Manuale di Conservazione

di Santer Reply S.p.A.

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	06/10/2014	Critelli Marika - Michele Gentili	Analista Conservazione - RSC
Verifica	02/03/2015	Michele Gentili	RSC
Approvazione	02/03/2015	Marco Pronzato	Rappresentante Legale

SECONDA EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	18/04/2017	Critelli Marika	Analista Conservazione
Verifica	02/05/2017	Giovanni Patella	BU Manager
Approvazione	02/05/2017	Laura Cerchio	Rappresentante Legale

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
1.0	02/03/2015	Definitivo	Approvato
1.1	02/05/2017	Variazione Organigramma, Ruoli e Responsabilità, Rappresentante Legale	Approvato

INDICE DEL DOCUMENTO

INDICE DELLE FIGURE

1 SCOPO E AMBITO DEL DOCUMENTO

Questo documento rappresenta una descrizione organica dei fondamenti giuridici e dei processi operativi su cui è basata l'attività di Conservazione di documenti informatici di Santer Reply S.p.A.

Al fine di consentire una più agevole ed efficace manutenzione della documentazione il documento è strutturato con diversi allegati:

- Specificità del contratto
- Allegato Tecnico
- Documenti di delega

Obiettivo della stesura del presente manuale e dei relativi allegati, comprese gli eventuali aggiornamenti evolutivi, è quello di fornire sempre un punto di riferimento univoco sull'intero sistema di conservazione, sia dal lato organizzativo e di processo che da quello tecnico a supporto.

La sua lettura dovrà restituire in ogni momento una fotografia sul reale stato del sistema, per far si che gli operatori coinvolti nel processo, possano comprendere le logiche e i flussi implementati per garantire l'adempimento di quanto previsto dalla normativa vigente in materia di conservazione.

Torna al Sommario

2 TERMINOLOGIA (GLOSSARIO E ACRONIMI)

Glossario dei termini e Acronimi	
AgID	Agenzia per l'Italia Digitale
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.
CAdES	CMS Advanced Electronic Signatures
Copia di Sicurezza	Copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 delle regole tecniche allegate al DPCM 03/12/2013 per i sistemi di conservazione.
Copia analogica del documento informatico	Documento analogico avente contenuto identico a quello del documento informatico da cui è tratto
Codice	Insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici
CA	Certification Authority
Documento Informatico	Rappresentazione informatica di un atto, fatto o dati giudicamene rilevanti.
Destinatario	Identifica il soggetto/sistema al quale il documento informatico è indirizzato
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; può essere identificato tramite l'estensione del file o tramite un attributo definito "mime-type"
FTP server	programma che permette di accettare connessioni in entrata e di comunicare con un Client attraverso il protocollo FTP
Funzione di Hash	Funzione matematica che genera, a partire da una evidenza informatica, un'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.
Firma Digitale	Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.
Firma Elettronica Avanzata	Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati (art. 1 comma 1 lettera q-bis) Decreto Legislativo del 7 marzo 2005 n. 82)
Integrità	Insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato.
***IdP*:**	strumento per rilasciare le informazioni di identificazione di tutti i soggetti che cercano di interagire con un Sistema; ciò si ottiene tramite un modulo di autenticazione che verifica un token di sicurezza come alternativa all'autenticazione esplicita di un utente all'interno di un ambito di sicurezza.
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 univoca.
Insieme minimo di metadati del documento informatico	Complesso dei metadati, la cui struttura è descritta nell'allegato 5 del D.P.C.M. 3 dicembre 2013, da associare al documento

	informatico per identificarne provenienza e natura e per garantirne la tenuta
Impronta	Sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione ad un'evidenza informatica di una funzione di hash.
Interoperabilità	Capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi
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
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.
Marca Temporale	Riferimento temporale che consente la validazione temporale, così come definita all'art. 1 comma 1 lettera i) D.P.C.M. del 30 marzo 2009. La marca temporale è opponibile a terzi
Metadati	Insieme di dati associati ad un documento informatico o ad 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.
Memorizzazione	Processo di trasposizione, su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici.
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.

OAIS	Open Archival information system
PAdES	PDF Advanced Electronic Signatures
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
Pacchetto di Archiviazione (PdA)	pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del DPCM 03-12-2013 e secondo le modalità riportate nel manuale di conservazione.
Pacchetto di Distribuzione (PdD)	pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta.
Pacchetto di Versamento (PdV)	pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione.
Presa in Carico	Accettazione da parte del SdC di un pacchetto di versamento in quanto conforme alle modalità previste dal MdC.
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 SdC. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale
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
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 che viene associata ad uno o più documenti informatici
Scarto	operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale. (DPCM 03- 12-2013 – Allegato 1)
UNI SinCro	UNI 11386:2010 – supporto all'interoperabilità nella conservazione e nel recupero

Torna al Sommario

3 NORMATIVA E STANDARD DI RIFERIMENTO

3.1 Normativa di riferimento

Il sistema di conservazione adottato da Santer Reply è adeguato alla normativa di riferimento in materia di conservazione attualmente in vigore:

- 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 al Sommario

3.2 Standard di riferimento

Il sistema di Conservazione adottato da Santer Reply S.p.A. è conforme agli standard di riferimento elencati nell'allegato 3 delle Regole Tecniche in materia di Sistema di conservazione:

- 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 al Sommario

4 RUOLI E RESPONSABILITA’

Lo svolgimento delle attività di conservatore richiede la presenza di più attori coinvolti nel processo, ognuno dei quali ha la responsabilità di specifiche attività da svolgere.

Il presente capitolo descrive i dati dei soggetti che nel tempo hanno assunto la responsabilità del sistema di conservazione, descrivendo in modo puntuale, in caso di delega, i soggetti, le funzioni e gli ambiti oggetto della delega stessa.

ruoli	nominativo	attività di competenza	periodo nel ruolo	eventuali deleghe
Responsabile del servizio di conservazione	Andrea Bertolini	- Definizione e attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione; - Definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente; - Corretta erogazione del servizio di conservazione all’ente produttore; - Gestione delle convenzioni, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.	13 anni	nessuna
Responsabile Sicurezza dei sistemi per la conservazione	Emilio Mantero	- Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; - segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e	3 anni in Santer Reply	

		individuazione e pianificazione delle necessarie azioni correttive.		
Responsabile funzione archivistica di conservazione	Marika Critelli	- 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.	7 anni di cui 5 in Santer Reply	
Responsabile trattamento dati personali	Emilio Mantero	- Controlla e verifica la garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali dandone riscontro al Responsabile della Conservazione ed anche al Legale Rappresentante Aziendale; - Controlla e verifica la garanzia che il trattamento dei dati affidati dai Clienti avvenga nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con	14 anni in Santer Reply	

		garanzia di sicurezza e di riservatezza dandone riscontro al Responsabile della Conservazione ed anche al Legale Rappresentante Aziendale		
Responsabile sistemi informativi per la conservazione	Emilio Mantero	- Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione; - monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore; - segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive; - pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione; - controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.	10 anni in Santer Reply	
Responsabile sviluppo e manutenzione del sistema di conservazione	Marcello Cecci	- Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione; - pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione; - monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione; - interfaccia con l'ente produttore relativamente alle modalità di trasferimento dei documenti e	7 anni di cui 5 in Santer Reply	

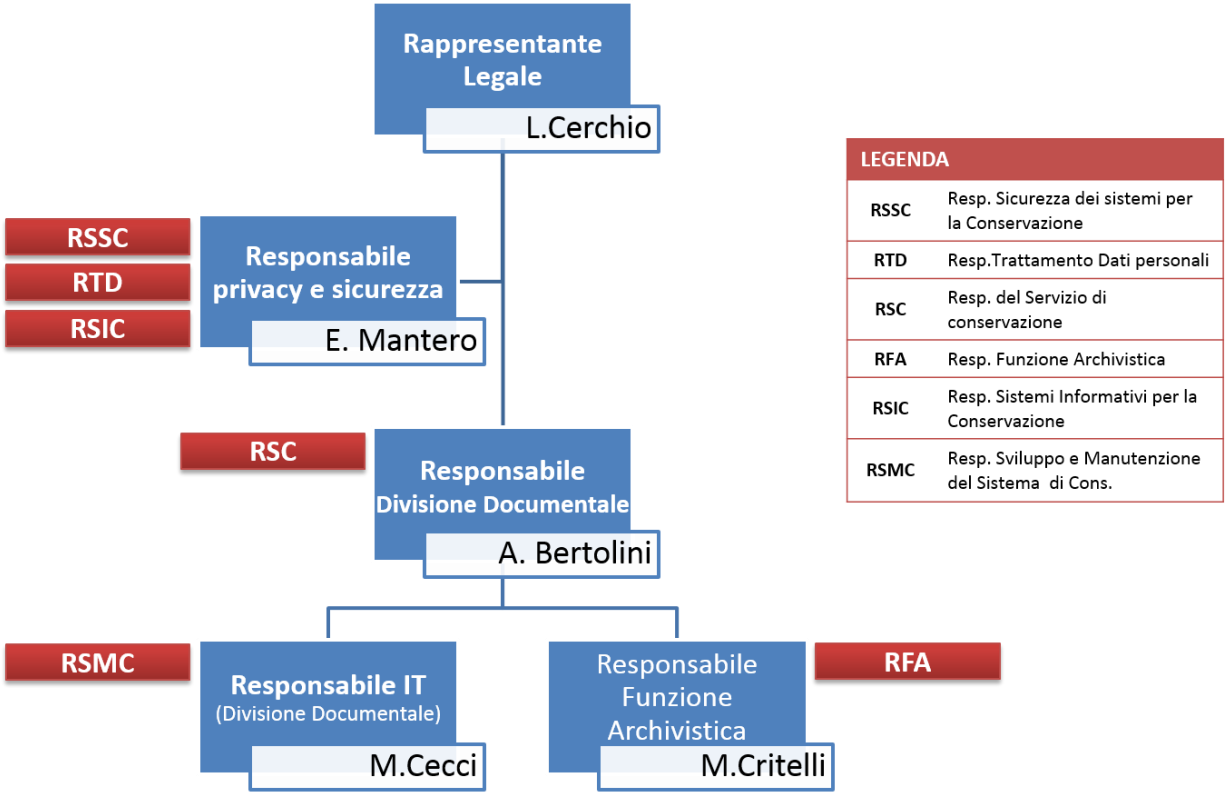
		fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche; - gestione dello sviluppo del portale connesso al servizio di conservazione.		

Torna al Sommario

5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Organigramma

Figura 1 - Organigramma



5.2 Strutture organizzative

Il presente capitolo descrive la struttura organizzativa comprensiva delle funzioni, delle responsabilità e degli obblighi dei diversi soggetti che intervengono nel processo di conservazione.

I ruoli e le responsabilità descritti di seguito fanno riferimento a quanto definito nell'art. 6 "Ruoli e Responsabilità" delle Regole Tecniche (DPCM 03-12-2013).

Torna al Sommario

5.2.1 Soggetti Esterni al sistema di Conservazione

Produttore

Il produttore è la 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.

Sottoscrive un contratto per le attività di conservazione assegnando a Santer Reply la gestione in outsourcing del processo di conservazione, identificando in Santer Reply la figura del Responsabile del servizio di conservazione in ottemperanza ai requisiti normativi in materia.

Nel ruolo del Produttore sono quindi compresi tutti gli enti che versano i documenti da conservare con gli opportuni metadati. Il Produttore si impegna a depositare i documenti informatici garantendone l'autenticità e l'integrità, nel rispetto delle norme sulla formazione e sui sistemi di gestione dei documenti informatici. In particolare, garantisce che il trasferimento dei documenti informatici venga realizzato utilizzando formati compatibili con la funzione di conservazione e rispondenti a quanto previsto dalla normativa vigente.

Le tipologie di documenti da trasferire, le modalità di versamento e i metadati sono concordati e specificati negli Allegati "Specificità del Contratto" stipulati con Santer Reply.

Il Produttore resta il responsabile del contenuto del Pacchetto di versamento (PdV) ed è tenuto a trasmetterlo al servizio di conservazione secondo le modalità operative descritte negli allegati "Specificità del Contratto".

All'interno dell'Ente viene nominato una soggetto **Responsabile della conservazione** ed i suoi riferimenti sono indicati nel documento "Specificità del contratto", nel quale sono anche riportate le attività e le responsabilità affidate al **Responsabile del servizio di conservazione** interno a Santer Reply.

Utente

L'Utente è una persona, ente o sistema che ha la possibilità di accedere al sistema di conservazione dei documenti informatici al fine di fruire delle informazioni di interesse conservate al suo interno (recupero dei documenti o di copie di interesse) nei limiti previsti dalle norme vigenti.

Il ruolo dell'Utente si può identificare, al momento, con l'Ente produttore, in relazione a specifici soggetti abilitati indicati dal Produttore stesso, che possono accedere esclusivamente ai documenti da esso stesso versati o solo ad alcuni di essi secondo le regole di visibilità e di accesso concordate negli Allegati "Specificità del Contratto".

Torna al Sommario

5.2.2 Soggetti Interni al sistema di Conservazione

I Clienti affidano in outsourcing il servizio di conservazione a Santer Reply, che assume le responsabilità di Responsabile della Conservazione in accordo con quanto previsto dal contratto, dagli allegati contrattuali e dagli articoli 5-6 del DPCM 3 Dicembre 2013, che ne delinea i compiti.

Santer Reply, attraverso nomina formale, incarica espressamente il **Responsabile del Servizio di Conservazione** (**RSC**), il quale, per competenza ed esperienza, garantisce la corretta esecuzione dei processi di conservazione definiti dalle norme, dal contratto e dagli allegati contrattuali.

Nell'esercizio delle sue funzioni, il Responsabile del servizio di Conservazione è coadiuvato da altri soggetti interni che intervengono nel processo:

- Responsabile Sicurezza dei sistemi per la Conservazione (**RSSC)**
- Responsabile Trattamento Dati personali (**RTD)**
- Responsabile Funzione Archivistica (**RFA**)
- Responsabile Sistemi Informativi per la Conservazione (**RSIC**)
- Responsabile Sviluppo e Manutenzione del Sistema di Conservazione (**RSMC**)

Di seguito viene proposta una matrice con le responsabilità degli attori interni al Sistema di Conservazione coinvolti nei singoli processi.

	RESPONSABILITÀ				
FASI	**RSC**	**RFA**	**RSIC**	**RSMC**	**RSSC**
Attivazione del servizio di conservazione (a seguito della sottoscrizione di un contratto);		x			
Acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento;	x				
Preparazione e gestione del pacchetto di archiviazione;	x				
Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione	x				

di duplicati e copie informatiche su richiesta;					
Scarto dei pacchetti di archiviazione;	x				
Conduzione del servizio di Conservazione	x		x		
Manutenzione del sistema di Conservazione				x	
Monitoraggio del sistema di conservazione	x				
Change Management	x	x	x	x	x

Torna al Sommario

5.2.2.1 *Attivazione del servizio di conservazione*

La fase di Attivazione del servizio di conservazione viene gestita dal "Project Management" designato da Santer Reply. In questa fase, molto importante, vengono definiti:

- il contratto di affidamento del servizio in cui vengono specificate le attività e le responsabilità affidate al conservatore, da parte del RdC;
- la parte specifica del Manuale di Conservazione, che formalizza tutti i dettagli del servizio ("Allegato Specificità del contratto");
- la parte di installazione, configurazione e messa in esercizio dei flussi di conservazione;
- la formazione degli utenti e dei referenti del cliente.

Responsabile e coordinatore operativo di questa fase è il **Responsabile della Funzione Archivistica** di Santer Reply.

Torna al Sommario

5.2.2.2 *Conduzione del servizio di conservazione*

La fase di conduzione del servizio di conservazione viene gestita dalla struttura che ha in carico la gestione e manutenzione della piattaforma SW Ready, usata da Santer Reply per lo svolgimento dei servizi di conservazione.

Questa fase decorre dall'avvenuta attivazione dei flussi di conservazione, formalizzata con un apposito verbale. In questa fase vengono gestite le seguenti attività:

- monitoraggio dei flussi di ingresso e di produzione;
- gestione copie di sicurezza;
- gestione backup;
- gestione delle anomalie;
- supporto a RdC ed utenti del servizio di conservazione;
- gestione degli incidenti e dei problemi

Responsabile di questa fase e il **Responsabile dei Sistemi Informativi per la Conservazione** che coinvolge, in caso di necessità, anche gli altri responsabili del servizio.

Torna al Sommario

5.2.2.3 Change management

Una particolare fase della conduzione è quella che riguarda attività di aggiornamento del sistema di conservazione. Per aggiornamento si intende:

- l'attivazione di nuovi flussi di ingresso al servizio di conservazione,
- la dismissione di flussi di conservazione esistenti,
- l'aggiornamento del sistema di conservazione hw e/o sw,
- la modifica del set dei metadati,
- la modifica delle regole di presa in carico,
- la modifica degli accordi di versamento,
- la modifica delle codifiche,
- la modifica della tipologia dei supporti di conservazione,
- l'attività di migrazione
- qualsiasi altra modifica che non sia di ordinaria conduzione

Responsabile e coordinatore operativo di questa fase è il **Responsabile della Funzione Archivistica di Conservazione** di Santer Reply il quale, opera in stretta sinergia e collaborazione

con la struttura gestita dal **Responsabile dei Sistemi Informativi della Conservazione** e, in caso di necessità, anche degli altri responsabili del servizio.

Torna al Sommario

6 OGGETTI SOTTOPOSTI A CONSERVAZIONE

Il presente capitolo descrive le tipologie degli oggetti sottoposti a conservazione, comprensive dell'indicazione dei formati gestiti e dei metadati da associare alle diverse tipologie di documenti.

Santer Reply, in conformità all'allegato 2 al Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 Regole tecniche in materia di sistema di conservazione, accetta formati che maggiormente garantiscano i principi di interoperabilità tra sistemi di conservazione. Al fine di assicurare una corretta gestione degli oggetti conservati è opportuno che i formati assicurino le seguenti caratteristiche::

- apertura,
- sicurezza,
- portabilità,
- funzionalità,
- supporto allo sviluppo,
- diffusione.

Di seguito viene riportato un breve elenco dei formati più diffusi accettatati da Santer Reply ed i relativi dettagli esplicativi:

Formato	Estensione	Tipo mime	Standard	Visualizzatore	Produttore visualizzatore
PDF	.pdf	*application/pdf*	ISO32000-1	Adobe Reader	Adobe Systems
PDF/A	.pdf	*application/pdf*	ISO 19005-1:2005 (vers. PDF 1.4) ISO 19005-2:2011 (vers. PDF 1.7)	Adobe Reader	Adobe Systems
TXT	.txt	*application/text*		Mozilla Chrome Internet Explorer	Firefox Google Microsoft
XML	.xml	*application/ xml e text/xml*		Mozilla Chrome Internet Explorer	Firefox Google Microsoft
TIFF	.tiff	*image/tiff*		Imagemagick	
JPG	.jpg .jpeg	*image/jpeg*	ISO/IEC 10918:1	Imagemagick	
OOXML	.docx, .xlsx, .pptx	*application/msword ed altri*	ISO/IEC DIS 29500:2008	Microsoft office	Tale formato deve garantire alcune caratteristiche che lo rendono adatto alla conservazione

					nel lungo periodo, tra queste l'embedding dei font, la presenza di indicazioni di presentazione del documento, la possibilità di applicare al documento la firma digitale XML
ODF	.ods, .odp, .odg, .odb	*application/vnd.oasis.opendocument.text*	ISO/IEC 26300:2006	*Libreoffice*	

Integrazioni alla presente tabella possono essere presenti nell'allegato "***Specificità del Contratto***".

Torna al Sommario

6.1 Oggetti conservati

Il sistema di conservazione digitale dei documenti informatici è configurato per accettare le seguenti tipologie di documenti:

- **Documenti rilevanti ai fini Tributari**
- **Documenti informatici**

In relazione ai diversi tipi di documenti informatici posti in conservazione, è previsto un "set minimo" di metadati come specificato nei paragrafi seguenti.

Oltre al set minimo di metadati, il Cliente può associare al documento informatico eventuali ulteriori metadati che, al pari del set minimo di metadati, sono oggetto di indicizzazione da parte del sistema. I metadati aggiuntivi sono specificati nel documento "Specificità del Contratto".

Torna al Sommario

6.1.1 Documenti rilevanti ai fini tributari

Il *Decreto del Ministro dell'Economia e delle Finanze 17 giugno 2014* interviene ad aggiornare e sostituire il precedente Decreto di riferimento del 23 gennaio 2004. Esso dispone le modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto e riprende le disposizioni in materia di documento informatico, firma elettronica e conservazione di cui al DPCM 22 febbraio 2013 e al DPCM 3 dicembre 2013.

Oggetto Conservato	**Documenti Rilevanti ai fini Tributari**
Descrizione:	Libro Giornale, Registri IVA, Fatture, FatturePA, ecc.
Caratteristiche:	Il Processo di Conservazione è effettuato entro tre mesi dal termine di presentazione delle dichiarazioni dei redditi.
Periodo di conservazione:	10 anni
Formati Gestiti e Visualizzatori:	*PDF – PDF/A (mime type: application/pdf) – Adobe Reader* *TIFF (mime type: image/tiff) – Imagemagick* *JPG (mime type: image/jpeg) – Imagemagick* *OOXML (mime type: application/msword ed altri) – Microsoft office* *Open Document Format (mime type: application/vnd.oasis.opendocument.text) - Libreoffice* *XML (mime type: application/xml e text/xml) – Mozilla Firefox* TXT (mime type: application/text) – Mozilla Firefox
Metadati minimi:	• NOME • COGNOME • (o) DENOMINAZIONE • CODICE FISCALE • PARTITA I.V.A. • DATA

Per i documenti di Tipo ***FatturaPA*** vengono conservate le relative Notifiche SDI di cui si riportano le specifiche di seguito:

Oggetto Conservato	**Notifica SDI**
Descrizione:	Notifiche di esito relative al Sistema di Interscambio
Caratteristiche:	Segue l'iter procedurale della Fattura da cui è stata generata
Periodo di conservazione:	10 anni
Formati Gestiti e Visualizzatori:	*XML (mime type: application/xml e text/xml) – Mozilla Firefox*
Metadati minimi:	• Tipo Notifica • + metadati minimi relativi alla fattura di riferimento

Torna al Sommario

6.1.2 Documenti informatici

Questa classe documentale include tutti i documenti informatici generici gestiti da un Ente anche di tipo Sanitario.

Oggetto Conservato:	**Documenti Informatici**
Descrizione:	Documenti generici di cui si voglia attuare la conservazione
Periodo di conservazione:	Variabili in base alla tipologia di documento conservato
Formati gestiti e Visualizzatori:	*PDF – PDF/A (mime type: application/pdf) – Adobe Reader* *TIFF (mime type: image/tiff) – Imagemagick* *JPG (mime type: image/jpeg) – Imagemagick* *OOXML (mime type: application/msword ed altri) – Microsoft office* *Open Document Format (mime type: application/vnd.oasis.opendocument.text) – LibreOffice* *XML (mime type: application/xml e text/xml) – Mozilla Firefox* TXT (mime type: application/text) – Mozilla Firefox

Metadati minimi:	• IDENTIFICATIVO UNIVOCO
	• RIFERIMENTO TEMPORALE (data di chiusura)
	• OGGETTO
	• SOGGETTO PRODUTTORE
	  ○ Nome
	  ○ Cognome
	  ○ CF
	• EVENTUALE DESTINATARIO
	  ○ Nome
	  ○ Cognome
	  ○ CF

Torna al Sommario

6.2 Pacchetto di versamento

L'invio dei documenti al sistema di conservazione da parte del produttore avviene tramite la consegna di un pacchetto di versamento avente una struttura dati di base comune.

Le specifiche e il formato del pacchetto di versamento, sono medesime per tutte le tipologie di documenti gestiti dal sistema di conservazione.

La struttura dati del Pacchetto di versamento è la seguente:

```
<?xml version="1.0"?>
-<soapenv:Envelopexmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
        <soapenv:Header/>
        -<soapenv:Body>
                <User>RDY_PRECAR</User>
                <Password>12345</Password>
                <IdEnte>AZI01</IdEnte>
                <CodiceCanale>FATPA</CodiceCanale>
                <CodiceUnivoco>TEST_AZI01_0001</CodiceUnivoco>
                <Documento> CONTIENE IL BASE64 DEL FILE TRASMESSO=</Documento>
                <Indici/>
                <HashSha1>56A7DCAF6ID151C5F1E8956DFA00CC216EC1R7N1</HashSha1>
                <NomeFile>IT99999999999_001.xml</NomeFile>
        </soapenv:Body>
 </soapenv:Envelope>
```

Per i dettagli, concordati con il soggetto Produttore, si faccia riferimento a quanto descritto nell'allegato "***Specificità del contratto***".

Successivamente i dati vengono memorizzati sulla seguente tabella Oracle:

TABLE_NAME	COLUMN_NAME	COMMENTS
TAB_DOC_WEB_SER	PRG_DOC_WEB_SER	(AUTO)
TAB_DOC_WEB_SER	DAT_INS	Data Inserimento
TAB_DOC_WEB_SER	DES_USR_INS	Utente che inserisce
TAB_DOC_WEB_SER	BIN_DOC	DOCUMENTO (*)
TAB_DOC_WEB_SER	BIN_IDX	XML CON INDICI (*)
TAB_DOC_WEB_SER	FLG_STA_CAR	stato (0=INSERITO, 1=ELABORATO, 9=ERRORE) (caricamento nel documentale)
TAB_DOC_WEB_SER	DES_LOG_ELA	LOG ELABORAZIONE (ED ERRORE)
TAB_DOC_WEB_SER	DAT_ELA	DATA ELABORAZIONE
TAB_DOC_WEB_SER	DES_COD_UNV_DOC	codice univoco del documento (*)
TAB_DOC_WEB_SER	DES_SH1_DOC	hash sha1 del documento (*)
TAB_DOC_WEB_SER	IND_STA_FIR_MAR	stato firma e marca (F=firmato, FM=firmato e marcato, N non firmato ne marcato
TAB_DOC_WEB_SER	DES_FIL_NAM	nome del file (*)
TAB_DOC_WEB_SER	FLG_ELA_FIR	0=no, 1=si, 9 = errore
TAB_DOC_WEB_SER	DES_LOG_FIR	log errore
TAB_DOC_WEB_SER	DAT_ELA_FIR	data elaborazione firma

TAB_DOC_WEB_SER	CDA_ENT	ente
TAB_DOC_WEB_SER	CDA_CAN	canale
TAB_DOC_WEB_SER	DAT_SCA_MAR	data scadenza marca temporale
TAB_DOC_WEB_SER	PRG_DOC_FIL	prg documento caricato nel documentale
TAB_DOC_WEB_SER	FLG_STA_CON	stato conservazione (tabella stati) 1=in attesa di elaborazione

Nell'ambito dei singoli contratti di conservazione e in maniera concordata tra il cliente, il *Responsabile della Conservazione* ed il Res*ponsabile della Funzione Archivistica di Conservazione* è prevista la possibilità di estendere il pacchetto di versamento affinché veicoli informazioni aggiuntive caratterizzanti della tipologia di documento trattato.

Torna al Sommario

6.3 Pacchetto di archiviazione

Il file di indice del PdA rispetta i requisiti richiesti dalla normativa ed è conforme alle specifiche standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010), standard nazionale riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione.

Il Pacchetto di Archiviazione per tutti i documenti gestiti dal sistema è costituito da:

- I **documenti fisici** nel formato definito per ciascuna tipologia;
- un **file dei metadati** in XML che descrive la struttura dei metadati custom contenuti all'interno dell'IPdA (vedi allegato "Specificità del contratto")
- l'**Indice del Pacchetto di Archiviazione** che differisce a seconda della tipologia documentale trattata (vedi Tab. 1 e 2)

Figura 2 - IPdA Fatture elettroniche

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<?xml-stylesheet type="text/xsl" href="FS_ReadyDoc.xsl"?>
<sntl:IdC xmlns:sntl="http://www.uni.com/U3011/sincro/" sntl:url="
http://www.uni.com/U3011/sincro/" sntl:version="1.0">
    <sntl:SelfDescription>
        <sntl:ID>1</sntl:ID>
        <sntl:CreatingApplication>
            <sntl:Name>Ready.Legal</sntl:Name>
            <sntl:Version>3.1.004</sntl:Version>
            <sntl:Producer>Santer Reply S.p.A.</sntl:Producer>
        </sntl:CreatingApplication>
    </sntl:SelfDescription>
    <sntl:VdC>
        <sntl:ID>AZI01_000001_150102</sntl:ID>
        <sntl:VdCGroup>
            <sntl:Label>Fatturazione PA</sntl:Label>
            <sntl:ID>SISGI</sntl:ID>
            <sntl:Description sntl:language="it">Fatturazione PA</sntl:Description>
        </sntl:VdCGroup>
        <sntl:MoreInfo sntl:XMLScheme="ReadyCustomMetadataScheme.Xml">
            <sntl:EmbeddedMetadata>
                <CustomMetadata>
                    <VdC-NumeroVolume>1</VdC-NumeroVolume>
                    <VdC-CodiceAzienda>AZI01</VdC-CodiceAzienda>
                    <VdC-Azienda>Azienda TEST001 S.p.A.</VdC-Azienda>
                    <VdC-PartitaIva>01234567890</VdC-PartitaIva>
                    <VdC-DataCreazione>02/01/2015 12.06.57</VdC-DataCreazione>
                    <VdC-TotNumDoc>2</VdC-TotNumDoc>
                    <VdC-Descrizione>Questo file e' un indice di conservazione per un
                    pacchetto di documenti sottoposti a processo di Conservazione
                    Sostitutiva in conformita' al DPCM del 03/12/2013.</VdC-Descrizione>
                </CustomMetadata>
            </sntl:EmbeddedMetadata>
        </sntl:MoreInfo>
    </sntl:VdC>
    <sntl:FileGroup>
        <sntl:Label>FATPA</sntl:Label>
        <sntl:File sntl:extension=".xml" sntl:format="application/xml">
            <sntl:ID>6</sntl:ID>
            <sntl:Hash sntl:function="SHA-256">
            B6E89197036003AF22310E7898D99942C24F136FBA15A64103FBDD730FD15605</sntl:Hash>
        </sntl:File>
        <sntl:MoreInfo sntl:XMLScheme="ReadyCustomMetadataScheme.Xml">
            <sntl:EmbeddedMetadata>
                <CustomMetadata>
                    <DOC-ID>6</DOC-ID>
                    <DOC-NomeFile>IT01234567890_0002X.XML</DOC-NomeFile>
                    <CessionarioCommittente>COMMITTENTE 0001</CessionarioCommittente>
                    <CodiceFiscale>8908989000</CodiceFiscale>
                    <DataDocumento>2014-12-05</DataDocumento>
                    <NumeroDocumento>0001</NumeroDocumento>
                    <IdDocTrasmittente>1234567_001</IdDocTrasmittente>
                    <IdSdi>1208909</IdSdi>
                    <TipoDocumento>TD01 - FATTURA</TipoDocumento>
                </CustomMetadata>
            </sntl:EmbeddedMetadata>
        </sntl:MoreInfo>
```

```
    </sntl:FileGroup>
    <sntl:FileGroup>
        <sntl:Label>FATPA</sntl:Label>
        <sntl:File sntl:extension=".xml" sntl:format="application/xml">
            <sntl:ID>7</sntl:ID>
            <sntl:Hash sntl:function="SHA-256">
            44E42FF13D9645E5CAE0C4A0EF5F1D3CEB4B674FC1373B256B694A6C97F36FCE</sntl:Hash>
        </sntl:File>
        <sntl:MoreInfo sntl:XMLScheme="ReadyCustomMetadataScheme.Xml">
            <sntl:EmbeddedMetadata>
                <CustomMetadata>
                    <DOC-ID>7</DOC-ID>
                    <DOC-NomeFile>IT01234567890_00004.XML</DOC-NomeFile>
                    <CessionarioCommittente>COMMITTENTE 0001</CessionarioCommittente>
                    <CodiceFiscale>80089789076</CodiceFiscale>
                    <DataDocumento>2014-12-10</DataDocumento>
                    <NumeroDocumento>0002</NumeroDocumento>
                    <IdDocTrasmittente>1234567_001</IdDocTrasmittente>
                    <IdSdi>1209763</IdSdi>
                    <TipoDocumento>TD04 - NOTA DI CREDITO</TipoDocumento>
                </CustomMetadata>
            </sntl:EmbeddedMetadata>
        </sntl:MoreInfo>
    </sntl:FileGroup>
    <sntl:Process>
        <sntl:Agent sntl:type="person" sntl:role="PreservationManager">
            <sntl:AgentName>
                <sntl:NameAndSurname>
                    <sntl:FirstName>Nome Responsabile Conservazione</sntl:FirstName>
                    <sntl:LastName>Cognome Responsabile Conservazione</sntl:LastName>
                </sntl:NameAndSurname>
            </sntl:AgentName>
            <sntl:Agent_ID sntl:scheme="TaxCode">IT:Codice Fiscale</sntl:Agent_ID>
        </sntl:Agent>
        <sntl:Agent sntl:type="person" sntl:role="Delegate">
            <sntl:AgentName>
                <sntl:NameAndSurname>
                    <sntl:FirstName>Nome Delegato Conservazione</sntl:FirstName>
                    <sntl:LastName>Cognome Delegato Conservazione</sntl:LastName>
                </sntl:NameAndSurname>
            </sntl:AgentName>
            <sntl:Agent_ID sntl:scheme="TaxCode">IT:Codice Fiscale</sntl:Agent_ID>
        </sntl:Agent>
        <sntl:TimeReference>
            <sntl:DetachedTimestamp sntl:extension=".m7m" sntl:format=
            "application/timestamp-reply">AZI01_000001_150102.XML.m7m</sntl:DetachedTimestamp>
            <sntl:TimeInfo>2015-01-02T12:06:57+01:00</sntl:TimeInfo>
        </sntl:TimeReference>
        <sntl:LawAndRegulations sntl:language="it">DPCM del 03/12/2013
        </sntl:LawAndRegulations>
    </sntl:Process>
</sntl:IdC>
```

Figura 3 - IPdA documenti informatici

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<?xml-stylesheet type="text/xsl" href="FS_ReadyDoc.xsl"?>
<sntl:IdC xmlns:sntl="http://www.uni.com/U3011/sincro/" sntl:url="
http://www.uni.com/U3011/sincro/" sntl:version="1.0">
    <sntl:SelfDescription>
        <sntl:ID>31</sntl:ID>
        <sntl:CreatingApplication>
            <sntl:Name>Ready.Legal</sntl:Name>
            <sntl:Version>3.1.004</sntl:Version>
            <sntl:Producer>Santer Reply S.p.A.</sntl:Producer>
        </sntl:CreatingApplication>
    </sntl:SelfDescription>
    <sntl:VdC>
        <sntl:ID>AZI01_000031_150113</sntl:ID>
        <sntl:VdCGroup>
            <sntl:Label>Documenti Human Resource</sntl:Label>
            <sntl:ID>DOCHR</sntl:ID>
            <sntl:Description sntl:language="it">Documenti Human Resource</sntl:Description>
        </sntl:VdCGroup>
        <sntl:MoreInfo sntl:XMLScheme="ReadyCustomMetadataScheme.Xml">
            <sntl:EmbeddedMetadata>
                <CustomMetadata>
                    <VdC-NumeroVolume>31</VdC-NumeroVolume>
                    <VdC-CodiceAzienda>AZI01</VdC-CodiceAzienda>
                    <VdC-Azienda>Azienda TEST_002</VdC-Azienda>
                    <VdC-PartitaIva>00878150700</VdC-PartitaIva>
                    <VdC-DataCreazione>13/01/2015 20.19.46</VdC-DataCreazione>
                    <VdC-TotNumDoc>2</VdC-TotNumDoc>
                    <VdC-Descrizione>Questo file e' un indice di conservazione per un
                    pacchetto di documenti sottoposti a processo di Conservazione
                    Sostitutiva in conformita' al DPCM del 03/12/2013.</VdC-Descrizione>
                </CustomMetadata>
            </sntl:EmbeddedMetadata>
        </sntl:MoreInfo>
    </sntl:VdC>
    <sntl:FileGroup>
        <sntl:Label>CEDOL</sntl:Label>
        <sntl:File sntl:extension=".pdf" sntl:format="application/pdf">
            <sntl:ID>72497</sntl:ID>
            <sntl:Hash sntl:function="SHA-256">
            7F371B5D47CEAF4CB2CFEA8872B8B249C47D22AA648FB5FD9BB820A0BC2E653B</sntl:Hash>
        </sntl:File>
        <sntl:MoreInfo sntl:XMLScheme="ReadyCustomMetadataScheme.Xml">
            <sntl:EmbeddedMetadata>
                <CustomMetadata>
                    <DOC-ID>72497</DOC-ID>
                    <DOC-NomeFile>CEDOL_7884320_PU-2014.PDF</DOC-NomeFile>
                    <Matricola>000001</Matricola>
                    <Cognome>BIANCHI</Cognome>
                    <Nome>LUCA</Nome>
                    <CodiceFiscale>BNCLCU67E08D745O</CodiceFiscale>
                    <Qualifica>H6PU1</Qualifica>
                    <Azienda>AZIENDA 0002 </Azienda>
                    <Sede>45690 - SEDE DI LINATE</Sede>
                    <Mese>12</Mese>
                    <Anno>2014</Anno>
                </CustomMetadata>
            </sntl:EmbeddedMetadata>
        </sntl:MoreInfo>
```

```
            </sntl:EmbeddedMetadata>
        </sntl:MoreInfo>
    </sntl:FileGroup>
    <sntl:FileGroup>
        <sntl:Label>CEDOL</sntl:Label>
        <sntl:File sntl:extension=".pdf" sntl:format="application/pdf">
            <sntl:ID>72498</sntl:ID>
            <sntl:Hash sntl:function="SHA-256">
            3C17A3BC90DDC141E8A5F21EAC88C704011D26BD76E898DF9816CDEECFB90663</sntl:Hash>
        </sntl:File>
        <sntl:MoreInfo sntl:XMLScheme="ReadyCustomMetadataScheme.Xml">
            <sntl:EmbeddedMetadata>
                <CustomMetadata>
                    <DOC-ID>72498</DOC-ID>
                    <DOC-NomeFile>CEDOL_7867890_AR-2014.PDF</DOC-NomeFile>
                    <Matricola>000001</Matricola>
                    <Cognome>ROSSI</Cognome>
                    <Nome>MARIO</Nome>
                    <CodiceFiscale>RSSMRA86E09D745O</CodiceFiscale>
                    <Qualifica>BEVCFG</Qualifica>
                    <Azienda>AZIENDA 0001 </Azienda>
                    <Sede>19089 - SEDE DI MILANO</Sede>
                    <Mese>12</Mese>
                    <Anno>2014</Anno>
                </CustomMetadata>
            </sntl:EmbeddedMetadata>
        </sntl:MoreInfo>
    </sntl:FileGroup>
    <sntl:Process>
        <sntl:Agent sntl:type="person" sntl:role="PreservationManager">
            <sntl:AgentName>
                <sntl:NameAndSurname>
                    <sntl:FirstName>Nome Responsabile Conservazione</sntl:FirstName>
                    <sntl:LastName>Cognome Responsabile Conservazione</sntl:LastName>
                </sntl:NameAndSurname>
            </sntl:AgentName>
            <sntl:Agent_ID sntl:scheme="TaxCode">IT:Codice Fiscale</sntl:Agent_ID>
        </sntl:Agent>
        <sntl:Agent sntl:type="person" sntl:role="Delegate">
            <sntl:AgentName>
                <sntl:NameAndSurname>
                    <sntl:FirstName>Nome Delegato Conservazione</sntl:FirstName>
                    <sntl:LastName>Cognome Delegato Conservazione</sntl:LastName>
                </sntl:NameAndSurname>
            </sntl:AgentName>
            <sntl:Agent_ID sntl:scheme="TaxCode">IT:Codice Fiscale</sntl:Agent_ID>
        </sntl:Agent>
        <sntl:TimeReference>
            <sntl:DetachedTimestamp sntl:encoding="binary" sntl:format=                                    p>
            "application/timestamp-reply">AZI01_000031_150113.XML.m7m</sntl:DetachedTimestamp>
            <sntl:TimeInfo>2015-01-13T20:19:46+01:00</sntl:TimeInfo>
        </sntl:TimeReference>
        <sntl:LawAndRegulations sntl:language="it">DPCM del 03/12/2013
        </sntl:LawAndRegulations>
    </sntl:Process>
</sntl:IdC>
```

Torna al Sommario

6.4 Pacchetto di distribuzione

Seguendo le indicazioni contenute nelle regole tecniche del DPCM del 3 dicembre 2013 all'art. 9, comma 1, lettera h, il Pacchetto di Distribuzione segue un tracciato dati coincidente con quello del Pacchetto di Archiviazione. Pertanto si applicano le stesse regole tecniche e di formato previste al punto 6.3 per il Pacchetto di Archiviazione.

Torna al Sommario

7 IL PROCESSO DI CONSERVAZIONE

Obiettivo del sistema di Conservazione di Santer Reply, denominato Ready.Legal, è quello di assicurare che i documenti ad esso affidati vengano gestiti e mantenuti correttamente, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità nel tempo, nel rispetto delle norme di legge che regolano questa materia.

Il sistema Ready.Legal riceve i Pacchetti di versamento dal sistema produttore e genera Pacchetti di Archiviazione e di Distribuzione, rispondendo a tutti i requisiti che la normativa pone per l'esibizione dei documenti informatici, arricchendo le informazioni che accompagnano i dati conservati e tracciando con opportuni Log tutte le attività che gli riguardano.

Torna al Sommario

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

L'invio dei Pacchetti di versamento da parte del produttore al sistema di conservazione, può avvenire attraverso canali diversi. Ogni canale messo a disposizione è provvisto di opportuni accorgimenti per la trasmissione dei dati in modalità sicura:

- mediante interfacce applicative di tipo web service attraverso connessione internet su canale criptato (https)
- mediante utilizzo di software client FTPS attraverso connessione internet su canale criptato.
- invio in allegato a una mail PEC che nativamente garantisce autenticità della provenienza e notifica di consegna in modalità sicura

Altre modalità di ricezione dei pacchetti di versamento potranno essere previste e saranno regolamentate nelle specificità del contratto.
La periodicità di invio dei documenti viene determinata dall'operatività delle procedure sui sistemi del Cliente e concordata con Santer Reply (giornaliera, mensile,….) in considerazione e nel rispetto dei termini normativi per la conservazione.

Il sistema di conservazione si assume la responsabilità della presa in carico di un PdV solo dopo che tutte le sue parti (l'Indice del PdV e relativi documenti) vengono correttamente ricevuti e superano con esito positivo i relativi controlli.

Tale operazione viene ufficialmente sancita dalla produzione del Rapporto di Versamento (RdV).

Tutte le operazioni eseguite dal processo di versamento, vengono registrate sul sistema informativo di Santer Reply nel log **wsDocPreCar_err.log**

Qui di seguito viene riportato un esempio di log :

Figura 4 - Esempio Log wsDocPreCar_err.log

```
[06/06/2014 08:05:23]  - Errore durante la scrittura del File nel Database: ORA-00001: violata restrizione di unicità
                (RDYSDITEST.UNQ_DOC_WEB_SER_001)
[06/06/2014 08:08:48]  - Errore durante la scrittura del File nel Database: ORA-00001: violata restrizione di unicità
                (RDYSDITEST.UNQ_DOC_WEB_SER_001)
[17/06/2014 12:14:43]  - Errore durante la connessione!!
[17/06/2014 12:14:43]  - Nessuna Connessione Attiva. RDYSDITES_PRECAR - pwdxxxxx
[17/06/2014 12:15:22]  - Errore durante la connessione!!
[17/06/2014 12:15:22]  - Nessuna Connessione Attiva. RDYSDITES_PRECAR - pwdxxxxx
[17/06/2014 12:15:33]  - Errore durante la connessione!!
[17/06/2014 12:15:33]  - Nessuna Connessione Attiva. RDYSDITES_PRECAR - pwdxxxxx
[19/06/2014 07:03:37]  - Errore durante la scrittura del File nel Database: ORA-12899: valore troppo grande per la colonna
                "RDYSDITEST"."TAB_DOC_WEB_SER"."DES_COD_UNV_DOC" (corrente: 23, massimo: 20)
[19/06/2014 07:04:13]  - Errore durante la scrittura del File nel Database: ORA-12899: valore troppo grande per la colonna
                "RDYSDITEST"."TAB_DOC_WEB_SER"."DES_COD_UNV_DOC" (corrente: 23, massimo: 20)
[09/07/2014 13:18:16]  - Errore durante la verifica Hash del File.
[26/09/2014 15:05:15]  - Errore durante la scrittura del File nel Database: ORA-00001: violata restrizione di unicità
                (RDYSDITEST.UNQ_DOC_WEB_SER_001)
[29/10/2014 09:28:26]  - Errore durante la verifica Hash del File.
[29/10/2014 09:34:51]  - Errore durante la verifica Hash del File.
[29/10/2014 12:00:30]  - Errore durante la verifica Hash del File.
[04/12/2014 19:53:37]  - Errore durante la scrittura del File nel Database: ORA-00942: tabella o vista inesistente
[04/12/2014 19:53:43]  - Errore durante la scrittura del File nel Database: ORA-00942: tabella o vista inesistente
[26/02/2015 17:19:35]  - Nessuna fattura insertita per il Codice Univoco 'ITXXXXXXXXXXX_50008
[26/02/2015 17:19:36]  - Nessuna fattura insertita per il Codice Univoco 'ITXXXXXXXXXXX_50009
[26/02/2015 17:19:36]  - Nessuna fattura insertita per il Codice Univoco 'ITXXXXXXXXXXX_50010
[27/02/2015 11:13:09]  - Nessuna fattura importata per prg_doc_web_ser 100819 - ORA-31011: Analisi XML non riuscita
[27/02/2015 11:20:35]  - Nessuna fattura importata per prg_doc_web_ser 100834 - 0
[27/02/2015 11:20:37]  - Nessuna fattura importata per prg_doc_web_ser 100835 - 0
[27/02/2015 11:20:38]  - Nessuna fattura importata per prg_doc_web_ser 100836 - 0
```

Il log riporta:

- Il riferimento temporale di inizio operazione;
- Il dettaglio dell'anomalia riscontrata;

Torna al Sommario

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

Per ogni pacchetto ricevuto, il sistema verifica che il contenuto sia rispondente a quanto definito negli accordi di servizio (formato dei file, presenza di metadati, eventuali verifiche sulla validità della firma, ecc.). *Ready.Legal* effettua automaticamente le seguenti verifiche sulla documentazione trasmessa dal soggetto produttore:

- Verifica dell'identificazione certa del soggetto produttore e del relativo Ente produttore attraverso il controllo delle autorizzazioni/credenziali del produttore versante e dei suoi eventuali incaricati/delegati ad effettuare il versamento;
- Verifica che i documenti Informatici oggetto del Processo di Conservazione Elettronica siano aderenti agli standard di formato accettati dal sistema;
- Verifica che i documenti informatici avviati alla conservazione trovino corrispondenza tra la loro evidenza informatica (Hash-256) e quella indicata nell'IPdV ;
- Verifica della presenza dei metadati minimi nell'IPdV;
- Verifica di coerenza tra contenuto del PdV ed IPdV (se presente), ovvero che tutti documenti siano presenti nel pacchetto e che non ve ne siano di non dichiarati;

Le verifiche eseguite sul PdV e l'esito di queste vengono inserite in un registro di LOG che riporta:

- Gli estremi identificativi dell'Indice del PdV
- L'esito del controllo
- L'eventuale motivo di scarto
- Data e ora dell'attività di verifica

Nei successivi paragrafi viene indicato come il sistema di conservazione traccia, in un registro di LOG, tutte le attività relative alle verifiche che vengono effettuate sui pacchetti di versamento ricevuti. Nel LOG viene riportata una registrazione cronologica delle verifiche effettuate. Riportiamo nel seguito, a titolo di esempio, quelle che sono le verifiche principali effettuate :

- Verifica del correttezza del soggetto produttore e del relativo Ente di riferimento
- Verifica dei metadati minimi rispetto alla tipologia del documento
- Verifica della conformità dei metadati inviati
- Verifica dell'hash riportato tra i metadati inviati dal soggetto produttore e l'hash effettivo del documento versato.

Torna al Sommario

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

Qualora le verifiche descritte al paragrafo 7.2 diano esito positivo, il sistema procederà con la generazione del Rapporto di Versamento. Tale rapporto viene formalizzato in un documento in formato Xml, identificato univocamente, che include:

- l'impronta del/dei pacchetti di versamento cui si riferisce
- l'elenco dei documenti acquisiti dal sistema 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.

Al fine di rendere più fruibile il rapporto di versamento, in funzione della tipologia e dei volumi di documenti previsti, possono essere definite e concordate con il Cliente ulteriori regole nella generazione del rapporto di versamento, al cui interno potranno essere incluse le informazioni di più PdV, utilizzando procedure automatizzate basate su schedulazioni temporali o legate al numero di pacchetti da trattare.

I Rapporti di Versamento generati seguono lo stesso iter di conservazione dei documenti contenuti nel Pacchetto di Versamento per quel che riguarda le politiche di scarto e di permanenza all'interno del sistema di conservazione.

La struttura dati del Rapporto di Versamento è la seguente :

Figura 5 - Rapporto di versamento

```
<?xml version="1.0" encoding="ISO-8859-15"?>
  <RdV>
     <CodTipoDoc>RPVER</CodTipoDoc>
     <DesTipoDoc>Rapporto di Versamento</DesTipoDoc>
     <RifTimeUtc>2014-12-22 10:54:10 +00:00</RifTimeUtc>
     <RdVDocGroup>
       <CodAzienda>AZI01</CodAzienda>
       <DesAzienda>AZIENDA DI TEST 0001</DesAzienda>
       <CodClasseDoc>SISGI</CodClasseDoc>
       <DesClasseDoc>Fatturazione PA</DesClasseDoc>
          <RdVDocDetail>
              <IdDoc>8</IdDoc>
              <CodTipoDoc>FATPA</CodTipoDoc>
              <DesTipoDoc>Fattura PA</DesTipoDoc>
              <DataInserimento>22/07/2014 01.40.47</DataInserimento>
              <NomeFile>IT101234567890_0002F.XML.p7m</NomeFile>
              <Hash>98EB3ABE4F0AB97B0E1A15EAF7F721616C7D95917682A080E708D5DAE1C1620D</Hash>
          </RdVDocDetail>
          <RdVDocDetail>
              <IdDoc>9</IdDoc>
              <CodTipoDoc>RCN</CodTipoDoc>
              <DesTipoDoc>Ricevuta di consegna</DesTipoDoc>
              <DataInserimento>22/07/2014 02.58.38</DataInserimento>
              <NomeFile>IT98765432101_0002F_RC_002.xml</NomeFile>
              <Hash>1O6777C08620E8A63F5A1A4A310D044C2259AD148DE580A332E7B7D181D48BFC</Hash>
          </RdVDocDetail>
          <RdVDocDetail>
              <IdDoc>124</IdDoc>
              <CodTipoDoc>NDE</CodTipoDoc>
              <DesTipoDoc>Notifica di esito</DesTipoDoc>
              <DataInserimento>17/11/2014 06.10.08</DataInserimento>
              <NomeFile>IT998877665540_000BI_NE_003.xml</NomeFile>
              <Hash>1K729B7976D2E43A2F04A4B911CD49A66615E69B6D504F23F96CB37975B12CA8</Hash>
          </RdVDocDetail>
          <RdVDocDetail>
              <IdDoc>189</IdDoc>
              <CodTipoDoc>NDT</CodTipoDoc>
              <DesTipoDoc>Notifica di decorrenza termini</DesTipoDoc>
              <DataInserimento>18/12/2014 08.49.25</DataInserimento>
              <NomeFile>IT00220055441_000EJ_DT_003.xml</NomeFile>
              <Hash>H8DBC2813175BFC5017F9614DD2ABD8D7A43EFC938ED4AA5163CA2A4FE1DF284</Hash>
          </RdVDocDetail>
     </RdVDocGroup>
  </RdV>
```

Il sistema tiene traccia, tramite LOG, di ogni operazione e verifica effettuata sui pacchetti di versamento ricevuti dai sistemi produttori.

Di seguito viene riportato un esempio di LOG di registrazione di un pacchetto di versamento inserito correttamente nel sistema di conservazione :

PRG_DOC_WEB_SER	70
DAT_INS	09/02/2015 11.21
DES_USR_INS	RDYSDITEST_PRECAR
BIN_DOC	<BLOB>

BIN_IDX	<CLOB>
FLG_STA_CAR	1
DES_LOG_ELA	
DAT_ELA	09/02/2015 11.26
DES_COD_UNV_DOC	TEST_0001
DES_SH1_DOC	39EF8601C909B20D539C155F1691EBB4361EB606
IND_STA_FIR_MAR	F
DES_FIL_NAM	IT01234567890_00047.xml
FLG_ELA_FIR	0
DES_LOG_FIR	
DAT_ELA_FIR	
CDA_ENT	AZI01
CDA_CAN	FATPA
DAT_SCA_MAR	
PRG_DOC_FIL	243
FLG_STA_CON	1

I metadati che indicano la corretta esecuzione del processo sono

FLG_STA_CAR	1
DES_LOG_ELA	
DAT_ELA	09/02/2015 11.26

a cui si associa anche L'Id del documento caricato ne sistema di conservazione che viene valorizzato con '243'.

PRG_DOC_FIL	243

Torna al Sommario

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

Tutti i controlli effettuati in fase di verifica del PdV costituiscono condizione necessaria per l'accettazione dello stesso. Nel caso in cui anche uno solo dei controlli sopra descritti non andasse a buon fine il PdV non verrebbe accettato e si produrrebbe così un rifiuto immediato.

Possibili cause di rifiuto sono:

- Documento non aderente agli standard di formato accettati dal sistema;
- Mancata corrispondenza tra l'evidenza informatica (Hash-256) del documento e quella indicata nell'IPdV ;

- Mancanza dei metadati minimi richiesti;
- Non coerenza tra contenuto del PdV ed IPdV (se presente), ovvero non tutti i documenti dichiarati risultano presenti nel pacchetto;

Le informazioni relative alla motivazione del rifiuto vengono inserite, anche in questo caso, nel registro di LOG come di seguito indicato a titolo di esempio:

RG_DOC_WEB_SER	47
DAT_INS	10/01/2015 12.48
DES_USR_INS	RDYSDITEST_PRECAR
BIN_DOC	<BLOB>
BIN_IDX	<CLOB>
FLG_STA_CAR	9
DES_LOG_ELA	17 – Metadati minimi mancanti
DAT_ELA	10/01/2015 12.53
DES_COD_UNV_DOC	TEST_0107
DES_SH1_DOC	54DD8601C909A54T539C643F3201ECE4361FE421
IND_STA_FIR_MAR	F
DES_FIL_NAM	IT01234567890_00056.xml
FLG_ELA_FIR	0
DES_LOG_FIR	
DAT_ELA_FIR	
CDA_ENT	AZI01
CDA_CAN	FATPA
DAT_SCA_MAR	
PRG_DOC_FIL	
FLG_STA_CON	1

I metadati che indicano la corretta esecuzione del processo sono

FLG_STA_CAR	9
DES_LOG_ELA	17 – Metadati minimi mancanti
DAT_ELA	10/01/2015 12.53

Tale rifiuto viene comunicato all'ente Produttore attraverso comunicazione via Email

La comunicazione contiene :

- Data e ora Trasmissione
- Descrizione Scarto
- L'identificativo univoco del soggetto Trasmittente

- Nome del file Trasmesso
- Codice Ente
- Hash

Torna al Sommario

7.5 Preparazione e gestione del pacchetto di archiviazione

Una vota completata la fase di verifica ed accettazione del PdV e formazione del Rapporto di Versamento il processo si conclude con la formazione per ogni PdV di un PdA.

La cadenza con cui vengono creati i pacchetti di archiviazione è stabilita in sede contrattuale con il produttore dei documenti. Il pacchetto di archiviazione è sempre omogeneo per tipologia di documenti contenuti al suo interno.

Al fine di garantire l'interoperabilità nel tempo dei sistemi di conservazione, l'indice del PdA viene formato secondo le regole tecniche definite nella norma UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.

I pacchetti di archiviazione generati, vengono firmati (attraverso standard CAdES) digitalmente dal Responsabile del sistema di conservazione o da un suo delegato e marcati temporalmente per assicurarne la validità nel corso del tempo.

Ad intervalli pianificati con una cadenza non superiore ad 1 anno rispetto alla data di presa in carico, il sistema di conservazione provvederà ad effettuare un controllo automatizzato sui Pacchetti di Archiviazione conservati. Il controllo si articolerà sui seguenti punti:

- Verifica di integrità del file del PdA firmato e marcato temporalmente rispetto a quanto memorizzato in fase di archiviazione.
- Verifica di ogni singolo documento contenuto all'interno del PdA calcolando l'hash SHA256 del documento e confrontandolo con il corrispondente valore riportato all'interno del Pacchetto di Archiviazione
- Verifica a livello base dell'integrità del file su riversato su file system effettuata calcolando l'hash del documento riversato e confrontandolo con quello memorizzato nel sistema di conservazione

Tale tipo di verifica fornisce adeguate garanzie sia in termini di disponibilità, immodificabilità che di leggibilità del file.

Torna al Sommario

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

Il sistema di conservazione permette, ai soli soggetti autorizzati, l'accesso anche da remoto, al documento conservato, e la produzione di un **Pacchetto di distribuzione**, che può essere consultato ed esibito attraverso il portale web.

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

L'accesso web consente al Produttore di ricercare i documenti e le aggregazioni versati, di effettuarne il download e di acquisire le prove delle attività di conservazione.

Inoltre, tramite l'interfaccia web, è possibile monitorare i versamenti effettuati, sia andati a buon fine che falliti e consultare tutta la documentazione relativa ai Rapporti di versamento.

Nel caso vengano riscontrate delle anomalie il Cliente può contattare il servizio di Help Desk, messo a disposizione sia tramite sistema di Trouble Ticketing che per telefono, per segnalare l'anomalia che verrà presa in carico e gestita secondo i tempi e modi previsti dal contratto di servizio specifico.

Ai fini della interoperabilità tra sistemi di conservazione, il sistema *Ready.legal* 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 attraverso l'utilizzo degli Indici di ricerca corrispondenti ai metadati specifici per ogni tipologia documentale.

Una volta ricercato il documento, attraverso apposite funzionalità, è quindi possibile effettuare il download automatico del PdD come file di tipo archivio compresso .zip contenente**.** Il documento del quale viene richiesta l'esibizione

- L' Indice del Pacchetto di Archiviazione di cui il documento esibito fa parte. Tale indice è sottoscritto con Firma Digitale e Riferito Temporalmente con Marca Temporale

Possono essere definite e concordate con il Cliente, ulteriori modalità di esibizione dei PdD, ad esempio tramite supporti auto consultanti, eventualmente meglio dettagliate nell'Allegato "Specificità del Contratto". 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). Qualora si verifichino anomalie relative all'integrità del PdD l'utente richiedente potrà richiedere supporto al servizio HelpDesk messo a disposizione direttamente da Santer Reply e, come indicato anche in precedenza, secondo i tempi e modi previsti dal contratto di servizio specifico.

Torna al Sommario

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

Nel caso in cui sia richiesta la **produzione di duplicati** informatici dei documenti conservati, è necessario effettuare la ricerca del documento informatico di interesse attraverso le funzionalità messe a disposizione dal sistema di conservazione *Ready.Legal*. Individuato il documento informatico di interesse, un' apposita funzione consente di effettuare il download del documento stesso, producendo quindi un duplicato.

Il documento informatico richiesto viene infatti estratto dal sistema in formato binario controllando che l'estrazione sia eseguita senza errori e quindi inviato all'utente che ne ha fatto richiesta.

La **produzione di copie,** invece, si rende necessaria solamente a seguito di obsolescenza tecnologica di un formato accettato in conservazione e determina, quale diretta conseguenza, l'avvio di una procedura di riversamento sostitutivo.

In questo caso, Santer Reply, previo perfezionamento di specifico accordo scritto (dove saranno concordati ruoli, modalità, e tempi), 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 a Santer Reply, questo viene eseguito in conformità a quanto previsto dal DMEF 17/06/2014 art. 4 comma 1.

Il RdC di Santer Reply, 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 da realizzare.

Più nel dettaglio, l'intervento del Pubblico Ufficiale viene richiesto nelle ipotesi disciplinate puntualmente dal CAD – Codice dell'Amministrazione Digitale ed in particolare quando occorra procedere alla predisposizione di:

- **Copie informatiche di documenti analogici** (art. 22, comma 5, CAD): in presenza di documenti analogici originali unici, la conformità della copia informatica all'originale deve essere autenticata da un notaio o altro Pubblico Ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico. I documenti analogici originali unici, per i quali è richiesto l'intervento obbligatorio del Pubblico Ufficiale, sono quelli individuati dal D.P.C.M. 21 marzo 2013 – Allegato A.

L’intervento del Pubblico Ufficiale può aversi inoltre quando richiesto espressamente dal Cliente laddove occorra produrre:

- **Copie analogiche di documenti informatici** (art. 23, comma 1, CAD)
- **Copie informatiche di documenti informatici** (art. 23-bis, co. 2, CAD)

La procedura con cui attivare l’intervento del pubblico ufficiale viene definita nell’Allegato “Specificità del Contratto” dove saranno concordati ruoli, modalità, tempi e corrispettivi.

Si fa presente che, generalmente nei contratti con le PA si tende a gestire le attività in capo al pubblico ufficiale direttamente all’interno dell’Azienda essendo in essa già prevista l’esistenza di tali figure.

Torna al Sommario

7.8 Scarto dei pacchetti di archiviazione

Lo scarto della documentazione è una procedura gestita dal sistema in modalità semiautomatica. Il procedimento si svolge secondo le seguenti fasi:

- In prossimità del termine del periodo di conservazione, stabilito negli accordi di servizio con il soggetto titolare, e indicato all’interno del manuale della conservazione, gli oggetti conservati vengono identificati come “prossimi allo scarto” dal Sistema di Conservazione che invia un Alert a tutti i soggetti responsabili del processo di conservazione;
- Il Responsabile del servizio di Conservazione estrae dal sistema l’elenco dettagliato dei Pacchetti da scartare che deve contenere almeno i seguenti dati:
    - tipologia dei documenti proposti per lo scarto
    - estremi cronologici
    - motivazione dello scarto
- L'elenco dei documenti è allegato al **Verbale di scarto** e sottoposto a sottoscrizione del Responsabile dell’Ente e del Responsabile del servizio di Conservazione;
- Il Responsabile del servizio di Conservazione procede al riversamento diretto dei Pacchetti da scartare presenti nell’elenco e dei relativi Indici di Conservazione su supporto digitale di adeguata capacità. Il supporto digitale contenente i Pacchetti riversati, viene consegnato all’Ente di appartenenza dietro firma di apposita ricevuta da parte dell’Ente;

- In ultimo, il Responsabile del servizio di Conservazione, procede alla cancellazione dei Pacchetti e dei relativi indici di conservazione dagli archivi digitali del sistema (copia primaria su DB e backup).

Nel caso in cui la procedura di scarto è relativa ad archivi pubblici o privati che rivestono interesse storico particolarmente importante, si attiva un alert e la procedura di scarto del pacchetto di archiviazione avviene solo previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo rilasciata al produttore secondo quanto previsto dalla normativa vigente in materia.

Pertanto, Santer Reply procederà allo scarto dei pacchetti di archiviazione del Cliente dal sistema di conservazione solo qualora ciò sia stato esplicitamente richiesto dal Cliente (secondo gli accordi definiti nell'allegato " ***Specificità del Contratto***"), dandone comunque preventiva informativa a mezzo PEC.

Torna al Sommario

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

Al fine di raggiungere un soddisfacente grado d'interoperabilità nei processi di migrazione, la struttura dell'indice del pacchetto di archiviazione viene realizzata da Santer Reply in conformità con quanto previsto dallo standard "Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali", ossia dalla norma UNI 11386 (SInCRO).

Ciò garantisce l'Azienda relativamente alla sua piena libertà, nel momento in cui lo decidesse, di rivolgersi ad altri fornitori senza alcun rischio di interpretazione delle informazioni conservate nei VdC.

Ulteriori garanzie sono assicurate dalle certificazioni conseguite: ISO 27001:2013 e ISO 9001:2008.

Torna al Sommario

8 IL SISTEMA DI CONSERVAZIONE

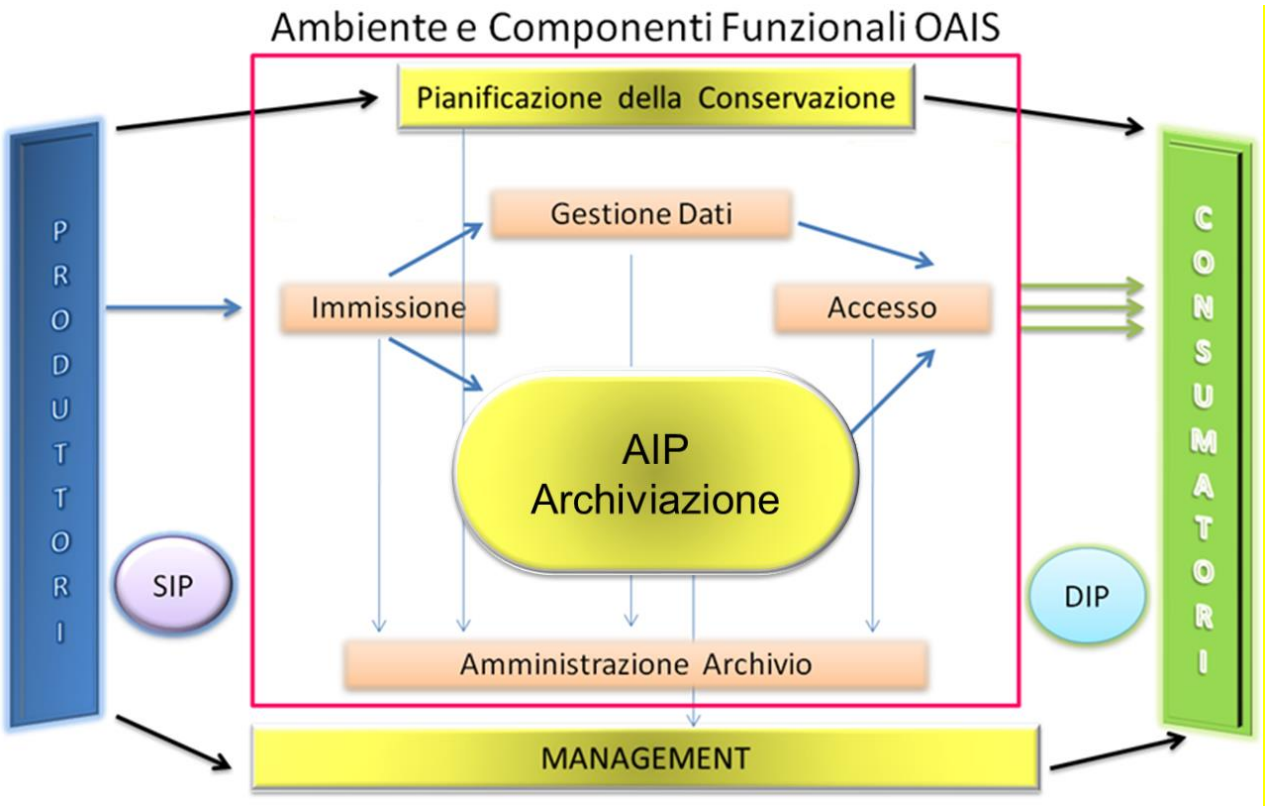
Nel presente capitolo vengono affrontate e descritte le componenti logiche, tecnologiche e fisiche coinvolte nel sistema di conservazione, con particolare attenzione agli aspetti di sicurezza ed alle procedure adottate per garantire la massima qualità del servizio erogato.

Torna al Sommario

8.1 Componenti Logiche

Le entità funzionali relative al Sistema di Conservazione ed al suo funzionamento possono essere riassunte nel modello OAIS di seguito rappresentato:

Figura 6 – Modello OAIS



Immissione

L'immissione dei dati si articola attraverso le fasi di:

- Presa in carico oggetti
- Verifica di quanto ricevuto

- Interventi di conversione
- Estrazione e creazione di metadati
- Trasferimento dell'informazione inviata e dei metadati associati al sistema per l'archiviazione

Archiviazione

L'Archiviazione è caratterizzata da :

- Affidabilità e funzionalità dei sistemi di immagazzinamento (storage)
- Integrità e fruibilità a lungo termine delle sequenze di bit stream che compongono i dati conservati
- Procedure di verifica di errore
- Politiche di recupero da disastro (disaster recovery) per mitigare gli effetti di eventi catastrofici

Gestione

La Gestione consiste in:

- Manutenzione dei database di cui è responsabile
- Esecuzione di ricerche e produzione di rapporti in risposta alle richieste provenienti da altre componenti funzionali dell'OAIS
- Aggiornamento del database non appena arrivino nuove informazioni o quando l'informazione esistente venga modificata o cancellata

Pianificazione

La Pianificazione consiste nella progettazione della strategia di conservazione dell'OAIS sia della sua revisione in risposta a cambiamenti tecnologici riguardanti oggetti archiviati.

Accesso

L'accesso si compone delle seguenti fasi:

- Elaborazione delle richieste ricevute relative al posseduto dall'OAIS

- Inoltro della richiesta al Data Management e la presentazione della risposta (ad esempio, una serie di risultati) all'utente
- Coordinamento tra il recupero dell'informazione e la consegna del contenuto richiesto
- Inoltro della richiesta all'Archival Storage e preparazione dell'oggetto digitale per la consegna

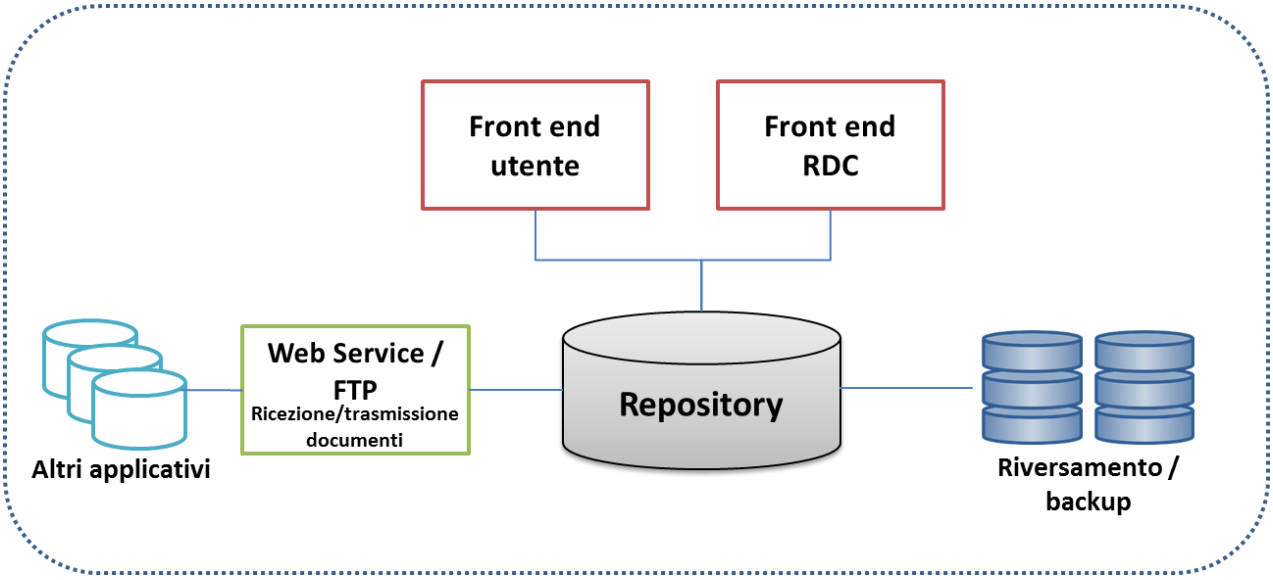
Amministrazione

L'Amministrazione consiste nel:

- Coordinamento delle attività degli altri cinque servizi di alto livello dell'OAIS.
- Interazione con i produttori (ad esempio la negoziazione degli accordi per la presentazione dei documenti)
- Interazione con gli utenti (per esempio, assistenza)
- Interazione con il Management (per esempio, l'implementazione e il mantenimento delle politiche e degli standard di archiviazione)
- Supervisione dei sistemi di archiviazione e di accesso, del monitoraggio delle prestazioni di sistema, e del coordinamento degli aggiornamenti del sistema.

Di seguito sono rappresentate le componenti che stanno alla base di quanto sopra descritto e di cui si compone il sistema di conservazione:

Figura 7 - Componenti Logiche del sistema



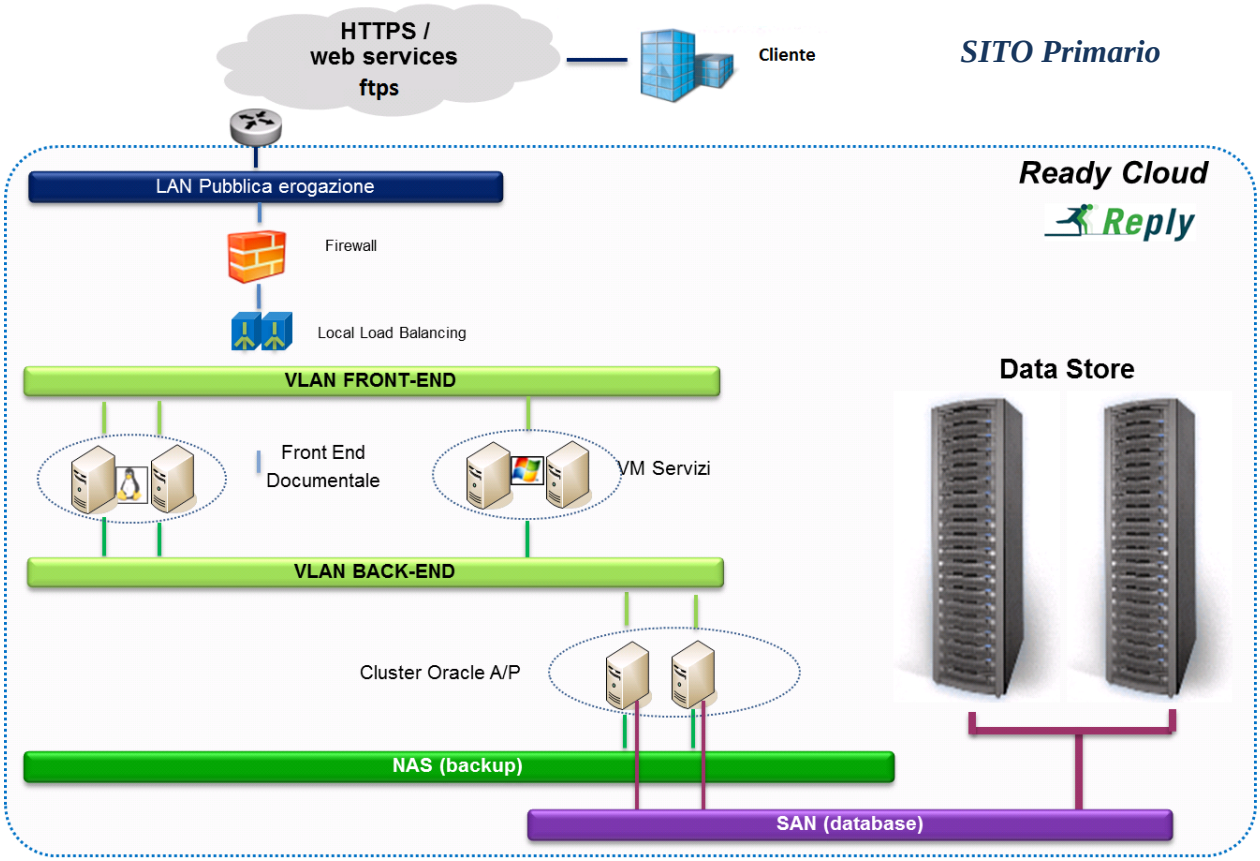
- **Repository documentale** che permette la memorizzazione sicura di tutti i documenti riversati
- **Interfaccia web per utente finale** con funzioni di ricerca, consultazione, esibizione dei documenti conservati
- **Interfaccia per Responsabile della Conservazione** (o delegato) con funzioni di amministrazione, conservazione, verifica, firma elettronica massiva
- **Interfaccia di tipo WEB SERVICE/FTP** per permettere integrazioni con altri sistemi per quanto riguarda la ricezione e trasmissione dei documenti presenti nel sistema.
- **Sistema di Riversamento e Backup** che permette la duplicazione ed il backup dei pacchetti conservati

Torna al Sommario

8.2 Componenti Tecnologiche

Di seguito lo schema infrastrutturale con le componenti SW e HW previste per l'erogazione del servizio:

Figura 8 - Componenti tecnologiche del sistema



Il "**Repository documentale**", ovvero il sistema dove fisicamente vengono memorizzati tutti i documenti è sviluppato su Oracle Database Enterprise Edition (11G). I documenti con l'insieme di metadati associati sono memorizzati all'interno di colonne di tipo "Blob" su tablespace cifrate. Ciò permette sia la cifratura del dato che la garanzia di consistenza ed integrità delle informazioni. Sia il documento che i metadati sono memorizzati nello stesso sistema (Oracle) che garantisce attraverso le funzionalità proprie del motore (Oracle Advanced Security) il rispetto di tutte le normative in termini di sicurezza e privacy. La configurazione del sistema è di scalabile (Oracle RAC). L'aumento delle capacità di elaborazione è gestita mediante l'aggiunta di "nodi".

L' "**Interfaccia web per l'utente finale**" consente all'utente di effettuare le normali operazioni di ricerca, consultazione, esibizione dei documenti conservati nonché documenti relativi al rapporto di versamento, indice del pacchetto di archiviazione etc. È sviluppata in PHP (HTML5, JQuery). L'autenticazione avviene attraverso la gestione utenti di Oracle o via protocollo LDAP.

L' "**Interfaccia per Responsabile della Conservazione**" è sviluppata in ambiente PHP, Microsoft C# . Essa consente di espletare le operazioni in carico al RDC o delegato.

L' "**Interfaccia WEB SERVICE**" è sviluppata in PHP e permette la cooperazione applicativa con altri sistemi.

il Sistema di Conservazione mette a disposizione dei web services per le operazioni di "presa in carico del documento" e per la successiva interrogazione sullo stato della conservazione ("info conservazione").

Attraverso il web service "wsDocPreCar" il sistema riceve in input il documento, il suo hash ed i metadati ad esso associati.

Il flusso applicativo, in sintesi, consiste nei seguenti passi:

- calcolo dell'hash (sha1) del file da inviare
- preparazione xml metadati
- invio del file (base64) con hash e metadati (xml in base64)
- ricezione risposta da parte del sistema di conservazione.

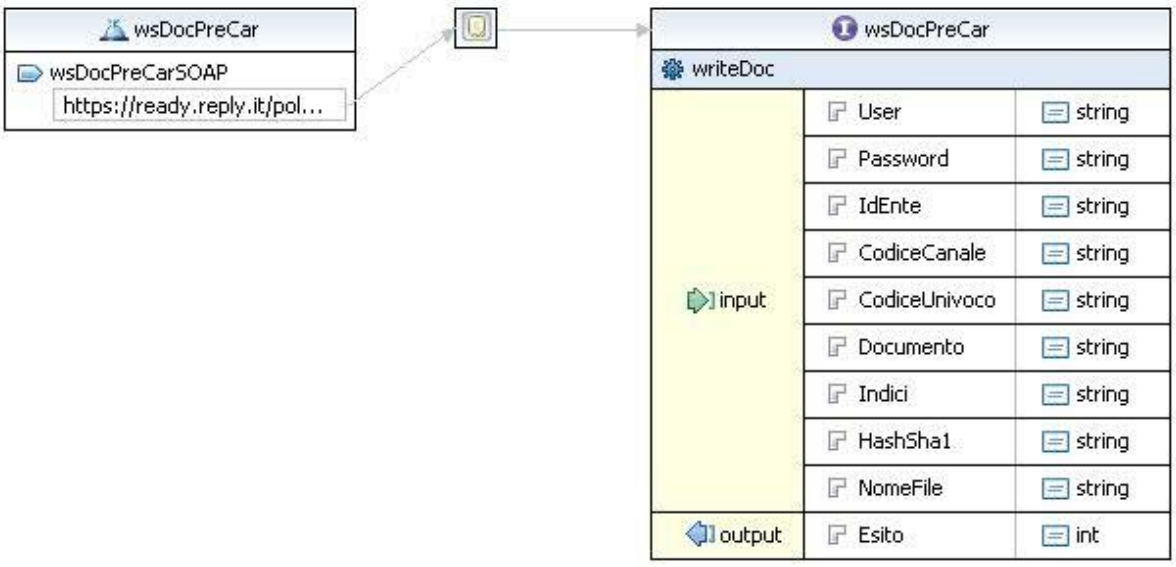
I servizi messi a disposizione sono:

- wsDocPreCar (presa in carico del documento)
- wsDocInfCon (info conservazione)

Torna al Sommario

8.2.1 Servizio wsDocPrecar

Figura 9 - servizio wsDocPrecar



Il sistema "richiedente" deve effettuare una chiamata al servizio **wsDocPreCar** per la richiesta di conservazione con i seguenti parametri di input:

PARAMETRO	DESCRIZIONE
User	User fornita da Reply per il servizio
Password	Password fornita da Reply per il servizio
IdEnte	Codice che identifica il sistema emittente (azienda)
CodiceCanale	Codice che identifica il canale sistema emittente
CodiceUnivoco	codice univoco documento fattura (id definito da sistema richiedente nella "presa in carico")
Documento	Documento in base64 (pdf, p7m, ecc...)
Indici	Documento in base64 contenente XML con metadati associati al file
HashSha1	Hash calcolato del contenuto del file
NomeFile	Nome del file

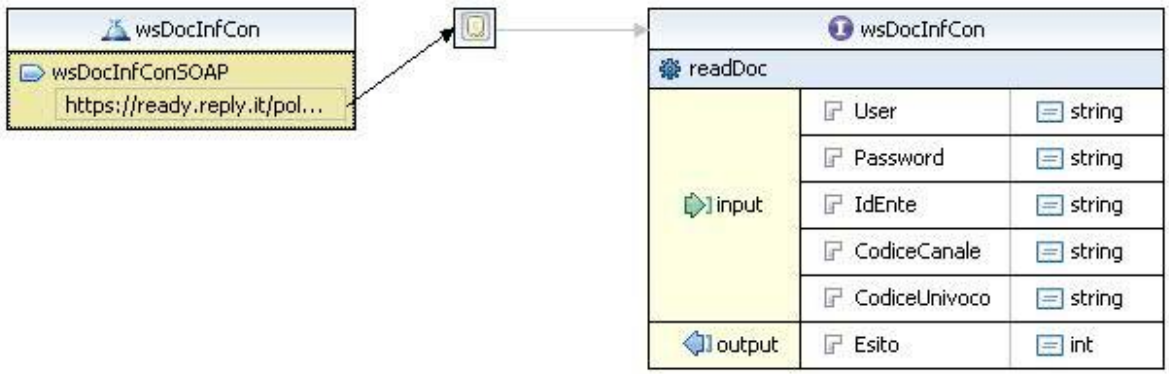
output del servizio

PARAMETRO	DESCRIZIONE
Esito	Esito chiamata (0=ok, 1...N=errore codificato in tabella errori)

Torna al Sommario

8.2.2 Servizio wsDocInfCon

Figura 10 - servizio wsDocInfCon



Il sistema "richiedente" deve effettuare una chiamata al servizio **wsDocInfCon** per avere informazioni sullo stato del documento:

con i seguenti parametri di input:

PARAMETRO	DESCRIZIONE
User	User fornita da Reply per il servizio
Password	Password fornita da Reply per il servizio
idEnte	Codice che identifica il sistema emittente
codiceCanale	Codice che identifica il canale sistema emittente
codiceUnivoco	codice univoco documento fattura (id definito da sistema richiedente nella "presa in carico")

output del servizio

PARAMETRO	DESCRIZIONE
Esito	0=Conservato, (1...n vedere tabella allegata)

Il Sistema di Riversamento permette il riversamento dei pacchetti di archiviazione su altro supporto (hard disk, dvd etc.) e può avvenire sia in maniera schedulata che "on demand".

I backup vengono effettuati giornalmente. In particolare:

- Viene eseguito un backup full del database Oracle + archivelog ogni giorno, più un ulteriore backup degli archivelog a metà giornata.
- Il database viene salvato con lo strumento RMAN.
- La politica di backup è: 1 backup full alla settimana + backup incrementale giornaliero
- La retention è di 28 giorni.
- Tutti gli accessi al database (amministrativi e non) vengono tracciati tramite Toll (tool custom di Telecom) che riversa le informazioni su syslog-ng
- Le copie di backup vengono conservate su nastro in appositi armadi ignifughi

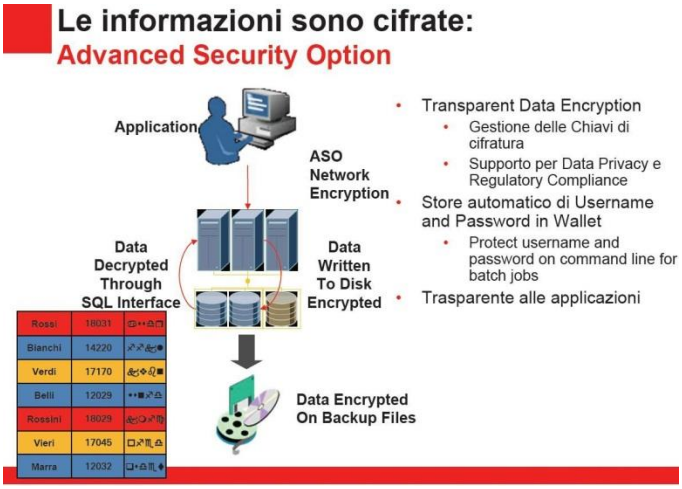
Torna al Sommario

8.2.3 Sicurezza del sistema

Il sistema ***Reade.Legal*** adotta delle particolari soluzioni che consento il filtraggio nativo delle informazioni in base all'utente che si collega al sistema. Tale filtro viene effettuato tramite logiche applicative che vengono direttamente "cablate" nella base dati. Tutte le informazioni vengono inoltre criptate per evitare la lettura non autorizzata delle informazioni anche a fronte di copie di sicurezza.

In particolare, le soluzioni adottate sono:

Figura 11 – Sicurezza del sistema



Virtual Private Database (VPD) che fornisce un meccanismo di controllo degli accessi a livello di records di una tabella. In tal modo si possono gestire gli utenti e le azioni che essi possono compiere all'interno del database dati i privilegi associati al suo nome utente e al suo ruolo, concedendo oppure negando l'accesso a particolari oggetti del database e assicurando così la protezione dei dati sensibili.

Oracle Advanced Security (ASO). Ai fini della tutela della privacy, i controlli di accesso devono garantire che i dati non possano essere rivelati accidentalmente o senza autorizzazione. Per garantire ciò viene utilizzato ASO che consente di cifrare in modo trasparente tutti i dati delle applicazioni, durante la permanenza nel database e nel momento in cui lasciano il database nella rete o tramite copie di backup.

Torna al Sommario

8.3 Componenti Fisiche

Il Sistema di Conservazione di Santer Reply, si basa su una infrastruttura resa disponibile tramite un Internet Data Center. Il sito primario, dove risiede il sistema di conservazione, è ubicato in :

- Data Center di Rozzano (MI) Viale Toscana 3

Il Data Center ha la certificazione ISO-27001 ed è dotato di sistemi evoluti di controllo degli accessi interni ed esterni, di rilevamento allagamenti-incendi e di continuità elettronica.

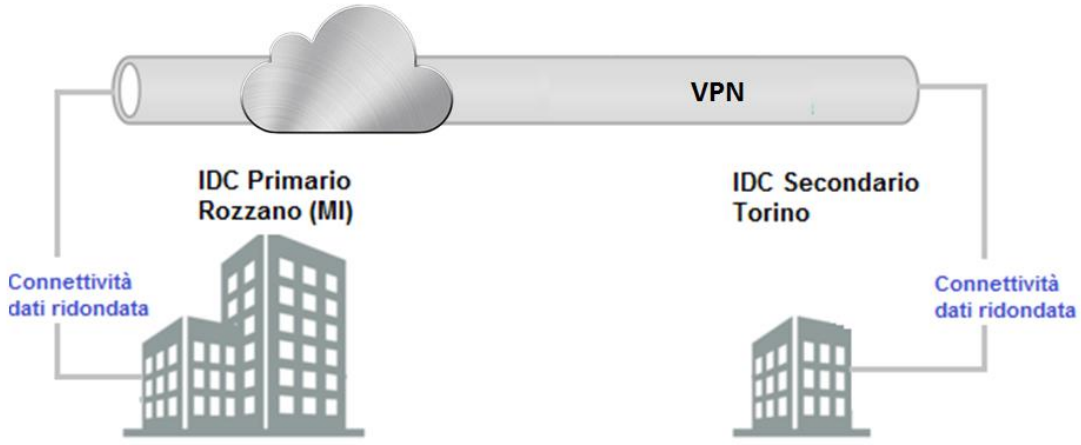
Il sito secondario è ubicato presso il data center di Reply in Torino.

Le caratteristiche del datacenter secondario sono del tutto assimilabili a quelle del datacenter primario, e consentono l'erogazione del servizio di conservazione nel caso non fosse disponibile il sito primario.

I Data center sono collegati tra loro tramite una rete di interconnessione, che risulta strutturalmente composta da:

- linee ad altissima capacità (2,5 Gbps) lungo le dorsali con maggior traffico di interscambio;
- linee a larga banda (155 Mbps) sempre in configurazione ridondata

Figura 12 - Schema iDC



Torna al Sommario

8.3.1 Business Continuity

Di seguito viene riportata una proposta di **Business Continuity Plan** adottati da Santer Reply . In particolare nel caso si verifichino i seguenti eventi:

- Conduzione sistemi IT - indisponibilità uffici
- Conduzione sistemi IT - interruzione servizi sistemistici (outsourcer)
- Indisponibilità sede fornitore servizi cartacei
- Blocco servizio IT causa danni software
- Indisponibilità personale

SINTESI ATTIVITÀ	RESPONSABILITÀ	DESCRIZIONE ATTIVITÀ
Rilevazione e dichiarazione crisi		
Comunicazione evento	- Tutti	Avvisare il Responsabile UO nel caso in cui si verifichi un evento negativo che può comportare la interruzione per più ore dei servizi interni o di quelli erogati ai clienti: - indisponibilità uffici - indisponibilità fornitore servizi cartacei - interruzione servizi di IAAS - blocco servizio causa danni software Nel caso in cui sia necessario evacuare una sede, il personale dovrà anche attenersi a quanto previsto dalle normative di emergenza per provvedere alla sicurezza delle persone
Prima valutazione evento	- Responsabile UO	Il Responsabile UO effettua una prima analisi dell'evento, eventualmente coinvolgendo DIR. Se l'evento ha comportato la distruzione di documenti cartacei non più recuperabili, Responsabile UO valuta l'ampiezza del danno.

SINTESI ATTIVITÀ	RESPONSABILITÀ	DESCRIZIONE ATTIVITÀ
Attivazione del Comitato della Crisi	- Responsabile UO	Se l'erogazione dei servizi ai clienti può essere interrotta per almeno mezza giornata, il Responsabile UO stabilisce un contatto con DIR in modo da coordinare le attività di gestione della crisi A seconda della durata prevista dell'interruzione e dalla sua causa, se maggiore di 1 giorno, Responsabile UO richiede la disponibilità dei siti alternativi (per gli operatori dell'unità organizzativa e dei fornitori, se il caso): • via Koch a Milano in caso di indisponibilità degli uffici • via Koch a Milano in caso di indisponibilità dei siti o dei servizi dei fornitori
Prime attività in caso di crisi		
Contattare gli operatori	- Responsabile UO	Se si è stabilito di attivare i servizi presso il sito alternativo di Milano, il Responsabile UO contatta gli operatori necessari per le attività, affinché si dirigano prontamente presso il sito di via Koch 1/4 a Milano: • Manutenzione servizi: 2 persone Il Responsabile UO ha disponibile l'elenco delle persone da contattare con i riferimenti. Vedere allegato per competenze personale.
Contattare i fornitori	- Responsabile UO	Il Responsabile UO dovrà stabilire con i fornitori le modalità di ripristino delle attività in emergenza, eventualmente mettendo a disposizione una sede di Santer. Il Responsabile UO e il suo delegato ha disponibile l'elenco dei fornitori da contattare con i riferimenti. Eventualmente, il Responsabile UO ricerca fornitori alternativi.

SINTESI ATTIVITÀ	RESPONSABILITÀ	DESCRIZIONE ATTIVITÀ
Comunicazione alla clientela	- Responsabile UO	Il Responsabile UO stabilisce cosa comunicare ai clienti: • "il servizio è interrotto per cause di forza maggiore e lo ripristineremo in x giorni; questi sono i nostri numeri per contattarci in questa fase di emergenza" • in caso di perdita di documenti non più recuperabili, aggiornamento • in caso di avvio di sistema IT di Disaster Recovery, concordare le modalità di riconfigurazione dei sistemi IT del cliente per il nuovo indirizzamento E' importante che i clienti siano chiamati il prima possibile, ma comunque dopo aver analizzato correttamente la situazione. Il Responsabile UO e il suo delegato hanno disponibile l'elenco dei clienti da contattare.
Avvio dei lavori presso il sito alternativo	- Operatori - Responsabile UO	Gli operatori contattati si trasferiscono presso il sito alternativo, iniziano i lavori di ripristino e aggiornano il Responsabile UO almeno ogni 2 ore.
Verifica correttezza dell'operatività in emergenza	- Operatori - Responsabile UO	Gli operatori, per ciascun servizio ripristinato, ne verificano le funzionalità e aggiornano il Responsabile UO, che aggiorna DIR.
Erogazione servizi in emergenza		
Ripristino attività IT	- Operatori - Responsabile UO	Il Responsabile UO, dopo aver verificato l'avvio dei servizi, richiede agli altri operatori di dirigersi presso il sito alternativo o di attivare le connessioni da altra sede e di erogare il servizio. Il Responsabile UO informa i clienti del riavvio dei servizi e spiegano loro eventuali limitazioni (per esempio: modifica numeri di telefono o riduzione delle prestazioni).
Ritorno alla normalità		

SINTESI ATTIVITÀ	RESPONSABILITÀ	DESCRIZIONE ATTIVITÀ
Attivazione procedura di ritorno alla normalità	- Responsabile UO - DIR - Capogruppo	DIR, il Responsabile UO e la Capogruppo valutano le modalità per ritornare alla normalità. Saranno considerati i seguenti punti: • predisposizione di piani di dettaglio per il rientro • valutazione dei dati persi e delle modalità di recupero • gestione delle interruzioni programmate e loro comunicazione agli utenti e alle parti interessate • comunicazione con le parti interessate
Chiusura dello stato di crisi	- DIR	A seguito del ritorno alla normalità, Responsabile UO dichiara chiuso lo stato di crisi e lo comunica a DIR. Al termine, il Responsabile UO, con DIR e la Capogruppo valuterà se intraprendere azioni di richiesta rimborso danni a valere sulla copertura assicurativa dell'incidente.

Torna al Sommario

8.4 Procedure di gestione e di evoluzione

Il sistema di conservazione *Ready.Legal* è stato progettato in modo da poter rispondere al meglio alle esigenze di natura: Legale Normativa, della Sicurezza delle Informazioni, della Continuità e della Sostenibilità Operativa.

La gestione del Sistema viene condotta in conformità agli standard di qualità e di sicurezza adottati da Santer Reply e formalizzati negli standard internazionali:

- **ISO 9001:2008**
- **ISO 27001:2013**

In particolare, Santer, promuove un approccio per processi nello sviluppo, attuazione e miglioramento del sistema di gestione per la qualità, al fine di accrescere la soddisfazione del cliente mediante l'osservanza dei requisiti del cliente stesso. Lo schema di riferimento è quello del miglioramento continuo, attraverso una corretta gestione delle risorse, la definizione di piani di

miglioramento e la verifica della loro attuazione ed attraverso un forte coinvolgimento dell'alta direzione aziendale, al fine di garantirne l'effettiva attuazione.

Le procedure del Sistema di Gestione della Qualità, le procedure del Sistema di Gestione della Sicurezza delle Informazioni, inclusi gli aspetti relativi alla sicurezza logica, fisica ed organizzativa di Santer costituiscono l'insieme di tutte le procedure con cui il sistema di conservazione viene gestito. Tali procedure, sono integrate da un gruppo di lavoro dedicato, composto tra gli altri dal Responsabile della Conservazione, il Responsabile della Funzione Archivistica di Conservazione, il Responsabile alla Sicurezza dei Sistemi per la Conservazione, il Responsabile Trattamento Dati, il Responsabile dei Sistemi Informativi per la Conservazione, il Responsabile Sviluppo e Manutenzione del Sistema di Conservazione, appositamente preposto alla verifica dell'evoluzione normativa ed al tempestivo adeguamento delle procedure e degli strumenti tecnici e tecnologici del sistema di conservazione.

9 MONITORAGGIO E CONTROLLI

Nel seguente capitolo vengono descritte le procedure di monitoraggio delle funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie.

Torna al Sommario

9.1 Procedure di monitoraggio

Santer Reply assicura la verifica periodica del corretto funzionamento del sistema di conservazione. Tale controllo avviene tramite apposite funzionalità di monitoraggio del software. Esse mostrano l'esito delle operazioni automatiche eseguite sul sistema di conservazione come la generazione dei pacchetti di archiviazione, job di firma, la chiusura dei pacchetti di archiviazione e la verifica dell'integrità degli archivi.

Oltre a questo tipo di verifica, vengono controllati anche i log delle operazioni medesime al fine di avere maggiore certezza di quanto effettivamente eseguito dal sistema di conservazione. Tutte queste informazioni sono controllate per ciascun singolo cliente.

Il controllo del buon funzionamento del sistema di conservazione avviene inoltre, monitorando il buon funzionamento fisico delle macchine nonché del software di base adibiti alla gestione del sistema di conservazione.

Torna al Sommario

9.2 Verifica dell'integrità degli archivi

Il Responsabile del servizio di conservazione o un suo delegato, provvede alla verifica periodica, con cadenza non superiore all'anno, della corretta funzionalità del sistema nella sua completezza, eseguendo un ciclo programmato di test e benchmark.

Verrà prodotto apposito verbale riportante l'elenco dei test effettuati e l'esito riscontrato. La verifica di integrità degli archivi è assolta in vari momenti:

- all'atto della sottoscrizione del Pacchetto;
- all'atto del riversamento diretto del Pacchetto;
- in modalità interattiva (a discrezione del responsabile della conservazione o suo delegato);
- temporizzata sull'intero registro dei Pacchetti (siano essi "aperti" o "chiusi").

Se il Pacchetto si trova in uno stato "chiuso" viene verificata sia la componente DB che la componente File System. In particolare i controlli saranno i seguenti:

- la prima è una verifica di quadratura generale rispetto ai numeri memorizzati all'atto della creazione del Pacchetto (Numero totale documenti presenti nel Pacchetto, Byte totale dei documenti inclusi nel Pacchetto).
- se il risultato è corretto, si procede alla verifica di dettaglio prendendo ogni singolo documento incluso nel Pacchetto e verificando che l'hash memorizzato sul DB coincida con l'hash ricalcolato in tempo reale.
- viene controllata in tempo reale l'integrità del file indice del pacchetto di Archiviazione verificando l'hash di riferimento salvato all'atto della creazione del Pacchetto con quello risultante dal campo CLOB che lo contiene all'atto della verifica
- si procede poi alla verifica di corrispondenza tra i valori hash dei singoli documenti salvati all'interno del file indice del pacchetto di Archiviazione con quanto memorizzato nel DB.

La verifica di integrità, come ogni altra fase del processo di conservazione è soggetta a tracciatura tramite LOG. Tutti i LOG delle attività vengono memorizzati con data e ora degli eventi. E' possibile stampare dei tabulati con i risultati delle verifiche. Al verificarsi di eventuali errori viene inviato un Alert a tutti i soggetti designati, contenente i dettagli dell'errore riscontrato.

Torna al Sommario

9.3 Soluzioni adottate in caso di anomalie

Nel caso in cui, a seguito delle verifiche di monitoraggio delle funzionalità del sistema e delle verifiche periodiche sull'integrità degli archivi, dovessero emergere delle anomalie, il sistema di conservazione innesca un sistema di Alert automatico a tutti i soggetti designati (incluso il Responsabile del sistema di Conservazione e il Responsabile dei sistemi informativi per la conservazione).

A seguito di un'attenta analisi per l'individuazione del problema, a seconda del tipo di anomalia riscontrata, il team addetto, procede all'implementazione delle opportune correzioni che risolvano il problema. A conclusione di tutto, verrà formalizzato un verbale in cui si darà evidenza al Soggetto Produttore del tipo di anomalia rilevata e della relativa gestione da parte del Conservatore.

Qualsiasi tipo di anomalia riscontrata viene inoltre tracciata all'interno del Registro degli Incidenti di Sicurezza o nel Registro delle non Conformità, in ottemperanza alle procedure previste dalla certificazione ISO 27001:2013 e ISO 9001:2008.

Torna al Sommario