservazione. Più precisamente, sono individuati i seguenti ruoli:

- **PRODUTTORE:** persona fisica o giuridica, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione;
- **UTENTE:** persona, ente o sistema che interagisce con i servizi del sistema di conservazione al fine di fruire delle informazioni di interesse.

Tali ruoli sono completati dalle figure designate quali “responsabili” dei servizi loro assegnati, come indicato al paragrafo 4 del presente Manuale, cui si rinvia.

L’attivazione del servizio di conservazione C.SOST avviene a seguito di formale accettazione dell’offerta e delle condizioni contrattuali di servizio da parte del Cliente, inclusi gli atti di nomina sottoscritti tra le parti per svolgere il ruolo di Responsabile del servizio di conservazione e Responsabile del Trattamento dei dati. L’Area Commerciale di COMDATA comunica l’attivazione del servizio di conservazione all’Area Amministrazione per la gestione dell’anagrafica Cliente, inviando tramite sistema aziendale la richiesta di attivazione operativa del Cliente all’Area Assistenza di COMDATA che, presa in carico l’attività, contatta il Cliente ed avvia la predisposizione dell’Allegato B - Specificità del Contratto.

Predisposta e condivisa la Scheda Servizio Cliente, validata dal Responsabile del servizio di conservazione di COMDATA e dal Cliente, l’area di Assistenza ingaggia l’Area di Produzione che avvia le attività di configurazione del servizio nella piattaforma C.SOST al fine di eseguire il collaudo.

Completato con esito positivo il collaudo, viene attivato il processo di rilascio descritto nel documento “ICT-PGA-0005 - Processo di Rilascio in Application Management Ed 03 - 12 luglio 2016.pdf” attivando la configurazione in ambiente di produzione.

Si passa quindi alla gestione del processo di conservazione dei documenti del Cliente.

Le attività sono organizzate per produrre la massima efficienza nell’ambito del processo di conservazione, il quale viene realizzato attraverso l’esecuzione di procedure informatiche atte allo scopo. A tale proposito, è stato previsto e pianificato un piano formativo per ogni risorsa adibita al servizio di conservazione. Il Responsabile del servizio di conservazione sovrintende e coordina comunque tutte le fasi del processo produttivo che possono essere raggruppate nelle seguenti attività principali:

- **alimentazione:** è la fase che dà avvio al processo di conservazione, con acquisizione dei pacchetti di versamento e rilascio del rapporto di versamento. La documentazione oggetto di conservazione può essere acquistata sotto forma di documento informatico;
- **elaborazione e conservazione:** è la fase caratterizzata dalla generazione del pacchetto di archiviazione e termina con l’apposizione della firma digitale del Responsabile ai documenti oggetto di conservazione e della marca temporale rilasciata da un Ente Certificatore Autorizzato. La fase è gestita direttamente dal Responsabile o da suoi eventuali delegati, dotati di poteri di firma, appositamente nominati ed incaricati per le specifiche attività.
- **esibizione:** consiste nella esibizione della documentazione conservata a norma a fronte di richieste da parte delle autorità competenti. I dispositivi di memorizzazione consentono una rapida ricerca e selezione del singolo documento in base agli indici di ricerca previsti dalla normativa. Tramite gli indici è immediato risalire al corrispondente documento ed effettuarne una copia. E’ altresì possibile rendere disponibili le informazioni richieste in fase di esibizione direttamente su supporto cartaceo.

[Torna al sommario](#)

## 6 OGGETTI SOTTOPOSTI A CONSERVAZIONE

Gli oggetti della conservazione sono trattati dal sistema di conservazione attraverso differenti pacchetti informativi denominati:

- **Pacchetti di versamento:** cioè i pacchetti con i quali, il soggetto produttore conferisce gli oggetti da conservare al sistema di conservazione
- **Pacchetti di archiviazione:** cioè i pacchetti con i quali il sistema di conservazione archivia i dati con garanzia di integrità e reperibilità nel tempo
- **Pacchetti di distribuzione:** cioè i pacchetti con i quali i dati archiviati sono resi disponibili alla comunità degli utenti abilitati per la consultazione.

### 6.1 Oggetti conservati

Il sistema di conservazione C.SOST è in grado di trattare e conservare le seguenti categorie documentali:

- documento informatico, fatta eccezione per i documenti per cui siano previste per legge specifiche modalità di trattamento. (es trattamento dati sensibili, dati giudiziari etc)
- fascicoli e aggregazioni informatiche;
- documenti informatici a rilevanza fiscale.
- Messaggi di poste elettronica certificata (PEC)

Le politiche di conservazione applicabili a predette categorie documentali sono compiutamente descritte al paragrafo 7 del presente Manuale.

### 6.2 Tipologie di documenti conservati

Documenti con rilevanza fiscale	<ul style="list-style-type: none"> <li>● Fatture attive</li> <li>● Fatture Passive</li> <li>● Libri e registri fiscali</li> <li>● DDT</li> <li>● Distinte meccanografiche</li> </ul>
Documenti del Lavoro	<ul style="list-style-type: none"> <li>● LUL</li> </ul>
Documenti clientela	<ul style="list-style-type: none"> <li>● Contratti</li> <li>● Corrispondenza</li> <li>● Documenti Acquisti</li> </ul>
Documenti Assicurativi	<ul style="list-style-type: none"> <li>● Libri e registri assicurativi</li> <li>● Polizze e appendici di polizza</li> <li>● Comunicazioni alla clientela</li> <li>● Dichiarazioni</li> </ul>
Documentazione Firma Elettronica Avanzata	<ul style="list-style-type: none"> <li>● Documenti Identità Cliente</li> <li>● Accettazione condizioni di utilizzo della FEA</li> </ul>



[Torna al sommario](#)

## 6.2.1 Metadati

I metadati per la conservazione utilizzati da C.SOST sono quelli minimi indicati e definiti nell'allegato 5 del D.P.C.M. 3 dicembre 2013 - Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 con riferimento al documento informatico, al documento amministrativo informatico e al fascicolo informatico o aggregazione documentale informatica.

In particolare, con riguardo al **documento informatico** sono utilizzati, secondo uno schema XML, i seguenti indici:

- a. Identificativo univoco e persistente;
- b. Data di chiusura;
- c. Oggetto;
- d. Soggetto produttore;
- e. Destinatario.

Quanto al **documento amministrativo informatico**, i metadati minimi sono quelli indicati agli articoli 9 e 19 del D.P.C.M. 3 dicembre 2013 - Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 relativamente alla segnatura di protocollo (in precedenza contenuti nel D.P.C.M. 31 ottobre 2000 - Regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica 20 ottobre 1998, n. 428 e nella Circolare AIPA del 7 maggio 2001, n. 28).

Si tratta quindi di:

- a. Codice identificativo dell'amministrazione;
- b. Codice identificativo dell'area organizzativa omogenea;
- c. Codice identificativo del registro;
- d. Data di protocollo;
- e. Progressivo di protocollo.

Quanto ai **fascicoli** e alle **aggregazioni informatiche** i metadati minimi utilizzati secondo lo schema XML sono:

- a. Identificativo univoco e persistente;
- b. Amministrazione titolare;

- c. Amministrazioni partecipanti;
- d. Responsabile del Procedimento;
- e. Oggetto;
- f. Documento.

Infine per i **documenti a rilevanza fiscale** si utilizzano i metadati minimi a tal fine individuati dall'art. 3, comma 1, lett. b) del D.M. 17 giugno 2014 - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto. Si tratta quindi di:

- a. Cognome;
- b. Nome;
- c. Denominazione;
- d. Codice fiscale;
- e. Partita IVA;
- f. Data;
- g. Numero Fattura/Numero protocollo IVA

[Torna al sommario](#)

## 6.2.2 Formati

Con riferimento all'Allegato 2 del DPCM del 3 dicembre 2013 “Regole Tecniche in materia di documento informatico e gestione documentale, protocollo informatico e conservazione di documenti informatici”) vengono qui elencati i Formati Digitali accettati da COMDATA e utilizzati per la formazione dei documenti informatici:

- PDF (ISO32000-1): Si specifica che, nel caso di utilizzo di questo formato, il Produttore si impegna a non spedire verso il sistema di conservazione documenti contenenti al proprio interno codice javascript, compressione, cifratura, funzionalità aggiuntive e plug-in.
- PDF/A
- TIFF
- JPG (ISO/IEC 10918:1)
- OOXML (ISO/IEC DIS 29500:2008)
- ODF (ISO/IEC 26300:2006)
- XML
- TXT

[Torna al sommario](#)

### 6.2.3 Formati di documenti firmati digitalmente

CAdES	ETSI TS 101 733
PadES	ETSI TS 102 778
XadES	ETSI TS 101 903

[Torna al sommario](#)

## 6.3 Pacchetto di versamento

La struttura del pacchetto di versamento è stata progettata per garantire da un lato la massima flessibilità da parte dei soggetti produttori e dall'altro per assicurare la sicurezza e l'eshaustività dei processi di validazione formale delle informazioni ricevute.

La natura del pacchetto è definita da uno schema XML che consente il trasferimento al sistema di conservazione delle informazioni sui documenti oggetto della conservazione e sugli attributi ad essi associati, attributi necessari al popolamento delle strutture dati utilizzate per il reperimento dei documenti all'interno degli archivi, ovvero per la distribuzione degli stessi alla comunità di utilizzatori.

Ciascun pacchetto di versamento è sempre relativo ad un insieme di documenti denominato pacchetto. Il pacchetto è costituito da due elementi primari strettamente correlati:

- Un file xml contenente le informazioni generali del pacchetto e gli indici dei documenti
- Uno o più documenti

Il pacchetto di versamento è consegnato dal produttore su una area di interscambio precedentemente definita. All'interno di questa area la cartella di file system dovrà essere costruita nel seguente modo:

- File xml a livello di root
- Directory a livello di root contenente singole immagini. Questa directory, può essere a sua volta suddivisa in sotto-directory senza nessun vincolo.

Il pacchetto di versamento è consegnato all'interno di un archivio compresso di tipo .ZIP che deve essere creato in modo che in fase di estrazione nella root di archivio sia presente il file xml e la directory delle immagini.

[Torna al sommario](#)

### 6.3.1 Struttura del file XML

Il file xml di input conterrà informazioni di testata a livello del pacchetto e informazioni di dettaglio a livello di singolo documento.

In particolare l'xml è così strutturato:

```
<ROOT>  
  <INFO>
```

```

</INFO>
<LIST_KEYS>
</LIST_KEYS>
<DOCUMENTS FAMILY="">
  <DOCUMENT>
    <INDEX_FIELDS>
    </INDEX_FIELDS>
    <LIST_LINK>
    </LIST_LINK>
    <DOCUMENT_PAGES>
    </DOCUMENT_PAGES>
  </DOCUMENT>
</DOCUMENTS>
</ROOT>
  
```

[Torna al sommario](#)

### 6.3.2 Informazioni di Testata del Pacchetto: NODO <INFO>

Il nodo <INFO> contiene le informazione riguardanti il pacchetto, quindi informazioni di testata. Il nodo e tutti i nodi figli indicati di seguito sono obbligatori. I figli nodo definiti sono i seguenti :

NODO	VALORE	NOTE
LOAD_DOCUMENTPATH	È il percorso relativo, partendo dall'xml, dove si trovano le immagini. Tale percorso viene concatenato al valore del nodo <PAGE> figlio di <DOCUMENT_PAGE> all'interno di <DOCUMENT>	Tale valore può essere vuoto se l'intero percorso relativo è indicato nel nodo <PAGE>, assieme al nome dell'immagine
CUSTOMER_ID	È l'identificativo univoco all'interno di C.SOST del cliente al quale appartiene il pacchetto	Il valore viene fornito ai sistemi esterni come costante. Si può omettere nel caso venga valorizzato il tag <PIVA_COD_FISC>
PIVA_COD_FISC	E' la partita IVA o il codice fiscale del cliente.	Si può indicare per identificare il cliente al posto del CUSTOMER ID.
MAP_ID	È l'identificativo univoco della mappa di conservazione all'interno della quale deve essere caricato il pacchetto.	Il valore viene fornito ai sistemi esterni come costante
COURIER_NAME	E' il nome del pacchetto	Tale valore deve essere univoco
SIGN_SINGLEDDOC	Indica se i documenti devono essere firmati singolarmente prima di essere conservati. Può assumere i valori "Y" o "S" (se devono essere firmati) o "N" (se non devono essere firmati)	

<HASH_TYPE>	Indica il tipo di algoritmo utilizzato per il calcolo dell'impronta dei singoli documenti. I possibili valori sono : <ul style="list-style-type: none"> <li>- SHA1</li> <li>- SHA256</li> <li>- SHA512</li> </ul> Il nodo ha un attributo denominato "CODE" che indica la codifica dell'impronta. I possibili valori sono i seguenti: <ul style="list-style-type: none"> <li>- HEX (esadecimale)</li> <li>- BASE64</li> </ul>	
-------------	---	--

Tabella 1: Struttura XML, nodo &lt;INFO&gt;

[Torna al sommario](#)

### 6.3.3 Definizione della chiave univoca dei documenti: NODO <LIST\_KEYS>

Il nodo <LIST\_KEYS> non è obbligatorio e, se non necessario, può essere omissso.

Viene utilizzato per indicare le chiavi univoche che identificano un documento. E' utilizzato dal processo di alimentazione per identificare eventuali documenti precedentemente caricati.

Nel caso in cui si voglia utilizzare, deve contenere al suo interno uno o più nodi figli denominati <KEYFIELD>.

Il valore di <KEYFIELD> deve essere il nome del campo (indice dei documenti) univoco.

Se vengono indicati più nodi <KEYFIELD> questi vengono utilizzati in "AND" dal processo di caricamento.

[Torna al sommario](#)

### 6.3.4 Lista dei documenti del pacchetto: NODO <DOCUMENTS>

Il nodo <DOCUMENTS> contiene l'elenco dei documenti appartenenti al pacchetto. Ogni documento è identificato da un nodo <DOCUMENT>.

Il nome <DOCUMENTS> ha un solo attributo:

- FAMILY: il valore di tale attributo è l'identificativo univoco della famiglia documentale di C.SOST nella quale devono essere conservati i documenti. Tale valore è una costante fornita ai sistemi esterni.

[Torna al sommario](#)

### 6.3.5 Informazioni di dettaglio dei documenti: NODO <DOCUMENT>

Tale nodo identifica e descrive un singolo documento del pacchetto. I suoi attributi sono i seguenti:

ATTRIBUTO	VALORE	NOTE
-----------	--------	------

OP_TYPE	Valore costante "INPUT"	
DOC_DATE	È la data ufficiale del documento. Per le fatture attive, per esempio, è la data di emissione	Formato DD/MM/YYYY

Tabella 2: Struttura XML, nodo &lt;DOCUMENT&gt;

I nodi figli di <DOCUMENT> sono i seguenti:

NODO	VALORE	NOTE
INDEX_FIELDS	Contiene l'elenco degli indici del documento. Ogni indice è rappresentato da un nodo <FIELD>. L'attributo "NAME" contiene il nome del campo da inserire, mentre l'attributo "VALUE" contiene il valore da inserire nel campo.	
LIST_LINK	Contiene l'elenco degli eventuali link ad altri documenti (associazioni) precedentemente archiviati su C.SOST. Un documento può essere associato a più documenti. Ogni link viene indicato con il nodo <LINK> figlio di <LIST_LINK>.	Il nodo <LINK> è descritto nella tabella successiva.
DOCUMENT_PAGES	Contiene un nodo figlio <PAGE> il cui valore è nome del documento da caricare comprensivo di percorso relativo a partire dall'xml. Il nodo <PAGE> può avere due attributi: <ul style="list-style-type: none"> <li>• <b>HASH</b> il cui valore è l'impronta del documento. L'impronta deve essere indicata nel formato e nella rappresentazione indicata nel tag HASH TYPE della sezione &lt;INFO&gt;</li> </ul>	N.B. Tale percorso viene concatenato al valore di <LOAD_DOCUMENTPATH> della sezione <INFO>

Tabella 3: Struttura XML, figli nodo &lt;DOCUMENT&gt;

[Torna al sommario](#)

### 6.3.6 Associazioni tra documenti: NODO <LINK>

Il nodo <LINK> rappresenta un link a un documento da associare a quello che si sta caricando.

Il documento a cui si desidera associare il documento corrente deve essere stato precedentemente caricato su C.SOST.

Il nodo <LINK> ha i seguenti attributi:

ATTRIBUTO	VALORE	NOTE
FAMILY	Identificativo univoco su C.SOST della famiglia documentale a cui appartiene il documento da associare.	Tale valore viene fornito ai sistemi esterni come costante
NOTE	È un campo testo dove si possono indicare eventuali note che	facoltativo

	descrivono il motivo dell'associazione dei due documenti	
--	--	--

Tabella 4: Struttura XML, nodo &lt;LINK&gt;

Nel nodo <LINK> si devono indicare le condizioni per individuare il documento da associare al documento corrente.

Si possono indicare più campi che identificano il documento; in questo caso verranno utilizzati in AND da C.SOST.

Ogni indice viene indicato nel nodo <FIELD\_LINK>.

Gli attributi di <FIELD\_LINK> sono i seguenti:

ATTRIBUTO	VALORE	NOTE
NAME	È il nome del campo su C.SOST (es.: numero fattura)	
VALUE	È il valore che il campo deve avere per identificare il documento da associare (es.: 12345)	

Tabella 5: Struttura XML nodo &lt;LINK&gt;

Esempio:

```
<LINK family="XX" NOTE="Note di associazione-facoltative" >
  <FIELD_LINK NAME="numero Documento" VALUE="123" />
  <FIELD_LINK NAME="dataDocumento" VALUE="20090128" />
  <FIELD_LINK NAME="piva_Cod_Fisc" VALUE="IT.12345678901" />
</LINK>
```

In questo caso il documento corrente verrà associato “logicamente” alla fattura n. 123 del 28/01/2009 del cliente IT.12345678901. L’associazione sarà biunivoca.

[Torna al sommario](#)

### 6.3.7 Esempio di tracciato XML valorizzato

La figura seguente riporta un esempio di struttura XML valorizzata in base alle regole precedentemente esposte.

```
<ROOT>
<INFO>
<LOAD_DOCUMENTPATH>01234567890_FTATT_20090205_1</LOAD_DOCUMENTPATH>
<CUSTOMER_ID></CUSTOMER_ID>
<PIVA_COD_FISC>12345678901</PIVA_COD_FISC>
<MAP_ID>1</MAP_ID>
<COURIER_NAME>01234567890_FTATT_20090205_1</COURIER_NAME>
<SIGN_SINGLEDIOC>N</SIGN_SINGLEDIOC>
<HASH_TYPE CODE="BASE64">SHA512</HASH_TYPE >
```

```

</INFO>
<LIST_KEYS>
  <KEYFIELD>SEZIONALE</KEYFIELD>
  <KEYFIELD>NUMERO_FATTURA</KEYFIELD>
  <KEYFIELD>ANNO</KEYFIELD>
</LIST_KEYS>
<DOCUMENTS FAMILY="1">
<DOCUMENT OP_TYPE="INPUT" DOC_DATE="03/02/2009">
  <INDEX_FIELDS>
    <FIELD NAME="NUMERO_FATTURA" VALUE="001" />
      <FIELD NAME="DATA_FATTURA" VALUE="20090203" />
    <FIELD NAME="PIVA_COD_FISC_CLIENTE" VALUE="IT.00891951006" />
    <FIELD NAME="RAG_SOCIALE_CLIENTE" VALUE="MARIO ROSSI" />
    <FIELD NAME="TIPO" VALUE="FT" />
    <FIELD NAME="CODICE_CLIENTE" VALUE="12345" />
    <FIELD NAME="UNIQUE_ID" VALUE="123" />
    <FIELD NAME="SEZIONALE" VALUE="A" />
    <FIELD NAME="BU" VALUE="XX" />
    <FIELD NAME="ANNO" VALUE="2009" />
    <FIELD NAME="SUB_CUSTOMER" VALUE="SUB " />
  <FIELD NAME="COMPANY" VALUE="COMPANY" />
</INDEX_FIELDS>
<DOCUMENT_PAGES>
  <PAGE HASH ="XXXXXXXXXXXXXXXXXXXXX">00001\01234567890_FTATT_20090205_1_00001.PDF</PAGE>
</DOCUMENT_PAGES>
</DOCUMENT>
<DOCUMENT OP_TYPE="INPUT" DOC_DATE="03/02/2009">
  <INDEX_FIELDS>
    <FIELD NAME="NUMERO_FATTURA" VALUE="002" />
      <FIELD NAME="DATA_FATTURA" VALUE="20090203" />
    <FIELD NAME="PIVA_COD_FISC_CLIENTE" VALUE="IT.00891951006" />
    <FIELD NAME="RAG_SOCIALE_CLIENTE" VALUE="MARIO ROSSI" />
    <FIELD NAME="TIPO" VALUE="FT" />
    <FIELD NAME="CODICE_CLIENTE" VALUE="12345" />
    <FIELD NAME="UNIQUE_ID" VALUE="123" />
    <FIELD NAME="SEZIONALE" VALUE="A" />
    <FIELD NAME="BU" VALUE="XX" />
    <FIELD NAME="ANNO" VALUE="2009" />
    <FIELD NAME="SUB_CUSTOMER" VALUE="SUB " />
  <FIELD NAME="COMPANY" VALUE="COMPANY" />
</INDEX_FIELDS>

  <DOCUMENT_PAGES>
    <PAGE HASH ="XXXXXXXXXXXXXXXXXXXXX">00001\01234567890_FTATT_20090205_1_00002.PDF</PAGE>
  </DOCUMENT_PAGES>
</DOCUMENT>
</DOCUMENTS>
</ROOT>

```

[Torna al sommario](#)

## 6.4 Pacchetto di archiviazione

La struttura del pacchetto di archiviazione selezionata è quella definita dallo standard UNI1138600\_2010



denominato “Supporto all’Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali” (SInCRO). Si riporta di seguito per una visione di immediatezza una rappresentazione grafica della struttura XML rimandando alla norma UNI1138600\_2010 per la descrizione di dettaglio.

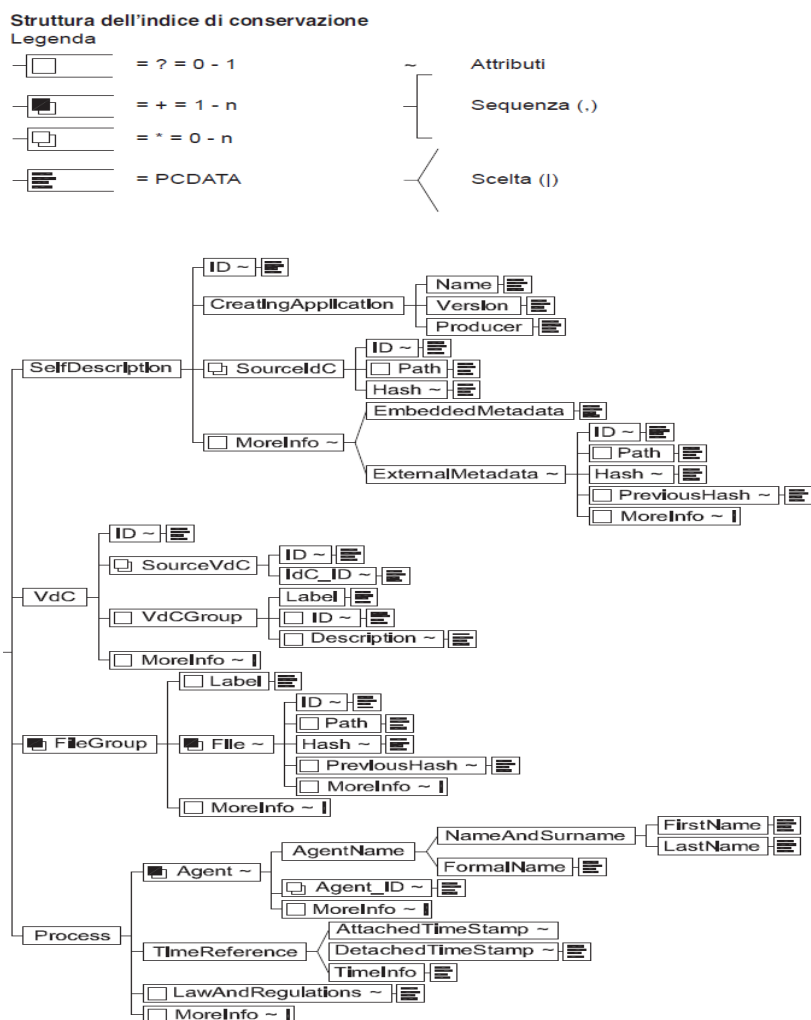


Figura 2 - Strutture XML SInCRO

[Torna al sommario](#)

## 6.5 Pacchetto di distribuzione

La struttura del pacchetto di distribuzione selezionata è la stessa adottata per il pacchetto di archiviazione,

ovvero quella definita dallo standard UNI1138600\_2010, denominato “Supporto all’Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali” (SInCRO).

Il pacchetto di Distribuzione è generato e reso disponibile al Cliente secondo la procedura indicata nel paragrafo 7.5 del presente Manuale.

[Torna al sommario](#)

## 7 IL PROCESSO DI CONSERVAZIONE

In questa sezione si descrivono:

1. le modalità di presa in carico di uno o più pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento;
2. la descrizione del processo di generazione e trattamento dei pacchetti di archiviazione;
3. la modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;

C.SOST è un’applicazione software che consente di implementare il processo di conservazione per le differenti tipologie di documenti per i quali la normativa stabilisce la possibilità di venire conservati in formato digitale, evitando di fatto l’obbligo di conservare i corrispondenti archivi cartacei.

A seconda della tipologia di documento che si vuole trattare l’applicazione è in grado di gestire le opportune differenze fornendo diversi percorsi strutturati identificati come Mappe di Conservazione di cui al capitolo 7.9 del presente Manuale, associate alle diverse tipologie di documenti.

All’interno del processo di conservazione si possono tuttavia individuare alcune attività che devono essere compiute indipendentemente dalla tipologia di documenti che si vogliono conservare.

La seguente figura schematizza il processo di conservazione implementato dall’applicazione C.Sost.

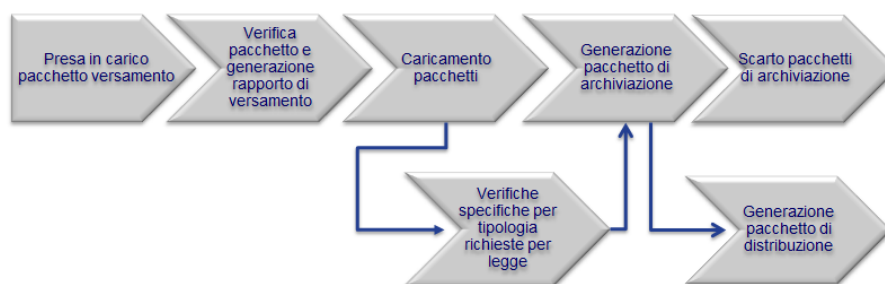


Figura 3 – Schema del Processo di Conservazione

[Torna al sommario](#)

## 7.1 Modalità di trasferimento dei pacchetti di versamento.

La modalità di alimentazione del sistema di conservazione C.Sost prevede il trasferimento dei pacchetti di versamento in una specifica area di interscambio. Il protocollo di trasferimento dei pacchetti di versamento è l'SFTP.

Viene messa a disposizione del Cliente un'area dedicata, con utente e password personali, dove il Cliente stesso può trasferire i pacchetti di versamento che saranno presi in carico dal sistema di conservazione..

Tuttavia esistono casi in cui il Cliente chiede modalità di trasferimento differenti (per es. prelievamento da una sua area SFTP o l'adozione di specifici software di trasferimento dati). Tali casi, se presenti, sono descritti nell'Allegato B (Specificità del contratto).

Indipendentemente dalla modalità di trasferimento tutti i pacchetti ricevuti sono sottoposti preventivamente ad analisi antivirus attraverso specifico software di analisi residente sui server che espongono il servizio SFTP.

Una volta che i pacchetti di versamento sono disponibili sull'area SFTP il sistema li prende in carico e dopo aver effettuato i controlli di correttezza formale procede alla generazione del "Rapporto di Versamento".

[Torna al sommario](#)

## 7.2 Verifica dei pacchetti di versamento e generazione del rapporto di versamento.

Il rapporto di versamento viene sempre creato a partire dal pacchetto di versamento. Se il formato del pacchetto non è quello standard previsto dal sistema ma è in un formato specifico concordato con il Cliente Produttore e descritto nell'allegato B – Specificità del Contratto, il rapporto di versamento viene generato, a partire dal pacchetto standard C.SOST creato da COMDATA su delega del cliente.

Esempi di pacchetti non standard:

- PDF con metadati nella naming convention
- TXT da convertire in PDF
- Pacchetti con metadati presenti in un formato custom del cliente
- Ecc.

Il rapporto di versamento è sempre caricato sul sistema ed è consultabile e scaricabile dal sito web di C.SOST.

[Torna al sommario](#)

### 7.2.1 Controlli sul pacchetto di versamento

I controlli effettuati sul pacchetto di versamento sono i seguenti:

- Verifica che il file xml sia valido;
- Verifica che il file xml sia ben formato secondo le schema;
- Verifica che il cliente e la tipologia documentale indicata siano configurati e attivi su C.SOST;
- Verifica che tutti i documenti referenziati nel file xml siano presenti sul file system;
- Verifica che tutti i documenti presenti su file system siano referenziati dentro l'xml dei metadati;
- Verifica che le impronte dei singoli documenti ricalcolate corrispondano a quelle indicate nel pacchetto di versamento;
- Verifica che i metadati obbligatori indicati nell'Allegato B (Specificità del contratto) siano stati valorizzati;
- Verifica che il formato dei metadati sia quello concordato con il Produttore e indicato nell'Allegato B (Specificità del contratto)..

Il rapporto di versamento è un file xml, firmato digitalmente dal responsabile della conservazione, contenente le seguenti informazioni relative al pacchetto di versamento:

- Esito del controllo del pacchetto di versamento, dove “esito” può assumere i seguenti valori:
  - OK
  - KO
- Data e ora di produzione del rapporto di versamento
- Nome del pacchetto di versamento ricevuto
- Impronta del pacchetto di versamento
- Dimensione del pacchetto di versamento
- Numero documenti contenuti nel pacchetto

Il file xml relativo al rapporto di versamento ha la seguente struttura:

```

<C.SOST version="x.y.z">
  <rapportoDiVersamento esito="" ID="">
    <ListaErrori> “Presente solo in caso di esito KO”
      <codiceErrore="" descrizione=""/>
      <codiceErrore="" descrizione=""/>
    </ListaErrori>
    <InfoPacchettoVersamento>
      <dataOraRapporto/>
      <nome Flusso/>
      <hashXml/>
      <dimensione Xml/>
      <dimensioneFlusso/>
      <numero_documenti/>
    </InfoPacchettoVersamento>
    <detailsRdv>
      “ qui viene inserito l'xml standard C.SOST dei metadati del pacchetto di versamento. Comprende quindi i metadati e le impronte dei documenti; in caso di errore, a livello di nodo <DOCUMENT> verrà aggiunto una attributo “errore” contenente la descrizione dell'errore relativo al documento.”
    </detailsRdv>
  </rapportoDiVersamento>
</C.SOST>
  
```

Dove:

- *Esito*: è l'esito del rapporto di versamento
- *ID*: identificativo univoco del rapporto di versamento all'interno del sistema di conservazione
- *dataOraRapporto*: è la data e ora di generazione del rapporto di versamento
- *NomeFlusso*: è il valore di "COURIER\_NAME" dell'xml standard C.SOST
- *hashXml*: è l'impronta del file xml dei metadati
- *dimensioneXml*: è la dimensione del file xml
- *dimensioneFlusso*: è la dimensione del file xml + tutti i documenti in esso linkati
- *NumeroDocumenti*: è il numero dei documenti contenuti nel pacchetto

I rapporti di versamento sono sottoposti a conservazione e sono collegati logicamente ai documenti a cui si riferiscono, quando il rapporto di versamento è positivo.

Il rapporto di versamento è consultabile e scaricabile sul sito web di C.SOST.

Informazioni di dettaglio: NODO <RapportoDiVersamento>

Tale nodo identifica il rapporto di versamento. I suoi attributi sono i seguenti:

ATTRIBUTO	VALORE	NOTE
Esito	Esito del rapporto di versamento	I valori possibili sono i seguenti: <ul style="list-style-type: none"> <li>• OK</li> <li>• KO</li> </ul>

Tabella 6: Struttura XML, attributi di < RapportoDiVersamento>

I suoi figli sono i seguenti:

- InfoPacchettoDiVersamento
- ListaErrori (facoltativa)
- detailsRdv

Informazioni di dettaglio NODO <InfoPacchettoDiVersamento>

NODI FIGLIO	VALORE	NOTE
dataOraRapporto	dd/mm/yyyy hh:mm:ss	Data e ora di generazione del rapporto di versamento
nome Flusso	Nome del pacchetto indicato nel tag COURIER NAME del pacchetto di	

	versamento	
hashXml	Hash del file XML	
DimensioneXml	Dimensione del file xml dei metadati	
DimensioneFlusso	Dimensione dello zip espressa in byte	
numeroDocumenti	Numero dei documenti contenuti nel pacchetto di versamento	

Tabella 7: Struttura XML, nodo nodi figli di &lt; InfoPacchettoDiVersamento&gt;

### Informazioni di dettaglio NODO <ListaErrori>

Tale nodo è presente soltanto se l'esito del rapporto di versamento è KO e contiene la lista degli errori riscontrati dalle procedure di verifica pacchetto di versamento.

E' una lista di <CodiciErrore> contenente il codice dell'errore riscontrato.  
 I suoi attributi sono i seguenti:

ATTRIBUTO	VALORE	NOTE
descrizione	Descrizione dell'errore riscontrato	

Tabella 8: Struttura XML, attributi di &lt; ListaErrori &gt;

### Informazioni di dettaglio: NODO <hashXml>.

I suoi attributi sono i seguenti:

ATTRIBUTO	VALORE	NOTE
HashType	Può assumere i seguenti valori: <ul style="list-style-type: none"> <li>• SHA1</li> <li>• SHA256</li> <li>• SHA512</li> </ul> Default: SHA512	Tipo di algoritmo utilizzato per generare l'hash
HashCode	Può assumere i seguenti valori: <ul style="list-style-type: none"> <li>• BASE64</li> <li>• HEX</li> </ul>	

### Codici di esito del rapporto di versamento

Codice	Descrizione
--------	-------------

OK	Presenza in carico positiva
KO	Presenza in carico fallita

### Codici di errore del rapporto di versamento

Codice	Descrizione
0001	Cliente non attivo o non presente
0002	Famiglia inesistente o non attiva per il cliente
0003	Documenti su file system mancanti ma referenziati nell'xml
0004	Documenti in xml mancanti ma presenti su file system
0005	Impronta non corrispondente
0007	Metadati obbligatori mancanti
0008	Formato o lunghezza metadati non consentita
0009	File indice xml non valido
0010	File indice xml non ben formato secondo lo schema
0017	File corrotto
0018	File protetto
0019	Metadati duplicati
9999	Errore generico; contattare l'amministratore del sistema.

[Torna al sommario](#)

### 7.2.2 Pacchetti di versamento conformi

All'esito delle verifiche positive viene generato il Rapporto di versamento **OK** e il pacchetto viene caricato sul sistema.

Sulle tabelle documentali del servizio di conservazione vengono archiviati i metadati relativi al pacchetto di versamento ricevuto.

In particolare vengono archiviate le seguenti informazioni:

- Soggetto produttore del pacchetto
- Data e ora in cui è stato accettato e firmato con il certificato del responsabile del servizio di conservazione
- Data di caricamento sul sistema
- Esito
- Nome del pacchetto di versamento
- Dimensione in MB del pacchetto di versamento
- Numero dei documenti contenuti nel pacchetto di versamento
- Dimensione file xml dei metadati
- Hash file xml dei metadati

[Torna al sommario](#)

### 7.2.3 Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie

All'esito delle verifiche negative viene generato il Rapporto di versamento KO e il pacchetto viene scartato.

Il soggetto produttore verrà informato tramite email automatica del rifiuto di un pacchetto di versamento; il body della mail conterrà l'elenco degli errori riscontrati sul pacchetto.

Se definito nell'allegato B il produttore può richiedere di ricevere il rapporto di versamento KO nell'area di interscambio utilizzata per l'invio dei pacchetti di versamento. In questo modo l'integrazione della comunicazione del dettaglio degli errori riscontrati tra i sistemi è completamente automatizzata.

Sulle tabelle documentali del servizio di conservazione vengono archiviati i metadati relativi al pacchetto di versamento ricevuto.

In particolare vengono archiviate le seguenti informazioni:

- Soggetto produttore del pacchetto
- Data e ora in cui è stato accettato e firmato con il certificato del responsabile del servizio di conservazione
- Data di caricamento sul sistema
- Esito
- Nome del pacchetto di versamento
- Dimensione in MB del pacchetto di versamento
- Numero dei documenti contenuti nel pacchetto di versamento
- Dimensione file xml dei metadati
- Hash file xml dei metadati

[Torna al sommario](#)

## 7.3 Caricamento del pacchetto di versamento sul sistema C.Sost

La fase di caricamento dei documenti sul sistema C.Sost può essere eseguita con due modalità differenti che sono concordate con il cliente e configurate nel sistema per il trattamento dei suoi pacchetti di versamento. Ad ogni tipologia di documenti trattati per il Cliente, sarà associata esclusivamente una delle due modalità di seguito descritte.

- Modalità a pacchetto completo: se il pacchetto di versamento contiene documenti da conservare che rispettano le regole prestabilite per la specifica tipologia (ad esempio per un pacchetto di fatture, queste dovranno rispettare la numerazione consecutiva), il pacchetto viene correttamente caricato sul sistema, viceversa in presenza di anomalie il processo di caricamento viene sospeso e il sistema genera una segnalazione. Il pacchetto non è conservato.
- Modalità a documento: prevede che il pacchetto di versamento sia incompleto e quindi possa contenere documenti



che non rispettino nel loro insieme i vincoli di controllo definiti per la specifica tipologia (ad esempio un pacchetto di fatture dove esistono buchi di numerazione, cioè dove qualche documento non è ancora stato prodotto). In questo caso il sistema provvede automaticamente a generare il più grande pacchetto che sia conforme e procede a conservarlo, in attesa che siano trasmessi i documenti mancanti. All'arrivo dei successivi documenti, il sistema provvede a generare e conservare automaticamente un nuovo pacchetto.

[Torna al sommario](#)

## 7.4 Preparazione e gestione del pacchetto di archiviazione

Conclusa la fase di caricamento sul sistema C.SOST del pacchetto di versamento del cliente, viene generato il pacchetto di archiviazione.

Ogni pacchetto di archiviazione è univocamente identificato all'interno del sistema.

Il pacchetto di documenti appartenenti ad un pacchetto di archiviazione è sempre omogeneo per tipologia di documenti contenuta al suo interno.

Per la generazione del pacchetto di archiviazione viene utilizzato, come richiesto dal decreto, il formato SinCro.

In particolare:

- viene generato un file xml secondo lo schema dello standard UNI SINCRO . Tale file verrà firmato con certificato digitale del Responsabile del servizio di conservazione e vi sarà altresì apposta una marca temporale. Viene quindi prodotta una busta p7m;
- i metadati minimi obbligatori stabiliti dal decreto vengono inseriti nel tag <MoreInfo> di ogni singolo <FileGroup> all'interno del file Sincro;
- opzionalmente può inoltre essere generato un file xml esterno e referenziato nell'xml UNI SINCRO all'interno del tag "MoreInfo" come ExternalMetadata, contenente i metadati specifici dei documenti. Verrà definito uno schema per ogni tipologia di documento. Tale file è facoltativo in quanto contiene metadati extra del documento che non fanno parte di quelli obbligatori.

[Torna al sommario](#)

## 7.5 Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione

I documenti conservati sono consultabili dalla interfaccia web di C.Sost accessibile via internet attraverso protocollo https.

L'accesso al sistema in modalità di consultazione è garantito agli Utenti opportunamente autorizzati, limitatamente agli archivi del Produttore di appartenenza e in base agli accordi contrattuali con esso intercorsi.

Attraverso opportuni criteri di ricerca è possibile individuare i documenti di interesse.

L'esibizione dei documenti è effettuata attraverso la generazione di un pacchetto di distribuzione che è possibile creare nelle seguenti modalità:

- Esibizione **“on the fly”**: si tratta dell'esibizione di un singolo documento ricercato sull'interfaccia di consultazione. L'applicazione mostra all'utente le informazioni relative alla firma digitale e la marca temporale apposte sul pacchetto di archiviazione a cui appartiene il documento oggetto di esibizione. E' inoltre possibile effettuare il download di un pacchetto zip contenente:
  - Il file Sincro di chiusura contenente il documento ricercato ed eventuali file correlati
  - Il documento stesso
- Esibizione su **supporto ottico rimovibile**: è possibile richiedere la produzione di un supporto DVD contenente uno o più pacchetti di distribuzione. In questo caso il pacchetto di distribuzione corrisponde a uno o più pacchetti di archiviazione. In questo caso il personale incaricato del trasporto dei supporti fisici viene scelto sulla base dei requisiti definiti dal Responsabile del servizio di conservazione ed in ogni caso saranno rispettate le seguenti istruzioni:
  - i supporti fisici non devono presentare riferimenti esterni (etichette) che possano permettere l'identificazione dell'ente produttore, dei dati contenuti, della loro tipologia etc.
  - i dati trasmessi sono protetti da sistemi crittografici
- Esibizione **selettiva**: attraverso una apposita funzionalità disponibile sull'interfaccia web di C.SOST è possibile richiedere la generazione di un pacchetto di distribuzione selettivo. Selezionando quindi più documenti, anche appartenenti a pacchetti di archiviazione differenti, il sistema genererà un file compresso contenente:
  - Tutti i documenti selezionati e oggetto di conservazione
  - Tutti i file Sincro, ed eventuali file referenziati, relativi ai pacchetti di archiviazione a cui appartengono i documenti selezionati.

Il pacchetto di distribuzione così generato sarà disponibile nelle modalità stabilite e riportate nell'allegato B – Specificità del contratto

[Torna al sommario](#)

## 7.6 Produzione di duplicati e copie informatiche

La conservazione dei pacchetti di archiviazione in C.Sost avviene su supporti sono magnetici ad alte capacità e performance, che garantiscono la ridondanza interna del dato. E' inoltre eseguito un backup periodico su tape magnetico.

Oltre a queste modalità, possono essere generati anche duplicati o copie su supporto ottico rimovibile, su specifica richiesta del Cliente. Tali copie sono tipicamente inviate al Cliente, oppure mantenute da Comdata.

Le copie possono essere generate automaticamente alla fine del processo di conservazione, oppure on-demand in qualsiasi momento. Nel secondo caso il Cliente inoltra la richiesta ai suoi riferimenti abituali (help desk o account) che poi provvedono alla veicolazione verso gli operatori interni.

La creazione di copie in caso di adeguamento del formato rispetto all'evoluzione tecnologica sarà presa in carico dal Responsabile del servizio della conservazione e dalle figure professionali coinvolte nel processo di conservazione in base alle specifiche del formato in questione e al know-how tecnologico a disposizione.

A fronte di questa analisi sarà progettata una soluzione di concerto con il soggetto Produttore del formato più idoneo per permettere la leggibilità del documento conservato.

Comdata richiede la presenza di un pubblico ufficiale nei casi in cui sia previsto il suo intervento assicurando allo stesso l'assistenza tecnica necessaria per l'espletamento delle attività al medesimo attribuite.

Ogni risorsa, comprese quelle di natura economica, necessaria per l'espletamento delle attività attribuite al pubblico ufficiale dovranno essere garantite e sostenute dal Cliente; pertanto, qualora il Cliente non se ne sia fatto carico direttamente, Comdata valuterà l'addebito dei costi e le spese, compresi gli onorari inerenti le attività prestate dal Pubblico Ufficiale, qualora la normativa ne richieda obbligatoriamente la presenza.

[Torna al sommario](#)

## 7.7 Scarto dei pacchetti di archiviazione

La legge prevede che per ciascuna tipologia di documenti informatici conservati a norma, i relativi pacchetti di archiviazione siano mantenuti nel Sistema di Conservazione per un periodo di tempo definito minimo definito per legge (es: documenti contabili 10 anni), trascorso il quale i pacchetti possono essere scartati e quindi rimossi dal sistema.

C.SOST consente di configurare il Sistema di Conservazione in modo tale da scartare i Pacchetti di Archiviazione al termine delle tempistiche previste dalla legge, così come esplicitato nelle specifiche Mappe di Conservazione di cui al capitolo 7.9 del presente Manuale.

Consente inoltre di gestire eventuali proroghe nel caso in cui il soggetto produttore abbia la necessità, per esempio per un procedimento in corso, di tenere conservato il documento per un periodo superiore a quello di legge o a quello concordato con il conservatore.

Con scadenza prefissata, un processo automatico di C.Sost, verifica se nell'archivio sono presenti pacchetti di archiviazione i cui tempi di minimi di permanenza sono naturalmente in scadenza oppure, nel caso di proroga, sta scadendo il periodo di estensione e quindi i pacchetti sono candidati per la procedura di scarto.

La lista dei pacchetti di archiviazione candidati per lo scarto è notificata per competenza al Responsabile della Conservazione del Cliente attraverso un messaggio PEC notificato all'indirizzo PEC comunicato dal Cliente a Comdata in fase di attivazione del servizio di conservazione.

Il processo di scarto prevede quindi i seguenti step:

- **Generazione automatica notifica PEC dei pacchetti in scadenza:** il soggetto produttore (Cliente) verrà avvisato tramite messaggio PEC che alcuni dei suoi pacchetti di archiviazione sono in scadenza e quindi, entro una determinata data saranno scartati, e conseguentemente rimossi in via definitiva dal sistema di conservazione.
- **Consultazione e proroga:** il soggetto produttore (Cliente) munito delle opportune credenziali di accesso al sistema, potrà consultare i pacchetti in scadenza e quindi candidati allo scarto e decidere se prolungarne il periodo di conservazione (proroga), oppure lasciare che proceda il processo di scarto. Opzionalmente, prima della scadenza segnalata dal sistema, può richiedere la creazione di un pacchetto di distribuzione contenente i pacchetti di archiviazione destinati ad essere scartati.
- **Conferma Operativa dello Scarto:** il Responsabile del Servizio di Conservazione di Comdata o un suo delegato, attraverso l'interfaccia del sistema, dovrà dare conferma dell'operazione di scarto dei pacchetti candidati, per autorizzare in via definitiva l'avvio della procedura di cancellazione dei pacchetti dal sistema.

Il tempo di conservazione dei pacchetti è definito per ogni diversa Mappa in Conservazione, in riferimento alla tipologia dei documenti gestiti.

Quando un pacchetto di archiviazione viene scartato, tutti i documenti e il file Sincro di chiusura vengono fisicamente eliminati dal sistema. Rimane comunque la traccia delle seguenti informazioni inerenti il pacchetto scartato:

- nome del pacchetto scartato
- tipologia
- numero documenti che conteneva
- dimensione
- data e ora in cui era stato conservato
- data e ora in cui è stato scartato dal sistema

Nel caso di archivi pubblici o privati di particolare interesse culturale, le procedure di scarto avvengono previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo.

[Torna al sommario](#)

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

C.SOST utilizza il file Sincro per la creazione del pacchetto di archiviazione e di distribuzione. Questo garantisce l'interoperabilità tra diversi sistemi di conservazione.

La Conservazione dei Pacchetti di Archiviazione avviene in regime di vigenza contrattuale. Dopo la cessazione del contratto decadono tutti gli obblighi e le responsabilità connesse al Servizio di Conservazione, compresa la nomina a Responsabile della Conservazione.

Tutti i Pacchetti di Archiviazione del Cliente in ogni caso saranno mantenuti nel sistema per il periodo previsto contrattualmente.

[Torna al sommario](#)

## 7.9 Mappe di conservazione.

Ogni pacchetto di documenti che è processato dal sistema di conservazione rappresenta l'unità minima di elaborazione prevista. I controlli, le verifiche e le lavorazioni sono quindi eseguiti sul pacchetto e per induzione sono applicati a tutti i documenti in esso contenuti.

L'elaborazione del pacchetto per la produzione del pacchetto di archiviazione è guidata e controllata da un sistema di workflow che implementa processi specifici per le diverse tipologie di documenti. I processi sono descritti attraverso le Mappe di Conservazione.

All'interno delle mappe sono definiti i passi elementari che devono essere portati a termine e le tempistiche massime entro cui devono essere svolti. Ogni passo elementare portato a termine identifica lo stato di avanzamento della lavorazione

[Torna al sommario](#)

## 8 IL SISTEMA DI CONSERVAZIONE

Il sistema di conservazione utilizzato da Comdata è denominato C.Sost ed è stato realizzato per conto di Comdata, dalla società Delta Progetti 2000, società controllata al 100% dal Comdata. La società Delta Progetti 2000 è integrata a livello organizzativo di Comdata, all'interno della sua divisione BU ICT.

La proprietà del sistema C.Sost è di Comdata, la quale affida a Delta Progetti 2000 le attività di manutenzione ordinaria ed evolutiva. Le singole attività sono commissionate da Comdata secondo le procedure standard degli acquisti di Comdata (RDA/Ordine). In questo senso quindi Delta Progetti 2000 sottostà al processo di ingaggio dei fornitori esterni secondo quanto definito dal documento H-PS-0003 ICT - DISCIPLINA DELLE TERZE PARTI e relativi riferimenti ai processi di qualità, in esso contenuti.

### 8.1 Componenti logiche

La seguente figura schematizza le componenti logiche della piattaforma C.Sost

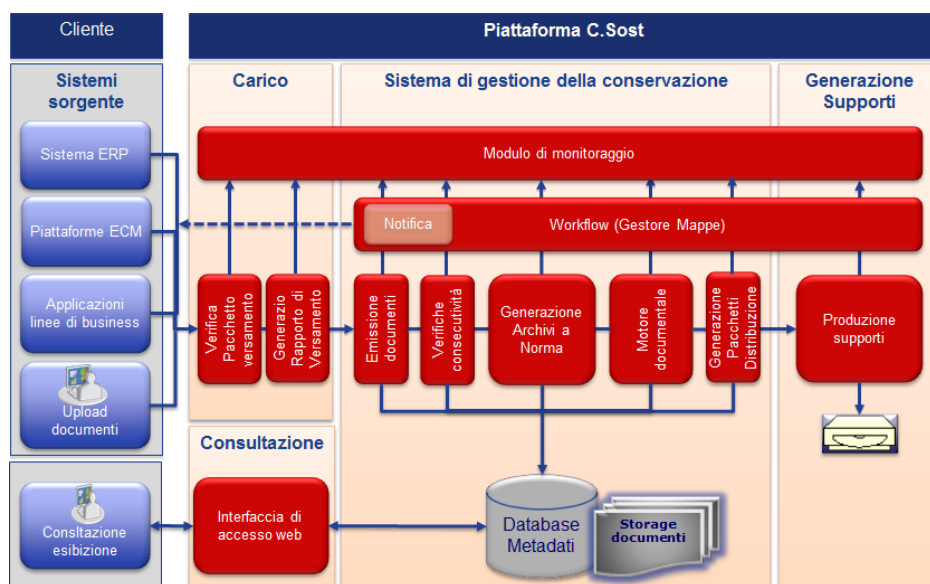


Figura 4 – Architettura logica del Sistema di Conservazione C.Sost

La piattaforma C.Sost consente la gestione end to end del processo di conservazione a norma conformemente a quanto indicato nel D.P.C.M. 3 dicembre 2013.

I principali moduli funzionali consentono la copertura dei seguenti aspetti del processo:

- **Presenza in carico e verifica dei documenti contenuti nel Pacchetto di Versamento:** vengono effettuate le procedure di controllo che garantiscono la conformità del pacchetto ai requisiti previsti

dalla normativa (ad esempio identificativo del soggetto produttore etc).

- **Verifica di consecutività per specifiche tipologie documentali:** contengono le procedure che consentono ad esempio la verifica della consecutività di numerazione delle fatture attive oppure la consecutività del numero di registrazioni per il LUL.
- **Generazione del Pacchetto di Archiviazione:** contengono le procedure che provvedono alla generazione, all'apposizione della firma ed alla marcatura temporale dei lotti e produce il "Pacchetto di Archiviazione". Il sistema genera pacchetti di archiviazione utilizzando, come xml di chiusura firmato e marcato, lo standard **SInCRO (UNI 11386)**
- **Motore documentale:** contiene le funzionalità di base per la ricerca dei documenti, la consultazione dei lotti di conservazione, la memorizzazione dei dati di tracciamento del processo, nonché tutte le funzioni di profilazione degli utilizzatori del sistema.
- **Generazione del Pacchetto di Distribuzione:** contiene le procedure che provvedono alla generazione del pacchetto di distribuzione. Il sistema genera pacchetti di archiviazione utilizzando, come xml di chiusura firmato e marcato, lo standard **SInCRO (UNI 11386)**
- **Interfaccia di accesso web:** è l'interfaccia utente che garantisce le funzionalità di ricerca, la consultazione dei documenti, e monitoraggio dello stato dei pacchetti di versamento, esibizione dei documenti.
- **Workflow:** è il modulo che consente di automatizzare e controllare le fasi del processo di conservazione previste per il corretto trattamento di una specifica tipologia di documenti. Per ciascuna tipologia, infatti, è prevista l'implementazione di una Mappa di conservazione, tecnicamente definita all'interno del motore di workflow. Dal momento dell'attivazione della mappa, a valle del caricamento di un pacchetto di documenti, il Workflow consente di eseguire automaticamente le attività previste, generando opportune segnalazioni al verificarsi di situazioni di anomalia e richiedendo in questo caso lo svolgimento di una attività manuale.
- **Modulo di Monitoraggio:** è il modulo che consente di verificare in maniera semplice e immediata lo stato di avanzamento dei lotti di documenti, all'interno del processo di conservazione.

[Torna al sommario](#)

## 8.2 Architettura tecnologica

L'applicazione è interamente sviluppata con tecnologia Microsoft .Net 4.5.

I principali componenti sono realizzati come servizi di windows e vengono attivati allo startup del sistema:

- **Orchestratore del workflow** - è il servizio principale della applicazione a cui è demandato il compito di attivare gli step di elaborazione previsti dallo specifico workflow di lavorazione. L'orchestratore attiva in modalità multithreading i singoli processi delegati allo svolgimento delle attività puntuali di elaborazione.
- **Generatore rapporto di versamento**- è il servizio che ha in carico la verifica della corretta conformazione del pacchetto di versamento e della generazione del rapporto di versamento. Il servizio carica inoltre il rapporto di

versamento sul sistema.

- **Loader pacchetti di versamento** – i pacchetti di versamento che hanno avuto esito di verifica positivo, sono presi in carico dal processo di caricamento che provvede ad elaborarli popolando adeguatamente la struttura dati dell'applicazione e memorizzando le immagini di documenti nelle aree di lavoro.  
**Verifica lotti** - implementa le logiche di controllo sulla correttezza formale dei lotti( es: consecutività numerazione fatture). Il processo a cui sono delegate le operazioni atomiche di verifica è realizzato come DLL.
- **Firma pacchetto e generazione pacchetto di archiviazione** - applica la firma e la marca temporale al pacchetto di conservazione attivando in modalità non assistita il dispositivo HSM e provvedendo alla generazione dell'archivio a norma nelle aree di archiviazione transitoria.
- **Generatore pacchetti di distribuzione** - prepara la struttura dati necessaria alla generazione del supporto.
- **Stoccaggio Archivi a Norma** - trasferisce gli archivi a norma dalle aree di archiviazione transitoria verso la struttura definitiva di archiviazione.
- **Notifica** - esegue la notifica di eventi o allarmi..

[Torna al sommario](#)

### 8.3 Architettura fisica

L'infrastruttura fisica del sistema C.SOST di conservazione può essere suddivisa in tre layer di seguito descritti:

1. **Primo livello**, rappresentato dallo strato *network* che è implementato dagli apparati *hardware* e *software* che garantiscono la segregazione del sistema e la protezione dagli accessi non autorizzati (modulo *firewall*). Le funzionalità pubbliche accedute dall'esterno sono gestite da sistemi di autenticazione e autorizzazione sofisticati. Tali funzionalità sono ridondate ed erogate tramite apparati di *load balancing*.
2. **Secondo livello**, tale livello è rappresentato da tutta l'infrastruttura *hardware* che eroga i principali servizi di conservazione come i trasferimenti dei pacchetti di versamento, la firma dei pacchetti di archiviazione e la generazione dei pacchetti di distribuzione.
3. **Terzo livello**, il *datastore* del sistema che contiene tutti i pacchetti di archiviazione e quindi i documenti sottoposti a conservazione .

La seguente figura schematizza l'architettura fisica della soluzione



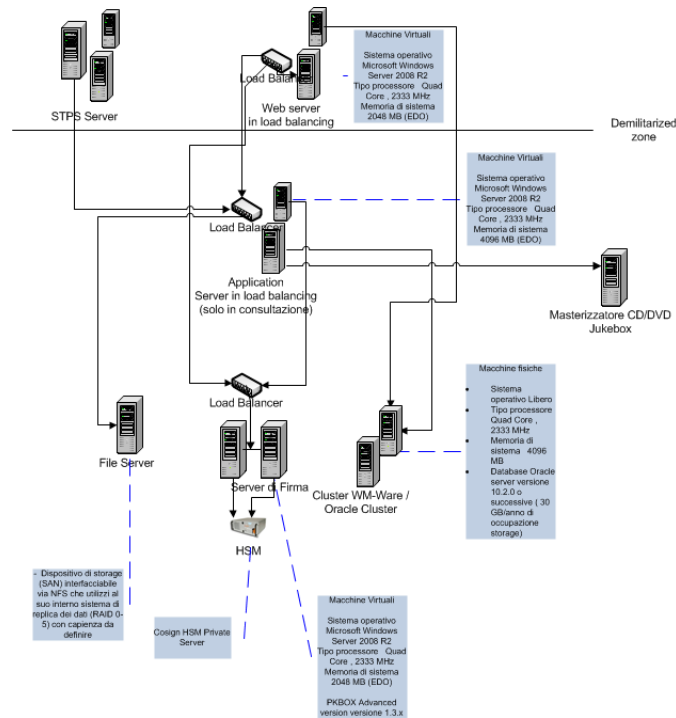


Figura 5 – Infrastruttura tecnica di erogazione del Sistema di Conservazione

[Torna al sommario](#)

## 8.4 Infrastruttura di erogazione

Il Gruppo Comdata dispone di due Data Center dedicati ai servizi di Conservazione, collocati a Rozzano (Milano) e La Spezia. I due siti distano tra loro più di 100km e sono configurati per erogare servizi in modalità di disaster recovery attraverso infrastrutture condivise e replicate.

Complessivamente i Data Center garantiscono una disponibilità globale dei sistemi del 99,9%, massimi standard di sicurezza fisica e logica e attività di gestione operativa e sistemistica a cura della struttura interna di IT Operations.



Figura 6 – Dislocazione geografica dei datacenter di erogazione Sistema di Conservazione

Il Data Center principale si trova a Rozzano, all’interno dell’Internet Data Center (IDC) di Telecom Italia. Il Data Center è dotato di avanzati sistemi e procedure che garantiscono al meglio la qualità dei servizi offerti:

- rilevazione fumi e spegnimento incendi;
- sistema anti allagamento ed anti intrusione;
- sistemi di condizionamento, continuità ed emergenza;
- controllo degli accessi fisici all’IDC e telecamere a circuito chiuso
- certificazione ISO/IEC 27001.

Il sito secondario è situato a La Spezia ed è dotato di:

- sistema di rilevazione fumi;
- sistema anti intrusione;
- sistemi di condizionamento, continuità ed emergenza;
- controllo degli accessi fisici al Data Center.
- certificazione ISO/IEC 27001.

[Torna al sommario](#)

### 8.4.1 Sistemi di Elaborazione e Archiviazione

La seguente figura rappresenta l’architettura fisica di erogazione della piattaforma C.Sost

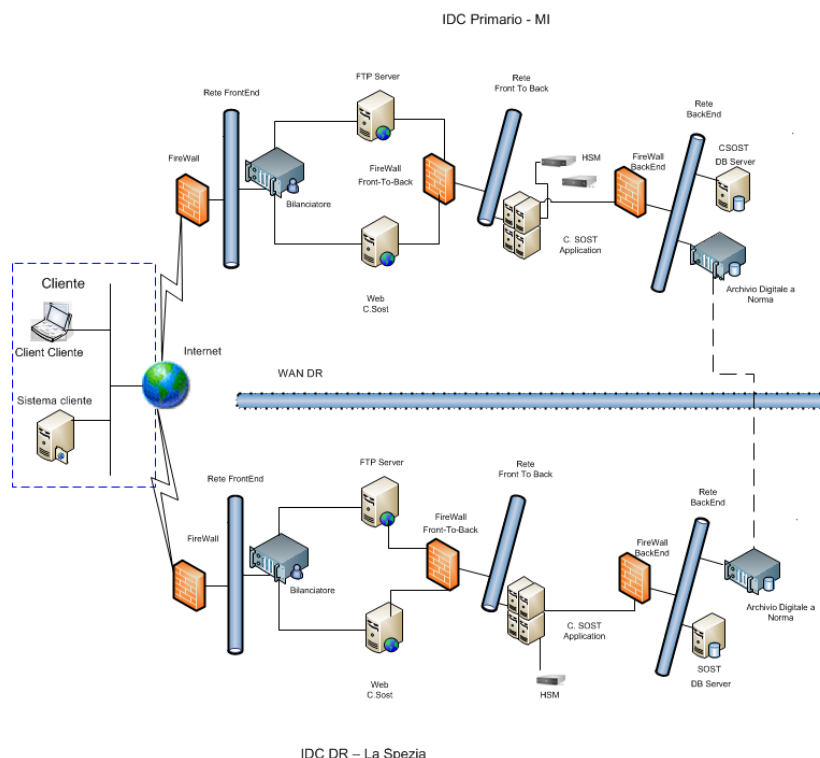


Figura 7 – Schema di infrastruttura tecnica di erogazione del Sistema di Conservazione

La struttura di rete del Data Center è organizzata a livelli con segregazione logica delle varie componenti infrastrutturali. Ogni livello è separato da gruppi di firewall fisici e/o virtuali in modalità High Availability. Tutti i livelli dispongono dei meccanismi di bilanciamento del traffico messi a disposizione dai bilanciatori hardware in High Availability. Il livello di front-end è dedicato alla ricezione dei dati da reti esterne e all'erogazione dei servizi web per la visualizzazione dei documenti.

I sistemi di bilanciamento si occupano anche della modalità di reverse proxy per non rendere direttamente accessibili i server applicativi.

[Torna al sommario](#)

### 8.4.2 Caratteristiche Hardware e Software dei Sistemi

Le piattaforma offerta è ospitata all'interno di una infrastruttura di elaborazione di livello "enterprise".

La soluzione si basa sulla combinazione di:

- server di elaborazione Microsoft Windows e Linux virtualizzati, basati sul sistema di virtualizzazione VmWare ESX 4 (Vsphere);
- sistemi hardware in tecnologia "blade", che consente ottima scalabilità, allocazione ottimale e gestione semplificata

delle risorse di elaborazione;

- supporto alle applicazioni basate sui sistemi operativi Linux – Microsoft Windows;
- sistema di storage su tecnologia leader di mercato;
- sistema di backup come ulteriore livello di protezione.

La maggior parte dei server applicativi è basata sull'implementazione di una infrastruttura di server virtuali gestita mediante il prodotto VMware ESX. Il datastore contenitore delle macchine VMware viene duplicato mediante il software di replica delle informazioni in rete geografica tra i due data center.

Nel caso di server attualmente non virtualizzabili (HSM, server di controllo e backup), questi sono replicati come ruoli nei due data center.

Il sistema di gestione dello storage è una Storage Area Network (SAN): si tratta di un'infrastruttura unificata flessibile, aggiornabile ed espandibile "on demand", compatibile con i protocolli FC (Fibre Channel) ed iSCSI (Internet SCSI).

La struttura della Storage Area Network è composta da due fabbriche distinte, ognuna delle quali composta, come dispositivi attivi, da due SAN switch fiber channel, due CPU di controllo del sistema di storage con alimentazione ridondata. L'espansione dalla SAN avviene attraverso l'aggiunta di enclosure disco anch'esse con alimentazione ridondata.

La coppia di switch permette di mettere in comunicazione in alta affidabilità le due controller pilotate dalle rispettive CPU con le enclosure mediante loop fiber channel che risultano quindi anch'essi ridondata.

L'aggiunta di dischi e di enclosure può essere effettuata a caldo senza avere disservizi sul servizio di erogazione dello storage verso i server.

I server vengono collegati alla SAN con un collegamento agli switch mediante un doppio canale fiber channel. Agli switch di SAN si appoggiano inoltre il sistema di gestione ed il sistema di backup.

Il sistema server di gestione è composto da un server collegato mediante un scheda dual con un doppio canale fiber channel a ciascuno dei due switch.

Il sistema di backup prevede un media server anch'esso collegato in fibra agli switch di storage area, a cui a sua volta è collegata anche l'unità che esegue i backup.

Sistemi di storage controller permettono la virtualizzazione degli spazi fisici e quindi la gestione ottimale degli spazi delle unità logiche che vengono presentate ai server.

Il Disaster Recovery geografico è realizzato utilizzando i meccanismi di replica delle storage area presenti nei data center. La replica dei dati avviene in modalità asincrona mediante il software messo a disposizione dai dispositivi per la replica dei dati.

[Torna al sommario](#)

## 8.4.3 Sistemi di Firma Digitale e Marca Temporale

### 8.4.3.1 Firma Digitale

Per le funzionalità specifiche di apposizione della firma digitale e della marca temporale ai documenti, la

soluzione integra componenti di mercato per l'utilizzo degli apparati HSM che ospitano i certificati di firma digitale automatica e per l'utilizzo dei servizi di Time Stamping resi disponibili dalle TSA accreditate presso l'AGID.

In particolare è integrata la Suite PK-Box di Intesi Group, che consente di implementare una soluzione di firma massiva in alta affidabilità.

Il sistema di firma massiva utilizza una coppia di HSM server Cosign HSM Private Server ed il software di firma PKBox di Intesi Group nella versione Enterprise.

Il sistema nel suo complesso offre la possibilità di memorizzare un numero illimitato di credenziali su database interno in modo da permettere la condivisione dei certificati tra tutti i server di firma.

Cosign HSM Private Server è certificato FIPS 140-2 Livello 3 e PCI-HSM v2.0 e certificato dall'organismo di controllo italiano OCSI.

PkBox è certificato come Dispositivo Sicuro di Firma (SSCD – Secure Signature Creation Device) che può quindi essere utilizzato per la realizzazione di soluzioni di Firma Digitale Remota Qualificata con piena validità legale, ai sensi della legislazione italiana ed europea.

#### 8.4.3.2 Marca Temporale

La soluzione non è vincolata ad utilizzare i servizi di marca temporale connessi ad una specifica Time Stamp Authority.

[Torna al sommario](#)

#### 8.4.4 Connettività

Per l'erogazione dei servizi proposti è previsto l'uso di connessioni protette tramite opportuni protocolli di crittografia standard (es. HTTPS, FTPS, SFTP) per garantire la riservatezza e la sicurezza dell'interscambio di informazioni tra il cliente e il IDC del Gruppo Comdata.

Per il trasferimento dei flussi dal Data Center del cliente verso i Data Center del Gruppo Comdata, sono supportate inoltre connessioni basate su software di trasferimento ad alta affidabilità (es Connect:Direct di Sterling Commerce).

L'allineamento dei dati per il Disaster Recovery utilizza la rete MPLS del Gruppo Comdata.

[Torna al sommario](#)

### 8.5 Luogo di conservazione dei documenti

I luoghi di conservazione dei documenti sottoposti al processo di Conservazione inclusi i documenti con rilevanza fiscale coincidono con i siti di esercizio della piattaforma C.Sost che sono di seguito indicati.

IDC Primario	IDC Comdata S.p.A.	C/O Data Center Telecom Italia Viale Toscana, 3 Rozzano (MI)
IDC secondario	IDC Comdata S.p.A.	C/O Comdata S.p.A.

Comdata comunica a tutti i clienti che utilizzano il servizio di Conservazione, eventuali variazioni dei suddetti luoghi almeno 10 giorni prima che la suddetta variazione diventi effettiva, in tempo utile per consentire, dove richiesto dalla norma, l'invio della comunicazione alle competenti autorità.

[Torna al sommario](#)

## 8.6 Sicurezza del sistema di conservazione

Comdata ha implementato un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) conforme alla norma ISO 27001. Nell'ambito del Sistema di Conservazione C.Sost sono adottate misure di sicurezza fisica, logica e organizzativa coerenti con tale SGSI e con la normativa vigente in tema di protezione dei dati personali (D.lgs. 196/2003).

### 8.6.1 Gestione della Privacy

Comdata esegue il trattamento dei dati personali in conformità a quanto previsto dal D.lgs. 196/2003 e dalla normativa vigente in materia; ciascun trattamento di dati personali è improntato ai principi di correttezza, liceità e trasparenza nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Tutte le misure minime di sicurezza obbligatorie previste dal DLgs 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali (Privacy), allegato B al medesimo e successivi provvedimenti del Garante sulla Privacy (in Italia) sono adottate.

Per assicurare la protezione dei dati personali sono adottati idonei sistemi di autenticazione informatica, di autorizzazione in relazione all'ambito del trattamento consentito ai singoli incaricati o classi omogenee degli stessi e di conservazione dei dati e delle copie di sicurezza. Periodicamente è verificata la corretta attribuzione agli incaricati delle abilitazioni di accesso e dei relativi profili di autorizzazione rilasciati.

Inoltre, è realizzata la formazione delle risorse che hanno accesso ai dati personali e è effettuata periodicamente l'analisi del rischio al fine di minimizzare i rischi di distruzione o perdita anche accidentale dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

La funzione Privacy (o in sua sostituzione il responsabile privacy della country) pianifica le attività necessarie per garantire la compliance della normativa in materia di protezione dei dati e individua di concerto con Information Security, per la sua parte di competenza, le modalità più opportune per l'applicazione delle misure di sicurezza.

## 9 PROCEDURE DI GESTIONE E DI MONITORAGGIO

Il servizio di conservazione è erogato da Infrastructure & Service Management di Comdata utilizzando l'applicazione C.Sost a supporto che regola gli step di processo in modo automatico.

L'applicazione segue un WorkFlow di lavorazione sulla base di una mappa di attività automatiche pre-configurate. Ogni attività automatica segnala l'esito dell'operazione tramite notifica e-mail al referente operativo.

Per erogare correttamente il servizio è fondamentale eseguire tutte le fasi di configurazione dei sistemi/applicazione al fine di garantire il corretto Start-Up.

[Torna al sommario](#)

### 9.1 Controllo del servizio

Il Referente Operativo del servizio di Conservazione definisce le modalità e le frequenze di controllo che devono essere effettuati dagli incaricati. I controlli sul processo hanno lo scopo di verificare che tutte le fasi dello stesso avvengano secondo quanto concordato e condiviso con il cliente e di monitorarne l'andamento. Si tratta di controlli di processo che riguardano trasversalmente tutte le lavorazioni e tutti i clienti.

Il controllo del servizio è effettuato dal Referente Operativo del servizio e dagli incaricati del controllo di Conservazione tramite il monitoraggio e l'analisi di:

- a) Monitoraggio integrato alla piattaforma C.Sost;
- b) Monitoraggio esterno alla piattaforma C.Sost.

Il Monitoraggio integrato avviene attraverso la verifica delle notifiche generate dalla piattaforma stessa. La piattaforma C.Sost garantisce l'applicazione del processo di Conservazione attraverso l'utilizzo di mappe di processo. Ogni mappa è composta da procedure automatiche, ogni procedura automatica al termine di ogni RUN genera una notifica e-mail di OK o KO che consente al personale operativo di intervenire attivamente nella soluzione di eventuali problemi (prendendo in carico la segnalazione e-mail di KO).

Il monitoraggio esterno alla piattaforma C.Sost è realizzato attraverso l'utilizzo dello strumento di Event Management Comdata (NAGIOS). In questo sistema sono state configurate sonde di monitoraggio che verificano lo stato di tutte le code di elaborazione della piattaforma C.Sost. La persistenza in una coda di elaborazione di documenti/lotti "Da Elaborare" per più di 2h genera un alert sul sistema di monitoraggio centrale.

Le notifiche gestite sono 3:

- a) **Notifica visiva:** Sul monitor della Control Room è visualizzato l'allarme, la struttura di Service Desk

Comdata rileva visivamente l'allarme e attiva via Trouble Ticket (con notifica telefonica in caso di allarmi che potrebbero indicare incidenti gravi) il riferimento di Application Management Comdata delegato alla soluzione del problema

b) **Notifica via e-mail:** è generata una notifica automatica ed inoltrata via e-mail al gruppo di Application Management delegato alla soluzione dei problemi C.Sost;

c) **Notifica via SMS:** è generata una notifica automatica ed inoltrata via sms al gruppo di Application Management delegato alla soluzione dei problemi C.Sost;

Owner del processo di gestione dell'allarme è il gruppo di Application Management. Questo gruppo esegue l'analisi del problema rilevato al fine di determinare fin da subito se il problema necessita di un intervento del cliente per essere risolto oppure l'entità del problema è tale da generare una notifica informativa verso il cliente. In caso affermativo il cliente viene informato via e-mail se il problema è particolarmente grave o urgente da risolvere il cliente viene informato anche telefonicamente.

[Torna al sommario](#)

## 9.2 Verifica dell'integrità degli archivi

Con cadenza non superiore a 36 mesi, la struttura operativa di esercizio, verifica lo stato di conservazione dei pacchetti di archiviazione, provvedendo, se necessario, al riversamento in base a quanto prescritto dall'Art. 7 comma g delle Regole Tecniche.

Il processo di verifica collaudo prevede un controllo su tutti i lotti di documenti che raggiungono il timing periodico di controllo.

Per ciascuno dei documenti oggetto del controllo sono effettuate le verifiche relative a:

- verifica della firma digitale e marca temporale apposta sul pacchetto conservato
- estrazione dei documenti contenuti nel pacchetto e per ciascuno ricalcolo dell'impronta e confronto con la relativa impronta contenuta nel file SINCRO di chiusura
- tracciamento su DB degli esiti di verifica
- segnalazione delle anomalie riscontrate

In caso di collaudo negativo si si procede con la duplicazione informatica dei dati utilizzando la copia di sicurezza, leggibile sul data storage secondario.

Il processo di verifica viene effettuato in modalità automatica, attraverso procedure software che sono schedate dal team di gestione operativa. Il processo genera con periodicità annuale un registro delle verifiche effettuate che viene firmato dal responsabile della conservazione ed archiviato nel sistema (dove e come è accessibile)

Verifiche Ispettive interne vengono pianificate dal responsabile della sicurezza, tenendo conto dello stato e dell'importanza dei processi e delle aree oggetto di verifica, nonché dei risultati delle precedenti verifiche.

Comdata verifica lo stato di conservazione dei pacchetti di archiviazione, e provvede alla produzione delle copie informatiche al fine di adeguare i formati in conformità a quanto previsto dall'art. 11 delle Regole



Tecniche e relativo Allegato 2, nel caso di evoluzione del contesto tecnologico e/o obsolescenza dei formati utilizzati.

### 9.2.1 Processo di gestione dell'obsolescenza

Il Responsabile Sviluppo e Manutenzione del sistema di conservazione monitorizza l'evoluzione delle tecnologie di gestione dei documenti e individua i formati che sono dichiarati fuori supporto dai diversi vendor. Verifica se all'interno degli archivi a norma sono presenti documenti in formato fuori supporto, individua di concerto con il vendor, la soluzione di migrazione più efficace e definisce la procedura di migrazione dei documenti, cioè la procedura di copia informatica di documenti informatici (Art 6 – dpcm 13 nov 2014)

I documenti migrati sono sottoposti ad un processo di verifica di consistenza che garantisce la corretta trasposizione dei contenuti informativi tra il vecchio ed il nuovo formato. A collaudo completato si procede all'inserimento dei documenti in un nuovo pacchetto di versamento che viene sottoposto al sistema di conservazione e segue l'iter standard dando origine al corrispondente PDA.

Il sistema mantiene comunque i PDA che contenevano i documenti in formato "obsoleto" nel sistema e crea una correlazione con i nuovi PDA contenenti i medesimi documenti, ottenuti per copia informatica.

[Torna al sommario](#)

## 9.3 Gestione delle segnalazioni

### 9.3.1 Pacchetti di versamento

La gestione delle segnalazioni relative alla non accettazione del pacchetto di versamento conferito al sistema C.Sost è eseguita da parte del Referente Operativo della Conservazione , assicurando le seguenti macro-attività:

- Informare, sulla base dei Controlli Impostati e quindi delle eventuali segnalazioni di KO, i referenti Tecnici del cliente ed eseguire l'analisi del problema volta a stabilire una soluzione concordata con i referenti Tecnici del Cliente e relativa implementazione operativa;
- Attivarsi, sulla base delle segnalazioni di anomalia ricevute dai referenti Tecnici del Cliente, per eseguire l'analisi del problema volta a stabilire una soluzione concordata con i referenti Tecnici del Cliente e relativa implementazione Operativa.

[Torna al sommario](#)

### 9.3.2 Anomalie di funzionamento del sistema C.Sost

Il servizio di conservazione , come descritto in precedenza è gestito all'interno della struttura Infrastructure & Service management della Direzione IT

Nell'ambito della struttura Infrastructure & Service management della Direzione IT si realizzano 4 processi fondamentali ITIL:

- Processo di **Event Management**: un evento è un cambio di stato che ha rilevanza ai fini della gestione di una configurazione di un servizio IT (potrebbe identificare un potenziale un malfunzionamento dell'infrastruttura IT).

Per rilevare questi cambi di stato sono utilizzati opportuni tool e sistemi di monitoraggio. Obiettivo del processo di event management è identificare e classificare l'evento e determinare l'azione preventiva più appropriata da eseguire. Il processo di event management è circoscritto alla struttura interna del Service Desk e coinvolge la figura del Responsabile dei Sistemi Informativi per la Conservazione.

- Processo di **Incident Management**: obiettivo del processo di incident management è di ripristinare le condizioni normali del servizio nel minimo tempo possibile assicurando che vengano garantiti i migliori livelli di servizio possibili. Il Responsabile funzione Archivistica, sulla base di Criticità rilevante (Es: mancato rispetto delle regole relative al processo di conservazione, Perdita di Dati etc.), informa il Responsabile del servizio di Conservazione al fine di concordare eventuali azioni risolutive e/o scalare ai Process Owner del Cliente e/o informare il Responsabile della Conservazione.
- Processo di **Problem management**: è il processo che si attua per identificare la causa primaria che ha dato luogo all'incidente (root cause) e per risolvere o prevenire eventuali problemi che tale causa può generare. Nel processo di problem management si valuta inoltre se la causa primaria comporti interventi specifici sulle infrastrutture o sulle applicazioni di Comdata o eventualmente del Cliente. Sono coinvolti in questo processo le figure di Responsabile della Archivistica, dei Sistemi Informativi e dello Sviluppo e Manutenzione del Sistema di Conservazione.
- Processo di **Change management**: fa parte del più ampio processo di Application Management che governa l'intero ciclo di vita delle applicazioni software dall'inizio della produzione fino alla dismissione. Le attività di Change management comportano in generale:
  - analisi e proposta di modifiche agli sviluppi software per manutenzione del software stesso
  - analisi e proposta di modifiche agli sviluppi software per migliorare la qualità del software
  - analisi e proposta di modifiche agli sviluppi software per garantirne la conformità
  - Sono coinvolti in questo processo le figure di Responsabile della Archivistica, dei Sistemi Informativi e dello Sviluppo e Manutenzione del Sistema di Conservazione

[Torna al sommario](#)

### 9.3.2.1 Procedure di Escalation

Nel caso in cui si verifichi un'anomalia che presenta criticità nel processo di risoluzione è prevista l'attivazione di una procedura di escalation. Nell'ambito del servizio, Comdata provvede a comunicare, i riferimenti interni della Direzione IT in grado di gestire tutti i livelli di Escalation.

L'escalation verticale definisce i processi di coinvolgimento nei diversi livelli di responsabilità (fino all'occorrenza al Top management) dell'organizzazione del Cliente e di Comdata, e si attiva quando le normali procedure di comunicazione falliscono.

Tale procedura si attiva in caso di grave impatto sull'erogazione del servizio ed ha lo scopo di informare il management aziendale sulla criticità in corso nelle seguenti condizioni:

- impossibilità di definire una soluzione prima del superamento della soglia di SLA
- necessità di ottenere risorse critiche da dedicare alla risoluzione dell'incident;
- necessità di informazioni sull'andamento della criticità.

Sono coinvolti in questo processo le figure di Responsabile della Conservazione, il direttore di IT e della BU ICT

[Torna al sommario](#)

## 9.4 Monitoraggio degli SLA

I livelli di Servizio (SLA) sono monitorati in real time in base agli strumenti messi a disposizione dal Committente e/o resi disponibili dalla struttura Infrastructure & Service Management.

Comdata dispone di una piattaforma di monitoraggio in grado di rilevare in real time anomalie o disservizi e di segnalarli con differenti livelli di gravità presso i monitor installati nella Contro Room. Le funzioni principali disponibili sono:

- monitoraggio dell'intera infrastruttura tecnologica
- progettazione e messa in esercizio sonde di Monitoraggio e Controllo dei Processi di Business;
- correlazione indicatori Applicativi e Infrastrutturali;
- implementazione e modifica di nuove regole di gestione degli allarmi;
- gestione degli allarmi vs. gli specialisti di area;
- gestione reportistica KPI-SLA.

Sono generati report di Sintesi Giornalieri, Mensili e Annuali che evidenziano una sola metrica: lo scostamento in giorni tra la data prevista conservazione dei documenti elettronici (data rilevata sulla base delle normative evidenziate nel manuale della conservazione ) e la data-ora conservazione.

[Torna al sommario](#)

## 9.5 Elaborazione della Reportistica

Un unico report ad uso interno con cadenze diverse è definito dal referente di servizio, secondo la seguente periodicità: giorno, mese, anno.

Il report è prodotto automaticamente ed evidenzia le informazioni di seguito elencate:

- Rag. Sociale: Ragione Sociale del Cliente che usufruisce del Servizio;
- Famiglia Documentale: Tipo di Famiglia documentale alla quale appartiene il - Documento Conservato;
- Nome pacchetto: Definizione Tecnica del Pacchetto al quale appartiene il Documento;
- Tot. Documenti: Totale Documenti appartenenti al Pacchetto Conservato.
- Numero primo documento: Identificativo del primo Documento presente nel Pacchetto Conservato.
- Numero ultimo documento: Identificativo dell'ultimo Documento presente nel Pacchetto Conservato.
- Data scadenza pacchetto: Data ultima
- Data conservazione: Data in cui il processo di Conservazione è Terminato.
- Scostamento in Giorni (KPI)
- SLA in GG

Il Report con cadenza Giornaliera è inoltrato al Referente Operativo della Conservazione e a tutti i suoi delegati ed incaricati. È generato da un batch schedulato ogni giorno.

I Report Mensili e Annuali sono inoltrati al Responsabile della Conservazione ed al suo sostituto.

[Torna al sommario](#)

## 9.6 Archiviazione dei documenti rilevanti ai fini del servizio

Il sistema C.Sost archivia in un'area riservata, i documenti rilevanti per il servizio di conservazione :

- Manuale della Conservazione
- Allegati B relativi alla specificità del contratto per ciascun cliente
- Registri di verifica

I documenti archiviati sono consultabili attraverso l'interfaccia web dell'applicazione da parte della struttura organizzativa che eroga il servizio di conservazione e dai clienti per i documenti strettamente di loro competenza.

[Torna al sommario](#)