In.Te.S.A. S.p.A.

Conservatore qualificato

ai sensi del Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici, emanato da AgID con det. 455/2021

Manuale del Conservatore

Codice documento: MdC_V28042025

OID: 1.3.76.21.20.1

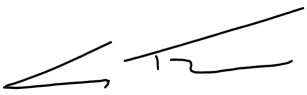
Redazione: Francesco De Cesare

Verifica: Maria Marchese

Approvazione: Luigi Traverso
(Responsabile del Servizio di Conservazione)

Data emissione: 28/04/2025

Versione: 08



Emissione

Azione:	**Nominativo**	**Data Revisione: 28/04/2025**
Redazione	Francesco De Cesare – Responsabile della funzione archivistica di Conservazione	
Verifica	Maria Marchese – Team Leader B2B Solutions	
Approvazione	Luigi Traverso – Responsabile del Servizio di Conservazione	

Registro delle revisioni

Versione n°: 08		**Data Revisione: 28/04/2025**
Descrizione modifiche:	Aggiornamento dei ruoli professionali, certificazioni e normativa di riferimento	
Motivazioni:	Aggiornamento normativa, inserimento certificazione ISO e cambio responsabile dei sistemi informativi	
Versione n°: 07		**Data Revisione: 31/01/2024**
Descrizione modifiche:	Revisione struttura del servizio	
Motivazioni:	Aggiornamento organizzativo	
Versione n°: 06		**Data Revisione: 15/11/2021**
Descrizione modifiche:	Aggiornamento loghi aziendali	
Motivazioni:	Cambio struttura societaria	
Versione n°: 05		**Data Revisione: 24/09/2021**
Descrizione modifiche:	Aggiornamento dei ruoli professionali	
Motivazioni:	Cambio responsabile del trattamento dei dati personali	
Versione n°: 04		**Data Revisione: 14/06/2021**
Descrizione modifiche:	Adeguamenti normativi	
Motivazioni:	Introduzione Linee Guida AgID	
Versione n°: 03		**Data Revisione: 29/01/2016**
Descrizione modifiche:	Adeguamento allo schema versione 2_1 pubblicato da AgID	
Motivazioni:	Richieste AgID	
Versione n°: 02		**Data Revisione: 24/11/2014**
Descrizione modifiche:	Precisazioni su Ruoli e Responsabilità	

Motivazioni:	Richieste AgID	
Versione n°: 01		***Data Revisione: 23/10/2014***
Descrizione modifiche:	Integrazioni e precisazioni richieste da AgID	
Motivazioni:	Richieste AgID	

Sommario

1 Scopo del documento 6
1.1 Ambito di riferimento ... 6
1.2 Struttura del Manuale del Conservatore ... 7
2 Terminologia (acronimi e glossario) 7
2.1 Acronimi ... 7
2.2 Glossario dei termini ... 9
3 Normativa e standard di riferimento 11
3.1 Normativa di riferimento ... 11
3.2 Standard di riferimento ... 12
4 Ruoli e responsabilità 13
4.1 Dettaglio dei ruoli e relativi compiti ... 15
4.1.1 Responsabile della Conservazione (Cliente) ... 15
4.1.2 Responsabile del Servizio di Conservazione ... 16
4.1.3 Responsabile della funzione archivistica di Conservazione ... 16
4.1.4 Responsabile dei sistemi informativi per la Conservazione ... 17
4.1.5 Responsabile dello sviluppo e della manutenzione del sistema di Conservazione ... 17
4.1.6 Responsabile della sicurezza dei sistemi per la Conservazione ... 17
4.1.7 Responsabile del Trattamento dei dati personali ... 18
5 Struttura organizzativa per il servizio di conservazione 18
5.1 Organigramma ... 18
5.2 Strutture organizzative ... 19
6 Oggetti sottoposti a conservazione 21
6.1 Oggetti conservati ... 21
6.2 Pacchetto di Versamento ... 23
6.3 Pacchetto di Archiviazione ... 24
6.4 Pacchetto di Distribuzione ... 25
7 Il processo di conservazione 26
7.1 Modalità di acquisizione dei Pacchetti di Caricamento per la loro presa in carico ... 27
7.2 Verifiche effettuate sui Pacchetti di Caricamento e sugli oggetti in essi contenuti ... 29
7.3 Accettazione dei Pacchetti di Caricamento e generazione del Rapporto di Versamento di presa in carico 29

7.4 Rifiuto dei Pacchetti di Caricamento e modalità di comunicazione delle anomalie 30
7.5 Preparazione e gestione del Pacchetto di Archiviazione 31
7.6 Preparazione e gestione del Pacchetto di Distribuzione ai fini dell'esibizione 32
7.6.1 Modalità via portale web 33
7.6.2 Modalità attraverso supporti di memorizzazione autoconsistenti 33
7.7 Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti 34
7.8 Scarto dei Pacchetti di Archiviazione 35
7.8.1 Modalità di restituzione e gestione della Cessazione del servizio di Conservazione 36
7.9 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori ... 36
8 Il sistema di conservazione 37
8.1 Componenti Logiche 38
8.2 Componenti Tecnologiche 40
8.3 Componenti fisiche 40
8.4 Procedure di gestione e di evoluzione 42
8.4.1 Conduzione e manutenzione del sistema di conservazione 42
8.4.2 Monitoring e sicurezza 43
8.4.3 Gestione e conservazione dei log 44
8.4.4 Change management 45
8.4.5 Verifiche periodiche di conformità e standard di riferimento 45
9 Monitoraggio e controlli 46
9.1 Procedure di monitoraggio 46
9.1.1 Sistema di monitoraggio sistemistico e applicativo 47
9.2 Verifica dell'integrità degli archivi 49
9.3 Soluzioni adottate in caso di anomalie 49
9.4 Protezione dei dati personali 52

1 Scopo 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, oltre ad essere prestatore di servizi fiduciari qualificati (QTSP- Qualified Trust Service Provider) ai sensi del Reg. (UE) 2024/1183 (eIDAS) per la firma elettronica, sigillo elettronico e validazione temporale elettronica (timestamp), iscritta al Marketplace AgID dei servizi di conservazione.

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) e dalle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici.

Per ottemperare a quanto indicato nel cap. 4.6 delle Linee Guida AgID ogni Titolare dell'Oggetto, cliente del servizio di conservazione INTESA, e, di conseguenza, ogni Responsabile della Conservazione, nell'ambito dello svolgimento dei compiti a lui assegnati dalla normativa, può liberamente far riferimento al presente documento nel proprio Manuale della Conservazione.

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 manuale: "Ruoli e responsabilità".

Nel Disciplinare tecnico, allegato al presente Manuale sono delineate le specificità del Servizio per il Cliente.

1.2 Struttura del Manuale del Conservatore

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. Il Manuale è, inoltre, pubblicato da Intesa sul proprio sito ufficiale.

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 al 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;
- Lettera di affidamento;
- Disciplinare tecnico (Allegato A al Manuale del Conservatore) – in precedenza definito Specificità del Contratto;
- Componenti tecnologiche del Sistema di Conservazione (Allegato B al Manuale del Conservatore);
- Eventuale documento di Analisi funzionale, per gli aspetti attinenti alle implementazioni tecniche della Conservazione, non allegato al presente Manuale del Conservatore, predisposto sulla base dello specifico contesto progettuale del Cliente;
- Piano di Cessazione del Sistema di Conservazione (documento riservato condiviso da Intesa con l'Agenzia per l'Italia Digitale (AgID).

2 Terminologia (acronimi e glossario)

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 AgID sulla formazione, gestione e conservazione dei documenti informatici
MdC	Manuale del Conservatore
PdA	Pacchetto di Archiviazione
PdC	Pacchetto di Caricamento
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
Allegato B	Documento contenente la descrizione tecnico-funzionale delle componenti logiche e fisiche del sistema 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 allo stesso tempo 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.
Lettera di affidamento	Documento formale, verificato e sottoscritto per approvazione dal Responsabile della Conservazione, attestante le informazioni anagrafiche, contrattuali e di riferimento per definire il perimetro di attuazione del servizio di conservazione in outsourcing.
Linee Guida	Linee Guida sulla formazione, gestione e conservazione dei documenti informatici pubblicate in Gazzetta Ufficiale n. 259 del 19 ottobre 2020
Manuale del Conservatore	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 di cessazione	Documento riservato, richiesto da AgID in merito all'iscrizione al Marketplace dei servizi di conservazione, in cui sono riepilogate le attività, i ruoli e le modalità in cui potrà essere gestita l'eventuale cessazione del sistema di conservazione.
Piano della sicurezza del sistema di conservazione	Documento riservato 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. 2024/1183 del Parlamento europeo e del Consiglio, del 11 aprile 2024 (eIDAS)
Trusted Doc	Servizio di conservazione di Intesa, erogato in modalità di outsourcing
Trusted Hub	Piattaforma tecnologica su cui è stanziato il 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, integrato con le modifiche introdotte dal Decreto Legislativo 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016";
- 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 per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005, nelle disposizioni attualmente vigenti indicate nelle Linee Guida emanate da AgID. [*Parzialmente abrogato dalle Linee Guida AgID in vigore dal 1° gennaio 2022*];
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005. [*Interamente abrogato dalle Linee Guida AgID in vigore dal 1° gennaio 2022*];
- 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. [*Interamente abrogato dalle Linee Guida AgID in vigore dal 1° gennaio 2022*];

- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82. [*Circolare interamente abrogata dal Regolamento AgID in vigore dal 1° gennaio 2022*];
- Regolamento (UE) N. 2024/1183 del Parlamento Europeo e de Consiglio del 11 aprile 2024 che modifica il Regolamento (UE) n. 910/2014 e per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale;
- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consigilio 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;
- Decreto Legislativo 4 settembre 2024, n. 138. Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148;
- Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici, emanato da AgID con det. 455/2021;
- Decreto Ministero Economia e Finanze 17 giugno 2014 "Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005";
- 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 G.U. n. 259 del 19 ottobre 2020.

3.2 Standard di riferimento

Gli standard ai quali il sistema Intesa è conforme e, ove previsto, qualificato sono:

- ISO 14721:2025 OAIS (Open Archival Information System);
- ISO 9001:2015, Quality management systems — Requirements;
- ISO/IEC 27001:2022, Information technology - Security techniques - Information security management systems – Requirements;
- ISO/IEC 27017:2015, Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services;
- ISO/IEC 27018:2019, Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors;
- ISO 37001:2025, Anti-bribery management systems — Requirements with guidance for use;

- 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;
- 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;
- ETSI TS 119 511 V1.1.1 (2019-06) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques;
- ETSI EN 319 401 V.3.1.0 (2024-06) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- 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;
- ISO 22313:2020, Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301;
- ISO 16363:2012, Space data and information transfer systems — Audit and certification of trustworthy digital repositories.

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. Nel presente documento, e in generale nella documentazione condivisa, viene inteso anche come Cliente.

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.

Nel processo standard predisposto, e descritto in questo manuale, la creazione del PdV è affidata a Intesa. Il PdV è infatti costituito dai sistemi Intesa al termine dell'iter, denominato di pre-ingest, in cui i documenti inviati dal Titolare dell'Oggetto, nel pacchetto informativo definito Pacchetto di Caricamento, vengono processati, se è prevista una fase di completamento tramite le funzionalità offerte da Intesa, e verificati, mediante l'esecuzione dei controlli normativi i cui esiti sono riportati nel Rapporto di Versamento.

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 di soggetti autorizzati, dal Cliente stesso, 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. Quest'ultimo è chiamato, altresì, a svolgere le necessarie attività di verifica e controllo in ossequio alle norme vigenti sui servizi affidati in outsourcing dalle PA, ove si tratti di una Pubblica Amministrazione.

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. L'affidamento, normato da specifica documentazione chiamata "Lettera di affidamento", consente di istituzionalizzare lo svolgimento, da parte del Conservatore, dei compiti elencati e delle attività richieste dalla normativa.

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, infine, è quel soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici.

4.1 Dettaglio dei ruoli e relativi compiti

Per assicurare un livello di qualità adeguato e soddisfacente nei servizi offerti, Intesa ha strutturato la propria organizzazione aziendale in processi. A livello complessivo dell'azienda, viene delineato il quadro generale delle procedure, nonché delle competenze e responsabilità ad esse associate.

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 con quanto previsto dalla normativa.

Intesa, come richiesto dalla normativa vigente, svolge la propria funzione con la massima cura e presidio mediante un gruppo di risorse specialistiche dedicate all'erogazione, gestione, supporto e presidio del Servizio, in base ad una solida 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 (Cliente)

Il Responsabile della Conservazione è una figura definita dal 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:

- Sottoscrizione formale della lettera di affidamento, su template fornito da Intesa, e partecipazione all'avvio del progetto di conservazione;
- Presa visione delle caratteristiche del Servizio reso disponibile da Intesa: 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, richiamando, per le parti tecniche di competenza, la documentazione disponibile (Disciplinare tecnico e Manuale del Conservatore).

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:

	Ruolo	Nominativo
1	Responsabile del servizio di conservazione	Luigi *TRAVERSO*
2	Responsabile della funzione archivistica di conservazione	Francesco *DE CESARE*

3	Responsabile del trattamento dei dati personali	Serena *DONEGANI*
4	Responsabile della sicurezza dei sistemi per la conservazione	Paolo *MAURINO*
5	Responsabile dei sistemi informativi per la conservazione	Matteo *ROTA*
6	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Marco *RASA*

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	
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 presenti nel 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 atte a garantire la conservazione, dalla fase di acquisizione da parte del produttore fino all'eventuale scarto, dei documenti informatici corredati dai relativi metadati, attraverso l'implementazione di adeguate procedure tecnologiche.

Gli oggetti digitali della conservazione sono trattati dal sistema di conservazione, così come previsto dallo standard OAIS, in pacchetti informativi che si distinguono in:

a) Pacchetti di Caricamento (struttura informativa che, nel processo standard, descrive l'oggetto documentale inviato dal Titolare dell'Oggetto nella fase di pre-ingest);
b) Pacchetti di Versamento;
c) Pacchetti di Archiviazione;
d) Pacchetti di Distribuzione.

Il modello concettuale di riferimento per la conservazione a lungo termine è il modello OAIS (standard ISO 14721) che ha introdotto nel panorama tecnico-normativo vigente i concetti relativi alla creazione, archiviazione e conservazione di pacchetti informativi.

Questi pacchetti sono composti, genericamente, da quattro elementi:

- Il contenuto informativo, cioè l'oggetto digitale 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 logiche, cioè i dati che indirizzano alla posizione logica del pacchetto informativo archiviato nel sistema di conservazione di Intesa;
- L'Indice del Pacchetto di Archiviazione, definito sulla base delle specifiche contenute nello standard UNI SINCRO, contenente le informazioni relative a: descrizione delle tipologie, informazioni di conservazione, informazioni sulla rappresentazione, informazioni riguardanti l'invio in conservazione, i formati dei file ed estensioni previsti, i riferimenti normativi e le modalità di versamento (che sono poi riprese e descritte in modo analitico nel Disciplinare tecnico).

L'interoperabilità tra i sistemi di conservazione dei soggetti che svolgono questa attività è garantita dall'applicazione delle specifiche tecniche dell'Indice 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, non esaustiva, dei principali formati ed estensione di file 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	ISO 32000	.pdf
PDF/A	Adobe Reader	Adobe	application/ pdf	ISO 19005	.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 utilizzato per formare i documenti informatici soggetti al processo di conservazione deve essere presente nell'Allegato 2 delle Linee Guida AgID, concordato preventivamente e riportato nell'apposita sezione del Disciplinare tecnico.

In particolare, AgID ha aderito all'iniziativa internazionale promossa dall'Open Preservation Foundation, con l'obiettivo di pubblicare regolarmente un elenco completo e aggiornato dei formati di file riconosciuti a livello globale, includendo per ciascuno informazioni chiave su interoperabilità e conservazione a lungo termine.

6.2 Pacchetto di Versamento

In sede di acquisizione dati, è previsto l'invio del documento in uno dei formati previsti dall'Allegato 2 delle Linee Guida. Come caratteristica fondamentale, indicata dalla normativa, il sistema di conservazione deve assicurare la fruibilità nel tempo 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 è riportata nel Disciplinare tecnico.

Il Cliente invia quindi alla piattaforma Intesa, nelle tempistiche e modalità operative concordate, i documenti da conservare corredati dalle strutture di indici da abbinare.

Nel processo standard Intesa il pacchetto informativo, inviato dal Titolare dell'Oggetto secondo le modalità concordate, si configura come Pacchetto di Caricamento non essendo presenti le strutture tecniche definitive e le componenti operative previste dal Pacchetto di Versamento (PdV).

Intesa, mediante gli accordi specifici, collabora alla definizione del Pacchetto di Versamento che, di conseguenza, viene a costituirsi sui sistemi Intesa al termine della fase definita di pre-ingest.

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

Il sistema di Conservazione è predisposto per gestire i formati di file che possono maggiormente garantire i principi di interoperabilità tra i sistemi stessi, in ottemperanza alla normativa vigente riguardante le specifiche tipologie documentali.

Vengono quindi scelti ed utilizzati, 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 dei metadati, secondo quanto previsto dall'Allegato 5 delle Linee Guida 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) sigillato e marcato temporalmente, il file Rapporto di Versamento (da qui RdV) firmato e marcato temporalmente, in caso di riversamento o di riconservazione interna il file IPdA del precedente processo, 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 delle 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 processo)
  - <previous_ipda.ext> (Eventuale file IPdA del precedente processo);
- 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 richiesti dalla normativa, indicati nell'Allegato 5 delle Linee Guida 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, da remoto, al documento conservato che può essere consultato ed esibito sia attraverso una modalità on-line attraverso il portale web Intesa, sia attraverso estrazioni autoconsistenti.

Il Pacchetto di Distribuzione è costituito da un file zip firmato con sigillo INTESA che contiene le medesime strutture del Pacchetto di Archiviazione. La differenza consiste nell'apposizione temporale del sigillo, difatti il Pacchetto di Distribuzione sigillato al momento della consultazione produce un'evidenza giuridica attestante oltre al contenuto del pacchetto, di qui la medesima struttura del PdA, anche la garanzia del corretto mantenimento della catena di conservazione. 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 obbligatori;
- Schema .xsd dei metadati custom (metadati memorizzati su struttura database e riportati nella sezione MoreInfo del xml SInCRO);
- Schema .xsd dei metadati (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, pertanto, è fornito di strumenti idonei per presentare i documenti conservati in caso di accessi, ispezioni e verifiche condotte da soggetti interni all'organizzazione del Cliente e/o agli enti competenti, come in caso di verifiche dell'Autorità o degli organismi competenti prescritti dalle norme vigenti per l'espletamento delle attività di controllo e di vigilanza.

7 Il processo di conservazione

Il processo di conservazione, descritto come istanza lineare, prevede la predisposizione di un Pacchetto di Versamento, contenente gli oggetti digitali da conservare corredati dai metadati previsti in base a norme definite (indice di conservazione), che viene trasmesso al sistema di conservazione secondo le modalità concordate tra Intesa e il Titolare dell'oggetto di conservazione. L'indice del Pacchetto di Versamento completa il Pacchetto di Versamento. Le attività che competono al Conservatore, provider affidatario del processo di conservazione, sono: la ricezione del PdC, completamento del PdV, la validazione del PdV, la trasformazione del PdV in PdA, il mantenimento del PdA in conservazione per le tempistiche stabilite contrattualmente e, in base alla necessità di business e di verifica, la visibilità al Titolare dell'oggetto di conservazione del PdD tramite le modalità di consultazione concordate, così come previsto dalle Linee Guida AgID.

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 contrattualmente sulla base della normativa, indipendentemente dall'evolversi del contesto tecnologico.

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

a) Pacchetti di Versamento: si tratta delle strutture informative contenenti i dati da conservare e consolidati dalla piattaforma di Intesa, corredate anche dai relativi metadati, secondo quanto concordato con il Cliente;
b) Pacchetti di Archiviazione (PdA): strutture dati, che nell'iter definito seguono al versamento, e tra le quali è presente anche l'IPdA predisposto secondo lo 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 durante il trasferimento logico alle procedure di conservazione. Queste procedure, tuttavia, supportano l'integrità del documento attraverso controlli automatici in ogni fase del processo.

Le verifiche e l'identificazione delle anomalie sono quindi effettuate a monte del processo, nell'ambito del sistema di versamento, dove vengono eventualmente rilevati e segnalati, mediante gli strumenti concordati, 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 attraverso la forma del Pacchetto di Versamento, che quindi contiene l'oggetto da conservare, e segue il processo di Conservazione previsto dalla normativa e, in modo particolare, dallo standard OAIS.

In riferimento alla normativa sulla conservazione dei documenti informatici a carattere civilistico e nel pieno rispetto di essa, Intesa ha scelto, valutandone i benefici e la coerenza con l'impostazione del servizio, di applicare il processo di conservazione a livello di singolo documento.

Infatti, il Pacchetto di Archiviazione creato per ciascun documento consente l'esibizione dello stesso con tutti i requisiti primari necessari per la sua completa verifica da parte delle autorità ispettive. Il documento, conservato singolarmente, potrà essere esibito in modo agevole in fase di giudizio e con valore probatorio riconosciuto 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 quindi portato alla definizione della soluzione attualmente in uso, la quale assume il singolo documento come elemento cardine del processo. Attraverso la gestione del pacchetto di versamento, dell'archiviazione e della distribuzione, essa realizza i vari passaggi richiesti dal CAD e dalle relative Linee Guida AgID.

7.1 Modalità di acquisizione dei Pacchetti di Caricamento per la loro presa in carico

Il Servizio di conservazione (denominato anche 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, per ulteriori dettagli sulle componenti tecnologiche del servizio si rimanda all'Allegato B al presente Manuale.

Il sistema, nella soluzione standard Intesa, prevede la gestione di diversi passaggi operativi, inclusi quelli legati alle attività di completamento dell'Oggetto digitale e all'esecuzione dei controlli previsti dalla normativa. Queste attività sono pianificate in una fase precedente rispetto al processo di Versamento.

In particolare, viene delineata una gestione del pacchetto informativo inviato dal Titolare dell'Oggetto, denominato appositamente Pacchetto di Caricamento. Questo pacchetto costituisce il nucleo documentale soggetto alle verifiche e azioni di completamento, ove previste dalla progettualità specifica, su cui il sistema di Conservazione interviene prima di cristallizzare il Pacchetto di Versamento.

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 fase del processo viene accuratamente registrata e archiviata in apposite tabelle del database dedicate al tracking/logging (log-registri), rendendole facilmente consultabili. I pacchetti informativi 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 recupero in caso di anomalia/errore 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 relative a 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, ad eccezione delle casistiche in cui l'invio viene effettuato dal Cliente oltre il termine normativo stabilito (es. casistiche di recupero del pregresso).

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 Caricamento e sugli oggetti in essi contenuti

Il sistema di versamento prevede, nella fase di pre-ingest, l'esecuzione di una serie di controlli di conformità, riconciliazione e correttezza sui documenti da conservare. In particolare, sono previsti:

- Controlli di conformità:
  - Verifica anagrafica dell'azienda mittente (Cliente/Titolare dell'oggetto di conservazione);
  - Verifica Formato ed estensione 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 Linee Guida AgID;
  - Presenza di tutte le informazioni definite per le specifiche categorie documentali obbligatorie.
- Controlli di correttezza:

  Nella fase di analisi preliminare vengono concordate le regole specifiche per l'esecuzione di eventuali controlli di univocità, duplicazione, coerenza e completezza dei documenti prima della conservazione, con segnalazione di eventuali documenti mancanti in base alle regole definite in accordo con il cliente.

I controlli sopra menzionati possono dare origine, eventualmente, ad errori bloccanti o non bloccanti, quindi eventualmente il rifiuto dei Pacchetti di Caricamento.

A tal proposito, il processo standard di Intesa non prevede il rifiuto del Pacchetto di Versamento, né il relativo Rapporto di Versamento negativo, ma esegue tutti i controlli previsti nella fase di pre-ingest. Di conseguenza, il rifiuto e la relativa segnalazione di errore riguardano esclusivamente al Pacchetto di Caricamento.

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

Dopo aver effettuato le verifiche sui Pacchetti di Caricamento e sugli oggetti digitali secondo quanto precedentemente indicato, gli stessi vengono accettati dal sistema con conseguente generazione di un messaggio di accettazione (ACK1). La corretta esecuzione dei controlli formali previsti consente la cristallizzazione del Pacchetto di Caricamento in Pacchetto di Versamento.

Al termine della fase di elaborazione del Pacchetto di Versamento e di controllo, viene, inoltre, generato il 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 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 e marcato temporalmente dal Responsabile del Servizio di Conservazione.

Il Servizio prevede la creazione di un Rapporto di Versamento per ogni oggetto digitale inviato dal Cliente.

Il Rapporto di Versamento è sottoscritto con firma elettronica qualificata del Responsabile del servizio di Conservazione di Intesa ed è conservato in correlazione al pacchetto di versamento in esso riportato; ricercando il pacchetto di versamento è possibile visualizzare il relativo Rapporto di Versamento.

7.4 Rifiuto dei Pacchetti di Caricamento e modalità di comunicazione delle anomalie

Il processo di conservazione è disegnato in modo da ridurre al minimo, pressocché zero, il rifiuto dei PdV. All'interno del workflow del servizio è infatti previsto una fase, denominata di pre-ingestion, necessaria per la corretta accettazione dei pacchetti informativi, denominati Pacchetti di Caricamento, che anticipano la verifica e segnalazione di anomalia.

Il mancato superamento dei controlli bloccanti sui Pacchetti di Caricamento genera degli eventi di anomalia che vengono notificati, mediante le modalità concordate, al Cliente.

Il processo standard Intesa, che include l'implementazione di adeguate verifiche e controlli nella fase di pre-ingest, stabilisce come numero massimo di rifiuti del Pacchetto di Versamento lo 0.

Eventuali anomalie e/o errori bloccanti vengono segnalati e comunicati al Cliente nelle fasi precedenti secondo le modalità stabilite.

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 workflow 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) nella modalità stabilita 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 Caricamento;
- Errori di tracciato e di contenuto dei metadati (es: 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 Caricamento;
- 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 nelle modalità concordate, come, ad esempio, 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 con estensione .p7m, dell'IPdA consente l'esibizione preliminare degli elementi del PdA, con già incorporati i requisiti primari e necessari per la sua completa verifica da parte delle autorità ispettive. Inoltre, il singolo documento può essere presentato per la valutazione e autenticazione da parte dei giudici o dai pubblici ufficiali in contesti di natura civilistica e tributaria.

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 (es.: ricevuto, conservato, ecc.).

In base alla tipologia documentale, vengono stabiliti in fase di setup le tempistiche di conservazione dei documenti assegnati dal sistema al momento della ricezione ed elaborazione del Pacchetto di Versamento.

Il Sistema di Conservazione è strutturato 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 sull'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 e 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, secondo le logiche di conservazione INTESA, coincide con quella dei Pacchetti di Archiviazione.

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

L'esibizione degli oggetti conservati viene concordata con il Cliente e può avvenire secondo lo standard di piattaforma di Intesa nelle modalità specifiche indicate nel Disciplinare tecnico del contratto, come ad esempio:

- Portale web Intesa;
- Web services;
- Supporti di memorizzazione autoconsistenti, se previsti;
- Altre modalità concordate.

Tramite il portale web Intesa si specifica che, anche selezionando più occorrenze da consultare come PdD il sistema mette a disposizione n singoli PdD, autoconsistenti e utilizzabili per le finalità previste.

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 sul database mediante un motore di ricerca personalizzato su ciascun indice associato al documento ed effettuarne la visualizzazione o il download, per la durata stabilita nel 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 e precedenti alla fase di versamento e archiviazione.

Gli utenti che possono accedere al sistema di consultazione sono 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 distribuiti, in via eccezionale e sconsigliato rispetto alla modalità tramite portale Web, per la consultazione anche attraverso l'utilizzo di supporti di memorizzazione auto consistenti, se richiesto dal Cliente e espressamente previsto nell'ambito delle specificità contrattuali.

In tal caso si procede con l'estrazione dei 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 eventuale parametro concordato con il Cliente per consentire la produzione di supporti autoconsistenti da consegnare al Cliente, se previsto dagli accordi contrattuali.

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 nel Disciplinare tecnico.

Gli indici di ricerca 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 e identificazione univoca del supporto fisico rimovibile (hard-disk o altro supporto specificatamente individuato), spedizione e consegna secondo le modalità concordate con il Cliente.

La consultazione dei Pacchetti di Distribuzione su supporto autoconsistente 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;
- Sono disponibili le seguenti funzioni sui documenti singoli:
  - 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 e secondo le modalità operative concordate, può procedere all'eventuale download di duplicati informatici.

Nei casi previsti dalla normativa, e a seguito di richiesta formale, il pubblico ufficiale può richiedere a Intesa la produzione di copie conformi dei documenti stessi.

Intesa mette a disposizione del pubblico ufficiale specifiche funzionalità prevedono l'accesso al portale di consultazione 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, di integrità degli stessi e di validità delle firme apposte attraverso l'uso di un verificatore di mercato prescelto dal pubblico ufficiale, 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 - definito contrattualmente sulla base dei requisiti normativi relativi alla specifica tipologia documentale – venga fornita al Cliente, con congruo preavviso, una segnalazione relativa ai documenti prossimi al termine del loro ciclo vita.

La procedura è configurata tramite la compilazione di una tabella nel 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 anni per gli altri documenti fiscalmente rilevanti o altre tempistiche, secondo quanto concordo contrattualmente con il Cliente ed indicato in Disciplinare tecnico).

Il sistema genera uno specifico report contenente l'elenco dei Pacchetti di Archiviazione con i documenti destinati allo scarto e un warning relativo alla loro imminente cancellazione. Segue lo scarto dei Pacchetti di Archiviazione e dei relativi riferimenti agli archivi logici, ad esclusione dei riferimenti necessari a riportare le informazioni relative allo scarto effettuato, che saranno mantenuti nei sistemi di Intesa ai fini di tracciatura delle operazioni svolte.

È previsto l'invio di una comunicazione al Titolare dell'Oggetto e al Responsabile della Conservazione indicato in anagrafica, tramite PEC all'indirizzo disponibile in anagrafica e via mail all'indirizzo ordinario associato. Le ricevute di ritorno verranno archiviate da Intesa e costituiranno il primo esito positivo del workflow di scarto. La cancellazione fisica dei dati avverrà a partire da 180 giorni dalla comunicazione formale, permettendo al Cliente e al relativo Responsabile della Conservazione di presentare, entro 90 giorni dalla comunicazione, eventuali richieste di estensione o restituzione dei documenti, che saranno consolidate contrattualmente e recepite come aggiornamento dei parametri del sistema o come attività operativa di estrazione e restituzione.

Qualora, a seguito della comunicazione formale, il Cliente desideri prolungare la conservazione dei documenti, potrà notificarlo entro 90 giorni dalla ricezione della stessa. In tal caso, si procederà all'adeguamento delle condizioni contrattuali che regolano questo aspetto.

La cancellazione, sia logica che fisica, riguarderà sia i documenti presenti nel Database della piattaforma così come quelli già riversati in archivi presenti su NAS.

7.8.1 Modalità di restituzione e gestione della 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 i documenti conservati, organizzati in archivi omogenei via connettore, o su altra modalità tecnica concordata, sulla base dei parametri concordati con il Cliente nella relativa attività procedurale.

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 concordato con il Cliente, rimanendo il rispetto delle tempistiche normative, non previste dal contratto, in esclusiva competenza del Cliente che, secondo le disposizioni normative vigenti, può procedere a riversare quanto conservato presso un Conservatore (definito subentrante). Il Cliente può quindi richiedere la restituzione dei dati, attraverso le modalità tecnico-operative concordante, e la conseguente liberazione di Intesa dagli obblighi derivanti dal 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 scartati dai sistemi di Intesa in modalità sicura.

Intesa, in conformità al Regolamento sui criteri per la fornitura dei servizi per la conservazione dei documenti informatici, ha redatto il proprio Piano di Cessazione in coerenza con l'Allegato B del Regolamento, inviando successivamente una copia ad AgID per la verifica e l'approvazione nell'ambito della qualificazione al Marketplace dei servizi di conservazione. Dopo aver ottenuto un esito positivo sulla documentazione presentata, Intesa è stata correttamente ammessa al Marketplace, che supera il precedente istituto dei Conservatori Accreditati, a partire dal 30 gennaio 2023.

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.

In caso di recesso o termine del contratto, se tale situazione è stata contemplata negli accordi contrattuali e prevede il mantenimento dell'obbligo di conservazione da parte di INTESA per il periodo stabilito, questo obbligo si limita alle attività di manutenzione applicativa, controllo del sistema, mantenimento dei pacchetti di archiviazione e gestione delle attività di scarto di fine vita.

In tal senso Intesa, nell'erogazione del servizio, opera attraverso le seguenti caratteristiche tecnologiche:

- Utilizzo, per la conservazione dei documenti, di formati ed estensioni di file prescritti dalle normative relative a garantire i requisiti di interoperabilità e di contrasto dell'obsolescenza tecnologica;
- 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 richiesto per le proprie precipue 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 e di cui è dubbio il valore di interoperabilità nel tempo.

Pertanto, nel momento in cui il soggetto produttore richieda il trasferimento dei Pacchetti di Archiviazione verso un altro Conservatore, le funzioni attivate da Intesa e garantite dal precedente elenco di requisiti del sistema di conservazione, permettono un rapido passaggio verso il nuovo provider 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.

Intesa, per quanto concerne il sistema di conservazione TDOC 2.0 definito sulla base dei requisiti contenuti nelle Linee Guida AgID, risulta corrispondente al modello n.5 descritto nel documento "Modelli di interoperabilità tra sistemi di conservazione" pubblicato da AgID a dicembre 2022.

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 come Certification Authority iscritto ad AgID. 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 provider di Conservazione.

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 e, in generale, le diverse componenti del servizio.

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.

Di seguito saranno riportate le informazioni relative all'infrastruttura del Servizio di Conservazione, maggiori dettagli relativi agli elementi indicati sono riportati nell'Allegato B al presente manuale: "Componenti tecnologiche del sistema di Conservazione"

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;
- Modulo PDF, che consente la trasformazione in PDF dei flussi ricevuti in vari formati: spool, AFP, TXT, CSV, XML, ecc.;
- Modulo Trusted Invoice per la formazione, trasmissione, ricezione e pubblicazione delle fatture elettroniche e relativi ACK e gestione dell'inoltro multicanale (Postalizzazione, e-mail, PEC, pubblicazione Web, inoltro SOGEI);
- Modulo Trusted Doc di Conservazione elettronica a norma, per la gestione del processo di generazione elettronica, di conservazione, pubblicazione dei documenti ed eventuale produzione dei supporti di memorizzazione e mantenimento delle caratteristiche di integrità, sicurezza, immodificabilità e leggibilità nel tempo;
- Modulo Trusted Exchange, che tramite una componente Server e una componente client (Trusted Client) consente la trasmissione Https di qualsiasi tipologia di flussi secondo una logica di richieste di servizio espresse in XML.
- Inoltre, la piattaforma dispone di una serie di "Connettori" che consentono l'interscambio controllato con altre piattaforme esterne, ampliabile nel tempo anche sulla base delle specifiche esigenze dei Clienti, quali:
  - Connettore Trusted Exchange;
  - Connettore SAP Concur (in partnership con ccelera);
  - Connettore MQ Series;
  - Connettore per SFTP;
  - Connettore Thema Spazio;
  - Connettore Connect Direct;
  - Connettore SOGEI;
  - Connettore PEC (Trusted PEC).

Peraltro, in funzione di specifiche esigenze dei clienti la piattaforma software è predisposta per l'estensione ad altre modalità di interscambio dati.

8.2 Componenti Tecnologiche

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

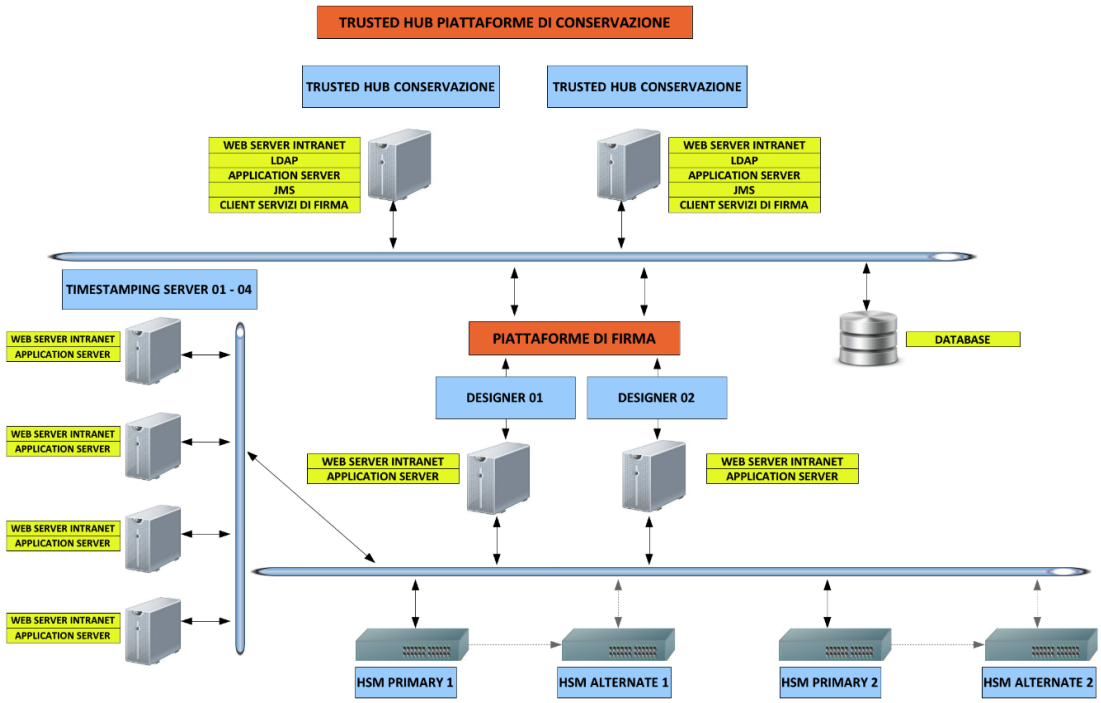


Figura 1: Componenti tecnologiche

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:

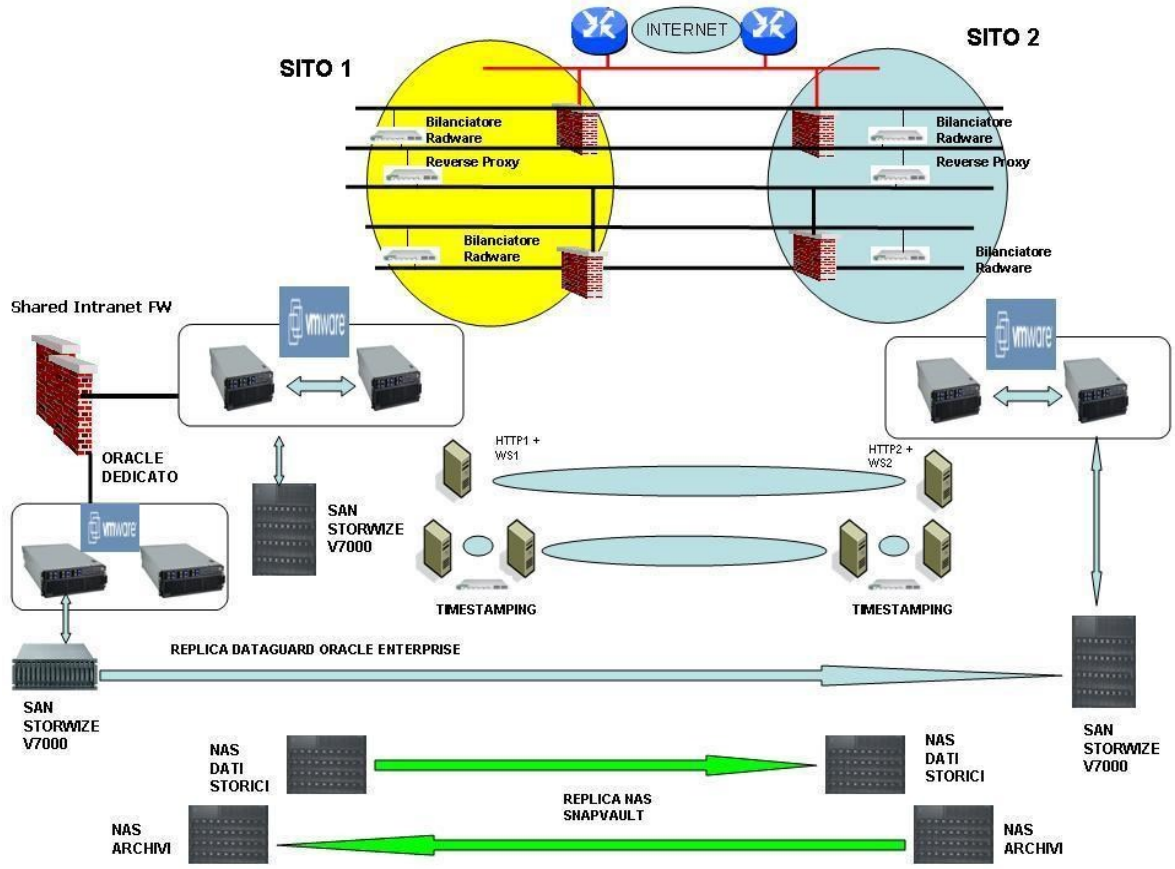


Figura 2: Componenti fisiche dei siti di conservazione

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 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 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 miglioramento 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, mirata ad 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, integrata con le linee guida certificate ISO 27017 e 27018, 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;
- Dal Regolamento Europeo 2016/679 del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

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 relativa 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 al trattamento dei documenti e relativa pubblicazione Web (accettazione dei pacchetti di versamento);
- Rapporto di versamento;
- ACK2: (rapporto di archiviazione) esecuzione del workflow interno inerente alla 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 e-mail al referente aziendale.

8.4.4 Change management

L'avvio di tale procedura, cosiddetta di Change management, 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.

Si definisce CHANGE una qualsiasi installazione o modifica di Hardware, Software o Procedure che modificano l'ambiente di produzione utilizzato per l'erogazione dei servizi per il Cliente.

La richiesta di Change può pervenire da diverse fonti, come ad esempio: richiesta Cliente, richiesta interna effettuata dal Capo Progetto; richiesta Gestione Applicativa; o chiunque abbia necessità di effettuare una modifica nell'ambito, generalmente, della direzione Delivery.

Una volta ricevuta la richiesta di modifica (Change), la funzione IT esegue le necessarie verifiche sulle informazioni condivise, valuta gli impatti e gli asset coinvolti, e pianifica la data del Change valutandone rischio e fattibilità, descrivendo dettagliatamente l'intervento. Dopo aver preparato la documentazione e completato le verifiche richieste, si richiede l'approvazione al manager, se necessario.

Al termine delle attività di Change, le cui procedure e modifiche sono adeguatamente monitorate e tracciate, la funzione IT conduce test funzionali e di non regressione per garantire il successo del Change. Vengono registrate tutte le attività svolte, e eventuali esiti negativi dei test di collaudo vengono segnalati ai team competenti.

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 affidati dal Responsabile della conservazione, tramite la sottoscrizione della lettera di affidamento, 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.

Per contrastare la progressiva obsolescenza dei formati ed estensione di file, specialmente in relazione a tempistiche di conservazione relativamente lunghe, è parte fondamentale degli accordi di versamento che i documenti inviati dal Titolare siano redatti con formati di file consigliati per la conservazione, così come disposto dall'Allegato 2 delle Linee Guida AgID. 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 disponibile un servizio dedicato di Help Desk per qualsiasi problematica relativa gli accessi o a eventuali anomalie nella trasmissione di documenti.

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

Questi gruppi prendono in carico il problema interagendo, se necessario, con gli specialisti di area (come ad esempio: piattaforma, infrastruttura fisica, connettività, DB, specifici servizi applicativi) e seguendo l'intera procedura fino alla risoluzione. Le azioni intraprese sono documentate nei log di sistema specifici, inseriti nel repository interno definito dal sistema di qualità aziendale.

Per garantire una corretta gestione del sistema di conservazione, Intesa elabora un registro cronologico del software dei programmi utilizzati, documentando le diverse versioni che si sono susseguite nel tempo. In aggiunta, viene redatto un registro cronologico degli eventi relativo alla gestione del sistema di conservazione, che include le risoluzioni adottate per correggere eventuali anomalie.

9.1 Procedure di monitoraggio

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

Il controllo e la gestione del sistema di Conservazione si basano sul monitoraggio continuo dell'ambiente e dei suoi singoli componenti, attraverso gli strumenti indicati di seguito, al fine di accertare la conformità 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 tramite il monitoraggio dell'ambiente e degli elementi critici, incluso l'esecuzione di attività gestionali come la verifica dello spazio disponibile, il mancato superamento dei livelli di soglia e la simulazione di log-on per il controllo di disponibilità dei servizi;
- Il monitoraggio dell'andamento del Servizio, la predisposizione o verifica di collaudi salvataggi periodici di dati o librerie, e l'eventuale predisposizione di dati di input e verifica dei risultati;
- La gestione delle modifiche ai parametri del Servizio (es. Abilitazioni utenze, Password), per adeguarlo velocemente alle mutate esigenze del Cliente;
- La gestione della sicurezza e degli accessi ai servizi per prevenire intrusioni e ingressi non autorizzati, articolata su diversi livelli (Rete, Sistema, Servizio Applicativo) e supportata da soluzioni tecnologiche avanzate, gestita da ruoli aziendali dedicati 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, svolta dalle persone più qualificate, un'effettuazione concentrata in apposite "finestre" temporali collocate in periodi di basso utilizzo ed u 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, permettendo di identificare 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, programmate o impreviste, con particolari attività di progettazione effettuate per circoscrivere e limitare l'impatto di possibili malfunzionamenti e attivare automaticamente o tempestivamente soluzioni alternative (es. routing, switch ecc.);
- La ripresa delle attività in caso di problemi mediante appropriate ed automatizzate attività di salvataggio di ambienti, librerie, applicazioni e dati, permettendo 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 hardware 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

Il sistema di monitoring INTESA è attualmente presente in parallelo su due piattaforme di checking:

- Modulo NAGIOS/NIMS+;
- Modulo CHECKMK.

Modulo NAGIOS/NIMS

Il modulo attualmente è ospitato su sistema operativo LINUX RED HAT e distribuito su due server, denominati FE e BE. La configurazione del sistema è progettata per assicurare l'alta disponibilità del servizio. A questo scopo, sono stati sviluppati diversi plug-in aggiuntivi, integrati con quelli nativi del prodotto open source di Nagios. Questa implementazione ha consentito l'aggiunta di varie funzionalità al sistema che altrimenti non sarebbero state disponibili, contribuendo così ad arricchirlo operativamente.

Ciascun plug-in di monitoraggio è progettato per gestire non solo il controllo specifico da effettuare, ma anche i parametri di riferimento e le soglie o regole per identificare i livelli di attenzione. Ogni plug-in opera autonomamente secondo una schedulazione propria, consentendo un monitoraggio più o meno frequente in base alle esigenze specifiche dell'oggetto o della funzionalità da monitorare.

Il sistema consente un monitoraggio articolato su tre diversi livelli:

- Monitoraggio di tipo infrastrutturale (host alive, service up/down, TCP/IP ports)
- Monitoraggio Applicativo configurato specificatamente sul sistema di conservazione (web appl checks), e su esplicite sonde di interrogazione di vari flussi applicativi, attraverso molteplici sql query, direttamente sui vari DATABASE (funzionalità SQL QUERY presente sul pacchetto software NIMS+).
- Monitoraggio di Business, fornito come servizio configurabile, attraverso programmi che tracciano la disponibilità dei check e quindi sono in grado di produrre reportistica ai fini di SLA / KPI.

Modulo CHECKMK:

In modulo in oggetto è anch'esso installato su due server bilanciati con sistema operativo LINUX RED HAT.

Il sistema è configurato per garantire l'alta disponibilità del servizio e rimane aperto per lo sviluppo di nuovi controlli su richiesta, sviluppabili mediante linguaggi di programmazione. Sono stati realizzati diversi plug-in aggiuntivi oltre la piattaforma Nagios/NIMS+. In particolare sono attualmente presenti le seguenti tipologie di controlli:

- Verifica delle dimensioni del filesystem e dei dischi, fisici e virtuali;
- Verifica delle dimensioni dei volumi NAS;
- Controlli su Websphere / applications;
- Accessi e raggiungibilità tramite HTTP(S) ai portali web;
- Stati di healthcheck su diverse applicazioni, in fase continua di migrazione (es. spring actuator, scadenze certificati, etc.);

È stato implementato il Business monitoring, come servizio all'interno del prodotto CHECKMK, che registra la disponibilità dei controlli e consente la generazione di report per la gestione di SLA / KPI.

Entrambi i moduli consentono di profilare le utenze degli operatori per fornire a ciascuno di loro una o più utenze di consultazione, in base alle specifiche attività di controllo assegnate. Ad ogni operatore è possibile assegnare la visibilità su specifici plugin (ACL) e l'utenza a uno o più gruppi di servizi. Tutti i controlli effettuati vengono razionalizzati per verificare lo stato dei vari layer applicativi, attraverso sonde standardizzate e

personalizzate in base a specifiche esigenze e agli accordi su SLO, SLA e KPI concordati con il Cliente, attualmente per entrambe le piattaforme di monitoring.

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 informatici conservati sono soggetti a specifici controlli/collaudi al fine di garantirne l'integrità nel tempo, per tutta la durata coincidente con gli obblighi di legge relativi alla tipologia di documentazione e ambito trattato (es. 10 anni per la documentazione fiscale), nonché in base a quanto concordato con il Cliente.

Intesa verifica lo stato di conservazione dei pacchetti di archiviazione, provvedendo a segnalare, se necessario, al Responsabile della Conservazione del Cliente le anomalie riscontrate e fornendo supporto per definire correttamente delle progettualità ai fini del riversamento, in base a quanto prescritto sia dal par 3.7 delle Linee Guida che dall'Allegato 2 delle Linee Guida stesse.

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 campione specifico 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 della scadenza relativa alla 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 responsabili delle attività di gestione e monitoraggio, che inseriscono direttamente una registrazione nel sistema di gestione problemi coinvolgendo il personale addetto alle attività correttive, oppure da un utente del Cliente che la segnala allo Help Desk (manutenzione correttiva).

Al contrario, l'esigenza di una nuova funzionalità può emergere da una richiesta/ordine del Cliente, da una proposta interna del Responsabile del Servizio o da un membro del supporto che identifichi una possibile miglioria (manutenzione evolutiva).

Il processo per la risoluzione dell'anomalia o intervenire in manutenzione correttiva/evolutiva si articola attraverso 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 integrare la nuova funzionalità all'interno del prodotto/servizio (nei casi di Manutenzione evolutiva) e assegna alla persona più idonea;
- Correzione/evoluzione: identificazione degli oggetti software responsabili del malfunzionamento o della nuova funzionalità e apportare le correzioni necessarie. Nel caso di un problema bloccante, in questa fase può' essere attivato un bypass per fornire una soluzione immediata che consenta di continuare l'utilizzo, eventualmente anche in misura ridotta;
- Collaudo: verifica 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. Successivamente, vengono apportate le modifiche anche alle altre versioni correnti del prodotto/servizio. Tutte le attività e i risultati della manutenzione del prodotto/servizio sono registrate in una apposita applicazione informatica, 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 reso disponibile al Cliente / Committente per l'utilizzo;
- 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).

Dalle attività di monitoraggio, supportate da appositi meccanismi automatici, vengono evidenziati eventuali problemi o il rischio di un loro accadimento. Vengono intraprese tempestivamente le azioni correttive opportune per evitare il deterioramento del servizio. Gli eventi, oltre alla loro risoluzione, vengono registrati tramite tool a supporto delle registrazioni e analizzati per 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 alla 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.

9.4 Protezione dei dati personali

Il servizio viene erogato da Intesa in qualità di Responsabile del Trattamento per la tutela dei dati personali, secondo quanto meglio descritto nella documentazione contrattuale di riferimento.

Il servizio, inoltre, è sottoposto alle regole di gestione e controllo previste dalle certificazioni in uso UNI ISO 27001, 27017 e 27018 che garantiscono la conformità ai controlli di sicurezza delle informazioni e ai controlli sulla sicurezza e protezione dei dati.

I ruoli, le responsabilità e le modalità di trattamento e le procedure di sicurezza sono quindi articolate nel rispetto delle predisposizioni normative e delle procedure di qualificazione del suddetto servizio.

-----FINE DEL DOCUMENTO-----