Manuale di conservazione

In.Te.S.A. SpA

Tipo Documento	Manuale di Conservazione
Società	*<Cliente>*
Redazione	In.Te.S.A. S.p.A.
Verifica e Approvazione	Agenzia per l'Italia Digitale Responsabile del Servizio di Conservazione Responsabile della Conservazione
Data emissione	23/10/2014
Data ultima revisione	29/01/2016

REVISIONI

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	05/09/2014	Maria Marchese	*TRUSTED DOC Solutions Consultant*
Verifica	15/09/2014	Luigi Traverso	*Responsabile del Servizio di Conservazione*
Approvazione	26/09/2014	Luca Altieri	*Direttore Generale*

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
MDC_V22102014	23/10/2014	Integrazioni e precisazioni richieste da AgID	Richieste AgID

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
MDC_V24112014	24/11/2014	Precisazioni su Ruoli e Responsabilità	Richieste AgID

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
MDC_V29012016	29/01/2016	Adeguamento allo schema versione 2_1 pubblicato dall'AgID	Richieste AgID

INDICE

1 Scopo e Ambito del documento

Il Manuale di Conservazione (di seguito anche "MdC") è il documento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 delle Regole Tecniche del sistema di conservazione.

Il presente Manuale descrive il sistema di conservazione di In.Te.S.A. S.p.A. (di seguito Intesa) denominato TrustedDoc, con evidenza dell'organizzazione, dei soggetti coinvolti e i ruoli svolti dagli stessi, del 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 procedimento di conservazione elettronica a norma di legge realizzato attraverso apposito Servizio in outsourcing per il Cliente.

La soluzione è erogata attraverso una piattaforma di servizio specializzata, ospitata nella server farm di Intesa e con adeguato supporto sistemistico per garantire l'integrità dei dati e per mantenere la piattaforma applicativa al massimo livello di disponibilità ed efficienza.

Conformemente a quanto previsto dalle Regole Tecniche in materia di sistema di conservazione (DPCM 3 dicembre 2013, di seguito "Regole Tecniche") all'art. 5 comma 2, lett. B, il servizio viene proposto da Intesa in qualità di "Terza parte fidata" e consente la conservazione elettronica a norma di legge di documenti elettronici e/o analogici, in outsourcing.

Intesa è inoltre Certification Authority accreditata CNIPA dal 2001 (oggi AgID) ed eroga i servizi di apposizione firme elettroniche e marche temporali con processi completamente integrati nativamente con quelli di emissione di documenti elettronici e conservazione a norma.

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 dalle Regole Tecniche e dal Codice dell'Amministrazione Digitale, si seguito anche "CAD" (Decreto.Legislativo 7 marzo 2005, n. 82 e successive modifiche/integrazioni).

Torna all'indice

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, anche accreditati come conservatori presso l'Agenzia per l'Italia digitale.

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

Nelle Specificità del Contratto, Appendice A, è delineato il processo che viene seguito per l'affidamento del Servizio da parte del Cliente.

Torna all'indice

1.2 Struttura del Manuale di conservazione

Il presente Manuale è prodotto in formato digitale da parte di Intesa (in collaborazione con il Cliente per quanto riguarda le Specificità del Contratto), fornito all'AgID per la pubblicazione sul sito istituzionale, archiviato in apposito repository del Servizio ad uso interno Intesa e messo a disposizione del Cliente.

Nel caso di eventuali aggiornamenti e adeguamenti del presente documento la nuova versione verrà fornita all'AgID per essere pubblicata sul sito istituzionale e resa disponibile al Cliente.

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

La redazione e gestione del Manuale della Conservazione ha costituito requisito imprescindibile per la procedura di accreditamento come conservatore presso l'Agenzia per l'Italia Digitale, quindi per il riconoscimento del possesso dei requisiti di più altro livello, in termini di qualità e sicurezza del Servizio erogato da Intesa.

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

- Appendice Specificità del Contratto (Appendice A al Manuale della Conservazione) – Documento di dettaglio (riferimenti normativi, ruoli, elementi di processo, tabelle tecniche dei documenti e pacchetti informativi)
- Appendice B al Manuale di conservazione – Documento di dettaglio con descrizione delle componenti tecnologiche del Sistema di Conservazione (piattaforma di erogazione del servizio, server farm e funzioni di CA). Per motivi di sicurezza e riservatezza, come previsto dalla Circolare AgID n.65 del 10 aprile 2014 - Documentazione per l'Accreditamento lett.n, tale Appendice è allegata come documento "Confidential" al Piano della Sicurezza del sistema di conservazione.
- Documento di Analisi funzionale, per gli aspetti attinenti le implementazioni tecniche della Conservazione, non allegato al presente Manuale della Conservazione, predisposto sulla base dello specifico contesto progettuale del Cliente.

Torna all'indice

2 Teminologia (glossario, acronimi)

Le definizioni di seguito elencate, utilizzate nell'ambito del presente Manuale, fanno riferimento a quanto riportato in Allegato 1 al DPCM 3 dicembre 2013.

TERMINE	DEFINIZIONE
accesso	operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici
accreditamento	riconoscimento, da parte dell'Agenzia per l'Italia digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo diconservazione
aggregazione documentale informatica	aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente
archivio	complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività
archivio informatico	archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico
autenticità	caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico
base di dati	collezione di dati registrati e correlati tra loro
certificatore accreditato	soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, dall' Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
ciclo di gestione	arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo
classificazione	attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati
Codice o CAD	decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni
codice eseguibile	insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici
conservatore accreditato	soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia digitale, il

	possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, dall'Agenzia per l'Italia digitale
conservazione	insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione
copia di sicurezza	copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 delle presenti regole tecniche per il sistema di conservazione
destinatario	Identifica il soggetto/sistema al quale il documento informatico è indirizzato
duplicazione dei documenti informatici	produzione di duplicati informatici
esibizione	operazione che consente di visualizzare un documento conservato e di ottenerne copia
evidenza informatica	una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica
formato	modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
funzione di hash	una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
generazione automatica di documento informatico	formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni
identificativo univoco	sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione
immodificabilità	caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso
impronta	la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash
insieme minimo di metadati del documento informatico integrità	complesso dei metadati, la cui struttura è descritta nell'allegato 5 del presente decreto, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato
interoperabilità	capacità di un sistema informatico di interagire con altri sistemi

	informatici analoghi sulla base di requisiti minimi condivisi
leggibilità	insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti
log di sistema	registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati
manuale di conservazione	strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 delle regole tecniche del sistema di conservazione
memorizzazione	processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici
metadati	insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 del DPCM 3/12/2013
pacchetto di archiviazione	Detto anche PdA, pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del DPCM 3/12/2013 e secondo le modalità riportate nel manuale di conservazione
pacchetto di distribuzione	pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta
pacchetto di versamento	pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato e descritto nel manuale di conservazione
pacchetto informativo	contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare
piano della sicurezza del sistema di conservazione	documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza
presa in carico	accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione
processo di conservazione	insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 10 delle regole tecniche del sistema di conservazione
produttore	persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di

	conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale.
rapporto di versamento	documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore
responsabile della conservazione	soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 delle regole tecniche del sistema di conservazione
responsabile del trattamento dei dati	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali
responsabile della sicurezza	soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza
riferimento temporale	informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento
sistema di conservazione	sistema di conservazione dei documenti informatici di cui all'articolo 44 del Codice
staticità	Caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione
utente	persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse

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

TERMINE	DEFINIZIONE
AgID	Agenzia per l'Italia Digitale
Appendice A	Appendice al presente Manuale, riporta la descrizione degli elementi di dettaglio del processo di conservazione, definito anche Specificità del Contratto
Appendice B	Appendice al presente Manuale, riporta la descrizione delle componenti tecnologiche del Sistema di Conservazione, trattasi di informazioni riservate
CA	Certification Authority, cioè ente accreditato per l'emissione e la gestione di certificati di firma qualificata
CAD	Codice dell'amministrazione digitale, Decreto.Legislativo 7 marzo 2005, n. 82 e successive modifiche/integrazioni

CAdES-T	Cryptographic Message Syntax Advanced Electronic Signature, formato standard di firma che genera una busta crittografica (file con estensione .p7m), con informazioni aggiuntive rispetto al formato base (CADES-BES) per includere la marca temporale
Cliente	Società Cliente ed eventualmente, le società del gruppo che hanno sottoscritto le opportune lettere di affidamento del Servizio di Conservazione.
CNIPA	Centro Nazionale per l' Informatica nella Pubblica Amministrazione
CRL	certificate revocation list, liste di certificati digitali revocati
DigitPA	In precedenza Centro nazionale per l'informatica nella pubblica amministrazione
DL	Decreto legge
DLgs	Decreto legislativo
DM	Decreto ministeriale
DMEF	Decreto Ministero dell'Economia e delle Finanze
DPCM	Decreto Presidente del Consiglio dei Ministri
DPR	Decreto del Presidente della Repubblica
HASH	Impronta informatica di un documento ottenuta applicando una "funzione di hash" e costituita da una sequenza di simboli binari.
HSM	Hardware Security Module, dispositivo che consente di ospitare diverse chiavi di firma e in grado di garantire elevatissimi livelli di sicurezza, affidabilità e performance in termini di velocità di esecuzione delle operazioni.
http	Hyper Text Transfer Protocol (identificativo convenzionale per un sito)
HTTPS	Secure Hyper Text Transmission Protocol. Protocollo sviluppato allo scopo di cifrare e decifrare le pagine Web che vengono inviate dal server ai client.
Intesa	Società In.Te.S.A. S.p.A. (anche Intesa)
IPdA	Indice del Pacchetto di Archiviazione – evidenza informatica associata ad ogni pacchetto di archiviazione contenente un insieme di informazioni articolate secondo lo standard SInCRO
L	Legge
NAS	Network Attached Storage, dispositivi ad alta capacità, sicurezza ed affidabilità per la memorizzazione dei dati
PAdES-T	PDF Advanced Electronic Signature, formato standard di firma su PDF, con informazioni aggiuntive rispetto al formato base (PADES-BES) per includere la marca temporale
PdA	Pacchetto di archiviazione
PDF	Portable Document Format
PKCS#7	Standard della sintassi dei messaggi crittografici, usato per firmare o criptare messaggi in una infrastruttura a chiave pubblica (PKI).

PKI	Public Key Infrastructure, cioè l'infrastruttura che crea e gestisce i certificati (qualificati) di firma elettronica basati su crittografia a chiave pubblica
Piano della Sicurezza Intesa	Piano della sicurezza del sistema di conservazione
PO	Process Owner
RDC	Responsabile della Conservazione
SinCRO	Supporto all'interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI11386:2010) - Standard nazionale in liguaggio xml, riguardante la struttura dell'insieme di dati a supporto del processo di conservazione
STS	Signature Time stamping, marca temporale apposta alla Firma mediante richiesta al servizio centralizzato di Time Stamping Server della Certification Authority Intesa per l'oggetto Firma
Trusted Doc	Servizio di conservazione di Intesa, erogato in modalità di outsourcing
Trusted Hub	Piattaforma tecnologica del Servizio di conservazione in outsourcing di Intesa
TSA	Time Stamping Authority, infrastruttura necessaria a realizzare e svolgere la funzione di timbratura temporale.
URL	Uniform Resource Locator (indica la modalità per individuare univocamente un sito Internet)
UTC	Universal Time Coordinated (Misura del tempo così come stabilito dall'International Radio Consultative Committee –CCIR)
Web	World Wide Web - principale servizio di Internet che permette di navigare e usufruire di un vasto insieme di contenuti

Torna all'indice

3 Normativa e standard di riferimento

3.1 Normativa di riferimento

La conservazione elettronica dei documenti di interesse civilistico-fiscale prevede l'esecuzione di un processo organizzativo ed informatico e l'adempimento delle disposizioni normative in vigore.

La normativa fiscale, direttamente applicabile nel caso di conservazione di documenti fiscalmente rilevanti, è comunque un significativo riferimento di processo nel caso di conservazione di documenti diversi.

In generale le modalità di formazione dei documenti informatici sono descritte dal Codice dell'Amministrazione Digitale (di seguito CAD, Decreto Legislativo 30 dicembre 2010, n. 235, modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale; successive modifiche e relative Regole Tecniche).

Le Regole Tecniche sui sistemi di conservazione introdotte dal DPCM 03/12/2013 e il Decreto del Ministero Economia e Finanze del 17 giugno 2014 definiscono il processo di conservazione elettronica a norma di legge.

La procedura informatica relativa all'emissione, alla conservazione ed alla esibizione dei documenti rilevanti ai fini fiscali è quindi disciplinata dal DMEF 17 giugno 2014 con un chiaro e diretto riferimento alle Regole Tecniche del CAD

Per il trattamento dei dati personali è necessario fare riferimento alle disposizioni del D.lgs 30 giugno 2003, N. 196.

Riferimento fondamentale per le tematiche di dematerializzazione, conservazione elettronica e fatturazione elettronica è quindi il Codice dell'Amministrazione Digitale.

Il CAD ha lo scopo di assicurare e regolare la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale utilizzando con le modalità più appropriate le tecnologie dell'informazione e della comunicazione all'interno della pubblica amministrazione, nei rapporti tra amministrazione e privati; disciplina anche l'uso del documento informatico nei documenti tra privati.

I riferimenti normativi e la prassi sono dettagliati nelle Specificità del Contratto, Appendice A al presente manuale.

Di seguito l'elenco dei principali riferimenti normativi italiani in materia, ordinati secondo il criterio della gerarchia delle fonti:

- Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;

- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.

Torna all'indice

3.2 Standard di riferimento

Gli standard a cui Intesa risponde sono:

- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- ETSI TR 101 533-2 V1.3.1 (2012-04)Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

Torna all'indice

4 Ruoli e responsabilità

Nel sistema di conservazione si individuano almeno i seguenti ruoli:

- produttore;
- utente;
- responsabile della conservazione.

I ruoli di produttore e utente sono svolti da persone fisiche o giuridiche interne o esterne al sistema di conservazione.

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

Il Cliente può affidare ad Intesa, in qualità di partner tecnologico, eventuali attività di carattere tecnico, volte alla generazione automatica del documento informatico, oggetto di conservazione.

L'utente richiede al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge. Trattasi quindi del Cliente o soggetti autorizzati all'accesso ai documenti (es. Autorità).

Il responsabile della conservazione definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia, ma può delegare la sua funzione come previsto dall' art. 6 comma 6 delle regole tecniche del CAD:

> "Il responsabile della conservazione, sotto la propria responsabilità, può delegare lo svolgimento del processo di conservazione o di parte di esso ad uno o più soggetti di specifica competenza ed esperienza in relazione alle attività ad essi delegate. Tale delega è formalizzata, esplicitando chiaramente il contenuto della stessa, ed in particolare le specifiche funzioni e competenze affidate al delegato."

Il responsabile della conservazione può inoltre decidere di affidare il processo/sistema di conservazione all'esterno, in outsourcing, in modo totale o parziale, a soggetti terzi pubblici o privati che offrono idonee garanzie organizzative e tecnologiche:

> "La conservazione può essere affidata ad un soggetto esterno, secondo i modelli organizzativi di cui all'articolo 5, mediante contratto o convenzione di servizio che preveda l'obbligo del rispetto del manuale di conservazione predisposto dal responsabile della stessa."

Nell'ambito della suddivisione delle attività, Intesa, persona giuridica, opera quindi nel ruolo di Conservatore, su affidamento formale da parte del Cliente, assumendo tutti i compiti e le funzioni previste dalla normativa per il ruolo di RDC.

Il Cliente identifica quindi il proprio Responsabile della Conservazione che a sua volta, avendone titolo e autorizzazione, attraverso la formalizzazione di un Contratto e di una specifica lettera, affida ad Intesa il procedimento di conservazione elettronica a norma di legge (Art. 6 comma 7 delle Regole Tecniche), attribuendo alla stessa i compiti del Responsabile della conservazione (definiti nel primo comma Art. 6 della Regole Tecniche).

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

I dati identificativi del Responsabile della conservazione del Cliente sono riportati in Appendice A, a seguito del processo indicato, il processo di conservazione è affidato al Conservatore Intesa.

Torna all'indice

4.1 Dettaglio dei ruoli e relativi compiti

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

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

Le attività sono assegnate in base ai ruoli aziendali definiti.

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

Le responsabilità attinenti ad Intesa, in qualità di Conservatore affidatario dal RCN, sono definite nella Lettera di Affidamento fornita dal Cliente in conformità a quanto previsto dalla normativa.

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

Inoltre, in specifici ambiti quali quello fiscale, gli interventi e le responsabilità sono da intendersi comunque non indipendenti dal Process Owner e dal Referente IT del Cliente, ad esempio nel contesto di verifiche a cura dell'Amministrazione finanziaria risulta fondamentale l'iterazione tra le figure coinvolte in Intesa e quelle identificate presso il Cliente stesso.

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 specificità del contratto - Appendice A, come dettagliatamente indicato nella dichiarazione tecnica organizzativa TD002, presentata all'AGID ai fini dell'accreditamento.

Torna all'indice

4.1.1 Responsabile della Conservazione e suo affidatario

Il DPCM 3 dicembre 2013 attribuisce al responsabile della conservazione (o suo soggetto affidatario, quale è Intesa per conto del Cliente) un ruolo essenziale nell'ambito delle procedure di conservazione elettronica: predispone, gestisce, presidia, controlla l'intero processo, appone al termine del processo la propria firma elettronica qualificata e la marca temporale, attestandone il corretto svolgimento.

Il DPCM dedica al responsabile della conservazione l'intero art. 7, attribuendogli precisi compiti e specifiche responsabilità.

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 opera d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei sistemi informativi.

L'art.7 del DPCM 3/12/2013 individua con molta precisione i compiti del responsabile della conservazione:

Art.7 comma 1, DPCM 3/12/2013

1. (…) In particolare il responsabile della conservazione:

a) definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente;

b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;

c) genera il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;

d) genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;

e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;

f) assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;

g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;

h) provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;

i) adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12;

j) assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;

k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;

l) provvede, per gli organi giudiziari e amministrativi dello Stato, al versamento dei documenti conservati all'archivio centrale dello Stato e agli archivi di Stato secondo quanto previsto dalle norme vigenti;

m) predispone il manuale di conservazione di cui all'art. 8 e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

In particolare, l'attività del responsabile della conservazione in collaborazione con il Conservatore risultano determinanti in diverse fasi del processo di conservazione:

- nella fase di apposizione di firma elettronica qualificata e marca temporale sui pacchetti di archiviazione e distribuzione; Intesa ha scelto di operare sui singoli documenti o sulle singole evidenze informatiche (art.9, comma 1, lett. f-g DPCM 3/12/2013);
- nel caso in cui sia previsto l'intervento di un ufficiale, spetta al responsabile della conservazione definire le opportune modalità di richiesta d'intervento in base alle specifiche esigenze del Cliente concordando con il Conservatore la presenza e assicurando allo stesso assistenza e risorse per l'espletamento delle attività a lui attribuite (art. 7 comma 1 lett.j, DPCM 3/12/2013)
- il responsabile della conservazione, in collaborazione con il Conservatore, riporta in Appendice A il dettaglio delle casistiche che richiedono la presenza del pubblico ufficiale se previste nell'ambito della tipologia documentale trattata o dello specifico processo definito in accordo con il Conservatore;
- il responsabile della Conservazione predispone il Manuale della Conservazione, in collaborazione con il Conservatore, descrivendo anche i dettagli specifici del progetto.

Torna all'indice

4.1.2 Responsabile del Servizio di Conservazione

Il processo di conservazione vede coinvolte, a vario titolo, differenti figure e differenti professionalità. Tutte le figure coinvolte sono coordinate dal responsabile del servizio di conservazione che è il punto di riferimento per le attività del conservatore.

Il responsabile del servizio di conservazione è colui che si occupa di definire e attuare le politiche complessive del sistema di conservazione, nonché di governare la gestione del sistema di conservazione; inoltre a lui spetta la definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente.

Torna all'indice

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.
E' 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.

Torna all'indice

4.1.4 Responsabile del Procedimento di Conservazione

Il responsabile del procedimento di conservazione, anche attraverso la struttura aziendale preposta, si occupa della corretta erogazione del servizio di conservazione all'ente produttore (Cliente), gestisce tutte le convenzioni, definisce gli aspetti tecnico-operativi e valida i disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.

E' il titolare del certificato di firma elettronica qualificata utilizzato per la sottoscrizione elettronica dei documenti ai fini della conservazione.

Torna all'indice

4.1.5 Responsabile dei sistemi informativi per la conservazione

Il responsabile dei sistemi informativi per la conservazione gestisce il corretto funzionamento di tutte le componenti hardware e software del sistema di conservazione. Si avvale di una struttura aziendale preposta alle specifiche attività, tiene quindi monitorati i livelli si servizio (SLA) concordati con il Cliente e segnala eventuali difformità degli SLA al Responsabile del servizio di conservazione individuando e pianificando le necessarie azioni correttive.

Controlla e verifica anche i livelli di servizio erogati da terzi segnalando le eventuali difformità al Responsabile del servizio di conservazione.

Infine pianifica lo sviluppo delle infrastrutture tecnologiche del sistema di conservazione.

Svolge le sue funzioni in stretta collaborazione con il Responsabile dello sviluppo e della manutenzione del sistema di conservazione.

Torna all'indice

4.1.6 Responsabile dello sviluppo e della manutenzione del sistema di conservazione

A tale responsabile compete il coordinamento dello sviluppo e della manutenzione delle componenti hardware e software del sistema di conservazione avvalendosi di una struttura aziendale preposta. Pianifica e tiene monitorati i progetti di sviluppo del sistema di conservazione oltre agli SLA relativi alla manutenzione del sistema di conservazione. Si interfaccia, inoltre, con il Cliente 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. A lui, infine, compete la gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.

E' colui che definisce il processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità dei documenti e delle aggregazioni documentali trasferite, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato;

Al responsabile dello sviluppo compete, in collaborazione con il responsabile della funzione archivistica di conservazione anche:

- la definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici;

- il monitoraggio del processo di conservazione e analisi per lo sviluppo di nuove funzionalità del sistema di conservazione.

Torna all'indice

4.1.7 Responsabile della sicurezza dei sistemi per la conservazione

Il responsabile della sicurezza dei sistemi per la conservazione si occupa del monitoraggio continuo e del rispetto dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; è suo compito segnalare ogni eventuale difformità al "responsabile del servizio di conservazione" e individuare e pianificare le necessarie azioni correttive.

Si avvale di una struttura aziendale preposta alle attività specifiche.

Torna all'indice

4.1.8 Responsabile del Trattamento dei dati personali

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

Il responsabile del trattamento dei dati personali garantisce che il servizio di conservazione sia realizzato ed erogato nel rispetto delle misure minime di sicurezza previste dal Codice della Privacy (D.Lgs. 196/2003 e relativo Disciplinare Tecnico).

Tutti gli operatori Intesa sono informati circa le corrette modalità di trattamento dei dati riservati.

Il Responsabile del trattamento dei dati personali verifica la designazione degli amministratori di sistema per i vari ambienti nell'ambito del sistema di conservazione.

Torna all'indice

4.1.9 Responsabili del Cliente: "Process Owner" e "Referente IT"

Il processo di conservazione elettronica prevede all'interno della struttura organizzativa del Cliente referenti con compiti e responsabilità specifiche in relazione all'ambito di competenza. Le figure coinvolte sono: il Process owner e il Referente IT.

I nominativi di tali riferimenti sono riportati in Appendice A.

Il Process Owner ed il Referente IT:

- sono responsabili della qualità dei processi che alimentano il servizio di conservazione a erogato da Intesa e dei relativi pacchetti informativi trasferiti all'outsourcer;
- segnalano i nominativi e le abilitazioni degli utenti che possono accedere al repository dei documenti oggetto del servizio di conservazione e ai pacchetti di distribuzione:
- richiedono, ove necessario, specifiche estrazioni dei pacchetti di distribuzione in archivi logici su supporti autoconsistenti ed indicano l'indirizzo esatto per il recapito;
- richiedono, ove necessario, l'intervento del RDC in occasione di ispezioni e/o di visite dell'Amministrazione finanziaria o altre autorità.

I principali compiti assegnati al Process owner sono:

- definire tutti gli standard del processo con il supporto tecnico di ICT;

- verificare la chiusura del processo di conservazione con l'ausilio di ICT, in termini di completezza di quanto inviato alla piattaforma di conservazione;
- attivare le procedure in caso di verifiche ispettive.

Il Referente IT del Cliente ha una responsabilità sulla gestione quotidiana del processo e quindi sovraintende il processo ordinario attraverso la gestione dei flussi informatici day by day.

I principali compiti assegnati al referente IT sono:

- monitorare i flussi informatici inoltrati dal Cliente verso Intesa., verificando che tutti i documenti previsti siano stati organizzati in pacchetti informativi ed inviati al sistema di conservazione in base alle specifiche tecniche concordate;
- analizzare l'esito delle operazioni svolte e le anomalie riscontrate, segnalate attraverso gli appositi rapporti di versamento ed anomalia, individuando le azioni correttive con il supporto del Process Owner per gli aspetti diversi da quelli tecnico-informatico;
- attivare e verificare la corretta gestione delle anomalie e la relativa comunicazione a Process Owner e Intesa
- supportare il Process Owner nell'attività di verifica di completamento del processo di conservazione in termini di completezza di quanto inviato alla piattaforma di conservazione;
- implementare le change request informatiche su richiesta del Process owner;
- supportare il Process owner nel caso di verifiche ispettive.

Torna all'indice

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.

Nell'ambito del team di lavoro sono stati evidenziati, in particolare, a fronte di ogni Direzione, i nominativi maggiormente significativi per i quali sono stati consegnati all'AgID i relativi Curricula e indicato il numero delle altre risorse coinvolte nelle attività del servizio di Conservazione (rif. documenti Intesa TD001 e TD002 presentati in fase di accreditamento all'AgID).

Torna all'indice

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:

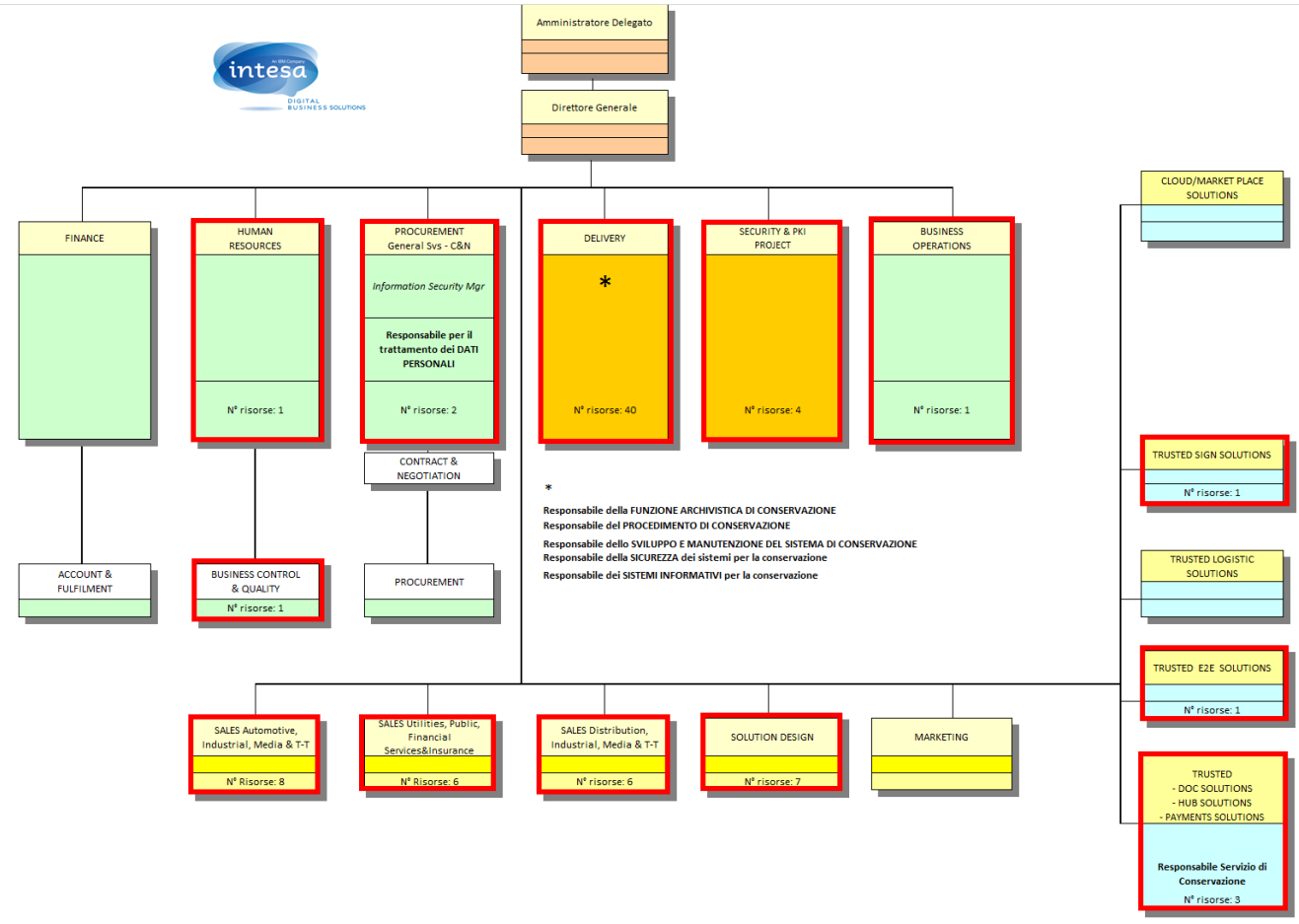

Figura 1:Organigramma e ruoli coinvolti

Torna all'indice

5.2 Strutture organizzative

Di seguito la tabella esplicativa delle Responsabilità che intervengono nelle principali funzioni che riguardano il servizio di conservazione.

Legenda	
RSC	Responsabile del servizio di conservazione
RSSC	Responsabile sicurezza dei sistemi per la conservazione
RA	Responsabile della funzione archivistica di conservazione
RTP	Responsabile trattamento dei dati
RSI	Responsabile sistemi informativi per la conservazione

RSM	Responsabile sviluppo e manutenzione del sistema di conservazione

Attività proprie di ciascun contratto di servizio di conservazione						
	Responsabilità					
	RSC	**RSSC**	**RA**	**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
Preparazione e gestione del pacchetto di archiviazione		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
Scarto dei pacchetti di archiviazione	X	X			X	X
Chiusura del servizio di conservazione	X	X	X	X	X	X

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

Torna all'indice

6 Oggetti sottoposti a conservazione

6.1 Oggetti conservati

Intesa gestisce, in qualità di outsourcer per centinaia di Clienti, molteplici tipologie di oggetti conservati e relative strutture dati, che dipendono dal settore di appartenenza (fiscale, assicurativo, bancario, industriale, etc) e dalle specifiche esigenze del Cliente.

Intesa adotta gli standard richiesti dalla normativa in termini di tipologie di formati e metadati, specificando di volta in volta nell'ambito delle Specificità del contratto - Appendice A del presente Manuale i relativi dettagli (tipologie documentali / struttura dei dati e numerosi altri elementi indicati nelle tabelle di cui alle Specificità del contratto Appendice A).

Di seguito la tabella generale degli oggetti sottoposti a conservazione, il cui dettaglio specifico per Cliente, concordato quindi con il soggetto produttore, è riportato in Specificità del contratto Appendice A.

formato del file	visualizzatore	produttore	tipo MIME	standard	estensione
PDF	Adobe Reader	Adobe	application/ pdf	ISO32000-1	.pdf
PDF/A	Adobe Reader	Adobe	application/ pdf		.pdf
XML	Internet Browser	W3C	application/xml text/xml		.xml
TXT	Internet Browser	Ai fini della conservazione nell'uso di tale formato, è importante specificare la codifica del carattere (Character Encoding) adottata			.txt
TIFF	Visualizzatore di immagini	Adobe	image/tiff		.tif
JPG	Visualizzatore di immagini	Joint Photographic Experts Group	image/jpeg	ISO/IEC 10918:1 i	.jpg , .jpeg
EML	Client di posta elettronica			RFC2822	.eml

Torna all'indice

6.2 Pacchetto di versamento

La tipologia di pacchetto di versamento e relativa struttura dati vengono concordate tra Intesa e il Cliente in qualità di produttore nel rispetto delle norme vigenti.

La struttura dati standard del pacchetto di versamento gestita nell'ambito del Servizio prevede l'invio del documento in uno dei formati previsti dall'Allegato 2 al DPCM 3/12/2013, corredato da una struttura metadati custom, in formato .csv.

Come indicato dalla normativa, il sistema di conservazione deve assicurare la reperibilità 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 (analisi archivistica).

La descrizione delle tipologie degli oggetti sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti e dei metadati da associare alle diverse tipologie (descrizione archivistica) viene riportata in Appendice A.

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

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

Nell'ambito dei documenti rilevanti ai fini fiscali la normativa richiede che siano consentite le funzioni di ricerca e di estrazione delle informazioni dagli archivi informatici in relazione almeno al cognome, al nome, alla denominazione, al codice fiscale, alla partita IVA, alla data o associazioni logiche di questi ultimi, laddove tali informazioni siano obbligatoriamente previste.

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

Vengono quindi scelti, in accordo con il Cliente e in conformità a quanto indicato nell'Allegato 2 al DPCM 3/12/2013, formati che possano consentire la leggibilità e la reperibilità del documento informatico nel sistema di conservazione, considerando le caratteristiche di apertura, sicurezza, portabilità, funzionalità, supporto allo sviluppo, diffusione.

Le tipologie di pacchetto di versamento gestite per il Cliente e le relative strutture dati concordate sono descritte nel dettaglio nelle Specificità del contratto – Appendice A.

Torna all'indice

6.3 Pacchetto di archiviazione

Il sistema di conservazione di Intesa prevede la gestione del pacchetto di archiviazione (documento firmato e marcato temporalmente) in base alle specifiche della struttura dati riportate dal DPCM 03/12/2013.

Il pacchetto di versamento acquisito dal sistema di conservazione viene sottoposto al processo di apposizione di firma elettronica e marca temporale, producendo il pacchetto di archiviazione.

Ogni pacchetto di archiviazione è rappresentato da un file firmato in modalità CAdES, in formato .p7m, corredato dall'Indice del pacchetto di archiviazione (IPdA) generato da Intesa.

La struttura dell'IPdA è definita in modo univoco per ciascuna tipologia documentale e descritta nelle Specificità del contratto - Appendice A. Tale struttura è conforme allo standard nazionale SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010), 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 del file SInCRO è stata definita da Intesa sulla base delle informazioni riportate nell'Allegato 4 (Specifiche tecniche del Pacchetto di Archiviazione) del DPCM 3/12/2013, verificata con il supporto di consulenti specialisti in materia.

La struttura xml del SInCRO prevede inoltre:

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

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

L'Indice del Pacchetto di Archiviazione viene firmato digitalmente attraverso lo standard CAdES generando quindi un file con estensione xml.p7m.

Attraverso correlazioni logiche, veicolate dal database della piattaforma di conservazione, ogni pacchetto di archiviazione è corredato da strutture dati documentate, consentendo il legame complessivo tra il pacchetto di archiviazione (file .p7m, singolo documento firmato e marcato) e i seguenti elementi:

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

Torna all'indice

6.4 Pacchetto di distribuzione

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

Ai fini della interoperabilità tra sistemi di conservazione, il sistema di Intesa prevede la produzione di pacchetti di distribuzione coincidenti con i pacchetti di archiviazione, quindi corredati dagli elementi di firma e marca temporale (Art. 9, comma 1 lett. h DPCM 3/12/2013), adottando analoghe modalità e funzioni di preparazione.

La tipologia e la struttura dei pacchetti di distribuzione coincidono quindi con quella dei pacchetti di archiviazione.

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

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

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

Apposite funzionalità consentono di effettuare la visualizzazione, la verifica di integrità o l'esportazione dei pacchetti di distribuzione.
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 nelle Specificità del Contratto (es. via Web Services, supporti fisici di memorizzazione).
Il Servizio quindi dispone di strumenti idonei ad esibire i documenti conservati, in caso di accessi, ispezioni e verifiche a cura di soggetti interni all'organizzazione del Cliente e/o agli enti competenti (in caso di verifiche dell'Autorità Finanziaria o degli organismi competenti previsti dalle norme vigenti ai fini dell'espletamento delle attività di controllo e di vigilanza).

Torna all'indice

7 Il processo di conservazione

In attuazione di quanto previsto dall'articolo 44, comma 1, del CAD, il sistema di conservazione di Intesa denominato TrustedDoc assicura la conservazione elettronica a norma di legge, tramite l'adozione di regole, procedure e tecnologie, dei documenti del Cliente, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità.

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

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

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

Come indicato all'articolo 4 delle Regole Tecniche del CAD sul sistema di conservazione, gli oggetti della conservazione sono trattati dal sistema di conservazione in pacchetti informativi che si distinguono in:

a) pacchetti di versamento:
   si tratta dei dati da conservare inviati dal Cliente alla piattaforma di Intesa, corredati dai relativi metadati, secondo quanto concordato con il Cliente.

b) pacchetti di archiviazione (PdA): documenti conservati a norma, ai quali viene apposta firma elettronica qualificata del conservatore Intesa e marca temporale su singolo documento, corredati da relativi metadati minimi, SInCRO e specifici indici di conservazione per la ricerca dei documenti (IpdA);

c) pacchetti di distribuzione: documenti conservati a norma, disponibili per la ricerca, consultazione ed esibizione, via portale web oppure da supporto auto consistente o altre modalità concordate con il Cliente e descritte nel presente documento.

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 multiazienda.

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

- configurazioni,
- processi applicati dai workflow compresi i processi 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 procedimento e suoi operatori una visione unitaria dei diversi processi di gestione, in particolare per le funzioni di monitoraggio, controllo ed *alerting*.

Il Servizio di conservazione di Intesa è basato su un'architettura fisica ed applicativa tesa e continuativa. La divisione tra il sistema di versamento e sistema di conservazione corrisponde

ad una separazione di natura logica, i documenti non sono quindi soggetti a trasferimenti tra ambienti che non siano attestati sulla medesima infrastruttura.

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

Le verifiche e l'identificazione delle anomalie sono quindi effettuate a monte del processo, nell'ambito del sistema di versamento, dove vengono eventualmente rilevati gli scarti. Le fasi successive avvengono sotto il monitoraggio del sistema di gestione, che controlla il corretto svolgimento del processo di conservazione e produce la relativa reportistica sia in relazione alle eventuali anomalie rilevate sia in riferimento a quanto correttamente conservato.

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

Con riferimento alla normativa relativa alla conservazione elettronica dei documenti a carattere civilistico e fiscale e nel pieno rispetto di essa, Intesa ha scelto di considerare quale pacchetto di versamento, su cui applicare il processo fino alla chiusura del pacchetto di archiviazione, il singolo documento.

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

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

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

Torna all'indice

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

Il Servizio di conservazione TrustedDoc consente il trasferimento dei dati e relativi metadati (pacchetto di versamento) 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, descritta in dettaglio nell'Appendice B del Manuale (allegato al Piano della Sicurezza).

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

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

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

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

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

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

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

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

Torna all'indice

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

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

- Controlli di conformità:
  - Verifica anagrafica dell'azienda mittente (Cliente/produttore)
  - Formato dei documenti
  - Presenza dei MetaDati previsti
  - Presenza di tutte le informazioni definite per le specifiche categorie documentali obbligatorie
  - Integrità del Pacchetto di Versamento in termini di contenuto e corrispondenza con relativi indici

- Controlli di correttezza:

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

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

Torna all'indice

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

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

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

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

Il rapporto di versamento è un documento informatico di tipo file testo e codifica UTF-8.

La struttura del record contiene un numero fisso di campi, tutti obbligatori, con lunghezza dei valori variabile, il carattere ";" (punto e virgola) viene utilizzato come carattere di separatore dei campi.

IL rapporto di versamento include l'impronta del/dei pacchetti di versamento cui si riferisce, l'elenco dei documenti acquisiti dalla piattaforma per la successiva conservazione, il riferimento temporale (UTC).

La tabella sotto elenca l'ordine ed il significato dei campi.

Nome campo	Posizione	Valore
Piattaforma	1	Sistema Intesa
ID documento (del pacchetto di versamento)	2	Identificatore univoco del documento nella piattaforma
Data di versamento	3	Data di caricamento del file nel sistema In formato UTC, pattern di stampa: yyyy-mm-dd'T'hh:mm:ss'Z'
Hash pacchetto di versamento	4	Hash SHA-1 del pacchetto di versamento

Nel sistema di conservazione di Intesa ad ogni rapporto di versamento viene assegnato un nome file univoco con estensione .txt e successivamente, dopo la sua conservazione con estensione .p7m.

Il Servizio prevede la creazione di un rapporto di versamento per ogni flusso inviato dal Cliente, contiene i riferimenti a pacchetti di versamento dello stesso Cliente e tipologia di documento. A livello fisico all'interno del file sono presenti 1 o più record (righe) ciascuno dei quali identifica univocamente il pacchetto di versamento acquisito nel sistema.

Al fine di rendere efficiente la generazione e fruibilità del rapporto di versamento, in funzione della tipologia di processo e dei volumi di documenti previsti, possono essere definite e concordate con il Cliente ulteriori regole l'identificazione dei pacchetti di versamento le cui informazioni saranno incluse all'interno di un unico rapporto di versamento, utilizzando procedure automatizzate basate su schedulazioni temporali o legate al numero di pacchetti da trattare.

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

Torna all'indice

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

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

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

Il processo di controllo è caratterizzato dunque da:

- Esecuzione del work flow di verifica
- Rilevamento e tracciatura dell'anomalia (tabella su data base e storicizzazione dell'attachment su casellario)
- generazione della segnalazione certa dell'errore con rifiuto del documento
- invio della segnalazione con relativa motivazione (rapporto di anomalia) in modalità email al referente aziendale del Cliente
- gestione attraverso contatto diretto con il referente per le diverse casistiche di errore che possono avere trattamenti e soluzioni differenziate

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

Il report di anomalia riporta:

- l'identificativo univoco del pacchetto di versamento rifiutato
- i relativi metadati univoci concordati con il Cliente (es. numero e data documento)
- la descrizione dell'errore rilevato.

Elenco delle anomalie gestite:

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

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

Tali comunicazioni vengono repertorizzate 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.

Torna all'indice

7.5 Preparazione e gestione del pacchetto di archiviazione

Al termine dell'attività di acquisizione/generazione e verifica del pacchetto di versamento, Intesa procede con la presa in carico dei documenti nell'ambito dei processi di firma e marca temporale quindi alla generazione e gestione del pacchetto di archiviazione.

Il sistema di conservazione viene attivato dal sistema di versamento al termine dei controlli indicati nei paragrafi precedenti, in base ad un processo teso, e continuativo tra i due ambiti (versamento e conservazione).

Il sistema di conservazione di Intesa prevede la gestione del pacchetto di archiviazione (documento firmato e marcato temporalmente) in base alle specifiche della struttura dati riportate dal DPCM 03/12/2013.

Ogni documento viene inviato in conservazione per mezzo di un pacchetto di Archiviazione contenente il singolo oggetto da conservare inteso come singolo documento.

Con riferimento alla normativa relativa alla conservazione elettronica dei documenti a carattere civilistico e fiscale e nel pieno rispetto di essa, Intesa ha scelto di considerare quale lotto, su cui applicare il processo fino alla relativa chiusura, il singolo documento e non un insieme di documenti. Il singolo documento corrisponde quindi al pacchetto di archiviazione, su cui applicare i vari steps richiesti dal CAD e relative Regole Tecniche del sistema di conservazione.

Il file di formato p7m del documento singolo permette l'esibibilità dello stesso con già a bordo i requisiti primari e necessari alla sua completa verifica da parte delle autorità ispettive.Il singolo documento potrà inoltre essere esibito in fase di giudizio ed essere autenticato dai giudici o dai pubblici ufficiali nelle cause di carattere civilistico e tributario.

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

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

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

Intesa provvede, per ogni singolo documento, all'apposizione della firma del responsabile del procedimento di conservazione di Intesa e della marca temporale come di seguito descritto:

- produzione dell'"impronta" del documento mediante algoritmo di Hashing SHA-256
- apposizione della firma all'"impronta" del documento mediante uso del certificato digitale del responsabile del processo di conservazione
- apposizione della marca temporale alla firma (Signature Time Stamping – STS), richiedendo il servizio al Time Stamping Server di Intesa

- creazione di un oggetto unico (file .p7m) in formato PKCS#7 contenente il documento, la firma e la marca temporale (Signature Time Stamping)

Le operazioni di apposizione di firma e marcatura temporale vengono effettuate nel rispetto delle normative specifiche in materia di firme e validazione temporale.

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

Con tali operazioni si completa il processo di conservazione a norma, 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 di firma del responsabile del procedimento 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.

Maggiori dettagli circa i servizi di firma digitale e marcatura temporale erogati da Intesa sono descritti in Appendice B.

Torna all'indice

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

La tipologia e la struttura dei pacchetti di distribuzione coincidono con quella dei pacchetti di archiviazione.

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

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

- Portale web Intesa (standard)
- Supporti di memorizzazione autoconsistenti (standard)
- Web services
- Single Sign-on
- Altre modalità concordate

Torna all'indice

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.

Il portale è configurato in base ad una specifica classificazione in relazione alle tipologie documentali in essere, quindi attraverso l'organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati.

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

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

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

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

Torna all'indice

7.6.2 Modalità attraverso supporti di memorizzazione autoconsistenti

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

In tal caso si procede con l'estrazione di pacchetti di distribuzione, per l'esibizione dei documenti conservati, organizzati in archivi logici (aggregazioni documentali informatiche, archivio informatico).

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

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

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

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

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

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

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

Il viewer, predisposto in versione multi-lingua, 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:

- Check integrità

  Il viewer applica su tutti i file contenuti sul supporto il medesimo criterio di verifica utilizzato dal server in fase di creazione dell'archivio informatico. In caso di corruzione dell'archivio viene emessa segnalazione di errore.

- Ricerca documentale

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

- Funzioni sui documenti singoli

  Sono disponibili le seguenti funzioni:

  - Visualizzazione del documento
  - Visualizzazione degli oggetti costituenti il PKCS#7 (impronta, firma, marca temporale,)
  - Estrazione degli oggetti costituenti il PKCS#7 (firma, marca temporale, PKCS#7 completo, file originale in chiaro)
  - Verifica dell'integrità del PKCS#7 con controllo di validità certificato di firma e marca temporale su file esterno di CRL e delle Certification Authority " trusted" .

- Funzioni su insiemi di documenti

  Sono disponibili le seguenti funzioni:

  a) Estrazione dei file PKCS#7 completi

  b) Verifica dell'integrità dei PKCS#7 con controllo di validità certificato di firma e marca temporale su file esterno di CRL e delle CA "trusted"

Torna all'indice

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

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

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

In merito alle procedure per la produzione di duplicati o copie di documenti, il Servizio di Intesa si attiene alle normative in merito, secondo quanto previsto dalle Regole tecniche in materia di formazione, trasmissione, conservazione, 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.

Per quanto riguarda il procedimento di generazione delle copie informatiche e delle copie per immagine su supporto informatico di documenti e scritture analogici rilevanti ai fini tributari, laddove il Cliente affidi il processo ad Intesa, questo viene eseguito in conformità a quanto previsto dal DMEF 17/06/2014 art. 4 comma 1.

Laddove si renda necessario per il processo di duplicazione/copia l'intervento del pubblico ufficiale, Intesa in base a quanto concordato con il Cliente, metterà a disposizione del medesimo un report in formato elettronico contenente gli indici dei documenti in attesa della sua firma e i relativi hash, per permettere, nella sua qualità di notaio, di certificare il processo di conformità attraverso le fasi successive.

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

- la visualizzazione e la selezione puntuale o massiva dei documenti elettronici
- le relative attività di verifica di conformità del documento elettronico rispetto al documento originale già a disposizione del pubblico ufficiale
- il download di documenti in locale, per permettere di procedere con la verifica di autenticità e integrità degli stessi attraverso l'uso di un verificatore di mercato prescelto, garantendo in questo modo la totale autonomia del processo di controllo e la massima garanzia di verifica.
- l'autorizzazione e l'attivazione del processo di firma digitale dei documenti proposti, attraverso uso di apposito certificato (intestato al pubblico ufficiale, rilasciato dalla CA Intesa con specifico limite d'uso a tal fine e custodito sugli HSM Intesa); a chiusura del processo verrà inoltre apposto il riferimento temporale
- la restituzione di apposito report in formato elettronico, a garanzia del completamento delle attività, con indicazione degli estremi dei documenti processati, tra cui indici identificativi, relativi hash dei documenti e data e ora di firma notarile. Ciò consentirà al pubblico ufficiale di fornire nel tempo la prova certa di quanto effettivamente certificato con la propria firma.

Nel caso di riversamento sostitutivo, con la necessità di intervento da parte del pubblico ufficiale, Intesa adotta un processo analogo a quello sopradescritto presentando al pubblico ufficiale i documenti da riversare.

Torna all'indice

7.8 Scarto dei pacchetti di archiviazione

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

Ad inizio anno e' schedulata una procedura che individua i dati che saranno oggetto di svecchiamento nell'arco dell'anno e provvede ad inoltrare comunicazione ai Clienti.

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

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

E' previsto l'invio di mail PEC, dove disponibile l'indirizzo, e di mail di posta ordinaria alla quale seguira' una raccomandata con ricevuta di ritorno che fa riferimento alla mail. Le ricevute di ritorno saranno conservate dal Gestore dei supporti presso il sito primario.

I dati verranno cancellati fisicamente dopo 3 mesi dalla ricevuta dell'ACK di avvenuta consegna delle mail PEC o dopo 6 mesi dall'invio delle mail ordinarie.

La cancellazione dei dati interessera' sia i documenti presenti su DB che quelli riversati in archivi presenti su NAS o su supporti ottici.

Qualora a fronte della mail di notifica il Cliente desideri mantenere ancora in vita i dati potra' notificarlo entro i 3 mesi dalla ricezione della medesima (6 in caso di invio di mail ordinaria) e si procedera' ad adeguare le condizioni contrattuali che regolano questo aspetto.

7.8.1 Chiusura del Servizio di Conservazione

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

In ipotesi di conclusione del Contratto o di recesso da parte del Cliente, o da parte di Intesa, in capo ad Intesa rimane l'obbligo della conservazione per il periodo richiesto dalle normative in relazione alla tipologia documentale conservata o in base a quanto diversamente concordato con il Cliente. Il Cliente potrebbe comunque richiedere la restituzione dei dati e la conseguente liberazione di Intesa dagli obblighi derivanti dall'art. 7 comma 1 del DPCM 03/12/2013.

In ipotesi di risoluzione del Contratto Intesa consegna i dati in suo possesso al Cliente, essendo liberata dall'obbligo di conservazione nonché dagli obblighi derivanti dall'art. 7 comma 1 del DPCM 03/12/2013.

In tutti i casi di restituzione dei dati questi vengono estratti in archivi logici all'interno dei quali sono presenti i pacchetti di archiviazione corredati dalle strutture dati standard (SInCRO, metadati custom e metadati minimi) la cui organizzazione è concordata con il Cliente.

Tali archivi vengono trasferiti su supporti di memorizzazione in base a quanto concordato con il Cliente per agevolare la successiva fruizione dei dati.

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

Torna all'indice

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

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

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

Il tema dell'interoperabilità, ossia la possibilità di interazione trasparente tra outsourcer di servizi in ambito di dematerializzazione, è sempre più presente sui tavoli di lavoro delle istituzioni cui Intesa partecipa in maniera proattiva.

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

- Utilizzo, per la conservazione dei documenti, di formati standard prescritti dalle normative in materia
- Adozione di formati di firma standard riconosciuti dagli Enti Certificatori in conformità alle specifiche PAdES-T, e CAdES-T, con applicazione della marca temporale
- La scelta adottata da Intesa di elaborare il singolo documento e non il lotto elimina completamente la necessità di costruire e gestire algoritmi proprietari, complessi ed articolati, necessari a trattare il documento sia nella fase di messa in conservazione sia nella delicata fase di esibizione verso le autorità competenti e in tutti i casi di controversia giudiziaria
- Il singolo documento viene così corredato di tutti gli attributi tecnico-normativi che facilitano qualsiasi operazione di portabilità o interoperabilità verso strutture esterne e si appoggia per l'abbinamento ai relativi indici a formati XML, attraverso l'applicazione dello standard SInCRO ampiamente riconosciuto per le proprie caratteristiche di interoperabilità.
- Ex Art.9, comma 1, lettera h (DPCM 3 Dicembre 2013), Intesa produce i pacchetti di archiviazione sempre coincidenti con i pacchetti di distribuzione.

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

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

Torna all'indice

8 Il sistema di conservazione

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

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

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

La piattaforma TrustedHub 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 TrustedHub è robusta e allo stesso tempo flessibile. Infatti si basa su middleware standard di mercato, affiancati da componenti proprietari per gestire, in modo snello e in autonomia, specificità come il tracking, l'administration, il workflow, la firma digitale, ecc.

I servizi erogati da Intesa e le relative infrastrutture sono ospitate presso le Server farm IBM 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 per gestire eventuali incrementi di volumi.

Attraverso l'utilizzo di adeguati storage l'infrastruttura è specificatamente progettata per applicazioni data-intensive con tecnologia a 4 Gbps, con cui si raggiungono elevate prestazioni di alta affidabilità.

Torna all'indice

8.1 Componenti Logiche

Di seguito lo schema delle componenti logiche specifiche del sistema di conservazione:

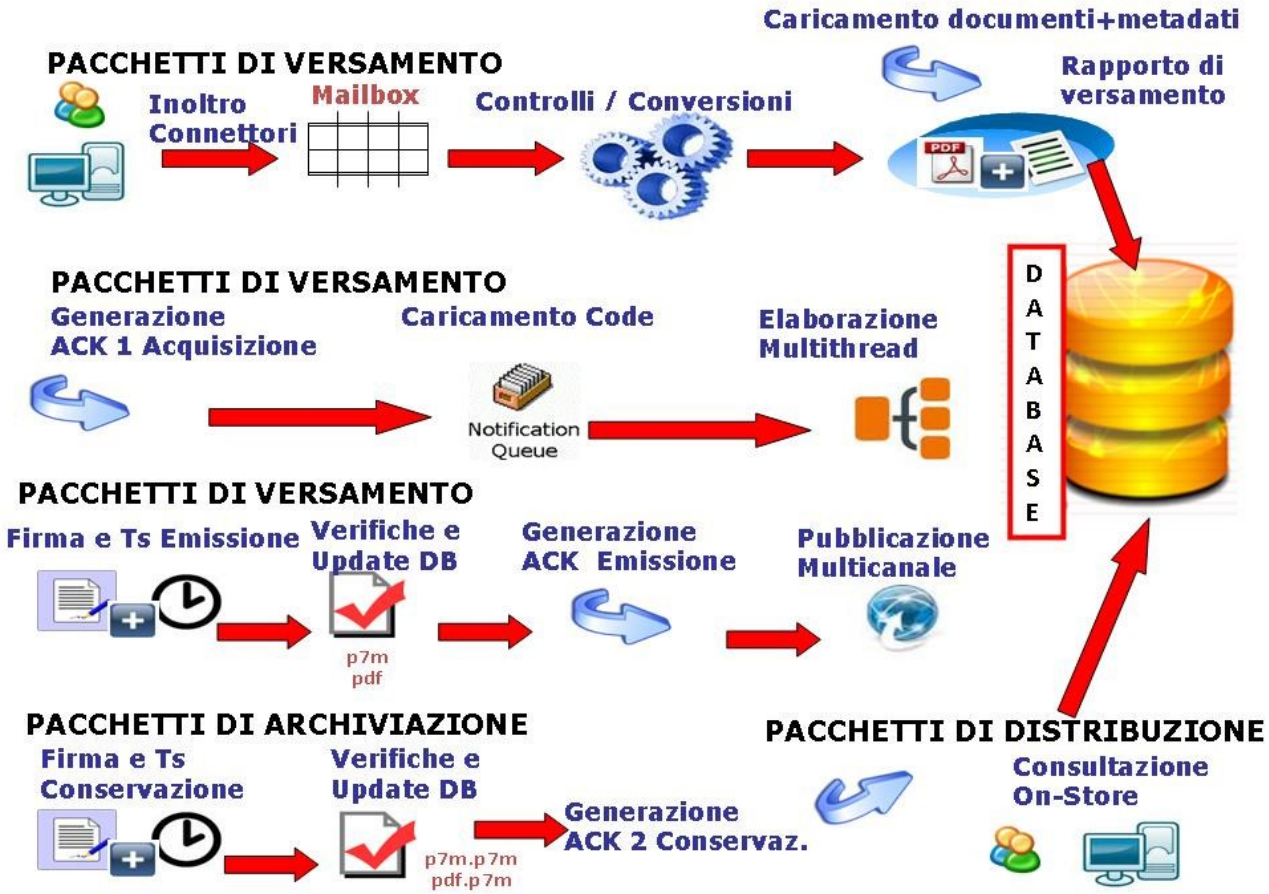

Figura 2: Schema delle componenti logiche

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

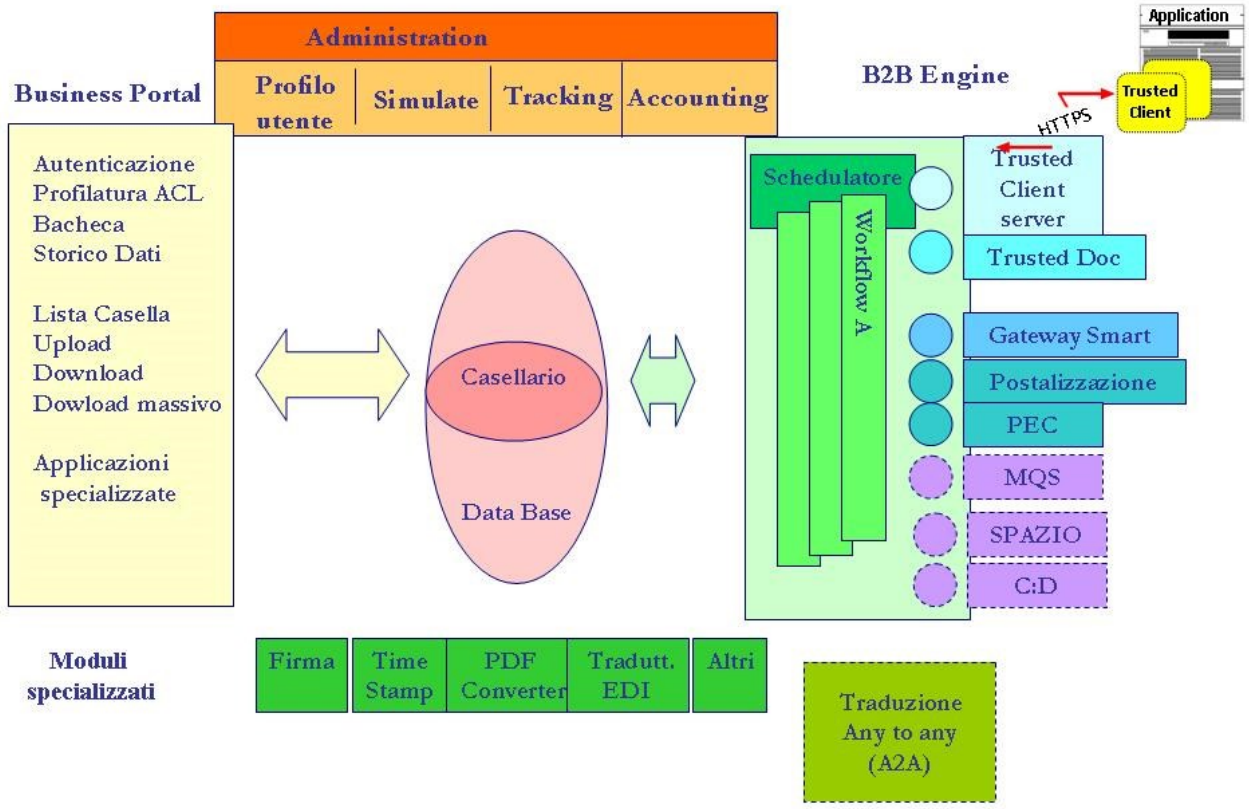

Figura 3: Schema delle componenti logiche

Per un maggiore dettaglio delle entità funzionali relative al sistema di conservazione e al suo funzionamento si rimanda all' Appendice B – Componenti tecnologiche, che data la riservatezza dei dati contenuti è allegata separatamente al presente Manuale, consegnata all'Agenzia perItalia Digitale in fase di accreditamento e successivi aggiornamenti e fornita al Cliente.

Torna all'indice

8.2 Componenti Tecnologiche

Per un maggiore dettaglio delle componenti tecnologiche che implementano il sistema di conservazione si rimanda all' Appendice B – Componenti tecnologiche, che data la riservatezza dei dati contenuti è allegata separatamente al presente Manuale, consegnata all'Agenzia per l'Italia Digitale in fase di accreditamento e successivi aggiornamenti e fornita al Cliente.

Torna all'indice

8.3 Componenti Fisiche

Per la descrizione delle componenti fisiche, dei siti di conservazione e delle connessione tra i diversi siti si rimanda all' Appendice B – Componenti tecnologiche, che data la riservatezza dei dati contenuti è allegata separatamente al presente Manuale, consegnata all'Agenzia per l'Italia Digitale in fase di accreditamento e successivi aggiornamenti e fornita al Cliente.

Torna all'indice

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 della 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 dell'area del Delivery 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 prevede la presenza di specifici "Responsabili di Manutenzione" dedicati a ciascuna delle aree di riferimento delle diverse linee di business.

In questo modo è possibile rispondere con efficienza crescente alle richieste di intervento dei Clienti, potendo far leva sulla acquisizione continua di esperienze sullo specifico prodotto servizio.

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

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

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

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

Torna all'indice

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 Regole tecniche di conservazione del CAD, Art. 12, comma 2, 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
- dalle policies del Gruppo IBM, presso il cui data center è presente la Server Farm di Intesa
- dalla certificazione ISO 27001:2006 del data center
- dalla certificazione ISO 27001:2013 per gli scope specifici: servizi di generazione/emissione di documenti elettronici, archiviazione digitale e conservazione sostituiva a norma e produzione di soluzioni di firma elettronica, firma elettronica avanzata, firma elettronica qualificata, posta elettronica certificata
- dal Codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196.

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

- sicurezza fisica e logica infrastrutturale;
- sicurezza logica applicativa;
- continuità

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

- Proteggere la trasmissione di informazioni contro perdite di dati, rivelazione o modifiche non autorizzate.
- Consentire l'accesso ai sistemi di erogazione solo a chi ne ha necessità (in relazione alle specifiche responsabilità) e disporre le conseguenti autorizzazioni.

- Condurre verifiche appropriate per garantire che i meccanismi di controllo funzionino effettivamente.

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

- amministrazione della sicurezza
- protezione degli ambienti di erogazione
- identificazione ed autenticazione degli utenti
- autorizzazioni all'accesso alle informazioni a diversi livelli

e si sviluppano nelle seguenti direzioni:

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

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

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

Torna all'indice

8.4.3 Gestione e conservazione dei log

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

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

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

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

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

- ACK 1: esecuzione del workflow interno inerenti il trattamento dei documenti e relativa pubblicazione Web (accettazione dei pacchetti di versamento)

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

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

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

Torna all'indice

8.4.4 Change management

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

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

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

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

Torna all'indice

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 dagli articoli 7 e 9 del DPCM 3/12/2013, con riferimento agli obblighi del Responsabile della conservazione e alle fasi del processo di conservazione.

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

Torna all'indice

9 Monitoraggio e controlli

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

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

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

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

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

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

Torna all'indice

9.1 Procedure di monitoraggio

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

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

- System Activity: Modulo web nell'ambito delle componenti del Servizio di Administration, ad uso interno da parte dei profili Administrator identificati all'interno di Intesa, in ambiente Websphere. Tale componente consente di verificare la corretta elaborazione dei flussi (richieste di servizio) inviati dal Cliente e in caso di anomalie di poter visionare la descrizione dell'errore per le necessarie azioni correttive.
- SysMonitor: insieme di procedure implementate su database interno attraverso linguaggio di programmazione, costituito da query specifiche schedulate in modo automatico che consentono di effettuare controlli applicativi (es. Elaborazione flussi, controllo periodicità flussi, controllo pacchetti di versamento, controllo pacchetti in attesa di archiviazione)
- Workflow specifici di controllo: procedure applicative eseguite contestualmente all'elaborazione dei pacchetti di versamento, sviluppate con personalizzazioni in relazione alla tipologia di flusso inviato e in base ad esigenze specifiche del Cliente.

- Check buchi: procedura di controllo sequenzialità su regole concordate con il Cliente
- NAGIOS: plugin di monitoraggio a tre livelli (sistemistico applicativo, di business) di seguito descritto

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

- Il controllo costante dei livelli di servizio, attraverso il monitoraggio dell'ambiente e degli elementi critici, compresa anche l'avvenuta esecuzione di attività gestionali, quali ad esempio la verifica dello spazio disponibile, il mancato superamento dei livelli di soglia e la simulazione di log-on per il controllo di availability dei servizi. I parametri più critici, nonché il loro andamento temporale, sono periodicamente consuntivati in un "Cruscotto" e riesaminati nell'ambito di riunioni periodiche di Direzione.
- Il monitoraggio dell'andamento del Servizio, la predisposizione o verifica di collaudi e di salvataggi periodici di dati o librerie e l'eventuale predisposizione di dati di input e verifica dei risultati.
- La gestione delle modifiche a parametri del Servizio (es. Abilitazioni utenze, Password, ecc.), in modo da poterlo adeguare velocemente alle mutate esigenze del Cliente.
- La gestione della sicurezza e degli accessi ai servizi, per evitare intrusioni e ingressi non autorizzati. La sicurezza è articolata su diversi livelli (di Rete, di Sistema, di Servizio Applicativo), supportata da appropriate ed avanzate soluzioni tecnologiche e gestita da appositi Ruoli aziendali, che effettuano attività di monitoraggio continuo e verifiche periodiche sulla completezza e validità delle soluzioni adottate (es. penetration tests).
- L'effettuazione controllata di ogni variazione agli ambienti operativi (HW, SW ecc.). Ogni richiesta di "Change" deve essere documentata, motivata, analizzata ed autorizzata. Una severa e preventiva analisi di impatto, da parte delle persone più qualificate, un'effettuazione concentrata in apposite "Finestre" temporali collocate in periodi di basso utilizzo ed un esaustivo collaudo, volto particolarmente a verificare la compatibilità retrograda, tendono a minimizzare i rischi di interruzioni del servizio.
- Il mantenimento e l'aggiornamento continuo delle configurazioni HW e SW relative ad ogni ambiente gestito. Tale controllo permette di identificare (anche storicamente) le componenti tecnologiche coinvolte nell'erogazione di ogni servizio, per meglio programmare eventuali attività di modifica e di ripristino.
- La gestione ottimale delle interruzioni di servizio, siano esse programmate o impreviste. Particolari attività di progettazione sono effettuate per circoscrivere e limitare l'impatto di possibili malfunzioni e per attivare automaticamente o tempestivamente soluzioni alternative (es. routing, switch ecc.).
- La ripresa delle attività in caso di problemi. Appropriate ed automatizzate attività di salvataggio di Ambienti, Librerie, Applicazioni e Dati, permettono un regolamentato ripristino (totale, settoriale o parziale) delle risorse, per una ripartenza tempestiva del/dei Servizi interrotti.
- Il mantenimento di un'elevata disponibilità ed affidabilità dei singoli componenti tecnologici, tramite specifici contratti di manutenzione programmata. Interventi finalizzati alla prevenzione di possibili problemi HW sono svolti periodicamente da personale esperto.
- Il mantenimento di un ambiente di lavoro appropriato per le attività da eseguire.

Torna all'indice

9.1.1 Sistema di monitoraggio sistemistico e applicativo NAGIOS

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

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

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

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

Il sistema consente un monitoraggio articolato su tre diversi livelli:

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

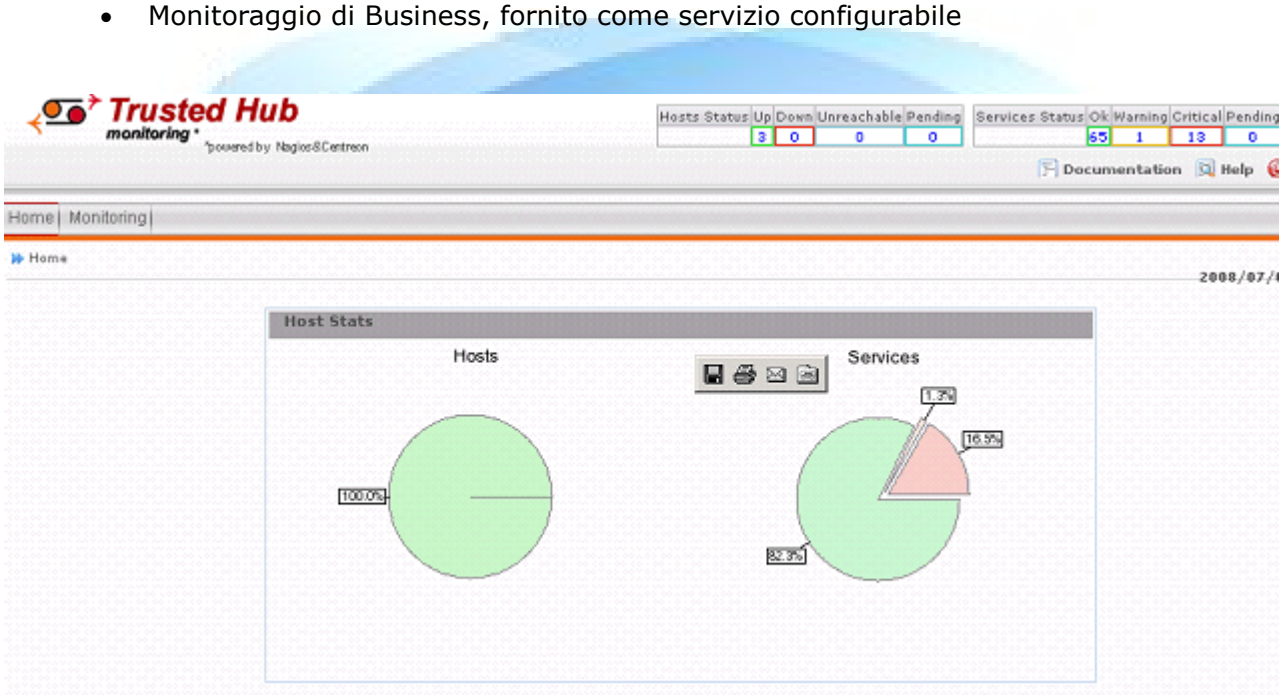

Figura 4: Schermata del cruscotto del sistema di monitoraggio

A scopo esemplificativo, nella figura precedente sono presenti due diagrammi a torta: il primo rappresenta un riepilogo dello stato dei server fisici, il secondo mostra un riepilogo dello stato dei servizi attestati su ciascun server.

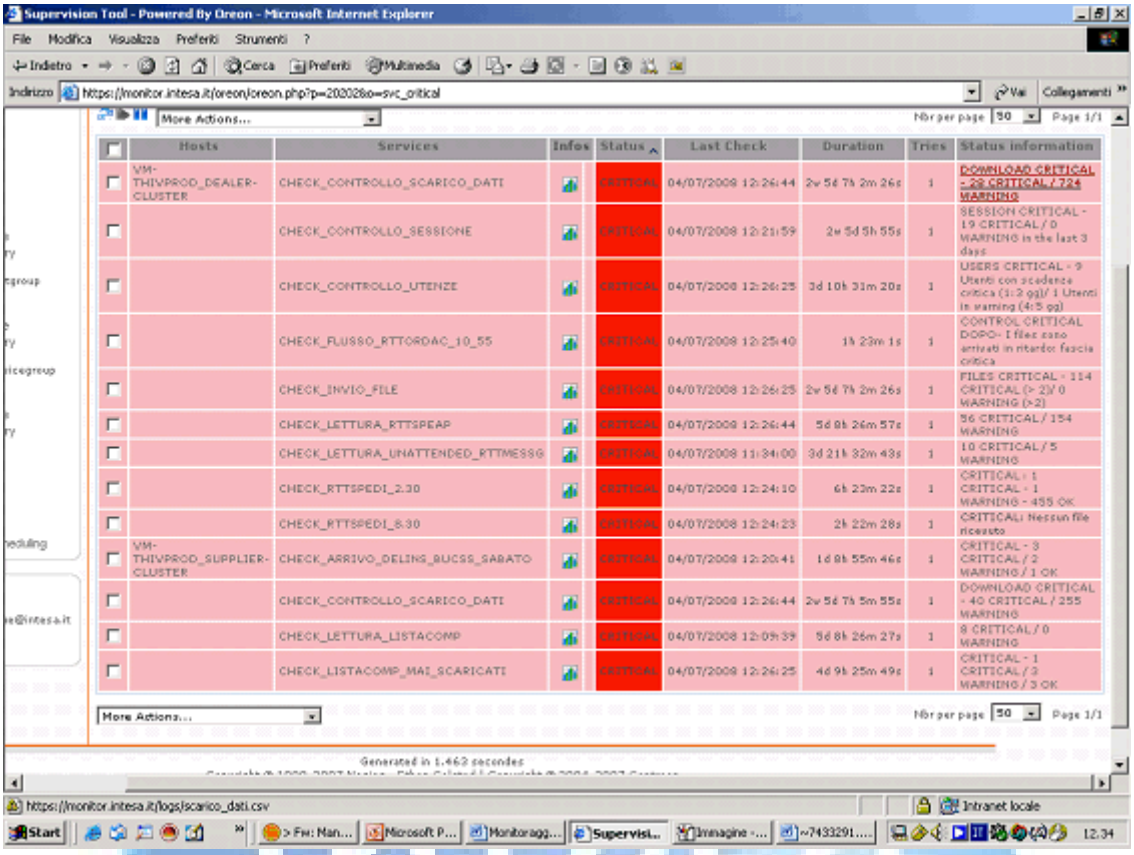

Figura 5: Finestra di Monitoring che evidenzia lo stato dei servizi

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

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

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

- Dischi fisici
- Webspere/Application Server
- Accesso Https
- Database

[Torna all'indice]

9.2 Verifica dell'integrità degli archivi

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

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

Intesa verifica, con cadenza non superiore a 36 mesi (ovvero in base a specifiche cadenze eventualmente pattuite in sede contrattuale e indicate nell'Appendice A), lo stato di conservazione dei pacchetti di archiviazione, provvedendo, se necessario, al riversamento in base a quanto prescritto dall'Art. 7 comma g delle Regole Tecniche.

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

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

- esibilità (leggibilità a campione, verificabilità)
- verifica della firma digitale e marca temporale
- correttezza e coerenza con i metadati

Il processo di collaudo viene effettuato in modalità automatica, fornisce return code precisi in caso di anomalia e prevede il controllo dell'integrità documenti, la verifica della firma e timestamp di una % prescelta sul totale dei pacchetti di archiviazione relativi ad una specifica tipologia documentale oggetto di collaudo.
L'esito della conclusione delle operazioni e della verifica sono riportate in un'apposita sezione su repository aziendale.

Torna all'indice

9.2.1 Dettaglio delle procedure periodiche di controllo degli archivi

Il responsabile del procedimento di conservazione, attraverso le figure preposte alla gestione degli archivi (di seguito anche "gestore degli archivi") presso il sito primario, effettua (tramite la funzionalità applicativa di seguito descritta) i collaudi evidenziati dall'apposita vista su tool interno Lotus Notes denominato "Trace Archivi". Le scadenze vengono automaticamente rilevate e segnalate sulla base delle impostazioni definite nell'ambito del tool "Trace Archivi", che mette in evidenza tutte le attività da evadere nel semestre in corso.

I collaudi vengono pianificati con cadenza non inferiore a tre anni e riguardano tutti gli archivi memorizzati presso il sito primario e quindi replicati in mirroring.

Il collaudo avviene tramite funzionalità automatica (richiamata attraverso il modulo applicativo TrustedDoc–Viewer) che rilascia un log contenente l'esito della verifica effettuata.

Per ogni archivio/supporto da collaudare, il gestore degli archivi presso il sito primario avvia la verifica dell'integrità attraverso l'utilizzo delle apposite funzionalità messe a disposizione dal Viewer (programma che consente la navigazione all'interno dell'archivio) (system/process control point, procedura interna CI00165).

- Dettaglio delle verifiche

a) Verifica di bilanciamento numero documenti (verifica tra il numero di file effettivi presenti all'interno dell'archivio e il numero degli indici riportato in un apposito file di controllo presente all'interno della struttura dati dell'archivio)

b) Verifica della dimensione dell'archivio/supporto (verifica della dimensione effettiva e di quanto riportato in un apposito file di controllo presente all'interno della struttura dati dell'archivio)

c) Controllo dell'integrità documenti (verifica dell'hash, della firma e timestamp di tutti o di una % prescelta sul totale dei documenti presenti all'interno dell'archivio)

- **Se esito positivo**
  - Visualizza a video che la verifica ha avuto esito positivo
- **Se esito negativo**
  - Visualizza a video che la verifica ha avuto esito negativo

Tutte le attività di verifica vengono indicate in un apposito file di log da utilizzare come traccia generale delle attività svolte.

Il gestore degli archivi presso il sito primario effettua inoltre un'ulteriore attività di verifica per accertare la leggibilità dell'archivio/supporto e la navigabilità.
Seleziona a campione alcuni documenti contenuti all'interno dell'archivio, procede alla visualizzazione del file originale accertando la corrispondenza tra i dati indice riportati dal viewer e quanto effettivamente presente all'interno del documento stesso.

Aggiorna la scheda sul tool "*Trace Archivi*" con data e esito del collaudo, allegando log ed eventuale ulteriore documentazione.

In caso di collaudo negativo si procede con il riversamento diretto dei dati utilizzando la copia di sicurezza, leggibile sull'ulteriore NAS.

Intesa verifica lo stato di conservazione dei pacchetti di archiviazione, provvedendo, se necessario:

- al riversamento diretto dei dati utilizzando il backup (mirroring) presente sulla struttura NAS ridondata, in caso di anomalie riscontrate durante il collaudo
- alla produzione delle copie informatiche al fine di adeguare i formati in conformità a quanto previsto dall'art. 11 delle Regole Tecniche e relativo Allegato 2, nel caso di evoluzione del contesto tecnologico e/o obsolescenza dei formati utilizzati.

Procede con la rimozione dei dati in modalità sicura o con la distruzione del supporto fisico di memorizzazione (CD/DVD) non più utilizzabile.
Inserisce da DB Lotus Notes "*Trace Archivi*" una nuova scheda archivio indicando nelle note la motivazione della creazione di un nuovo archivio.

Torna all'indice

9.3 Soluzioni adottate in caso di anomalie

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

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

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

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

Qualora dalle attività di monitoraggio sopra indicate, supportate da appositi meccanismi automatici, vengano evidenziati eventuali problemi o il rischio di un loro accadimento, sono tempestivamente intraprese le azioni correttive opportune per evitare il deterioramento del servizio. Di tali eventi, in aggiunta alla loro risoluzione, viene tenuta adeguata traccia, tramite tool a supporto delle registrazioni (vedi in particolare "System Activity", "Schede di Manutenzione Sw" e "Conservazione a Norma – Trace Archivi") e viene fatta un'analisi allo scopo di aggiornare, se necessario, le misure di sicurezza in atto.

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

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

1. **Help desk di 1° livello:**

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

I compiti principali della struttura di Help Desk sono:

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

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

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

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

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

2. **Supporto di secondo livello:**

E' 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:**

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 il processo di conservazione, nelle comunicazioni inerenti la gestione operativa del Servizio TrustedDoc, svolgendo le sue funzioni in stretta collaborazione con il Capo Progetto e con le figure specialistiche di Intesa con competenze tecnico-normative.

Torna all'indice

Firmato da:
Luca Altieri
Codice fiscale: LTRLCU70P02F704T
Valido da: 16-04-2014 9:34:00 AM a: 16-04-2017 10:03:20 AM
Certificato emesso da: IN.TE.S.A. Certification Authority, IN.TE.S.A. S.p.A., IT
Motivo: Approvo il documento