Manuale della Conservazione

INTESA SPA

MDC_V15112021

Firmato da:
Luigi Traverso
Codice fiscale: TRVLGU65S25L219Q
Organizzazione: IN.TE.S.A. S.p.A./05262890014
Valido da: 16-04-2021 07:22:17 a: 15-04-2025 12:15:28
Certificato emesso da: IN.TE.S.A. Certification Authority, IN.TE.S.A. S.p.A., IT
Riferimento temporale 'SigningTime': 16-11-2021 09:29:32
Motivo: Approvo il documento

Emissione

Azione	Data	Nominativo	Funzione
Redazione	15/11/2021	Francesco De Cesare	SCS consultant
Verifica	15/11/2021	Luigi Traverso	Responsabile del Servizio di conservazione
Approvazione	15/11/2021	Luigi Traverso	Responsabile del Servizio di conservazione

Registro delle revisioni

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
MDC_V22102014	23/10/2014	Integrazioni e precisazioni richieste da AgID	Richieste AgID
MDC_V24112014	24/11/2014	Precisazioni su Ruoli e Responsabilità	Richieste AgID
MDC_V29012016	29/01/2016	Adeguamento allo schema versione 2_1 pubblicato dall'AgID	Richieste AgID
MDC_V14062021	14/06/2021	Adeguamenti diversi	Introduzione Linee Guida AGID
MDC_V24092021	24/09/2021	Aggiornamento dei ruoli professionali	Cambio responsabile del trattamento dei dati personali
MDC_V15112021	15/11/2021	Aggiornamento loghi aziendali	Cambio struttura societaria

Intesa

Sommario

1 Scopo e ambito del documento

Il presente manuale descrive il sistema di conservazione di In.Te.S.A. S.p.A. (di seguito Intesa) denominato Trusted Doc, definisce le competenze, i ruoli e le responsabilità degli attori coinvolti nel processo di conservazione dei documenti e il modello di funzionamento. Vengono riportate la descrizione del processo, delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento del sistema di conservazione.

In particolare, sono descritte le procedure operative adottate da Intesa per il processo di conservazione elettronica a norma di legge realizzato attraverso apposito Servizio per il Cliente.

Intesa è inoltre prestatore di servizi fiduciari qualificati (QTSP- Qualified Trust Service Provider) ai sensi del Reg. (UE) 910/2014 (eIDAS) per la firma elettronica, sigillo elettronico e validazione temporale elettronica (timestamp).

Il documento descrive le procedure adottate da Intesa secondo quanto definito dal contratto stipulato tra le parti e nel relativo Allegato Tecnico, in conformità alle normative e prassi in materia.

Il manuale riassume i compiti che sono descritti dal Codice dell'Amministrazione Digitale, di seguito anche "CAD" (Decreto Legislativo 7 marzo 2005, n. 82 e successive modifiche/integrazioni).

1.1 Ambito di riferimento

Il Servizio di conservazione erogato in modalità di Full Outsourcing è supportato dall'articolo 44 del CAD in base al quale la conservazione può essere svolta affidandola, in modo totale o parziale, ad altri soggetti, pubblici o privati che offrono idonee garanzie organizzative e tecnologiche e di protezione dei dati personali.

Il Cliente, ovvero il titolare dell'oggetto di conservazione affida il processo di conservazione ad Intesa e ai suoi responsabili interni nelle varie funzioni previste dalla normativa, descritte nel relativo Capitolo del presente MdC, "Ruoli e Responsabilità".

Nel Disciplinare tecnico, Allegato A sono delineate le specificità del Servizio per il Cliente.

1.2 Struttura del Manuale di conservazione

Il presente Manuale è prodotto in formato digitale da parte di Intesa (in collaborazione con il Cliente per quanto riguarda il Disciplinare tecnico), archiviato in apposito repository del Servizio ad uso interno Intesa e messo a disposizione del Cliente.

Nel caso di eventuali aggiornamenti e adeguamenti del presente documento la nuova versione verrà resa disponibile al Cliente.

Nel caso di eventuali aggiornamenti e adeguamenti del Disciplinare tecnico, da entrambe le parti, viene inviata copia al Responsabile della Conservazione e/o Responsabile di progetto del Cliente.

Nel presente documento sono parzialmente descritti aspetti architetturali e processi in essere, per un maggior dettaglio tecnico/funzionale si rimanda ai seguenti documenti:

- Contratto del servizio di conservazione;
- Disciplinare tecnico (Allegato A al Manuale della Conservazione) – in precedenza definito Specificità del Contratto;
- Eventuale documento di Analisi funzionale, per gli aspetti attinenti le implementazioni tecniche della Conservazione, non allegato al presente Manuale della Conservazione, predisposto sulla base dello specifico contesto progettuale del Cliente.

2 Terminologia (glossario e acronimi)

2.1 Acronimi

Di seguito i principali acronimi utilizzati nel documento e relative definizioni:

Acronimo	DEFINIZIONE
AgID	Agenzia per l'Italia Digitale
CAD	Codice dell'amministrazione digitale, Decreto Legislativo 7 marzo 2005, n. 82 e successive modifiche e integrazioni
IPdA	Indice del Pacchetto di Archiviazione – evidenza informatica associata ad ogni pacchetto di archiviazione contenente un insieme di informazioni articolate secondo lo standard SInCRO
IPdV	Indice del Pacchetto di Versamento
LLGG	Linee Guida sulla formazione, gestione e conservazione dei documenti informatici
MdC	Manuale della Conservazione
PdA	Pacchetto di archiviazione
PdD	Pacchetto di Distribuzione
PdV	Pacchetto di Versamento

RDC	Responsabile della Conservazione
RSC	Responsabile del Servizio di Conservazione
RSSC	Responsabile Sicurezza dei Sistemi per la Conservazione
RFA	Responsabile della Funzione Archivistica di conservazione
RTP	Responsabile del Trattamento dei dati Personali
RSI	Responsabile Sistemi Informativi pe la conservazione
RSM	Responsabile Sviluppo e Manutenzione del sistema di conservazione
RdV	Rapporto di versamento
SInCRO	Supporto all'interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI11386) - Standard nazionale in linguaggio xml, riguardante la struttura dell'insieme di dati a supporto del processo di conservazione
SLA	Monitoraggio del mantenimento dei livelli di servizio

2.2 Glossario dei termini

Di seguito un glossario dei termini utilizzati nel testo e relative definizioni:

Acronimo	DEFINIZIONE
Affidabilità	Caratteristica che, con riferimento a un sistema di gestione documentale o conservazione, esprime il livello di fiducia che l'utente ripone nel sistema stesso, mentre con riferimento al documento informatico esprime la credibilità e l'accuratezza della rappresentazione di atti e fatti in esso contenuta.
Allegato A	Disciplinare tecnico del presente manuale, riporta la descrizione degli elementi di dettaglio del processo di conservazione
Autenticità	Caratteristica in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto, un oggetto è autentico se nel contempo è integro e completo, non

	avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze.
Conservatore	Soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici.
Conservazione	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti.
Documento informatico	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
HASH	Impronta informatica di un documento ottenuta applicando una "funzione di hash" e costituita da una sequenza di simboli binari.
Integrità	Caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità.
Interoperabilità	Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi.
Linee Guida	Linee Guida sulla formazione, gestione e conservazione dei documenti informatici pubblicate in Gazzetta Ufficiale n. 259 del 19 ottobre 2020
Manuale della Conservazione	Documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture.
Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi.
Prestatore di servizi qualificati	Sono soggetti che rilasciano certificati qualificati a norma del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014 (eIDAS)
Trusted Doc	Servizio di conservazione di Intesa, erogato in modalità di outsourcing
Trusted Hub	Piattaforma tecnologica del Servizio di conservazione in outsourcing di Intesa

3 Normativa e standard di riferimento

3.1 Normativa di riferimento

Di seguito l'elenco dei principali riferimenti normativi italiani in materia:

- Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68 - Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005
- Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014, Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché' di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005
- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82
- REGOLAMENTO (UE) N. 910/2014 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE

- REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
- Decreto Ministero Economia e Finanze 17.06.2014 "Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005"
- Decreto Ministero Economia e Finanze del 3 aprile 2013, n. 55 "Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'art. 1, commi da 209 a 213, della legge 24 dicembre 2007. Pubblicato in G.U. n. 118 del 22 maggio 2013"
- Linee Guida sulla formazione, gestione e conservazione dei documenti informatici pubblicate in Gazzetta Ufficiale n. 259 del 19 ottobre 2020.

3.2 Standard di riferimento

Gli standard a cui Intesa risponde sono:

- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- ETSI TR 101 533-2 V1.3.1 (2012-04) Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- UNI 11386:2020 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

4 Ruoli e responsabilità

Nel sistema di conservazione si individuano almeno i seguenti ruoli:

- Titolare dell'oggetto della conservazione;
- Produttore dei PdV;
- Utente abilitato;

- Responsabile della conservazione;
- Conservatore.

Il titolare dell'oggetto di conservazione è il soggetto produttore degli oggetti digitali di conservazione.

Il produttore dei PdV è una persona fisica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Si tratta generalmente del soggetto incaricato alla produzione e/o gestione dei documenti e/o relativi metadati da inviare al sistema di conservazione, responsabile del contenuto del documento.

Nel caso di affidamento del servizio di conservazione a terzi, il produttore di PdV provvede a generare e trasmettere al sistema di conservazione i pacchetti di versamento nelle modalità e con i formati concordati con il conservatore e descritti nel manuale di conservazione del sistema di conservazione. Provvede inoltre a verificare il buon esito dell'operazione di trasferimento al sistema di conservazione tramite la presa visione del rapporto di versamento prodotto dal sistema di conservazione stesso.

L'utente abilitato è la 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; richiede al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge. Trattasi quindi del cliente o soggetti autorizzati all'accesso ai documenti.

Il responsabile della conservazione definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.

Il responsabile della conservazione, sotto la propria responsabilità, può delegare lo svolgimento delle proprie attività o parte di esse a uno o più soggetti, che all'interno della struttura organizzativa, abbiano specifiche competenze ed esperienze. Tale delega, riportata nel manuale di conservazione, deve individuare le specifiche funzioni e competenze delegate.
Nel caso in cui il servizio di conservazione venga affidato ad un conservatore, le attività suddette o alcune di esse, ad esclusione della predisposizione e aggiornamento del manuale della conservazione, potranno essere affidate al responsabile del servizio, rimanendo in ogni caso inteso che la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile, rimane in capo al responsabile della conservazione, chiamato altresì a svolgere le necessarie attività di verifica e controllo in ossequio alle norme vigenti sul servizi affidati in outsourcing dalle PA.

Il Cliente identifica quindi il proprio Responsabile della Conservazione che, a sua volta, avendone titolo e autorizzazione affida ad Intesa il processo di conservazione elettronica a norma di legge.

Rimane in carico al Responsabile della conservazione vigilare sulla corretta esecuzione del processo di conservazione: sul conservatore grava la responsabilità contrattuale nei confronti del cliente.

I dati identificativi del Responsabile della conservazione sono riportati nel disciplinare tecnico e, a seguito dell'affidamento, il processo di conservazione è affidato al Conservatore.

Il conservatore è quel soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici.

4.1 Dettaglio dei ruoli e relativi compiti

Allo scopo di garantire un adeguato e soddisfacente livello di qualità dei servizi offerti, la struttura aziendale di Intesa è organizzata per processi; a livello aziendale è quindi definito il quadro generale di riferimento delle procedure e delle relative competenze e responsabilità.

Ogni collaboratore, individualmente o come partecipante ad un team, per competenza, si attiene alle indicazioni delle procedure e delle istruzioni aziendali definite.

Le attività sono assegnate in base ai ruoli aziendali definiti.

Anche il processo di Conservazione è posto in essere sulla base di questo quadro organizzativo sia per gli aspetti di erogazione che di monitoraggio.

Le responsabilità attinenti ad Intesa, in qualità di Conservatore affidatario del servizio di conservazione sono definite nel disciplinare tecnico fornito al Cliente in conformità a quanto previsto dalla normativa.

Come richiesto sempre dalla normativa, Intesa svolge la propria funzione con la massima cura e presidio attraverso un gruppo di risorse specialistiche dedicate all'erogazione, gestione, supporto, presidio del Servizio, in base ad una stabile organizzazione interna aziendale. In tal modo garantisce la presenza di personale qualificato e diversificato in base alle specifiche esigenze, munito di preparazione professionale e di conoscenze tecniche adeguate, disponibile all'interazione con il responsabile della conservazione del Cliente nelle varie fasi del Servizio.

I ruoli definiti all'interno dell'organizzazione di Intesa e svolti nell'ambito del processo di conservazione sono descritti nel seguito, i riferimenti specifici sono riportati in disciplinare tecnico.

4.1.1 Responsabile della Conservazione

Il Responsabile della Conservazione è il Cliente - nella persona fisica formalmente designata all'interno dell'Azienda titolare dei documenti oggetto di conservazione - quale responsabile dell'insieme delle attività finalizzate alla conservazione a norma dei documenti informatici nell'ambito del contratto di outsourcing verso Intesa.

Nella gestione dell'intero processo di conservazione il RDC si rende garante, oltre che nei confronti del soggetto per cui opera anche nei confronti delle autorità fiscali, della corretta gestione del processo secondo principi di sicurezza stabiliti e documentati, adottando procedure di tracciabilità in modo tale da garantire la corretta gestione dei pacchetti informativi, la conservazione, l'accessibilità al singolo documento e la sua esibizione.

Il responsabile della conservazione all'interno della propria organizzazione opera d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei sistemi informativi.

Le attività del responsabile della conservazione in collaborazione con il Conservatore risultano determinanti in diverse fasi del processo di conservazione:

- Nella fase di apposizione del sigillo sull'indice del pacchetto di archiviazione e sul pacchetto di distribuzione; Intesa ha scelto di operare sui singoli documenti o sulle singole evidenze informatiche;
- Il responsabile della conservazione, in collaborazione con il Conservatore, riporta in Disciplinare tecnico il dettaglio delle casistiche che richiedono la presenza del pubblico ufficiale/notaio se previste nell'ambito della tipologia documentale trattata o dello specifico processo definito in accordo con il Conservatore;
- Il responsabile della Conservazione predispone il Manuale della Conservazione, in collaborazione con il Conservatore, descrivendo anche i dettagli specifici del progetto.

4.1.2 Responsabile del Servizio di Conservazione

Le attività del Responsabile del Servizio di Conservazione sono le seguenti:

- Definizione e attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione;
- Definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente;
- Corretta erogazione del servizio di conservazione all'ente produttore;
- Gestione delle convenzioni, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.

4.1.3 Responsabile della funzione archivistica di conservazione

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.
È la figura che svolge, attraverso la struttura aziendale preposta, i seguenti compiti:

- Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato;
- Definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici;
- Monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione;
- Collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.

4.1.4 Responsabile dei sistemi informativi per la conservazione

Le attività del Responsabile dei sistemi informativi per la conservazione sono le seguenti:

- Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione
- monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore

- segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive
- pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione
- controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.

4.1.5 Responsabile dello sviluppo e della manutenzione del sistema di conservazione

Le attività del Responsabile dello sviluppo e della manutenzione del sistema di conservazione sono le seguenti:

- Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione;
- Pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione;
- Monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione;
- Interfaccia con l'ente produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche;
- Gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.

4.1.6 Responsabile della sicurezza dei sistemi per la conservazione

Le attività del Responsabile della sicurezza dei sistemi per la conservazione sono le seguenti:

- Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza;
- segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.

4.1.7 Responsabile del Trattamento dei dati personali

Le attività del Responsabile del Trattamento dei dati personali sono le seguenti:

- Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali;
- garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.

5 Struttura organizzativa per il servizio di conservazione

La struttura organizzativa di Intesa si articola secondo una visione di management volta alla focalizzazione di alcune figure rilevanti nei ruoli specifici richiesti nell'ambito del processo di conservazione.

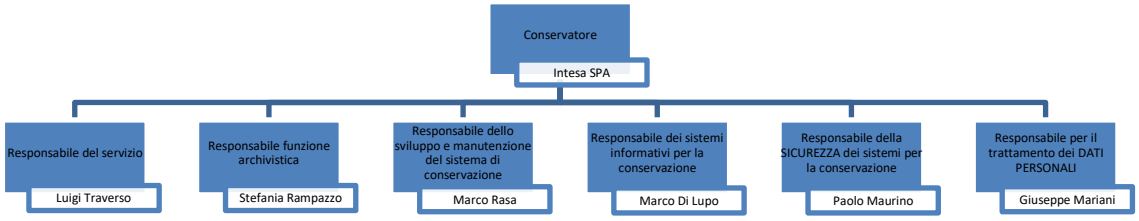
INTESA ha evidenziato e designato le figure professionali che compongono il team di lavoro sulla Conservazione dei documenti.

Il team è formato da risorse che operano nelle diverse aree aziendali per garantire la corretta esecuzione del servizio relativamente a tutte le problematiche tecnico/organizzative peculiari del servizio di cui trattasi.

Sono state quindi definite le opportune procedure organizzative interne per garantire il coordinamento univoco delle risorse del team affinché il loro lavoro si svolga in piena coerenza con i contenuti del servizio e con gli obiettivi di qualità dell'azienda.

5.1 Organigramma

Di seguito lo schema dell'organigramma interno di Intesa, dove si evidenziano le aree aziendali e i ruoli coinvolti nel sistema di conservazione:



5.2 Strutture organizzative

Di seguito lo schema dell'organigramma interno di Intesa, dove si evidenziano le aree aziendali e i ruoli coinvolti nel sistema di conservazione:

Legenda	
RDC	Responsabile della conservazione
RSC	Responsabile del servizio di conservazione
RSSC	Responsabile sicurezza dei sistemi per la conservazione
RFA	Responsabile della funzione archivistica di conservazione
RTP	Responsabile trattamento dei dati personali
RSI	Responsabile sistemi informativi per la conservazione
RSM	Responsabile sviluppo e manutenzione del sistema di conservazione

Attività ricoperte dal ruolo dei responsabili del servizio di conservazione						
	Responsabilità					
	RSC	**RSSC**	**RFA**	**RTP**	**RSI**	**RSM**
Attivazione del servizio di conservazione (a seguito della sottoscrizione di un contratto)	X	X	X	X	X	X
Acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento	X	X	X			X

Preparazione e gestione del pacchetto di archiviazione	X	X	X			X
Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta	X	X	X	X		X
Scarto dei pacchetti di archiviazione	X	X	X		X	X

	Attività proprie di gestione dei sistemi informativi					
	Responsabilità					
	RSC	**RSSC**	**RFA**	**RTP**	**RSI**	**RSM**
Conduzione e manutenzione del sistema di conservazione		X				X
Monitoraggio del sistema di conservazione		X			X	X
Change management	X	X			X	X
Verifica periodica di conformità a normativa e standard di riferimento	X		X	X		

6 Oggetti sottoposti a conservazione

6.1 Oggetti conservati

Il sistema di conservazione di Intesa è dotato di funzionalità tali da assicurare, dalla presa in carico dal produttore fino all'eventuale scarto, la conservazione, tramite l'adozione di procedure tecnologiche dei seguenti oggetti: i documenti informatici con i metadati (informazioni sulla conservazione).

Gli oggetti digitali della conservazione sono trattati dal sistema di conservazione in pacchetti informativi che si distinguono in:

a) Pacchetti di versamento;
b) Pacchetti di archiviazione;
c) Pacchetti di distribuzione.

Il modello concettuale di riferimento per la conservazione a lungo termine è il modello OAIS che è basato sulla creazione, archiviazione e conservazione di pacchetti informativi che sono entità composte di quattro elementi:

- Il contenuto informativo, cioè l'oggetto digitale (da conservare) e l'insieme delle informazioni che ne permettono la rappresentazione e la comprensione a livello utente;
- Le informazioni sulla conservazione che comprendono quelle di identificazione, di contesto, di provenienza e di integrità;
- Le informazioni "sull'impacchettamento", cioè i dati che indirizzano alla posizione logica del pacchetto informativo archiviato nel sistema di conservazione di Intesa;
- Gli oggetti sottoposti a conservazione con la descrizione delle tipologie, le informazioni di conservazione, le informazioni sulla rappresentazione, le periodicità di invio in conservazione, il periodo di durata della conservazione, i formati dei file previsti, i riferimenti normativi e le modalità di versamento (che sono descritti nel disciplinare tecnico).

L'interoperabilità tra i sistemi di conservazione dei soggetti che svolgono questa attività è garantita dall'applicazione delle specifiche tecniche del pacchetto di archiviazione definite dalla norma UNI 11386 - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.

Di seguito la tabella generale degli oggetti sottoposti a conservazione, il cui dettaglio specifico per Cliente, concordato quindi con il soggetto produttore, è riportato in disciplinare tecnico.

formato del file	visualizzatore	produttore	tipo MIME	standard	estensione
PDF	Adobe Reader	Adobe	application/ pdf	ISO32000	.pdf
PDF/A	Adobe Reader	Adobe	application/ pdf	ISO19005	.pdf

XML	Internet Browser	W3C	application/xml text/xml		.xml
TIFF	Visualizzatore di immagini	Adobe	image/tiff	ISO 12234	.tif, .tiff
JPEG	Visualizzatore di immagini	Joint Photographic Experts Group	image/jpeg image/jpg		.jpg, .jpeg
EML	Client di posta elettronica		application/email	RFC-5322 RFC2822	.eml

Ogni altro formato file deve essere concordato preventivamente ed integrato in disciplinare tecnico.

6.2 Pacchetto di versamento

In sede di acquisizione dati, è previsto l'invio del documento in uno dei formati previsti dall'Allegato 2 alle Linee Guida. Come indicato dalla normativa, il sistema di conservazione deve assicurare la fruibilità dei documenti conservati.

Il processo di conservazione elettronica dei documenti prevede quindi l'identificazione delle tipologie documentali e la gestione di campi indice, associati ai documenti, per la loro corretta identificazione.

La scelta degli indici da associare ai documenti viene effettuata in funzione della tipologia dei documenti da conservare e alle necessità di ricerca, in collaborazione con il Cliente, in relazione alle specifiche esigenze e contesto.

La descrizione delle tipologie degli oggetti sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti e dei metadati da associare alle diverse tipologie viene riportata nel disciplinare tecnico.

Il Cliente invia quindi alla piattaforma Intesa i documenti da conservare corredati dalle strutture di indici da abbinare.

L'indicizzazione dei documenti può eventualmente essere effettuata dalle procedure elaborative di Intesa in base a quanto specificatamente concordato con il Cliente.

Il sistema conservazione è predisposto per gestire i formati che possono maggiormente garantire i principi di interoperabilità tra i sistemi di conservazione e in base alla normativa vigente riguardante specifiche tipologie documentali.

Vengono quindi scelti, in accordo con il Cliente e in conformità a quanto indicato nell'Allegato 2 alle Linee Guida, i formati che possano consentire la leggibilità e l'interoperabilità del documento informatico nel sistema di conservazione.

Ogni PDV è riferito ad un oggetto versato ed è identificato in modo univoco.

Il pacchetto di versamento è costituito dai seguenti oggetti:

- L'indice del pacchetto di versamento;
- L'oggetto versato;
- Il file di metadati previsti dalle LG AGID;
- Eventuali schemi XSD.

6.3 Pacchetto di archiviazione

Il pacchetto di Archiviazione (da qui PDA) è un file contenitore (formato zip non compresso) che, al suo interno, contiene il documento originale versato, il file Indice del Pacchetto di Archiviazione (da qui IPdA) firmato (con sigillo) e marcato temporalmente, il file rapporto di versamento (da qui RdV) firmato e marcato temporalmente, in caso di riversamento il file IPdA del precedente conservatore, i file di schema xsd e un file ReadMe.txt.

Il PDA, con naming PDA.INTESA.IDHUB.ID.zip, sarà così composto:

- ReadMe.txt (file di testo che descrive composizione, la tipologia e significato dei file presenti);
- PIndex.INTESA.IDHUB.ID.xml.p7m (File IPDA dell'oggetto versato);
- pdv\ (Cartella contenente il PdV)
  - <DOC.INTESA.IDHUB.ID.ext> (Oggetto Versato)
  - <MT.INTESA.IDHUB.ID.xml> (File metadatazione allegato 5 LLGG);
- rdv\ (Cartella contenente il Rapporto di versamento)
  - RDV.INTESA.IDHUB.ID.xml.p7m (File Rapporto di Versamento);
- ipda_previous\ (Eventuale cartella contenente gli IPDA del precedente conservatore)
  - <previous_ipda.ext> (Eventuale file IPDA del precedente Conservatore);
- xsd\ (Cartella degli schemi utilizzati nel pacchetto Informativo)

Il file IPdA è conforme allo standard nazionale SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386), lo standard riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione che prevede una specifica articolazione per mezzo del linguaggio formale XML.

La struttura xml del SInCRO prevede inoltre:

- un'ulteriore sezione "MoreInfo" che consente di specificare i metadati soggettivi (indici "custom" specifici, derivanti dalla particolare classe documentale cui l'indice si riferisce) definiti da Intesa in accordo con il Cliente in relazione al tipo documento trattato
- i metadati minimi richiesti dalla normativa, indicati nell'Allegato 5 delle LG AGID.

Tali strutture aggiuntive di "MoreInfo" fanno riferimento a specifici files di schema, presenti all'interno del pacchetto di archiviazione e richiamati all'interno dell'xml del SInCRO.

L'IPdA ed il RdV vengono firmati digitalmente attraverso lo standard CAdES generando quindi un file con estensione xml.p7m.

6.4 Pacchetto di distribuzione

Il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, al documento conservato che può essere consultato ed esibito sia attraverso una modalità on-line (base di dati) attraverso portale web Intesa, sia attraverso i supporti auto consistenti.

Il pacchetto di distribuzione è costituito da un file zip firmato con sigillo INTESA che contiene le medesime strutture del Pacchetto di Archiviazione. Per la descrizione delle singole strutture dati si rimanda al paragrafo precedente.

Attraverso correlazioni logiche, veicolate dal database della piattaforma di conservazione, ogni pacchetto di distribuzione è corredato da strutture dati documentate, consentendo il legame complessivo tra il pacchetto di distribuzione e i seguenti elementi:

- Struttura dati xml SInCRO (in formato xml.p7m), comprensiva di sezioni MoreInfo per metadati custom e metadati minimi;
- Schema .xsd dei metadati custom (metadati memorizzati su struttura database e riportati nella sezione MoreInfo del xml SInCRO);
- Schema .xsd dei metadati minimi (metadati memorizzati su struttura database e riportati nella sezione MoreInfo del xml SInCRO).

La ricerca dei documenti avviene tramite l'utilizzo delle chiavi di ricerca corrispondenti ai metadati specifici per ogni tipologia di flusso documento.

Apposite funzionalità consentono di effettuare la visualizzazione, la verifica di integrità o l'esportazione dei pacchetti di distribuzione e di copia degli oggetti conservati.

Eventuali specifiche ed ulteriori modalità di esibizione che consentano il collegamento e integrazione con i sistemi del Cliente possono essere valutate congiuntamente tra il Cliente e Intesa e riportate nel disciplinare tecnico (es. via Web Services, supporti fisici di memorizzazione).

Il Servizio, quindi, dispone di strumenti idonei ad esibire i documenti conservati, in caso di accessi, ispezioni e verifiche a cura di soggetti interni all'organizzazione del Cliente e/o agli enti competenti (in caso di verifiche dell'Autorità Finanziaria o degli organismi competenti previsti dalle norme vigenti ai fini dell'espletamento delle attività di controllo e di vigilanza).

7 Il processo di conservazione

Il processo di conservazione prevede la preparazione di un pacchetto di versamento, contenente gli oggetti digitali da conservare corredati di metadati definiti in base a norme definite (indice di conservazione) che deve essere trasmesso al sistema di conservazione secondo le modalità concordate tra Intesa e il titolare dell'oggetto di conservazione. L'indice di conservazione completa il pacchetto di versamento. Le attività che

competono al conservatore gestore del deposito di conservazione sono la ricezione del PdV, la validazione del PDV, la trasformazione del PdV in PdA e la trasmissione al titolare dell'oggetto di conservazione del PdD una volta richiesto.

Le componenti funzionali del sistema di conservazione Trusted Doc assicurano il trattamento dell'intero ciclo di gestione dell'oggetto conservato nell'ambito del processo di conservazione.

Il sistema attribuisce un identificativo univoco di piattaforma che ne consente l'individuazione in modo diretto e persistente.

Il sistema garantisce l'accesso all'oggetto conservato, per il periodo prescritto dalla norma, indipendentemente dall'evolversi del contesto tecnologico.

Come indicato nel paragrafo 4.2 delle LG AGID, gli oggetti della conservazione sono trattati dal sistema di conservazione in pacchetti informativi che si distinguono in:

a) Pacchetti di versamento: si tratta strutture dati da conservare ricevuti dalla piattaforma di Intesa, corredate anche dai relativi metadati, secondo quanto concordato con il cliente;
b) Pacchetti di archiviazione (PdA): strutture dati che seguono al versamento tra le quali è presente anche l'IPdA in standard SInCRO;
c) Pacchetti di distribuzione: strutture dati previste in sede di esibizione.

Il servizio di conservazione di Intesa è configurato in modo da poter gestire i dati di diverse aziende, creando ambienti rigorosamente separati per ciascuna entità opportunamente identificabili tramite una specifica codifica di sistema ed eventualmente disponibile negli indici al momento dell'acquisizione dei documenti sulla piattaforma nel caso di gruppi multi-azienda.

Il sistema è predisposto per poter gestire, in maniera uniforme ma garantendo la completa separazione di:

- Configurazioni;
- Processi applicati dai workflow compresi quelli di firma;
- Pacchetti informativi (versamento, archiviazione, distribuzione);
- Monitoring;
- Flussi di dati in input ed in output.

Pur mantenendo gestioni distinte per le diverse aziende, il sistema consente al Responsabile del servizio di conservazione e suoi operatori una visione unitaria dei diversi processi di gestione, in particolare per le funzioni di monitoraggio, controllo ed alerting.

I documenti inseriti nel sistema di versamento e soggetti alle opportune verifiche durante il caricamento, non sono esposti a rischi di alterazioni né modifiche in fase di trasferimento logico alle procedure di conservazione, che comunque verificano, con procedure automatiche, in ogni fase del processo l'integrità del documento.

Le verifiche e l'identificazione delle anomalie sono quindi effettuate a monte del processo, nell'ambito del sistema di versamento, dove vengono eventualmente rilevati gli scarti. Le fasi successive avvengono sotto il monitoraggio del sistema di gestione, che controlla il corretto svolgimento del processo di conservazione e

produce la relativa reportistica sia in relazione alle eventuali anomalie rilevate sia in riferimento a quanto correttamente conservato.

Ogni documento viene inviato al sistema di conservazione per mezzo di un pacchetto di versamento contenente l'oggetto da conservare.

Con riferimento alla normativa relativa alla conservazione elettronica dei documenti a carattere civilistico e nel pieno rispetto di essa, Intesa ha scelto di effettuare il processo su ogni singolo documento.

Infatti, il pacchetto di archiviazione riferito ad ogni singolo documento permette l'esibizione dello stesso con già presenti i requisiti primari e necessari alla sua completa verifica da parte delle autorità ispettive. Il singolo documento potrà inoltre essere esibito in fase di giudizio ed essere autenticato dai giudici o dai pubblici ufficiali nelle cause di carattere civilistico e tributario.

La tracciabilità stessa del singolo documento nell'ambito del processo di conservazione viene garantita ed eventualmente resa disponibile via pubblicazione web per i vari status del documento (ricevuto e conservato).

Tali valutazioni hanno dunque dato vita alla soluzione che considera il singolo documento quale pacchetto di versamento, archiviazione ed eventualmente distribuzione su cui applicare i vari steps richiesti dal CAD e relative Linee Guida.

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

Il Servizio di conservazione Trusted Doc consente il trasferimento dei dati e relativi indici in modalità sicura con protocollo Https o attraverso altre modalità concordate con il Cliente, sempre nell'ottica di salvaguardia della sicurezza dei dati inoltrati.

Intesa eroga i servizi nella propria Server Farm.

Gli oggetti di conservazione ricevuti sulla piattaforma Intesa generano delle richieste di servizio (RS) alle quali vengono attribuite degli identificativi univoci (IDRS) che permettono di tracciare le attività svolte durante la lavorazione, dalla presa in carico fino alla creazione dei pacchetti di archiviazione. Ogni step elaborativo viene opportunamente repertorizzato su specifiche tabelle del data base dedicate al tracking/logging (log-registri) consultabili. I pacchetti di versamento ricevuti subiscono, durante le fasi elaborative, dei salvataggi progressivi su data base primario, unico punto di consistenza della piattaforma, ridondato su istanza secondaria, tramite funzioni di "data guard".

La storicizzazione del dato durante il processo elaborativo ne permette un restart/recupero in caso di failure procedurale.

La periodicità di invio dei documenti al sistema di conservazione viene determinata dall'operatività delle procedure sui sistemi del Cliente e concordata con Intesa (giornaliera, mensile, ecc…) in considerazione dei termini normativi per la conservazione.

In fase di setup del servizio vengono definite le specifiche del pacchetto di versamento e della relativa struttura di metadati in corrispondenza di ogni tipologia documentale.

Vengono prodotti i metadati da associare ai documenti da inviare in conservazione, integrando quelli già definiti in fase di produzione. I metadati sono in particolare integrati con l'indicazione del Sistema di Conservazione cui inviare il documento.

Ogni documento viene inviato al Sistema di Conservazione, identificato tramite opportune regole definite sulla base della tipologia documentale e delle informazioni contenute nei metadati del documento stesso.

Le attività di Intesa in corrispondenza di ciascuna tipologia documentale vengono effettuate seguendo i tempi di invio dei documenti al sistema di conservazione ed entro il termine massimo di conservazione stabilito dalla normativa.

Sulla base di quanto concordato con il Cliente e in base alle necessità legate alla tipologia documentale, Intesa configura i workflow di elaborazione e tutte le necessarie parametrizzazioni per un corretto trattamento dei documenti.

7.2 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti

Il sistema di versamento prevede l'esecuzione di una serie di controlli di conformità, riconciliazione e correttezza sui documenti da conservare. In particolare:

- Controlli di conformità:
  - Verifica anagrafica dell'azienda mittente (Cliente/Titolare dell'oggetto di conservazione);
  - Verifica Formato dei file. Il sistema di conservazione provvede a eseguire la verifica del formato di ciascun file versato, secondo le specifiche indicate nell'allegato 2 delle LLGG;
  - Presenza di tutte le informazioni definite per le specifiche categorie documentali obbligatorie.
- Controlli di correttezza:

  In fase di analisi sono concordate le regole puntuali per l'esecuzione di eventuali controlli di univocità, duplicazione, coerenza e completezza dei documenti ante conservazione, con segnalazione di eventuali documenti mancanti in relazione alle regole definite in accordo con il cliente.

I controlli sopra menzionati danno origine ad eventuali errori bloccanti o non bloccanti, quindi eventualmente il rifiuto dei pacchetti di versamento.

7.3 Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico

Dopo aver effettuato le verifiche sui pacchetti di versamento e sugli oggetti digitali secondo quanto precedentemente indicato, gli stessi vengono accettati dal sistema con conseguente generazione di un messaggio di accettazione (ACK1).

Al termine della fase di elaborazione del pacchetto di versamento e di controllo, viene, inoltre, generato un rapporto di versamento.

Il rapporto di versamento è un oggetto digitale di tipo XML che attesta l'avvenuta presa in carico da parte del sistema di conservazione di più pacchetti di versamento inviati dal produttore, e che quindi hanno passato con esito positivo i diversi controlli previsti.

IL rapporto di versamento include l'ID file della piattaforma INTESA, l'impronta e la data di versamento di ogni oggetto di conservazione.

Nel sistema di conservazione di Intesa ad ogni rapporto di versamento viene assegnato un nome file univoco e successivamente, è firmato cades. p7m dal Responsabile del Servizio di Conservazione.

Il Servizio prevede la creazione di un rapporto di versamento per ogni flusso inviato dal Cliente, contiene i riferimenti a pacchetti di versamento dello stesso Cliente e tipologia di documento.

Il rapporto di versamento è sottoscritto con firma elettronica qualificata del responsabile del servizio di conservazione di Intesa ed è conservato con correlazione automatica ai pacchetti di versamento in esso riportati; ricercando il pacchetto di versamento è possibile visualizzare il relativo rapporto di versamento.

7.4 Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie

Il processo di conservazione è disegnato in modo da ridurre al minimo il rifiuto dei PdV. All'interno del workflow del servizio è previsto una pre-ingestion necessaria per la corretta accettazione dei pacchetti.

Il mancato superamento dei controlli bloccanti sui pacchetti di versamento genera degli eventi di anomalia che verranno notificati al Cliente.

L'insieme degli eventi viene collezionato e descritto per la successiva notifica al referente del Cliente, con il quale verranno concordate le azioni per il completamento del processo.

Il processo di controllo è caratterizzato dunque da:

- Esecuzione del work flow di verifica;
- Rilevamento e tracciatura dell'anomalia (tabella su data base e storicizzazione dell'attachment su casellario);
- Generazione della segnalazione certa dell'errore con rifiuto del documento;

- Invio della segnalazione con relativa motivazione (rapporto di anomalia) in modalità email al referente aziendale del Cliente;
- Gestione attraverso contatto diretto con il referente per le diverse casistiche di errore che possono avere trattamenti e soluzioni differenziate.

La corretta modalità di controlli è condivisa e concordata in fase di analisi con il Cliente.

La notifica di anomalia riporta:

- L'identificativo univoco del pacchetto rifiutato;
- I relativi indici univoci concordati con il Cliente (es. numero e data documento);
- La descrizione dell'errore rilevato.

Elenco delle anomalie gestite:

- Formato errato del pacchetto di versamento;
- Errori di tracciato e di contenuto dei metadati (tipo dato errato, lunghezze errata);
- Assenza totale o parziale dei Metadati, con riferimento alle obbligatorietà definite per le specifiche categorie documentali;
- Errore riscontrato nell'ambito della verifica dell'integrità del Pacchetto di Versamento;
- Errore di duplicazione in relazione alle regole di univocità stabilite;
- Errore nel controllo di sequenzialità dei documenti, in relazione alle regole concordate (procedura "check buchi").

I report di anomalia costituiscono quindi uno strumento operativo di verifica e comunicazione con il Cliente.

Tali comunicazioni vengono registrate nell'ambito dell'applicazione di posta aziendale, su apposito database, dedicato al Servizio di conservazione ed in uso esclusivo a soggetti opportunamente profilati ed incaricati.

7.5 Preparazione e gestione del pacchetto di archiviazione

Al termine dell'attività di acquisizione e verifica del pacchetto di versamento, Intesa procede con la trasformazione dei PdV in pacchetto di archiviazione.

Il sistema di conservazione di Intesa prevede la gestione del pacchetto di archiviazione in base alle specifiche della struttura dati riportate dalle Linee Guida.

Il pacchetto di archiviazione è composto da:

- Oggetto digitale;
- Metadati;
- Indice del pacchetto di archiviazione;
- Rapporto di versamento.

Il file di formato .p7m dell'IPdA permette l'esibizione dello stesso con già a bordo i requisiti primari e necessari alla sua completa verifica da parte delle autorità ispettive. Il singolo documento potrà inoltre essere esibito

di giudizio ed essere autenticato dai giudici o dai pubblici ufficiali nelle cause di carattere civilistico e tributario.

La tracciabilità stessa del singolo documento nell'ambito del processo di conservazione viene garantita ed eventualmente resa disponibile via pubblicazione web per i vari status del documento (ricevuto, conservato).

In base alla tipologia documentale, vengono stabiliti in fase di setup i tempi di conservazione dei documenti correttamente assegnati dal sistema al momento della ricezione del Pacchetto di Versamento.

Il Sistema di Conservazione è strutturato configurato per gestire il periodo di conservazione di ciascun documento sulla base della classe documentale, in base alla normativa vigente e al contratto di Servizio.

Le operazioni di apposizione di sigillo e marcatura temporale su IPdA sono effettuate nel rispetto delle normative specifiche in materia di firme e validazione temporale.

Tale processo permette di rispondere ai requisiti di autenticità, immodificabilità, integrità, staticità.

Con tali operazioni si completa il processo di conservazione elettronica, viene aggiornato lo stato del documento all'interno del processo di tracking con l'esito di avvenuta conservazione, e generato apposito report, il rapporto di archiviazione (ACK2) messo a disposizione del Cliente con le relative informazioni.

Il certificato del sigillo del responsabile del servizio di conservazione è rilasciato dalla CA Intesa e memorizzato nei dispositivi HSM, in grado di garantire elevati livelli di sicurezza, affidabilità e performance in termini di velocità di esecuzione delle operazioni di firma.

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

La struttura dei pacchetti di distribuzione coincide con quella dei pacchetti di archiviazione.

I pacchetti di distribuzione, risultanti dal processo di apposizione di sigillo elettronico e marca temporale, sono rappresentati da file con estensione .p7m e messi a disposizione del soggetto produttore e di Intesa, in qualità di soggetto conservatore.

L'esibizione degli oggetti conservati viene concordata con il cliente e può avvenire secondo lo standard di piattaforma di Intesa o altre modalità specifiche indicate nel disciplinare tecnico del contratto:

- Portale web Intesa;
- Supporti di memorizzazione autoconsistenti;
- Web services;
- Single Sign-on;
- Altre modalità concordate.

7.6.1 Modalità via portale web

La consultazione dei documenti avviene con modalità web tramite accesso al portale Intesa con protocollo Https, sfruttando le funzioni online native della piattaforma.

Le funzionalità di consultazione consentono di ricercare i documenti conservati su database mediante un motore di ricerca personalizzato su ciascun indice associato al documento ed effettuarne la visualizzazione, la verifica di integrità o il download, per la durata del contratto di servizio.

Il servizio consente di trattare anche i pacchetti di distribuzione caratterizzati da più livelli di firma relativi ai processi di generazione/emissione/ tenuta elettronica dei documenti, da parte del Cliente precedenti al processo di versamento e archiviazione.

Gli utenti che possono accedere al sistema di consultazione devono essere opportunamente registrati e profilati.

La profilatura è definita sulla base delle specifiche fornite dal Cliente, consentendo la definizione dei profili degli utenti e delle relazioni tra di essi e il controllo degli accessi.

7.6.2 Modalità attraverso supporti di memorizzazione autoconsistenti

I pacchetti di distribuzione possono essere consultati anche attraverso l'utilizzo di supporti di memorizzazione auto consistenti se richiesto dal Cliente nell'ambito delle specificità contrattuali.

In tal caso si procede con l'estrazione di pacchetti di distribuzione, per l'esibizione dei documenti conservati, organizzati in archivi logici.

Con archivio logico di conservazione si intende l'organizzazione logica dei documenti oggetto del processo di conservazione elettronica, definita per tipologia, periodo di competenza o altro parametro concordato con il Cliente per consentire la produzione di supporti auto consistenti da consegnare al Cliente, se previsto.

Durante questa attività sono definiti il numero degli archivi e le denominazioni da attribuire agli stessi per le diverse tipologie di documenti con le relative chiavi di ricerca e le caratteristiche dei supporti di memorizzazione, così come descritto in allegato A.

Gli indici di ricerca (metadati) per la consultazione sono concordati e definiti in fase di analisi del Servizio.

Al fine di tracciare tutti i dettagli relativi alla produzione e alla memorizzazione dei pacchetti di distribuzione su supporti esterni, specifiche funzioni applicative del servizio generano un report di acknowledgement (ACK3) che consente di tracciare l'avvenuta attività sia a livello di sistema che nell'ambito del data base preposto alla tracciatura degli archivi e supporti generati.

Durante la fase di generazione dei supporti si innesca la procedura di verifica e di controllo tra il numero di pacchetti effettivi presenti all'interno dell'archivio e il numero degli indici riportati in un apposito file di controllo. In caso di incongruenza viene generato un log di errore consentendo quindi le necessarie attività di verifica.

In caso positivo si conclude l'attività di produzione dell'archivio e si procede con le attività di riconciliazione, masterizzazione ed identificazione univoca del supporto fisico rimovibile (USB o altro), spedizione o consegna secondo le modalità concordate con il cliente.

La consultazione dei pacchetti di distribuzione su supporto si basa sull'utilizzo di un software di visualizzazione (viewer) realizzato da Intesa e presente sul supporto stesso, che comprende le funzionalità di ricerca, verifica, visualizzazione e download.

Il viewer è realizzato in linguaggio Java al fine di renderlo compatibile con i sistemi operativi di mercato e di garantirne la massima longevità. Non prevede il riconoscimento di licenze per componenti di software in esso contenuti e quindi non comporta costi aggiuntivi di distribuzione.

Il viewer supporta le funzionalità sintetizzate nel seguito:

- Ricerca documentale

Sulla base dei metadati definiti che descrivono (tramite file XML) la struttura dell'archivio, viene presentata una maschera di ricerca che presenta i campi di selezione e i relativi operatori. I documenti che soddisfano i criteri di ricerca vengono elencati con eventuale paginazione. È possibile selezionare una specifica colonna per effettuare ordinamenti crescenti o decrescenti;

- Funzioni sui documenti singoli

Sono disponibili le seguenti funzioni:

- Visualizzazione del documento

- Visualizzazione degli oggetti costituenti il PKCS#7 (impronta, firma, marca temporale,)

- Estrazione degli oggetti costituenti il PKCS#7 (firma, marca temporale, PKCS#7 completo, file originale in chiaro)

- Verifica dell'integrità del PKCS#7 con controllo di validità certificato di firma e marca temporale su file esterno di CRL e delle Certification Authority "trusted".

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

Il cliente, attraverso la visualizzazione dei pacchetti di distribuzione, può procedere all'eventuale download di duplicati informatici.

Tramite apposita richiesta può richiedere a Intesa la produzione di copie conformi dei documenti stessi.

Le funzionalità a disposizione del pubblico ufficiale, tramite accesso al portale con utenza e password, consentono:

- La visualizzazione e la selezione puntuale o massiva dei documenti elettronici;
- Le relative attività di verifica di conformità del documento elettronico rispetto al documento originale già a disposizione del pubblico ufficiale;

- Il download di documenti in locale, per permettere di procedere con la verifica di autenticità e integrità degli stessi attraverso l'uso di un verificatore di mercato prescelto, garantendo in questo modo la totale autonomia del processo di controllo e la massima garanzia di verifica.

7.8 Scarto dei pacchetti di archiviazione

Il Servizio di Conservazione di Intesa prevede che, in prossimità della scadenza del periodo di conservazione elettronica, definito e con congruo preavviso, sia fornita al Cliente segnalazione dei documenti prossimi al termine del ciclo vita.

La procedura è parametrizzata tramite la compilazione di una tabella di database applicativo nella quale sono censite tutte le tipologie di documenti conservati distinte per Cliente, tipo documento e periodo di retention (es. 5 anni per il LUL, 10 per gli altri documenti o altre tempistiche concordate contrattualmente con il Cliente ed indicate in disciplinare tecnico).

Il sistema genera apposito report con l'elenco dei pacchetti di archiviazione contenenti i documenti destinati allo scarto e il warning circa l'imminente cancellazione, quindi, scarto dei pacchetti di archiviazione e degli archivi logici dai sistemi di Intesa.

È previsto l'invio di mail PEC, dove disponibile l'indirizzo o di mail. Le ricevute di ritorno saranno conservate dal Gestore dei supporti presso il sito primario. I dati verranno cancellati fisicamente dopo un congruo periodo di avviso

La cancellazione dei dati interesserà sia i documenti presenti su DB che quelli riversati in archivi presenti su NAS.

Qualora a fronte della mail di notifica il Cliente desideri mantenere ancora in conservazione i documenti potrà notificarlo entro 1 mese dalla ricezione della medesima e si procederà ad adeguare le condizioni contrattuali che regolano questo aspetto.

7.8.1 Cessazione del Servizio di Conservazione

In caso di richiesta del cliente e su specifico accordo tra le parti, al termine del periodo di conservazione, Intesa consegna gli originali dei dati conservati, organizzati in archivi omogenei via connettore o su adeguati supporti di memorizzazione auto consistenti sulla base dei parametri concordati con il Cliente.

In ipotesi di conclusione del contratto o di recesso da parte del Cliente, o da parte di Intesa, in capo ad Intesa rimane l'obbligo della conservazione per il periodo richiesto dalle normative in relazione alla tipologia documentale conservata o in base a quanto diversamente concordato con il cliente. Il cliente potrebbe comunque richiedere la restituzione dei dati e la conseguente liberazione di Intesa dagli obblighi derivanti par 4.5 delle Linee Guida.

In ipotesi di risoluzione del Contratto o di cessazione del servizio, Intesa consegna i dati in suo possesso al Cliente, essendo liberata dall'obbligo di conservazione nonché dagli obblighi derivanti dal par 4.5 delle Linee Guida.

In tutti i casi di restituzione dei dati questi vengono estratti in archivi logici all'interno dei quali sono presenti i pacchetti corredati dalle strutture dati standard la cui organizzazione è concordata con il Cliente.

Al termine delle operazioni di restituzione i dati vengono rimossi dai sistemi di Intesa in modalità sicura.

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

Intesa, grazie alla struttura implementata per la tenuta dei dati conservati, permette una naturale interoperabilità ed integrazione con altre soluzioni di conservazione e/o piattaforme di gestione documentale.

Inoltre, anche di fronte ad eventuali evoluzioni normative e tecnologiche assolutamente prevedibili nel tempo, Intesa è in grado di adeguarsi tempestivamente, essendo da sempre la conversione e la trasformazione dei formati caratteristica essenziale del core business di Intesa.

In tal senso, Intesa già opera, attraverso le seguenti caratteristiche tecnologiche:

- Utilizzo, per la conservazione dei documenti, di formati standard prescritti dalle normative in materia;
- Adozione di formati di firma standard riconosciuti dagli Enti Certificatori in conformità alle specifiche PAdES-T, e CAdES-T, con applicazione della marca temporale;
- La scelta adottata da Intesa di elaborare il singolo documento e non il lotto elimina completamente la necessità di costruire e gestire algoritmi proprietari, complessi ed articolati, necessari a trattare il documento sia nella fase di messa in conservazione sia nella delicata fase di esibizione verso le autorità competenti e in tutti i casi di controversia giudiziaria;
- Il singolo documento viene così corredato di tutti gli attributi tecnico-normativi che facilitano qualsiasi operazione di portabilità o interoperabilità verso strutture esterne e si appoggia per l'abbinamento ai relativi indici a formati XML, attraverso l'applicazione dello standard SInCRO ampiamente riconosciuto per le proprie caratteristiche di interoperabilità.

Intesa, nell'ambito dei propri processi, adotta formati nel pieno rispetto degli standard riconosciuti e, a maggior tutela e garanzia dei clienti, non utilizza formati proprietari, spesso presenti sul mercato ma di complessa portabilità.

Pertanto, nel momento in cui il soggetto produttore (cliente di Intesa) richieda il trasferimento dei pacchetti di archiviazione verso altro conservatore, le funzioni attivate da Intesa e garantite dalle precedenti elencazioni dei requirements del sistema di conservazione, permettono un rapido passaggio verso il nuovo sistema di conservazione. Si tratta di funzioni di esportazione controllata dei pacchetti di archiviazione, dei relativi indici del pacchetto di archiviazione (IPdA) e dei metadati di ricerca.

8 Il sistema di conservazione

Il sistema di conservazione assicura, dalla presa in carico fino all'eventuale scarto, la conservazione degli oggetti digitali in esso conservati, tramite l'adozione di regole, procedure e tecnologie, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità come indicato nelle Linee Guida al par 4.1.

Il Servizio di conservazione elettronica a norma di legge di Intesa, denominato Trusted Doc, è basato sulla piattaforma proprietaria di Intesa, Trusted Hub, come descritta nel seguito.

Il Servizio, per l'importanza che riveste, è stato completamente sviluppato da Intesa, consentendo di allineare tempestivamente la soluzione con le normative, le best practice di mercato e di personalizzarlo nel tempo per arricchire i servizi erogati.

L'infrastruttura di Servizio Trusted HUB, utilizzata per l'erogazione ai Clienti del Servizio di conservazione in outsourcing Trusted DOC, nasce da oltre 25 anni di esperienza di Intesa nella gestione dei documenti elettronici e da oltre 10 anni da certificatore iscritto a AgID per la Firma Digitale. Integra così, in modo nativo, le funzionalità di un hub preposto al trattamento e allo scambio di ingenti mole di documenti elettronici con le funzionalità e le garanzie che può offrire Intesa in qualità di Certification Authority e Conservatore.

La piattaforma Trusted Hub è quindi integrata nativamente con le funzionalità di firma erogate da Intesa stessa in qualità di Certification Authority, la firma massiva dei documenti viene effettuata utilizzando HSM che offrono una potente accelerazione crittografica, gestione hardware delle chiavi e consentono la gestione di più profili di configurazione. Sono particolarmente indicati per processi come la generazione dei documenti elettronici all'origine e la conservazione a norma, dove la sicurezza e le performance sono prioritarie.

Tecnologicamente aggiornata, l'infrastruttura del Trusted Hub è robusta e allo stesso tempo flessibile. Infatti, si basa su middleware standard di mercato, affiancati da componenti proprietari per gestire, in modo snello e in autonomia, specificità come il tracking, l'administration, il workflow, la firma digitale, ecc…

I servizi erogati da Intesa e le relative infrastrutture sono ospitate presso le Server farm INTESA ubicate in siti connessi in Campus su rete geografica ad alta velocità. L'infrastruttura è composta da partizioni virtuali e server fisici ed è completamente ridondata sul sito primario e duplicata nel sito di Disaster Recovery.

Il Servizio in virtù della modularità derivante dalla sua infrastruttura/configurazione è scalabile e quindi adeguato a gestire eventuali incrementi di volumi.

Attraverso l'utilizzo di adeguati storage, l'infrastruttura è specificatamente progettata per applicazioni data-intensive con cui si raggiungono elevate prestazioni di alta affidabilità.

8.1 Componenti Logiche

La piattaforma, di cui si riporta l'architettura logica nel disegno che segue, può essere suddivisa in una serie di "Moduli Base" necessari per:

- La definizione delle Comunità, le relazioni, gli utenti e i loro profili;

- Le attività di system administrator;
- Le attività del sistema di conservazione;
- La gestione del portale web;
- La gestione dei workflow elaborativi;
- Lo store & forward dei documenti non sincroni (mailbox);
- il monitoraggio e il tracking dei flussi e dei documenti all'interno di essi.

A tali componenti di base si aggiungono i "Moduli specializzati", richiamati per specifiche elaborazioni sui flussi e/o sui dati sulla base delle regole di workflow:

- Modulo Time Stamping, per la marcatura temporale dei documenti a fini probatori;
- Modulo Firma Digitale Massiva, che con l'utilizzo di apposite apparecchiature ad alta sicurezza consente la firma centralizzata dei documenti.

Di seguito lo schema delle componenti logiche della piattaforma Trusted HUB di Intesa sulla quale è allocato il sistema di conservazione:

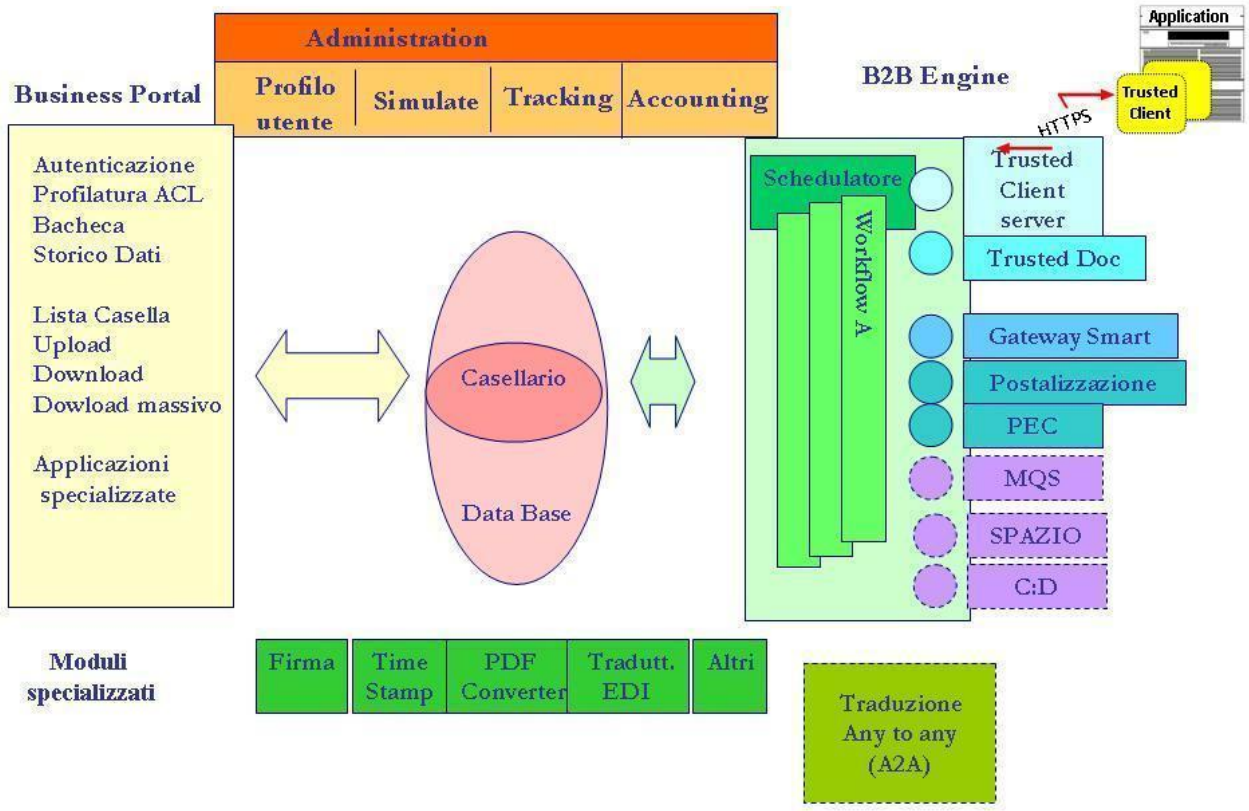


Figura 1: Schema delle componenti logiche

8.2 Componenti Tecnologiche

Di seguito lo schema delle componenti tecnologiche del sistema di conservazione precedentemente descritte.

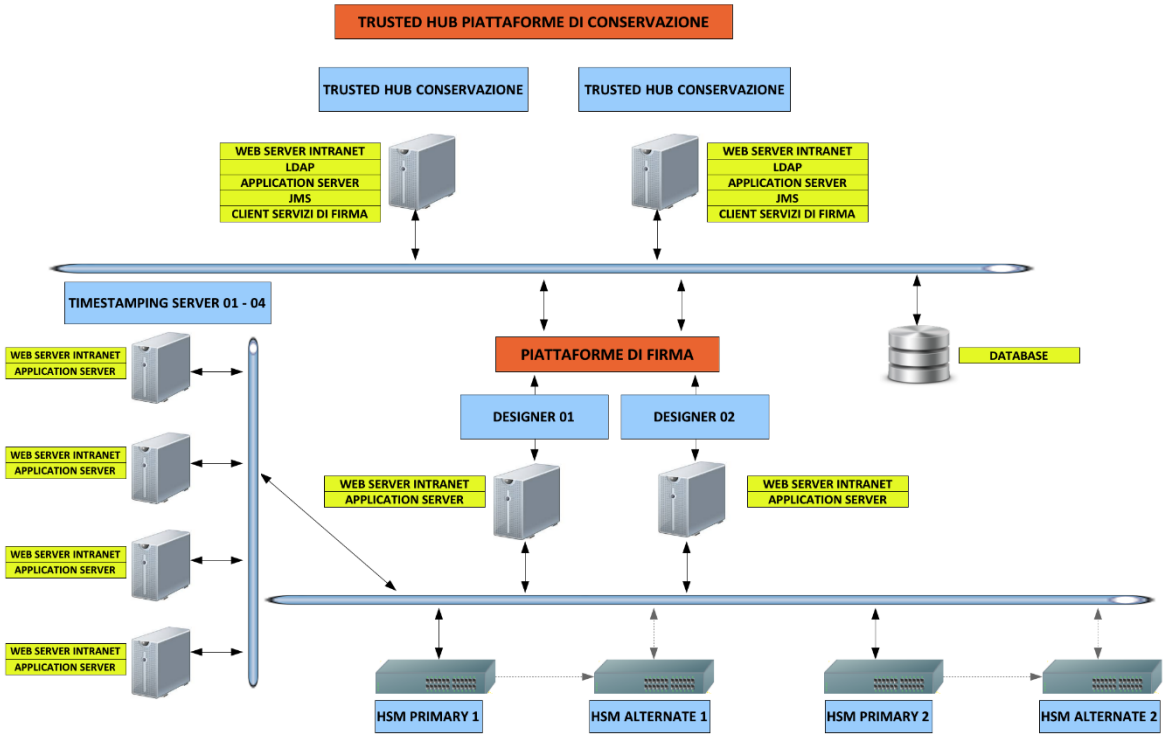


Figura 2: Componenti tecnologiche

8.3 Componenti fisiche

Per l'erogazione del servizio di conservazione è stata adottata la tecnologia Virtual Machine VMware nella versione più avanzata ESXi.

Di seguito la descrizione delle componenti tecnologiche dei siti di conservazione:

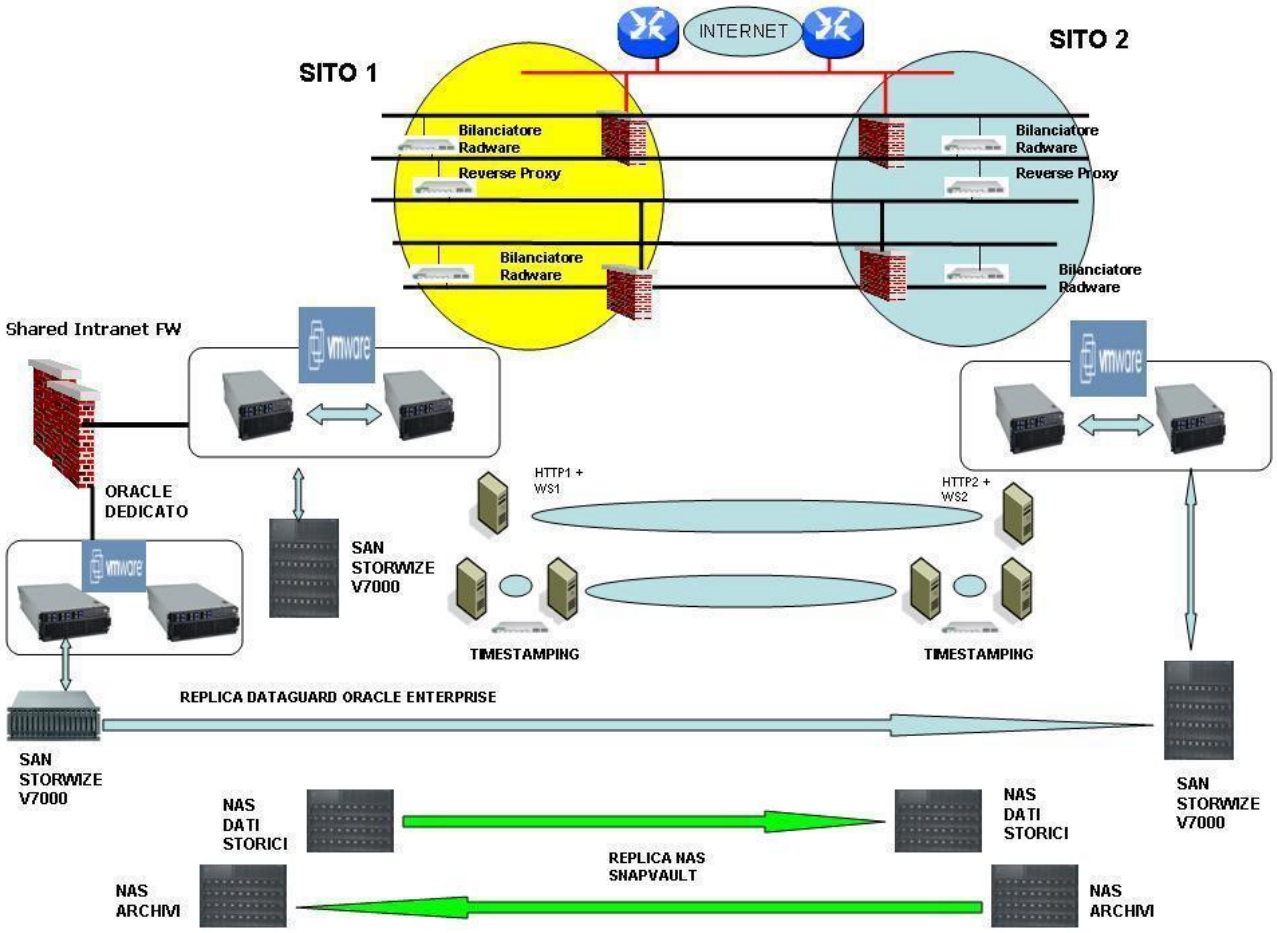


Figura 3: Componenti fisiche dei siti di conservazione

L'ambiente VMware è realizzato da server xSeries IBM di ultima generazione che condividono, tramite doppio switch in fibra ottica per connessioni incrociate e ridondanti, più Storage Area Network (SAN) Storwize V7000 con TIER SSD per garantire alte performance.

La piattaforma VMware riprende concetti già ampiamente sperimentati e consolidati in ambienti Enterprise Mainframe, dove su host estremamente affidabili e scalabili sono create partizioni completamente isolate e gestibili dinamicamente sia a livello di risorse che di storage.

Le macchine virtuali (VM) utilizzano in modo condiviso o diretto uno storage di alto livello HW che garantisce le operazioni di Vmotion (spostamento della VM a caldo da host a host senza fermo delle attività). Le VM possono essere definite con estrema flessibilità rispondendo a requisiti di scalabilità orizzontale e verticale.

Attraverso il Virtual Center possono essere modificate dinamicamente le risorse (CPU, RAM, I/O, network) in modo da ottimizzare le performance di ogni singola VM.

8.4 Procedure di gestione e di evoluzione

8.4.1 Conduzione e manutenzione del sistema di conservazione

Il Sistema di conservazione di Intesa è stato strutturato con l'obiettivo di perseguire la conduzione e la manutenzione dei documenti e delle piattaforme ad esso dedicate, nonché il mantenimento del controllo e l'evoluzione delle piattaforme.
La gestione del sistema di conservazione è svolta dalle figure preposte in considerazione della tipologia di attività da svolgere e azioni da intraprendere.
I vari reparti operativi di Intesa svolgono rispettivamente le attività di propria competenza sulla base di un coordinamento volto ad una visione unitaria del sistema.
Le attività si classificano in:

- Attività sistemistica: manutenzione delle componenti dell'infrastruttura e della loro evoluzione, monitoraggio del corretto funzionamento della struttura;
- Attività di gestione applicativa e del software: gestione dell'evoluzione e delle azioni correttive ed evolutive, rilasci applicativi, sviluppo workflow e procedure;
- Attività di monitoraggio applicativo specifico per il Cliente: attività di monitoraggio quotidiano dei processi e workflow di piattaforma;
- Attività di supporto al cliente: supporto a fronte di anomalie segnalate alla struttura di helpdesk;
- Attività manutenzione hardware: gestione e manutenzione dell'infrastruttura hardware al fine di garantire il buon funzionamento della stessa. Pianificazioni di eventuali azioni di intervento.

L'organizzazione di Intesa risponde con efficienza crescente alle richieste di intervento dei Clienti, potendo far leva sulla acquisizione continua di esperienze sullo specifico prodotto servizio.

Sono gli stessi Responsabili di Manutenzione, per quanto riguarda prodotti software di produzione Intesa, a suggerire implementazioni in termini di manutenzione evolutiva; per i prodotti di Terze Parti rappresentano invece la controparte definita verso il Produttore o Distributore per riportare problemi, richieste, proposte di enhancement e per proporre interventi specializzati presso il Cliente.

Quando si evidenzia un anomalo comportamento del servizio/ prodotto (non conforme alle relative specifiche), viene attivato il processo di Manutenzione correttiva.

La manutenzione correttiva/evolutiva prevede una sequenza proceduralizzata di fasi, che intendono assicurare la completezza ed efficacia delle correzioni/implementazioni effettuate:

- Rilevazione anomalia (per i casi di Manutenzione Correttiva) e/o esigenza di intervento (per i casi di Manutenzione Evolutiva);
- Diagnosi, approvazione e assegnazione;
- Correzione;
- Collaudo;
- Rilascio;

- Propagazione.

8.4.2 Monitoring e sicurezza

Il sistema di conservazione prevede adeguati presidi tecnologici e infrastrutturali volti a garantire misure di alta affidabilità e disaster recovery in linea con le indicazioni della normativa in materia e con le prassi adottate sul mercato.

In base a quanto stabilito dalle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici par. 4.10, i soggetti privati appartenenti ad organizzazioni che già adottano particolari regole di settore per la sicurezza dei sistemi informativi adeguano il sistema di conservazione a tali regole.

Nell'erogazione del Servizio di conservazione Trusted Doc di Intesa, gli aspetti della sicurezza rispettano i principi espressi:

- Dalle policies aziendali di Intesa;
- Dalla certificazione ISO 27001 per gli scopi specifici: servizi di generazione/emissione di documenti elettronici, archiviazione digitale e conservazione elettronica a norma e produzione di soluzioni di firma elettronica, firma elettronica avanzata, firma elettronica qualificata, posta elettronica certificata;
- Dal Codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196.

La sicurezza delle informazioni investe elementi di carattere fisico, logico e gestionale, la relativa gestione viene implementata sotto diversi aspetti:

- Sicurezza fisica e logica infrastrutturale;
- Sicurezza logica applicativa;
- Continuità.

A fronte delle esigenze di protezione di dati ed informazioni è definito uno specifico sistema che risponde ai seguenti criteri:

- Proteggere la trasmissione di informazioni contro perdite di dati, rivelazione o modifiche non autorizzate;
- Consentire l'accesso ai sistemi di erogazione solo a chi ne ha necessità (in relazione alle specifiche responsabilità) e disporre le conseguenti autorizzazioni;
- Condurre verifiche appropriate per garantire che i meccanismi di controllo funzionino effettivamente.

Per quanto riguarda la sicurezza logica sotto il profilo strutturale le procedure previste attengono a:

- Amministrazione della sicurezza;
- Protezione degli ambienti di erogazione;
- Identificazione ed autenticazione degli utenti;

- Autorizzazioni all'accesso alle informazioni a diversi livelli.

e si sviluppano nelle seguenti direzioni:

- Garanzia della riservatezza e della confidenzialità delle informazioni trasmesse dal Cliente mediante l'utilizzo di un'appropriata architettura di rete;
- Garanzia dell'integrità dei dati trasmessi attraverso l'utilizzo di opportuni e avanzati protocolli di comunicazione;
- Garanzia dei dati archiviati tramite autorizzazioni controllate fornite da apposite applicazioni informatiche (es. ACL).

Per quanto riguarda confidenzialità e riservatezza, i prodotti di software di base utilizzati e le procedure gestionali adottate sono concepite con lo scopo di assicurare al Cliente che:

- Le sue informazioni siano logicamente individuate e l'accesso ad esse sia consentito solo a chi è autorizzato;
- Le autorizzazioni all'accesso siano correntemente valide e sotto controllo;
- In caso di eventuali violazioni siano disponibili procedure di segnalazioni e siano attive procedure di riesame di tali tentativi.

8.4.3 Gestione e conservazione dei log

Il sistema di conservazione repertorizza i log di accesso al sistema operativo e alle applicazioni della piattaforma. Tali log sono oggetto di conservazione.

Inoltre, Intesa mantiene presso la propria infrastruttura, e rende disponibili per il Cliente in caso di verifiche, i log delle ricezioni dei flussi inoltrati dal Cliente e i log applicativi delle elaborazioni avvenute sui sistemi Intesa, per 90 (novanta) giorni rispettivamente dalla data di ricezione e da quella di elaborazione.

Durante la fase di erogazione del Servizio, Intesa mette a disposizione la propria struttura di gestione allo scopo di monitorare il corretto andamento dei flussi di dati e intraprendere opportune azioni in caso di malfunzionamenti, errori e situazioni critiche in generale.

Si evidenzia che il processo di Intesa è gestito per singolo documento permettendo quindi un monitoraggio completo semplice ed efficace.

In prima analisi l'attività di monitoraggio è riferita a:

- ACK 1: esecuzione del workflow interno inerenti il trattamento dei documenti e relativa pubblicazione Web (accettazione dei pacchetti di versamento);
- Rapporto di versamento;
- ACK2: (rapporto di archiviazione) esecuzione del workflow interno inerenti la conservazione a norma; è generato un flusso contenente l'elenco di tutti i documenti appartenenti al pacchetto di conservazione e relativo esito dell'operazione e in caso di errore l'indicazione della tipologia di errore riscontrato. Il flusso di ritorno indica il codice univoco relativo al pacchetto di conservazione assegnato.

Intesa per ciascun flusso invia al Cliente i vari esiti (ACK) utilizzando tracciati record in formato standard CSV, o in base ai formati concordati tra con il Cliente, consentendo un'eventuale riconciliazione dello stato sui propri sistemi.

Tali report possono essere inoltre, in base a quanto concordato con il Cliente, inoltrati via email al referente aziendale.

8.4.4 Change management

Tale procedura è eseguita da Intesa con l'obiettivo di tracciare tutte le evoluzioni e le modifiche apportate agli oggetti di sviluppo utilizzati per le implementazioni applicative attraverso apposito tool di versioning.

Gli sviluppatori acquisiscono gli oggetti con operazioni di check in, apportano le necessarie modifiche e/o correzioni, consolidano tali attività rispettivamente in ambiente di sviluppo, collaudo e infine produzione con rispettive operazioni di check out, attraverso versionamenti che vengono memorizzati a livello di file system di piattaforma per tutti gli ambienti sopra citati.

Il responsabile della configurazione autorizza i passaggi tra i vari ambienti (promozione), vengono eseguiti test di non regressione, compare, merge, gestione contesa oggetto tra sviluppatori.

Ad attività ultimate viene effettuato il definitivo deploy in ambiente di produzione.

8.4.5 Verifiche periodiche di conformità e standard di riferimento

Il responsabile del Servizio di Conservazione verifica il sistema di conservazione nelle sue varie componenti, logiche, tecnologiche e fisiche, in aderenza a quanto richiesto dalle Linee guida, con riferimento agli obblighi del Responsabile della conservazione e alle fasi del processo di conservazione.

Tali verifiche vengono eseguite nel rispetto delle procedure interne di audit, documentate da istruzioni operative aziendali e relazionate attraverso i relativi verbali di svolgimento ed esito.

9 Monitoraggio e controlli

Il sistema di conservazione di Intesa prevede l'adozione di misure e strumenti specifici per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità.

Gli strumenti a disposizione consentono la verifica e il monitoraggio della corretta funzionalità del sistema di conservazione, a livello di gestione sistemistica e applicativa delle varie componenti dello stesso.

È previsto un apposito servizio di Help Desk per qualsiasi problema riguardante gli accessi o specifiche anomalie su trasmissioni di documenti.

Il sistema di monitoraggio sistemistico e applicativo di Intesa rileva le anomalie specifiche del sistema di conservazione e le segnala attraverso appositi alert ai gruppi di gestione organizzati per competenza.

Tali gruppi prendono in carico il problema interfacciandosi se necessario con gli specialisti di area (per esempio: piattaforma, infrastruttura fisica, connettività, DB, specifici servizi applicativi, ecc…) e seguendolo fino alla risoluzione. Le azioni intraprese sono documentate nei log di sistema specifici, inseriti nel repository interno definito dal sistema di qualità aziendale.

Ai fini della corretta gestione del sistema di conservazione Intesa predispone il registro cronologico del software dei programmi in uso nelle eventuali diverse versioni succedute nel tempo e il registro cronologico degli eventi di gestione del sistema di conservazione, comprensivo delle risoluzioni adottate per rimuovere eventuali anomalie.

9.1 Procedure di monitoraggio

Ai fini del monitoraggio del sistema di conservazione Intesa adotta tools e procedure atte ad analizzare le varie componenti del sistema, a rilevare eventuali anomalie per consentire l'intervento e il coinvolgimento delle figure competenti per la risoluzione delle criticità.

Il controllo e la gestione del sistema di Conservazione sono basati sul monitoraggio continuo dell'ambiente e dei suoi singoli componenti, tramite gli strumenti e i tools di seguito indicati per accertare la rispondenza dei parametri fondamentali del servizio ai requisiti contrattuali e di qualità:

La gestione centralizzata e controllata delle operazioni di erogazione è regolamentata da specifiche procedure e strumenti che garantiscono:

- Il controllo costante dei livelli di servizio, attraverso il monitoraggio dell'ambiente e degli elementi critici, compresa anche l'avvenuta esecuzione di attività gestionali, quali ad esempio la verifica dello spazio disponibile, il mancato superamento dei livelli di soglia e la simulazione di log-on per il controllo di availability dei servizi;
- Il monitoraggio dell'andamento del Servizio, la predisposizione o verifica di collaudi e di salvataggi periodici di dati o librerie e l'eventuale predisposizione di dati di input e verifica dei risultati;
- La gestione delle modifiche a parametri del Servizio (es. Abilitazioni utenze, Password, ecc.), in modo da poterlo adeguare velocemente alle mutate esigenze del Cliente;
- La gestione della sicurezza e degli accessi ai servizi, per evitare intrusioni e ingressi non autorizzati. La sicurezza è articolata su diversi livelli (di Rete, di Sistema, di Servizio Applicativo), supportata da appropriate ed avanzate soluzioni tecnologiche e gestita da appositi ruoli aziendali, che effettuano attività di monitoraggio continuo e verifiche periodiche sulla completezza e validità delle soluzioni adottate (es. penetration tests);
- L'effettuazione controllata di ogni variazione agli ambienti operativi (HW, SW ecc.). Ogni richiesta di "Change" deve essere documentata, motivata, analizzata ed autorizzata. Una severa e preventiva analisi di impatto, da parte delle persone più qualificate, un'effettuazione concentrata in apposite "Finestre" temporali collocate in periodi di basso utilizzo ed un esaustivo collaudo, volto particolarmente a verificare la compatibilità retrograda, tendono a minimizzare i rischi di interruzioni del servizio;
- Il mantenimento e l'aggiornamento continuo delle configurazioni HW e SW relative ad ogni ambiente gestito. Tale controllo permette di identificare (anche storicamente) le componenti

tecnologiche coinvolte nell'erogazione di ogni servizio, per meglio programmare eventuali attività di modifica e di ripristino;

- La gestione ottimale delle interruzioni di servizio, siano esse programmate o impreviste. Particolari attività di progettazione sono effettuate per circoscrivere e limitare l'impatto di possibili malfunzioni e per attivare automaticamente o tempestivamente soluzioni alternative (es. routing, switch ecc.);
- La ripresa delle attività in caso di problemi. Appropriate ed automatizzate attività di salvataggio di ambienti, librerie, applicazioni e dati, permettono un regolamentato ripristino (totale, settoriale o parziale) delle risorse, per una ripartenza tempestiva dei Servizi interrotti;
- Il mantenimento di un'elevata disponibilità ed affidabilità dei singoli componenti tecnologici, tramite specifici contratti di manutenzione programmata. Interventi finalizzati alla prevenzione di possibili problemi HW sono svolti periodicamente da personale esperto;
- Il mantenimento di un ambiente di lavoro appropriato per le attività da eseguire.

9.1.1 Sistema di monitoraggio sistemistico e applicativo NAGIOS

Il sistema di monitoraggio è stato realizzato a partire dal modulo Open Source NAGIOS, su sistema operativo LINUX RED HAT. Il sistema è configurato in modo da garantire l'alta disponibilità del servizio.

Sono stati realizzati molteplici plug-in in aggiunta a quelli nativi del prodotto. Questo ha permesso di aggiungere diverse funzionalità, altrimenti non disponibili, che hanno arricchito il sistema.

Ogni plug-in di monitoraggio recepisce, oltre allo specifico controllo da effettuare, i parametri di riferimento e le soglie o regole per identificare i livelli di attenzione.

Ogni plug-in è schedulato in modo autonomo, permettendo un controllo più o meno frequente in base alle necessità dello specifico oggetto/funzione da monitorare.

Il sistema consente un monitoraggio articolato su tre diversi livelli:

- Monitoraggio Sistemistico;
- Monitoraggio Applicativo specificamente configurato sul sistema di conservazione;
- Monitoraggio di Business, fornito come servizio configurabile.

Il sistema permette di profilare le utenze degli operatori in modo da poter fornire ad ognuno di essi una o più utenze di consultazione, in relazione alle specifiche attività di controllo assegnate.

Ad ogni operatore è possibile quindi assegnare la visibilità su specifici plug-in (ACL) ed assegnare l'utenza a uno o più gruppi di servizi.

Nell'ambito dei controlli sistemistici viene verificato lo stato dei vari layer applicativi, attraverso sonde standardizzate oppure personalizzate in base a specifiche esigenze e SLO - SLA concordate con il Cliente:

- Dischi fisici;
- Websphere/Application Server;
- Accesso Https;

- Database.

9.2 Verifica dell'integrità degli archivi

I pacchetti di archiviazione sono memorizzati da Intesa su supporti di memorizzazione distinti in storage di massa ad alta affidabilità (NAS) e automaticamente ridondati su siti geograficamente distinti.

I documenti conservati elettronicamente vengono sottoposti ad appositi controlli/collaudi al fine di garantirne l'integrità nel tempo, per tutto l'arco temporale coincidente con quelli che sono gli obblighi di legge in considerazione della tipologia di documentazione e ambito trattato (es. 10 anni per la documentazione fiscale) e di quanto concordato con il Cliente.

Intesa verifica lo stato di conservazione dei pacchetti di archiviazione, provvedendo, se necessario, al riversamento in base a quanto prescritto par 3.7 delle Linee Guida.

Il processo di collaudo prevede un controllo di integrità di tutti i documenti, organizzati in archivi logici e conservati nei diversi siti e un controllo di congruenza su un significativo numero di documenti.

I controlli di integrità sono relativi alla non alterazione del dato nel tempo, i controlli di congruenza sono effettuati in relazione a:

- Esibizione (leggibilità a campione, verificabilità);
- Verifica del sigillo e marca temporale;
- Correttezza e coerenza con i metadati.

L'esito della conclusione delle operazioni e della verifica sono riportate in un'apposita sezione su repository aziendale.

9.3 Soluzioni adottate in caso di anomalie

Un'anomalia del sistema di conservazione può essere evidenziata dalle figure di Intesa addette alle attività di gestione e monitoraggio che inseriscono direttamente una registrazione nel sistema di gestione problemi coinvolgendo il personale addetto alle attività correttive o da un utente del Cliente che la segnala allo Help Desk (manutenzione correttiva).

L'esigenza di una nuova funzionalità al servizio può invece essere evidenziata da una nuova richiesta/ordine del Cliente, da una proposta interna del Responsabile del Servizio o da una persona del supporto che evidenzi una possibile miglioria (manutenzione evolutiva).

Il processo per la risoluzione dell'anomalia o intervento correttivo/evolutivo si struttura con le seguenti fasi operative:

- Rilevazione anomalia e/o esigenza di intervento evolutivo;
- Diagnosi e assegnazione: questa fase si occupa di diagnosticare la causa del malfunzionamento (nei casi di Manutenzione correttiva) o la possibilità di integrazione della nuova funzionalità

all’interno del prodotto/servizio (nei casi di Manutenzione evolutiva) e provvedere all’assegnazione alla persona più adeguata;

- Correzione/evoluzione: vengono identificati gli oggetti software responsabili del malfunzionamento, o della nuova funzionalità, ed apportarvi le correzioni necessarie. Nel caso si tratti di un problema bloccante, in questa fase può’ essere attivato un bypass, per predisporre una soluzione immediata che consenta di continuare l’utilizzo, eventualmente anche in misura ridotta;
- Collaudo: consente di verificare che il prodotto/servizio modificato risolva il malfunzionamento segnalato o risponda ai nuovi requisiti funzionali e testare la non regressività delle correzioni effettuate. I test sono svolti con particolare attenzione agli aspetti di non-regressione delle modifiche apportate alle altre componenti dell’applicazione. Un attento esame viene poi effettuato per apportare le modifiche anche alle altre versioni correnti del prodotto/servizio. Tutte le attività ed i risultati della manutenzione del prodotto/servizio sono registrate in una apposita applicazione informatica "Schede manutenzione SW", che costituisce una importante banca dati valida per un riesame della qualità dei prodotti e delle segnalazioni di anomalie da parte di ogni cliente;
- Rilascio: il prodotto/servizio o l’applicazione modificata viene messa a disposizione del Cliente / Committente, in modo che la possa utilizzare;
- Propagazione: la modifica viene propagata, se previsto, ad altre piattaforme target del prodotto/servizio o dell’applicazione;
- Struttura di assistenza post-vendita: la struttura di assistenza post-vendita è erogata attraverso il Customer Care di Intesa (Helpdesk).

Qualora dalle attività di monitoraggio sopra indicate, supportate da appositi meccanismi automatici, vengano evidenziati eventuali problemi o il rischio di un loro accadimento, sono tempestivamente intraprese le azioni correttive opportune per evitare il deterioramento del servizio. Di tali eventi, in aggiunta alla loro risoluzione, viene tenuta adeguata traccia, tramite tool a supporto delle registrazioni e viene fatta un’analisi allo scopo di aggiornare, se necessario, le misure di sicurezza in atto.

Inoltre, è a disposizione dei Clienti un servizio di Customer Care “Help Desk” composto da persone addestrate sulle procedure di Conservazione e sulla verifica della disponibilità e dello stato dei servizi.

La struttura di supporto al Cliente è organizzata su 2 livelli:

1. **Help desk di 1° livello:**

Provvede ad acquisire e registrare la chiamata, fornire assistenza sulle funzionalità del sistema, identificare e per quanto possibile risolvere il problema riscontrato dall’utente ovvero passarlo al secondo livello di competenza. Provvede inoltre ad avvisare l’utente della risoluzione dei problemi da esso segnalati al termine del ciclo dell’intervento utilizzando i canali di accesso/contatto previsti

I compiti principali della struttura di Help Desk sono:

- Fornire assistenza ai Clienti per garantire continuità nell’erogazione dei servizi;
- Fornire informazioni sui servizi;

- Ricevere e registrare segnalazioni di problemi;
- Analizzare i problemi, attribuire un livello di gravità e fornire una loro risoluzione, che può essere temporanea oppure provvisoria (supporto di primo livello);
- Coinvolgere gli esperti che forniscono un supporto di secondo livello, ovvero specialisti che hanno competenze specifiche nell'area interessata, nel caso che il problema non possa essere direttamente risolto;
- Mantenere un contatto continuo con il Cliente per tenerlo informato sulla risoluzione dei problemi critici che lo riguardano;
- Chiudere i problemi congiuntamente con il Cliente comunicando l'avvenuta risoluzione.

Ogni soluzione identificata viene verificata nella sua completezza ed efficacia dal risolutore prima di essere fornita al cliente.

Durante tutta la fase di gestione dei problemi la struttura di Help Desk effettua un continuo monitoraggio sullo stato di avanzamento delle soluzioni ed esegue le eventuali azioni di sollecito nei confronti degli esperti che le devono definire, al fine di garantire che le stesse vengano attuate entro i target fissati.

Un'apposita applicazione informatica (HDA) supporta il flusso esecutivo e la registrazione delle segnalazioni.

Appositi misuratori e un'adeguata reportistica garantiscono un efficace controllo della funzionalità ed efficacia del supporto di primo e secondo livello ed il raggiungimento dei livelli di servizio previsti.

2. **Supporto di secondo livello:**

È costituito dagli specialisti dei servizi e dei prodotti oggetto di fornitura. Essi vengono chiamati in causa dal supporto di primo livello ogni qualvolta quest'ultimo non è in grado di risolvere un eventuale problema posto dall'utente.
La struttura di secondo livello non è quindi una unità organizzativa, ma una struttura virtuale, che si estende orizzontalmente a seconda delle aree tecniche di competenza e verticalmente anche a livelli superiori di specializzazione. La struttura di secondo livello comprende quindi gruppi con competenze sistemistiche, con il compito di risolvere i problemi di complessità tale da non poter essere risolti dall'helpdesk di primo livello a cui comunicherà il termine dell'intervento o competenze applicative con il compito di risolvere i problemi di complessità tale da non poter essere risolti dall'helpdesk di primo livello a cui comunicherà il termine dell'intervento.

3. **Supporto specialistico Trusted Doc (Legal Archiving):**

Si tratta di una struttura di secondo livello, operativa in ambito applicativo, creata specificatamente per i progetti di conservazione a norma.
Tale struttura supporta il Cliente su problematiche specifiche inerenti al processo di conservazione, nelle comunicazioni inerenti la gestione operativa del Servizio Trusted Doc, svolgendo le sue funzioni in stretta collaborazione con il Capo Progetto e con le figure specialistiche di Intesa con competenze tecnico-normative.