

Manuale del Responsabile della Conservazione

In.Te.S.A. SpA

Tipo Documento	Manuale del Responsabile della Conservazione
Società	<Cliente>
Redazione	In.Te.S.A. S.p.A.
Verifica e Approvazione	Agenzia per l'Italia Digitale Responsabile della Conservazione
Data emissione	26/09/2014

	MANUALE RDC	MRDC_V26092014
---	----------------	----------------

REVISIONI

Revisione n°	Prima emissione	Data Revisione:	gg/mm/aaaa
Descrizione modifiche:	Prima emissione		
Motivazioni:	-		

Revisione n°	Seconda emissione	Data Revisione:	gg/mm/aaaa
Descrizione modifiche:		
Motivazioni:		

INDICE

1	Premessa	4
1.1	Scopo del Manuale	4
1.2	Contesto di riferimento	5
1.2.1	Processo di delega del Responsabile della Conservazione	5
1.2.2	Riferimenti a documentazione di dettaglio	5
1.3	Normativa e prassi di riferimento	5
1.4	Definizioni	6
1.5	Convenzioni di lettura e acronimi	10
2	Ruoli e responsabilità	12
2.1	Dettaglio dei ruoli e relativi compiti	13
2.1.1	Responsabile della Conservazione e suo delegato	13
2.1.2	Responsabile del Servizio di Conservazione	15
2.1.3	Responsabile della funzione archivistica di conservazione	15
2.1.4	Responsabile del Procedimento di Conservazione	15
2.1.5	Responsabile dei sistemi informativi per la conservazione	15
2.1.6	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	16
2.1.7	Responsabile della sicurezza dei sistemi per la conservazione	16
2.1.8	Responsabile del Trattamento dei dati personali	16
2.1.9	Responsabili del Cliente: "Process Owner" e "Referente IT"	17
3	Il processo di conservazione	19
3.1	Invio dei documenti alla piattaforma Intesa	20
3.2	Sistema/interfaccia di versamento	20
3.2.1	Indici e formati	21
3.2.2	Controlli del sistema di versamento e gestione eccezioni	22
3.2.3	Rapporto di versamento	22
3.3	Sistema di conservazione	23
3.3.1	Generazione dell'Indice del pacchetto di Archiviazione (IpdA) e metadati minimi	23
3.3.2	Apposizione della firma digitale e marca temporale	24
3.4	Modalità di consultazione ed esibizione documenti conservati – pacchetti di distribuzione	24
3.4.1	Modalità via portale web	25
3.4.2	Modalità attraverso supporti di memorizzazione autoconsistenti (se richiesto)	25
3.5	Mantenimento dei dati conservati a norma	26
3.5.1	Collaudo periodico dei documenti conservati	27
3.5.2	Procedure per la produzione di duplicati o copie	27
3.5.3	Distruzione/restituzione dei documenti conservati elettronicamente	28
3.6	Portabilità dei dati conservati	28
3.6.1	Interoperabilità	28
3.7	Monitoraggio del sistema di conservazione	29
3.7.1	Sistema di monitoraggio sistemistico e applicativo	29
4	Sicurezza del sistema di conservazione	30

	MANUALE RDC	MRDC_V26092014
---	----------------	----------------

1 Premessa

1.1 Scopo del Manuale

Il Manuale di Conservazione è lo strumento 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 <.....> (di seguito anche <.....>).

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).

Il presente Manuale è prodotto in formato digitale da parte di Intesa in collaborazione con il Cliente, pubblicato in apposito repository del Servizio ad uso interno Intesa e fornito al Cliente.

Nel caso di eventuali aggiornamenti e adeguamenti, da entrambe le parti, viene inviata copia al Responsabile di progetto del Cliente o Intesa.

La redazione e gestione del Manuale della Conservazione costituisce 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.

	<p style="text-align: center;">MANUALE RDC</p>	<p style="text-align: center;">MRDC_V26092014</p>
---	--	---

1.2 Contesto 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 Cliente ha scelto di delegare il ruolo di Responsabile della Conservazione ad una figura esterna rispetto al gruppo stesso incaricando Intesa, accettando quindi la candidatura presentata da Intesa stessa attraverso la propria soluzione proposta in sede di formulazione dell'offerta.

In Appendice A è delineato il processo che viene seguito per la delega del Responsabile della Conservazione da parte del Cliente.

1.2.1 Processo di delega del Responsabile della Conservazione

Il processo operativo di delega del Responsabile della Conservazione è riportato in Appendice A.

1.2.2 Riferimenti a documentazione di dettaglio

Nel presente documento sono parzialmente descritti aspetti architeturali e processi in essere.

Per un maggior dettaglio tecnico/funzionale si rimanda ai seguenti documenti:

- Appendice A al Manuale del RDC – Documento di dettaglio del processo (riferimenti normativi, ruoli, descrizione del processo, tabelle tecniche dei documenti e pacchetti informativi)
- Appendice B al Manuale del RDC – Documento di 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 al Piano della Sicurezza del sistema di conservazione.
- Documento di Analisi funzionale, per gli aspetti attinenti le implementazioni tecniche della Conservazione a Norma, non allegato al presente Manuale del RDC, predisposto sulla base dello specifico contesto progettuale del Cliente.

1.3 Normativa e prassi 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.

	<p style="text-align: center;">MANUALE RDC</p>	<p style="text-align: center;">MRDC_V26092014</p>
---	--	---

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 indicati nell'Appendice A al presente manuale.

1.4 Definizioni

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 di conservazione
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

	<p style="text-align: center;">MANUALE RDC</p>	<p style="text-align: center;">MRDC_V26092014</p>
---	--	---

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

	<p style="text-align: center;">MANUALE RDC</p>	<p style="text-align: center;">MRDC_V26092014</p>
---	--	---

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

	<p style="text-align: center;">MANUALE RDC</p>	<p style="text-align: center;">MRDC_V26092014</p>
---	--	---

<p>sistema di conservazione</p>	<p>sistema di conservazione dei documenti informatici di cui all'articolo 44 del Codice</p>
<p>staticità</p>	<p>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</p>
<p>utente</p>	<p>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</p>

1.5 Convenzioni di lettura e acronimi

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
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 delega per l'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 linguaggio 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

2 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."

"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 Responsabile delegato del processo di Conservazione dal Cliente, assumendo tutti i compiti e le funzioni previste dalla normativa per il ruolo di RDC.

Come già precisato dalla Risoluzione dell'Agenzia delle Entrate del 13 agosto 2009 n. 220, anche l' articolo 5, comma 2, della delibera CNIPA, riferendosi genericamente alle "persone", ammetteva la possibilità di delegare la responsabilità del procedimento di conservazione anche a soggetti diversi dalle persone fisiche:

Cit.: "Pertanto, si ritiene che l'istante possa delegare il servizio di conservazione sostitutiva dei documenti rilevanti ai fini tributari ad uno o più operatori, sia persone fisiche che persone giuridiche."

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

specificata lettera, delega Intesa ad effettuare il procedimento di conservazione elettronica a norma di legge (Art. 6 comma 6 e 7 delle Regole Tecniche), attribuendo alla stessa i compiti del Responsabile della conservazione (definiti nel primo comma Art. 6 della Regole Tecniche).

I dati identificativi del Responsabile della conservazione sono riportati in Appendice A, a seguito del processo indicato Intesa è delegata dal Responsabile della Conservazione del Cliente.

2.1 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 delegato dal RCN sono definite nella Lettera di Delega 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 Appendice A.

2.1.1 Responsabile della Conservazione e suo delegato

Il DPCM 3 dicembre 2013 attribuisce al responsabile della conservazione (o suo delegato, 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) predispose 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 risulta determinante 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 pubblico ufficiale, spetta al responsabile della conservazione (o suo delegato) definire le opportune modalità di richiesta d'intervento in base alle specifiche esigenze del Cliente concordando con quest'ultimo 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)

- riporta in Appendice A il dettaglio delle casistiche che richiedono la presenza del pubblico ufficiale se previste nell'ambito della tipologia documentale trattato o dello specifico processo definito in accordo con il Cliente;
- predispone il Manuale della Conservazione, in collaborazione con il Cliente, descrivendo anche i dettagli specifici del progetto.

2.1.2 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.

2.1.3 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.

2.1.4 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.

2.1.5 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 di 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.

2.1.6 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.

2.1.7 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.

2.1.8 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.

2.1.9 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 sovrintende 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.

3 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*.

3.1 Invio dei documenti alla piattaforma Intesa

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)

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.

3.2 Sistema/interfaccia di versamento

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.

In fase di setup del servizio vengono definite le specifiche del pacchetto di versamento e del relativo indice 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.

3.2.1 Indici e formati

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.

3.2.2 Controlli del sistema di versamento e gestione eccezioni

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

- Controlli di conformità:
 - Formato dei documenti
 - Presenza dei MetaDati previsti
 - Presenza di tutte le informazioni definite per le specifiche categorie documentali obbligatorie
 - Integrità del Pacchetto di Versamento
- 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.

Il mancato superamento dei controlli bloccanti genera la segnalazione della situazione errata al referente del Cliente al fine di concordare la migliore modalità per il completamento del processo. Il processo di controllo è caratterizzato dunque da:

- segnalazione certa dell'errore con rifiuto del documento
- invio della segnalazione con relativa motivazione (rapporto di anomalia) in modalità sincrona e/o via email al referente aziendale del Cliente
- gestione attraverso contatto 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.

3.2.3 Rapporto di versamento

Al termine della fase di acquisizione, preparazione del pacchetto di versamento e di controllo, viene generato un rapporto di versamento, identificato univocamente, che 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).

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 Servizio prevede la creazione di un rapporto di versamento per ogni flusso inviato dal Cliente contenente quindi molteplici pacchetti di versamento (file in formato .csv , quindi campi con delimitatori e lunghezza variabile), il rapporto di versamento è sottoscritto con firma elettronica qualificata del responsabile del procedimento di conservazione di Intesa.

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.

3.3 Sistema di conservazione

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.

3.3.1 Generazione dell'Indice del pacchetto di Archiviazione (IpDA) e metadati minimi

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 conservato è quindi 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 in 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 prevede inoltre un'ulteriore sezione "MoreInfo" che consente di introdurre i metadati soggettivi (indici "custom" specifici, derivanti dalla particolare classe documentale cui l'indice si riferisce) definiti da Intesa in accordo con il Cliente e i metadati minimi richiesti dalla normativa, indicati nell'Allegato 4 (Specifiche tecniche del Pacchetto di Archiviazione) delle Regole Tecniche in materia di conservazione.

L'Indice del Pacchetto di Archiviazione viene firmato digitalmente attraverso lo standard CADES.

3.3.2 Apposizione della firma digitale e marca temporale

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.

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 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.

3.4 Modalità di consultazione ed esibizione documenti conservati – pacchetti 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). 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.

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).

3.4.1 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 effettuare 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 archiviazione caratterizzati da più livelli di firma relativi ai processi di firma per generazione/emissione/ tenuta elettronica dei documenti, da parte del Cliente precedenti al processo di versamento e conservazione.

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.

3.4.2 Modalità attraverso supporti di memorizzazione autoconsistenti (se richiesto)

I pacchetti di distribuzione possono essere consultati anche attraverso l'utilizzo di supporti di memorizzazione auto consistenti.

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.

La consultazione dei documenti 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"

3.5 Mantenimento dei dati conservati a norma

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

3.5.1 Collaudo periodico dei documenti conservati

Intesa verifica, con cadenza non superiore a 36 mesi, 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 su un significativo numero di documenti.

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

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

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.

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.

3.5.2 Procedure per la produzione di duplicati o copie

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.

3.5.3 Distruzione/restituzione dei documenti conservati elettronicamente

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

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.

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.

3.6 Portabilità dei dati conservati

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.

3.6.1 Interoperabilità

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.

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.

3.7 Monitoraggio del sistema di conservazione

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.

3.7.1 Sistema di monitoraggio sistemistico e applicativo

Il sistema di monitoraggio è configurato in cluster (2 server fisici) 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 schedato in modo autonomo, permettendo un controllo più o meno frequente in base alle necessità dello specifico oggetto/funzione da monitorare.

Il sistema consente un monitoraggio articolato su tre diversi livelli:

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

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

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

4 Sicurezza del sistema di conservazione

Il Servizio è erogato su un'infrastruttura proprietaria di Intesa, logicamente e fisicamente isolata, descritta in Appendice B.

La trasmissione di dati in input e output al sistema di conservazione avviene in modalità protetta tramite protocolli di comunicazione crittografati in base a quanto concordato con il Cliente.

La soluzione 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 27001:2005 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.

In merito alla disponibilità del Servizio, l'architettura adottata prevede l'impiego di accorgimenti volti a minimizzare il rischio di indisponibilità e/o la durata della non disponibilità stessa.

Inoltre il Servizio è sottoposto a costanti rilevazioni di parametri critici che consentono di prevenire situazioni di deterioramento delle prestazioni.

Qualora si verifichi un problema bloccante, è prevista l'analisi della situazione e la determinazione della migliore soluzione.

Da un punto di vista operativo sono previsti e posti in essere, parallelamente ai processi attinenti l'erogazione dei servizi, processi volti a misurare alcuni parametri allo scopo di rilevare tempestivamente eventuali scostamenti e/o deterioramenti.

Il monitoraggio dell'ambiente e di specifici parametri fornisce elementi di valutazione alle figure sistemistiche, al Responsabile della Sicurezza e al Responsabile dello sviluppo e manutenzione, per intraprendere azioni preventive o correttive rispetto alle soluzioni adottate in occasione di eventi critici.

Nell'erogazione del servizio Intesa effettua l'analisi dei rischi sul proprio sistema di conservazione, con riferimento sia alle componenti organizzative che infrastrutturali, includendo anche gli aspetti relativi al coinvolgimento di enti esterni (fornitori/outsourcers), come riportato nel documento "Piano della sicurezza", parte integrante della documentazione fornita alle autorità competenti ai fini dell'accreditamento.

Le autorizzazioni di accesso ai sistemi di conservazione sono assegnate secondo il principio del minimo privilegio e della separazione dei compiti e verificate periodicamente. Ad ogni persona autorizzata è inoltre assegnata un'utenza personale e univoca. Le utenze di gruppo sono ammesse solo per specifiche eccezioni espressamente autorizzate.

Per quanto riguarda le procedure di sicurezza relative alla gestione dei pacchetti di archiviazione, questi sono memorizzati da Intesa su supporti di memorizzazione distinti in storage di massa ad alta affidabilità (NAS). I pacchetti di archiviazione sono soggetti 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 materia di documentazione fiscale, civilistica e di altra natura e comunque in base agli accordi tra il Cliente ed Intesa.

Le caratteristiche della piattaforma di Servizio, i criteri adottati per la gestione sicura dello storage e per il recovery della piattaforma, che permettono di rispondere ai requisiti di sicurezza del sistema di conservazione sono descritti in Appendice B.