Manuale di Conservazione

di Insiel S.p.A.

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	21/04/2016	Stefano Cociancich	Responsabile funzione archivistica di conservazione
	21/04/2016	Massimiliano Occhioni	Responsabile dello sviluppo e della manutenzione del sistema di conservazione
Verifica	18/09/2018	Elisabetta Bombardieri	Responsabile servizio di conservazione
Approvazione	18/09/2018	Elisabetta Bombardieri	Responsabile servizio di conservazione

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
2	28/10/2010	Vedi IIT-CS-RG-06 Registro delle versioni del manuale IIT-CS-MP-01	
3	20/12/2011	Vedi IIT-CS-RG-06 Registro delle versioni del manuale IIT-CS-MP-01	
4	12/10/2012	Vedi IIT-CS-RG-06 Registro delle versioni del manuale IIT-CS-MP-01	
5	17/07/2013	Vedi IIT-CS-RG-06 Registro delle versioni del manuale IIT-CS-MP-01	
6	16/12/2013	Vedi IIT-CS-RG-06 Registro delle versioni del manuale IIT-CS-MP-01	
7	08/10/2015	Vedi IIT-CS-RG-06 Registro delle versioni del manuale IIT-CS-MP-01	
8	21/04/2016	Adozione modello AgID	
9	01/06/2016	Par. 5.1 Adeguamento denominazioni Strutture a seguito adozione nuovo organigramma aziendale in vigore dal 01/06/2016	
10	21/07/2016	Integrazioni richieste da AgID con nota prot. 19048 del 20/07/2016	
11	25/08/2016	Ulteriori integrazioni relative al monitoraggio	
12	05/09/2016	Modifiche chieste da Agid con e-mail d.d. 05/09/2016 14:28	
13	30/11/2016	Aggiunto schema sito di Disaster Recovery e classe documentale LDO (Lettera Dimissione Ospedaliera)	
14	26/07/2017	Par. 2 Adeguamento definizioni di “documento informatico” e di “firma digitale” al Dlgs 26 agosto 2016 Par. 4 Aggiornamento nomine Responsabile del Servizio Par. 5.1 Adeguamento denominazioni Strutture in seguito all’adozione del nuovo organigramma aziendale	

		Par. 5.2 Adeguamento attività in capo alle strutture organizzative in seguito all'adozione del nuovo organigramma aziendale Par. 6 Aggiunta classe documentale DECC "Decreti Consiglio regionale" Par. 6 Aggiornamento metadati classe documentale FASC "Fascicoli informatici" Par. 7.3 Aggiornamento in seguito a change tecnologico per passaggio a supporti di backup LTO6 Par. 7.6 Aggiunta ulteriori dettagli su trasmissione del pacchetto di distribuzione Par. 8 Modifica prodotti operativi infrastrutturali utilizzati	
15	12/01/2018	Par. 2 Aggiunto sigla DPO per "Data Protection Officer" Par. 3 Aggiunto "Regolamento (UE) 2016/679" Par. 5.1 e par. 5.2 Modifica organigramma e strutture organizzative in seguito a nomina del DPO di Insiel	
16	18/09/2018	Par. 4 Aggiornamento nomina Responsabile trattamento dati personali Par. 5.1 e par. 5.2 Modifica organigramma e strutture organizzative in seguito all'aggiornamento nomine a Par. 4 Par. 6 Aggiunta formato PNG Par. 6 Semplificazione elenco e descrizioni classi documentali Par. 7.2 Descrizione trattamento automatico anomalie Par. 9.2 Modifica modalità verbalizzazione verifiche backup	

INDICE DEL DOCUMENTO

1. SCOPO E AMBITO DEL DOCUMENTO

Nel presente manuale sono descritte l'organizzazione, le modalità operative e l'infrastruttura per mezzo delle quali Insiel S.p.A., in qualità di soggetto affidatario della Regione Friuli Venezia Giulia, gestisce il servizio di conservazione nel rispetto della normativa vigente e in accordo a quanto previsto dal Disciplinare di servizio sottoscritto con la medesima.

Gli Enti del territorio regionale, che intendono avvalersi del servizio, devono nominare un proprio Responsabile della conservazione, redigere un proprio Manuale della conservazione e sottoscrivere un Disciplinare con la Regione Friuli Venezia Giulia; negli allegati al proprio manuale l'Ente indica le tipologie documentali (classi di documenti) la cui conservazione è affidata alla Regione. I modelli per il contratto di servizio vengono messi a disposizione all'indirizzo http://autonomielocali.regione.fvg.it/aall/opencms/AALL/SIAL/Conservazione_sostitutiva/index.html.

1.1 Gestione del documento

La revisione del documento viene eseguita con cadenza almeno semestrale ed è in carico al Responsabile del servizio di conservazione, al Responsabile della funzione archivistica di conservazione, al Responsabile del trattamento dei dati personali, al Responsabile della sicurezza dei sistemi per la conservazione, al Responsabile dei sistemi informativi per la conservazione e al Responsabile dello sviluppo e della manutenzione del sistema di conservazione.

Torna al sommario

2. TERMINOLOGIA (GLOSSARIO, ACRONIMI)

Glossario dei termini e Acronimi	
AgID	Agenzia per l'Italia Digitale (ex AIPA ex CNIPA ex DigitPA)
AOO	Area Organizzativa Omogenea
CA	Certification Authority (indica l'Autorità di certificazione di un dispositivo di firma digitale)
CAD	Codice dell'amministrazione digitale
DICOM	Digital Imaging and COmmunications in Medicine è uno standard che definisce I criteri per la comunicazione, la visualizzazione, l'archiviazione e la stampa di informazioni biomediche
DPCM	Decreto Presidente del Consiglio dei Ministri
DGR	Deliberazione della Giunta Regionale
DPR	Decreto Presidente della Repubblica
DPO	Data Protection Officer
HTTP	Hyper Text Transfer Protocol. Protocollo di trasferimento di un ipertesto tra client e server
HTTPS	Secure Hyper Text Transmission Protocol. Protocollo sviluppato per cifrare e decifrare le pagine Web inviate dal server ai client

OAIS	ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
PDF	Portable Document Format
PKI	Public Key Infrastructure (infrastruttura necessaria per creare, gestire, conservare e revocare i certificati delle firme elettroniche basati su crittografia a chiave pubblica)
RCE	Responsabile della Conservazione dell'Ente
RSC	Responsabile del Servizio di Conservazione
RUPAR	Rete Unitaria Pubblica Amministrazione Regionale
SAQ	Servizio Assicurazione Qualità
SFTP	Secure File Transfer Protocol
SGD	Sistema di gestione documentale
SQI	Sistema Qualità Insiel
SSL	Secure Socket Layer. standard per la comunicazione interprocesso utilizzato dal protocollo TCP/IP su internet.
TSA	Time Stamping Authority
URL	Uniform Resource Locator (indica univocamente una risorsa internet)
UTC	Coordinated Universal Time (Tempo coordinato universale)
XML	eXtensible Markup Language, ovvero linguaggio che definisce un meccanismo sintattico per estendere o controllare il significato di altri linguaggi marcatori
XSD	XML Schema Definition, specifica tecnica per la generazione di file XML
certificato qualificato	certificato elettronico conforme ai requisiti di cui all'allegato I alla direttiva 1999/93/CE e all'art.28 del CAD rilasciato da un certificatore che risponde ai requisiti di cui all'allegato II della medesima direttiva (CAD, art.1 lettera f)
chiave asimmetrica	coppia di chiavi collegate logicamente, una privata ed una pubblica, tali per cui le sottoscrizioni con chiave privata possono essere lette dalla corrispondente chiave pubblica senza che dalla pubblica si possa mai risalire alla privata
classe documentale	tipologia di unità documentaria ai fini della conservazione
comunità designata	gruppo di potenziali utilizzatori che devono essere mantenuti in condizione di accedere e comprendere l'informazione conservata
conformance statement	il conformance statement è un documento autocertificativo in cui il

	costruttore indica tutti i campi DICOM implementati sulla macchina, dettagliando anche quelli proprietari. La condivisione di questi documenti di conformità permette l'integrazione fra le apparecchiature.
conservazione a lungo termine	azione di mantenimento delle informazioni a lungo termine, in una forma indipendente e comprensibile da una comunità di riferimento e corredate da evidenze che ne supportino l'autenticità (ISO14721, definizione "conservazione a lungo termine").
dicomdir	file che fornisce l'indice e le informazioni di riepilogo per tutti i file DICOM presenti sul supporto considerato
disponibilità	requisito che esprime la certezza di poter utilizzare un'informazione o risorsa. Le informazioni devono essere sempre accessibili a chi ne ha diritto senza restrizioni non riconducibili a norme di legge (CAD, art 1 lettera o)
dispositivo di firma sicuro	particolare componente hardware in cui è possibile attivare la propria chiave privata mediante accesso con modalità note e riconducibili solo al legittimo proprietario.
documento	rappresentazione analogica o digitale di atti, fatti e dati, intelligibili direttamente o attraverso un processo di elaborazione elettronica, che ne consenta la presa di conoscenza a distanza di tempo (DM 23 gennaio 2004 Modalità di assolvimento degli obblighi fiscali)
documento informatico	documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. (CAD, art 1 lettera p)
firma digitale	particolare firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra di loro, che consentono, al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, di rendere manifesta e di verificare l'autenticità e l'integrità di un documento informatico o di un insieme di documenti informatici. (CAD, art 1 lettera s)
firma elettronica	insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica (CAD, art 1 lettera q)
firma elettronica avanzata	insieme di dati in forma elettronica allegati oppure connessi ad un documento informatico, che consentono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo e che sono collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati. (CAD, art 1 lettera q bis)
firma elettronica qualificata	firma elettronica avanzata, basata su un certificato elettronico qualificato e creata mediante un dispositivo di firma sicuro (CAD,

	art 1 lettera r)
funzione di hash	una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti (DPCM 22 febbraio 2013)
impronta	sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione di un'opportuna funzione di hash (DPCM 22 febbraio 2013)
lungo termine	un intervallo di tempo sufficientemente ampio da dover considerare l'impatto prodotto sulle informazioni conservate, dai cambiamenti delle tecnologie o della comunità di utenti. Tale periodo si estende indefinitamente nel futuro. (ISO14721, definizione di "lungo termine")
marca temporale	il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo (DPCM 22 febbraio 2013, art.1 lettera i)
modality	nel contesto delle immagini medicali, per modality si intende una qualsiasi apparecchiatura utilizzata per acquisire immagini del corpo (es.: radiografie, risonanze magnetiche)
riservatezza delle informazioni	requisito di sicurezza che esprime la protezione da divulgazione non autorizzata delle informazioni, che devono essere accessibili direttamente o indirettamente solo alle persone che ne hanno diritto e sono espressamente autorizzate a conoscerle.
secondary capture	la Secondary Capture (SC) è la produzione di un' immagine in formato DICOM a partire da un formato non-DICOM.
sop class	lo standard DICOM si basa sul modello concettuale definito "Service Object Pair" (SOP) e definisce gli attributi propri di un oggetto quale un ricovero, un paziente o un'immagine e le operazioni che su di essi si possono eseguire. La combinazione di un oggetto e dei servizi corrispettivi prende il nome di SOP, mentre l'insieme delle SOP relative ad un unico oggetto costituisce una SOP Class.
sistema	applicazione/servizio che deve essere disponibile agli aventi diritto in termini di esercizio e disponibilità dell'informazione
disponibilità richiesta ad un sistema	tempo in cui il sistema deve essere utilizzabile in conformità alle funzionalità previste, esclusi i tempi programmati per la manutenzione, rispetto alle ore concordate per l'esercizio
periodo criticità servizio	data/periodo in cui il dato o il servizio deve essere tassativamente erogato per esigenze specifiche del business, quali scadenze o

	presentazione dei dati
tempo di ripristino richiesto (Recovery Time Objective)	tempo entro il quale un processo informatico ovvero il Sistema Informativo primario deve essere ripristinato dopo un disastro o una condizione di emergenza (o interruzione), al fine di evitare conseguenze inaccettabili.
obiettivo temporale di recupero (Recovery Point Objective)	indica la perdita dati tollerata: rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di un evento imprevisto.

Torna al sommario

3. NORMATIVA E STANDARD DI RIFERIMENTO

3.1 Normativa di riferimento

Alla data l'elenco dei principali riferimenti normativi italiani in materia, ordinati secondo il criterio della gerarchia delle fonti, è costituito da:

- 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 Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Disciplinare che regola i rapporti tra Regione FVG e Insiel approvato con Delibera di Giunta n° 667 del-11 aprile 2013;
- L.R. 14 luglio 2011, n. 9 – "Disciplina del sistema informativo integrato regionale del Friuli Venezia Giulia";
- Accordo di servizi quadro fra Regione Friuli Venezia Giulia e Insiel s.p.a rep. 8655 del 28/12/2005 per la gestione del sistema informativo regionale;
- Legge 15 marzo 1997, n. 59, (comma 2 dell'articolo 15) - recita: "Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge.";
- Decreto Legislativo 23 gennaio 2002, n. 10 – Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche;
- Decreto Legislativo. 7 marzo 2005, n. 82 - "Codice dell'amministrazione digitale" e s.m.i.;
- Decreto Legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali

(G.U. n. 174 del 29 luglio 2003);

- Decreto del Presidente della Repubblica del 28/12/2000 n. 445 “Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa”;
- Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013 Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 Regole tecniche in materia di conservazione ai sensi degli articoli 20, comma 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 N. 65 del 10 aprile 2014 AGID e allegati Modalità per l’accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82;
- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

Torna al sommario

3.2 Standard di riferimento

Si riportano di seguito gli standard di riferimento seguiti nell'implementazione del sistema di conservazione di INSIEL ed elencati nell’allegato 3 delle Regole Tecniche in materia di Sistema di conservazione con indicazione delle versioni aggiornate

- 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 RESPONSABILITÀ

ruoli	nominativo	attività di competenza	periodo nel ruolo	eventuali deleghe
Responsabile del servizio di conservazione	dott.ssa Elisabetta Bombardieri	definire e attuare le politiche complessive del sistema di conservazione, nel governo del sistema e nella definizione delle caratteristiche e dei requisiti del sistema in conformità alla normativa vigente. Egli garantisce la corretta erogazione del servizio di conservazione all'ente produttore, gestisce le convenzioni, definisce gli aspetti tecnico-operativi e valida i disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione del servizio di conservazione.	dal 17/07/2017	
	dott.ssa Luisa Semolic	c.s.	dal 10/09/2015 al 17/07/2017	
	dott.ssa Elisabetta Bombardieri	c.s.	dal 01/07/2009 al 09/09/2015	
Responsabile Sicurezza dei sistemi per la conservazione	sig. Alessandro Masolin	rispettare e monitorare i requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza, nel segnalare eventuali difformità al RSC e nell'individuare e pianificare le necessarie azioni correttive	dal 16/05/2016	
Responsabile funzione archivistica di conservazione	ing. Stefano Cociancich	definire e gestire il processo di conservazione e in particolare di stabilire le modalità di trasferimento, di acquisizione, di verifica dell'integrità, di descrizione archivistica dei documenti e delle aggregazioni documentali trasmessi dall'Ente produttore; il Responsabile della funzione archivistica definisce gli insiemi di metadati che caratterizzano documenti e fascicoli	dal 16/05/2016	

		informatici inviati in conservazione; egli si occupa inoltre di definire le modalità di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato, di monitorare il processo di conservazione e di effettuare l'analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione; collabora con l'Ente produttore ai fini del trasferimento in conservazione dei documenti e gestisce i rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza		
Responsabile trattamento dati personali	dott. Andrea Soro	garantire il rispetto delle vigenti disposizioni in materia di trattamento dei dati personali e nel vigilare che il trattamento dei dati affidati dai Clienti avvenga nel rispetto delle istruzioni impartite dal titolare, con garanzia di sicurezza e di riservatezza	dal 12/09/2018	
	dott. Andrea Crosilla	c.s.	dal 06/07/2015 al 12/09/2018	
Responsabile sistemi informativi per la conservazione	sig. Alessandro Masolin	gestire l'esercizio delle componenti hardware e software del sistema di conservazione, nel monitorare il mantenimento dei livelli di servizio (SLA) concordati con l'Ente produttore, nel segnalare le eventuali difformità degli SLA al RSC, individuando e pianificando le necessarie azioni correttive; egli inoltre pianifica lo sviluppo delle infrastrutture tecnologiche del sistema di conservazione, controlla e verifica eventuali servizi erogati da terzi	dal 16/05/2016	
Responsabile sviluppo e manutenzione del sistema di conservazione	dott. Massimiliano Occhioni	progettare e coordinare lo sviluppo e la manutenzione delle componenti hardware e software del sistema di conservazione, nel pianificare e monitorare i progetti di sviluppo del sistema di conservazione, monitorare gli SLA relativi alla manutenzione del sistema di conservazione, interfacciarsi con l'Ente produttore relativamente alle modalità tecniche di trasferimento dei documenti e dei fascicoli informatici e relativi formati; egli si occupa inoltre dell'evoluzione	dal 16/05/2016	

		tecnologica hardware e software, delle eventuali migrazioni verso nuove piattaforme tecnologiche e di gestire lo sviluppo di siti web e portali connessi al servizio di conservazione		

Torna al sommario

5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Organigramma

Insiel S.p.A. nasce nel 1974 come Società Finsiel in partnership con la Regione Autonoma Friuli Venezia Giulia, che nel 2005 acquisisce il 100% del pacchetto azionario. A partire dal 2008, a seguito del D. Lgs. n. 223/2006 (Decreto Bersani), con lo scorporo delle attività di mercato, Insiel svolge servizi in regime di "in house providing". I rapporti tra Regione e Insiel, in attuazione a quanto previsto dall'art. 9 della Legge Regionale 14 luglio 2011, n. 9, sono regolati da un Disciplinare, redatto ed approvato dalla Giunta Regionale con propria delibera n. 667 dell'11 aprile 2013; in esso vengono definiti la tipologia ed il contenuto dei servizi resi da Insiel, tra cui la conservazione dei documenti prodotti dall'Amministrazione.

La Regione Friuli Venezia Giulia mette a disposizione il sistema di conservazione, svolto per tramite di Insiel, agli Enti del territorio regionale. Per accedervi, essi devono, in via preliminare, aver nominato un proprio Responsabile della conservazione, adottato il manuale di conservazione e sottoscritto un disciplinare di servizio con l'Amministrazione regionale. L'informazione conservata è resa disponibile alla Comunità designata, formata dai Responsabili della conservazione degli enti, dai loro eventuali delegati e dall'Autorità giudiziaria. Il processo si svolge secondo le modalità contenute nel presente documento.

Nella seguente tabella sono riportate le strutture organizzative coinvolte nel servizio di conservazione con le descrizioni dei rispettivi compiti assegnati.

Struttura	**Inquadramento**	**Compito**
Application Services – Servizi di conservazione	Divisione Service Delivery & Operations	Gestire l'operatività del Servizio di conservazione
Data Center Services	Divisione Service Delivery & Operations	Gestire l'infrastruttura della server farm
Network Operation Center	Divisione Service Delivery & Operations	Gestire l'infrastruttura di rete
IT Security	Direzione Central Staff	Occuparsi delle problematiche della sicurezza IT
Facility Management & Logistics	Direzione Central Staff	Erogare il servizio di trasferimento dei supporti di backup dal Data Center di Trieste alla sede di Udine
Direzione HR & Organization	Direzione generale	Gestire le problematiche inerenti il

Development		trattamento dei dati
Organization, Training & Development	Direzione Human Resources & Organization Development	Gestire la formazione
Health Demand	Health & Social Care	In caso di DR collaborare per l'attivazione del sito secondario

Torna al sommario

5.2 Strutture organizzative

Struttura	Attività
Application Services – Servizi di conservazione	• Definizione e gestione di processi, gestione degli aspetti archivistici, sviluppo di classi documentali, analisi archivistica per lo sviluppo di nuove funzionalità; • attivazione del servizio di conservazione (a seguito della sottoscrizione di un disciplinare da parte dell'Ente richiedente e della Regione FVG) • acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento; • preparazione e gestione del pacchetto di archiviazione; • preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta; • scarto dei pacchetti di archiviazione; • chiusura del servizio di conservazione (al termine di un contratto)
Data center services	• conduzione e manutenzione del sistema di conservazione; • monitoraggio del sistema di conservazione; • change management;
IT Security	• verifica periodica di conformità a normativa e standard di riferimento • change management
Facility Management & Logistics	• collabora alla gestione del pacchetto di distribuzione qualora l'Ente ne richieda la consegna tramite corriere • gestisce il trasporto dei supporti contenenti le copie di backup
Direzione HR & Organization Development	• gestione del trattamento dei dati personali nel rispetto delle normative europee e nazionali in materia di privacy • verifica periodica di conformità a normativa e standard di riferimento • change management

Health Demand	• in caso di disastro collabora nelle attività di ripristino del servizio sul sito secondario

Torna al sommario

6. OGGETTI SOTTOPOSTI A CONSERVAZIONE

Oggetti conservati

Le caratteristiche degli oggetti sottoposti a conservazione sono descritte negli allegati ai manuali della conservazione della Regione e degli Enti affidatari, che costituiscono parte integrante dei disciplinari di servizio. Sul sito della Regione, nella sezione dedicata alle autonomie locali, all'indirizzo

http://autonomielocali.regione.fvg.it/aall/opencms/AALL/SIAL/

sono disponibili informazioni generali sulla conservazione, è scaricabile la documentazione per aderire al servizio e le tipologie documentali per le quali il servizio è disponibile.

I formati dei documenti informatici accettati dal sistema di conservazione sono quelli elencati nell'allegato 2 al DPCM 3 dicembre 2013, recante "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". Al fine di soddisfare quanto richiesto dall' articolo 21, comma 2, del d.lgs. 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale - CAD), e, come espressamente previsto dalle regole tecniche di cui al DPCM 22 febbraio 2013, i documenti informatici non devono contenere macroistruzioni o codici eseguibili.

Per ogni classe documentale è configurabile un insieme di formati accettati, scelti tra i seguenti:

FORMATI AMMESSI

Estensione	Tipo MIME
PDF	application/pdf
GIF	image/gif
JPG e JPEG	image/jpeg
PNG	image/png
TIF e TIFF	image/tiff
BMP	image/bmp
RTF	application/rtf
TXT	text/plain
XML	application/xml, text/xml
HTML	text/html
DOCX (Office Open	application/vnd.openxmlformats-
XLSX (Office Open XML)	application/vnd.openxmlformats-
ODT	application/vnd.oasis.opendocument.text
ODP	application/vnd.oasis.opendocument.presentation
ODG	application/vnd.oasis.opendocument. graphics
ODB	application/vnd.oasis.opendocument.base
ODS	application/vnd.oasis.opendocument.spreadsheet

EML (rfc822, rfc2822)	message/rfc822 e message/rfc2822

MARCHE TEMPORALI

Estensione	Descrizione
TSR	TimeStampResponse
TST e TS	TimeStampToken

FORMATI DI SOTTOSCRIZIONE

Estensione	Descrizione
P7M	Busta di firma CAdES-BES
PDF	Firma PAdES
XML	Firma XAdES

FORMATI CHE CONTENGONO ALTRI FILE

Estensione	Descrizione
TSD	TimeStampedData
M7M	File firmato digitalmente e marcato

FORMATI PARTICOLARI PER DOCUMENTI SANITARI

Estensione	Descrizione
CDA2	Estensione del documento clinico strutturato CDA
DCM	Standard DICOM

Il RCE ha facoltà di estendere la tipologia di formati accettati.

Nel verificare altri formati, quali, ad esempio XLS (Microsoft Excel), DOC (Microsoft Word) e PPT (Microsoft PowerPoint), il sistema, durante la fase di presa in carico, genera un'anomalia e i documenti vengono accettati dal sistema previa specifica autorizzazione da parte del RCE.

Il sistema di conservazione rende disponibili i software necessari alla visualizzazione del contenuto dei documenti informatici conservati.

Nel sistema è stato introdotto il concetto di classe documentale, mediante il quale si definiscono le caratteristiche di una tipologia di unità documentaria soggetta a conservazione e si individuano le informazioni necessarie a qualificarla e identificarla univocamente. Essa ha metadati propri e parametri specifici di comportamento ai fini della conservazione. Alcuni metadati, o attributi di base, sono comuni a tutte classi documentali, mentre altri sono specifici e quindi caratteristici di ciascuna classe. L'unità minima presa in carico dal sistema di conservazione è composta un documento informatico principale e da un set minimo di metadati.

L'erogazione del servizio di conservazione, riferita alla tipologia di utenza, può presentare caratteristiche particolari, nel senso che non tutte le classi documentali sono disponibili a tutti gli Enti. In particolare per le Amministrazioni del Servizio Sanitario Regionale sono rese disponibili alcune classi

appositamente definite per poter gestire documenti di particolare natura, come ad esempio i referti e le immagini diagnostiche.

Per ogni classe documentale sono definite contrattualmente le tempistiche di generazione dei pacchetti di versamento, la composizione delle unità documentarie, i formati ed i relativi visualizzatori.

I metadati relativi ad un'unità documentaria sono gestiti tramite un file di formato xml, il cosiddetto file xml dichiarativo, che entra a far parte del pacchetto di versamento predisposto dal produttore, con funzione primaria di indice del pacchetto di versamento.

La Regione FVG ha definito un insieme di metadati comuni a tutte le tipologie documentali, che vengono memorizzati nella prima parte dell'indice del pacchetto di versamento. La restante parte è variabile e il contenuto dipende dalla particolare classe documentale trattata. Nel seguito sono presenti le descrizioni dei contenuti specifici propri di ogni classe documentale.

Torna al sommario

Classe "ADWEB": atti deliberativi e determine

Comprende i documenti informatici delle unità documentarie riferite agli atti amministrativi (ad es. le delibere adottate da organi collegiali, gli atti monocratici quali le determine, ecc.). E' prevista la presenza di almeno un documento informatico firmato digitalmente per ciascuna unità documentaria.

Torna al sommario

Classe "CONTRATTO": contratti

Comprende i documenti informatici delle unità documentarie riferite sia agli Atti pubblici Amministrativi digitali ricevuti dagli Ufficiali Roganti che ai contratti in generale.

Torna al sommario

Classe "COREL": corrispondenza elettronica

Comprende i documenti informatici delle unità documentarie registrate sui registri di protocollo generale associati alle Aree Organizzative Omogenee degli Enti.

Torna al sommario

Classe "FLUSSO_FATTURE" e "FATTURA": fattura elettronica

In questa tipologia ricadono le fatture elettroniche così come individuate dal Decreto Ministeriale 3 aprile 2013, n. 55. Le fatture elettroniche sono veicolate dal Sistema di Intercambio (SdI), ai sensi del D.M. 7 marzo 2008, emanato in attuazione della legge 24 dicembre 2007, n. 244; il SdI è controllato dall'Agenzia delle Entrate che si occupa di riceverle dal mittente e recapitarle al destinatario, generando le opportune ricevute/notifiche.

Le fatture sono contenute in file di formato XML (cosiddetti flussi di fatture), firmati digitalmente con firma XAdES o CAdES; ogni file può contenere una o più fatture (più fatture con la stessa intestazione).

Sono istituite le classi documentali:

- **FLUSSO FATTURE**: documento firmato digitalmente, veicolato dal Sistema di Interscambio;
- **FATTURA**: dal punto di vista amministrativo/gestionale, assume rilevanza la singola fattura, in quanto legata a contratti/ordini. Le singole fatture, estratte dai flussi firmati in entrata e in uscita, sono sottoposte al processo di conservazione una volta conclusa la ricezione e/o l'invio di tutti gli esiti previsti dalla normativa. Alla fattura, rappresentata da un file XML non firmato, vengono allegate le ricevute e le notifiche prodotte dal Sistema di Interscambio.

I file XML non necessitano di particolari visori, infatti è possibile visualizzarne il contenuto con un semplice editor di testo. Tuttavia esse referenziano, al loro interno, fogli di stile pubblicati sul sito istituzionale www.fatturaPA.gov.it, che vengono, anch'essi, sottoposti al processo di conservazione.

Torna al sommario

Classe "REGPROT": registro giornaliero di protocollo

In questa tipologia ricadono i documenti digitali prodotti ai sensi dell'art. 7, comma 5 del DPCM 3 dicembre 2013 "Regole tecniche per il protocollo informatico ai sensi dell'articolo 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005".

Torna al sommario

Classi documentali per la conservazione dei mandati informatici

In questa tipologia di documenti ricadono i flussi prodotti dalla gestione del mandato informatico; le tipologie documentali generate negli scambi dell'Ente con la propria Tesoreria sono:

- **Mandati di pagamento** – classe documentale **MAND**
- **Reversali di incasso** – classe documentale **REVE**
- **Ricevute applicative su mandati di pagamento** – classe documentale **RA_MAND**
- **Ricevute applicative su reversali di incasso** – classe documentale **RA_REVE**
- **Provvisori di uscita** – classe documentale **PROVV_MAND**
- **Provvisori di incasso** – classe documentale **PROVV_REVE**

Torna al sommario

Classe "PD": atti per la Giunta regionale

Classe documentale riservata all'Amministrazione Regionale. Comprende i documenti informatici delle unità documentarie riferite agli atti di competenza della Giunta regionale che pervengono al Segretariato Generale per l'iscrizione all'ordine del giorno delle sedute di Giunta: proposte di deliberazione, disegni di legge, relazioni ecc.

Torna al sommario

Classe “DGR”: atti della Giunta regionale

Classe documentale riservata all’Amministrazione Regionale. Comprende i documenti informatici delle unità documentarie riferite agli atti adottati dalla Giunta regionale: delibere e generalità di Giunta.

Torna al sommario

Classe “DPREG”: decreti del Presidente della Regione

Classe documentale riservata all’Amministrazione Regionale. Comprende i documenti informatici delle unità documentarie riferite ai Decreti del Presidente della Regione.

Torna al sommario

Classe “BUR”: Bollettino Ufficiale della Regione

Classe documentale riservata all’Amministrazione Regionale. Comprende i documenti informatici delle unità documentarie riferite al Bollettino Ufficiale della Regione ed i suoi supplementi (ordinari o straordinari).

Torna al sommario

Classe “DEC: Decreti Assessori e Direttori

Classe documentale riservata all’Amministrazione Regionale. Comprende i documenti informatici delle unità documentarie riferite ai Decreti degli Assessori, dei Direttori e più in generale dei soggetti delegati.

Torna al sommario

Classe “DECC: Decreti del Consiglio regionale

Classe documentale riservata all’Amministrazione Regionale. Comprende i documenti informatici delle unità documentarie riferite ai Decreti prodotti nell’ambito del Consiglio regionale del Friuli Venezia Giulia.

Torna al sommario

Classe “ODG”: Ordini del giorno e convocazioni sedute della Giunta regionale

Classe documentale riservata all’Amministrazione Regionale. Comprende i documenti informatici delle unità documentarie riferite alle lettere di convocazione delle sedute della Giunta regionale ed i relativi ordini del giorno.

Torna al sommario

Classe “PV”: Processi verbali della Giunta regionale

Classe documentale riservata all’Amministrazione Regionale. Comprende i documenti informatici delle unità documentarie riferite ai processi verbali delle sedute della Giunta regionale.

Torna al sommario

Classe “RAPP”: Rapporti di prova dell’ARPA

Classe documentale riservata all’Amministrazione Regionale. Comprende i documenti informatici delle unità documentarie riferite ai rapporti di prova dell’Agenzia Regionale per la Protezione Ambientale.

Torna al sommario

Classe “REFE”: Referti

Classe documentale riservata alle strutture del Sistema Sanitario Regionale. Comprende i documenti informatici delle unità documentarie relative ai referti prodotti dalle Aziende Sanitarie/Ospedaliere.

Torna al sommario

Classe “LDO”: Lettera Dimissione Ospedaliera

Classe documentale riservata alle strutture del Sistema Sanitario Regionale. Comprende i documenti informatici delle unità documentarie relative alle lettere di dimissione ed alle lettere di trasferimento di pazienti tra reparti prodotte dalle Aziende Sanitarie/Ospedaliere.

Torna al sommario

Classe “STUDI”: immagini diagnostiche

Classe documentale riservata alle strutture del Sistema Sanitario Regionale. Comprende i documenti informatici delle unità documentarie riferite agli studi prodotti in formato digitale dai sistemi PACS. Negli studi, oltre alle immagini, sono presenti anche il file dicomdir e, talvolta, anche un file con l’evidenza delle immagini selezionate dal medico in fase di refertazione.

Qualora i processi di conservazione rilevino, all’interno degli Studi, la presenza di oggetti proprietari, salveranno, tra i metadati della serie, anche l’identificativo della SOP Class proprietaria e la sua descrizione. E’ necessario sottolineare che il contenuto informativo di tali oggetti potrà essere reso intelligibile esclusivamente mediante dispositivi compatibili a quelli che li hanno prodotti, dispositivi non disponibili durante l’esibizione. E’ opportuno che nel caso di oggetti proprietari, il medico refertante produca sempre le secondary capture.

Torna al sommario

Classe “FASC”: Fascicoli informatici

In questa classe documentale ricadono le aggregazioni logiche di documenti informatici gestite mediante la metodologia della fascicolazione elettronica.

Torna al sommario

6.1 Pacchetto di versamento

In base a quanto descritto per le classi documentali, il pacchetto di versamento, oltre che dall’unità documentaria (documento principale e allegati) è costituito da un file xml suddiviso concettualmente in due sezioni: la prima comprende metadati comuni a tutte le classi documentali, la seconda comprende i metadati specifici definiti per la classe documentale trattata. Si riporta a titolo di esempio un pacchetto relativo alla classe documentale REGPROT.

```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<conservazione xmlns="http://conservazione.insiel.it/regprot_1_0">
  <chiaveAccesso>XXXXXXXXXXXXXXXXXXXXXX</chiaveAccesso>
  <ente>XXXXXX</ente>
  <area>PROTOCOLLO</area>
  <ufficio>CORRISPONDENZA</ufficio>
  <idClasseDoc>REGPROT</idClasseDoc>
  <verClasseDoc>1.0</verClasseDoc>
  <idDocSgd>REGPROT-PROTGEN-GEN-2015-20151010</idDocSgd>
  <versSgd>0</versSgd>
  <dataInvio>2015-10-11+02:00</dataInvio>
  <origTipo>D</origTipo>
  <allegati>
    <allegato>
      <nomeOriginale>registroProtocollo.xml</nomeOriginale>
      <improntaTipo>SHA-256</improntaTipo>
      <impronta>346C485338F31F2828389E09042D4ECA21BFD1AC787BD5BFA1667C2A3E34ECB5</impronta>
      <mime>text/xml</mime>
      <mime_ver>NA</mime_ver>
    </allegato>
    <allegato>
      <nomeOriginale>registroProtocolloAggiornamenti.xml</nomeOriginale>
      <improntaTipo>SHA-256</improntaTipo>
      <impronta>346C485338F31F2828389E09042D4ECA21BFD1AC787BD5BFA1667C2A3E34ECB5</impronta>
      <mime>text/xml</mime>
      <mime_ver>NA</mime_ver>
    </allegato>
  </allegati>
  <metadati>
    <codiceAOOREGPROT>XXXXXXXX</codiceAOOREGPROT>
    <descrizioneAOOREGPROT>Comune XXXXXXXXX</descrizioneAOOREGPROT>
    <codiceRegistroAOOREGPROT>XXX</codiceRegistroAOOREGPROT>
    <descrizioneRegistroAOOREGPROT>Protocollo generale</descrizioneRegistroAOOREGPROT>
    <annoREGPROT>2015</annoREGPROT>
    <dataREGPROT>2015-10-10+02:00</dataREGPROT>
    <tipoREGPROT></tipoREGPROT>
  </metadati>
</conservazione>
```

E’ previsto che tale file sia sottoscritto digitalmente dal produttore, anche con procedura massiva, a garanzia d’integrità dei metadati trasmessi al sistema di conservazione. Di seguito un esempio di rapporto di versamento:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<rdv:RdV xmlns:rdv="http://conservazione.insiel.it/rdv/" rdv:version="1.0"
rdv:url="http://conservazione.insiel.it/rdv/">
    <rdv:SelfDescription>
        <rdv:ID rdv:scheme="local">RDV_82744_1</rdv:ID>
```

```
    </rdv:SelfDescription>
    <rdv:FileGroup>
        <rdv:Label>33163197</rdv:Label>
        <rdv:File rdv:encoding="binary" rdv:format="application/x-pkcs7-mime">
            <rdv:ID>97535328</rdv:ID>
            <rdv:Path>33163197/xmlDichiarativo.xml.p7m</rdv:Path>
            <rdv:Hash rdv:function="SHA-
256">FE106F0731E80274F299B9DEBDF74ECE1E8AE3411C9CDBE4B9D29E40580FD09B</rdv:Hash>
            <rdv:Firmatario>
                <rdv:Version>3</rdv:Version>
                <rdv:IssuerDN>CN=Actalis Qualified Certificates CA G1,OU=Qualified
Certification Service Provider,O=Actalis S.p.A./03358520967,C=IT</rdv:IssuerDN>
                <rdv:SerialNumber>9157847794454628090</rdv:SerialNumber>
                <rdv:SubjectDN>DNQ=2303-1370975338808, CN=XXXX GGGGGG,
SERIALNUMBER=IT:HHHHSSS58T46L424A, GIVENNAME=XXXX, SURNAME=GGGGGG, O=INSIEL/00118410323,
C=IT</rdv:SubjectDN>
                <rdv:NotBefore>2015-10-21T16:46:25.000+02:00</rdv:NotBefore>
                <rdv:NotAfter>2018-09-18T00:00:25.000+02:00</rdv:NotAfter>
                <rdv:SigAlgName>SHA256WITHRSA</rdv:SigAlgName>
            </rdv:Firmatario>
        </rdv:File>
        <rdv:File rdv:encoding="binary" rdv:format="text/xml">
            <rdv:ID>97535329</rdv:ID>
            <rdv:Path>33163197/registroProtocollo.xml</rdv:Path>
            <rdv:Hash rdv:function="SHA-
256">EF9CB5D6BA5EF16EF3E129F1A01DC7D88B5AAE25CA349015FC83E09BF5088FC6</rdv:Hash>
        </rdv:File>
        <rdv:File rdv:encoding="binary" rdv:format="text/xml">
            <rdv:ID>97535330</rdv:ID>
            <rdv:Path>33163197/registroProtocolloAggiornamenti.xml</rdv:Path>
            <rdv:Hash rdv:function="SHA-
256">EF9CB5D6BA5EF16EF3E129F1A01DC7D88B5AAE25CA349015FC83E09BF5088FC6</rdv:Hash>
        </rdv:File>
    </rdv:FileGroup>
    <rdv:Process>
        <rdv:TimeReference>
            <rdv:TimeInfo>2016-02-22T04:20:58.900+01:00</rdv:TimeInfo>
        </rdv:TimeReference>
    </rdv:Process>
</rdv:RdV>
```

Ogni rapporto di versamento viene marcato temporalmente e conservato insieme al pacchetto di archiviazione.

Torna al sommario

6.2 Pacchetto di archiviazione

Si riporta nel seguito la struttura dell'Indice del Pacchetto di archiviazione adottato in conformità allo standard SInCRO UNI 11386:2010.

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns:sincro="http://www.uni.com/U3011/sincro/"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://www.uni.com/U3011/sincro/" elementFormDefault="qualified"
attributeFormDefault="qualified">
        <xs:annotation>
                <xs:documentation xml:lang="en">Definition of simple
types</xs:documentation>
        </xs:annotation>
        <xs:simpleType name="Label">
                <xs:restriction base="xs:string"/>
        </xs:simpleType>
        <xs:simpleType name="Path">
                <xs:restriction base="xs:anyURI"/>
        </xs:simpleType>
        <xs:simpleType name="Name">
                <xs:restriction base="xs:string"/>
        </xs:simpleType>
        <xs:simpleType name="Version">
```

```
                <xs:restriction base="xs:string"/>
        </xs:simpleType>
        <xs:simpleType name="Producer">
                <xs:restriction base="xs:string"/>
        </xs:simpleType>
        <xs:simpleType name="TimeInfo">
                <xs:restriction base="xs:dateTime"/>
        </xs:simpleType>
        <xs:simpleType name="FirstName">
                <xs:restriction base="xs:string"/>
        </xs:simpleType>
        <xs:simpleType name="LastName">
                <xs:restriction base="xs:string"/>
        </xs:simpleType>
        <xs:simpleType name="FormalName">
                <xs:restriction base="xs:string"/>
        </xs:simpleType>
        <xs:simpleType name="EmptyString">
                <xs:restriction base="xs:string">
                        <xs:maxLength value="0"/>
                </xs:restriction>
        </xs:simpleType>
        <xs:annotation>
                <xs:documentation xml:lang="en">Definition of attributes</xs:documentation>
        </xs:annotation>
        <xs:attribute name="version" type="xs:NMTOKEN" fixed="1.0"/>
        <xs:attribute name="url" type="xs:anyURI" fixed="http://www.uni.com/U3011/sincro/"/>
        <xs:attribute name="XMLScheme" type="xs:anyURI"/>
        <xs:attribute name="scheme" type="xs:string" default="local"/>
        <xs:attribute name="canonicalXML" type="xs:boolean"/>
        <xs:attribute name="function" type="xs:NMTOKEN" default="SHA-1"/>
        <xs:attribute name="extension" type="xs:NMTOKEN"/>
        <xs:attribute name="language" type="xs:language" default="it"/>
        <xs:attribute name="format" type="xs:string"/>
        <xs:attribute name="encoding">
                <xs:simpleType>
                        <xs:restriction base="xs:NMTOKEN">
                                <xs:enumeration value="7bit"/>
                                <xs:enumeration value="8bit"/>
                                <xs:enumeration value="base64"/>
                                <xs:enumeration value="binary"/>
                                <xs:enumeration value="quotedprintable"/>
                                <xs:enumeration value="xtoken"/>
                        </xs:restriction>
                </xs:simpleType>
        </xs:attribute>
        <xs:attribute name="normal" type="xs:dateTime"/>
        <xs:attribute name="type">
                <xs:simpleType>
                        <xs:restriction base="xs:NMTOKEN">
                                <xs:enumeration value="person"/>
                                <xs:enumeration value="organization"/>
                        </xs:restriction>
                </xs:simpleType>
        </xs:attribute>
        <xs:attribute name="otherRole" type="xs:string"/>
        <xs:attribute name="role">
                <xs:simpleType>
                        <xs:restriction base="xs:NMTOKEN">
                                <xs:enumeration value="PreservationManager"/>
                                <xs:enumeration value="Operator"/>
                                <xs:enumeration value="PublicOfficer"/>
                                <xs:enumeration value="Delegate"/>
                                <xs:enumeration value="OtherRole"/>
                        </xs:restriction>
                </xs:simpleType>
        </xs:attribute>
        <xs:annotation>
                <xs:documentation xml:lang="en">Definition of complex
types</xs:documentation>
        </xs:annotation>
        <xs:complexType name="EmbeddedMetadata">
                <xs:complexContent>
                        <xs:extension base="xs:anyType"/>
```

```
                </xs:complexContent>
        </xs:complexType>
        <xs:complexType name="Identifier">
                <xs:simpleContent>
                        <xs:extension base="xs:NMTOKEN">
                                <xs:attribute ref="sincro:scheme"/>
                        </xs:extension>
                </xs:simpleContent>
        </xs:complexType>
        <xs:complexType name="Agent_ID">
                <xs:simpleContent>
                        <xs:extension base="xs:string">
                                <xs:attribute name="scheme" use="required">
                                        <xs:simpleType>
                                                <xs:restriction base="xs:NMTOKEN">
                                                        <xs:enumeration
value="TaxCode"/>
                                                        <xs:enumeration
value="VATRegistrationNumber"/>
                                                        <xs:enumeration
value="NationalHealthCareAuthority"/>
                                                        <xs:enumeration
value="OtherScheme"/>
                                                </xs:restriction>
                                        </xs:simpleType>
                                </xs:attribute>
                                <xs:attribute name="otherScheme" type="xs:string"/>
                        </xs:extension>
                </xs:simpleContent>
        </xs:complexType>
        <xs:complexType name="Description">
                <xs:simpleContent>
                        <xs:extension base="xs:string">
                                <xs:attribute ref="sincro:language"/>
                        </xs:extension>
                </xs:simpleContent>
        </xs:complexType>
        <xs:complexType name="MoreInfo">
                <xs:choice>
                        <xs:element name="EmbeddedMetadata"
type="sincro:EmbeddedMetadata"/>
                        <xs:element name="ExternalMetadata" type="sincro:File"/>
                </xs:choice>
                <xs:attribute ref="sincro:XMLScheme" use="required"/>
        </xs:complexType>
        <xs:complexType name="Hash">
                <xs:simpleContent>
                        <xs:extension base="xs:string">
                                <xs:attribute ref="sincro:canonicalXML"/>
                                <xs:attribute ref="sincro:function" use="required"/>
                        </xs:extension>
                </xs:simpleContent>
        </xs:complexType>
        <xs:complexType name="PreviousHash">
                <xs:simpleContent>
                        <xs:extension base="sincro:Hash">
                                <xs:attribute name="relatedIdC" type="xs:NMTOKEN"
use="required"/>
                        </xs:extension>
                </xs:simpleContent>
        </xs:complexType>
        <xs:complexType name="CreatingApplication">
                <xs:sequence>
                        <xs:element name="Name" type="sincro:Name"/>
                        <xs:element name="Version" type="sincro:Version"/>
                        <xs:element name="Producer" type="sincro:Producer"/>
                </xs:sequence>
        </xs:complexType>
        <xs:complexType name="LawAndRegulations">
                <xs:simpleContent>
                        <xs:extension base="xs:string">
                                <xs:attribute ref="sincro:language"/>
                        </xs:extension>
                </xs:simpleContent>
```

```
        </xs:complexType>
        <xs:complexType name="SourceIdC">
                <xs:sequence>
                        <xs:element name="ID" type="sincro:Identifier"/>
                        <xs:element name="Path" type="sincro:Path" minOccurs="0"/>
                        <xs:element name="Hash" type="sincro:Hash"/>
                </xs:sequence>
        </xs:complexType>
        <xs:complexType name="SourceVdC">
                <xs:sequence>
                        <xs:element name="ID" type="sincro:Identifier"/>
                        <xs:element name="IdC_ID" type="sincro:Identifier"/>
                </xs:sequence>
        </xs:complexType>
        <xs:complexType name="VdCGroup">
                <xs:sequence>
                        <xs:element name="Label" type="sincro:Label"/>
                        <xs:element name="ID" type="sincro:Identifier" minOccurs="0"/>
                        <xs:element name="Description" type="sincro:Description"
minOccurs="0"/>
                </xs:sequence>
        </xs:complexType>
        <xs:complexType name="VdC">
                <xs:sequence>
                        <xs:element name="ID" type="sincro:Identifier"/>
                        <xs:element name="SourceVdC" type="sincro:SourceVdC"
minOccurs="0" maxOccurs="unbounded"/>
                        <xs:element name="VdCGroup" type="sincro:VdCGroup"
minOccurs="0"/>
                        <xs:element name="MoreInfo" type="sincro:MoreInfo"
minOccurs="0"/>
                </xs:sequence>
        </xs:complexType>
        <xs:complexType name="FileGroup">
                <xs:sequence>
                        <xs:element name="Label" type="sincro:Label" minOccurs="0"/>
                        <xs:element name="File" type="sincro:File"
maxOccurs="unbounded"/>
                        <xs:element name="MoreInfo" type="sincro:MoreInfo"
minOccurs="0"/>
                </xs:sequence>
        </xs:complexType>
        <xs:complexType name="File">
                <xs:sequence>
                        <xs:element name="ID" type="sincro:Identifier"/>
                        <xs:element name="Path" type="sincro:Path" minOccurs="0"/>
                        <xs:element name="Hash" type="sincro:Hash"/>
                        <xs:element name="PreviousHash" type="sincro:PreviousHash"
minOccurs="0"/>
                        <xs:element name="MoreInfo" type="sincro:MoreInfo"
minOccurs="0"/>
                </xs:sequence>
                <xs:attribute ref="sincro:encoding" default="binary"/>
                <xs:attribute ref="sincro:extension"/>
                <xs:attribute ref="sincro:format" use="required"/>
        </xs:complexType>
        <xs:complexType name="SelfDescription">
                <xs:sequence>
                        <xs:element name="ID" type="sincro:Identifier"/>
                        <xs:element name="CreatingApplication"
type="sincro:CreatingApplication"/>
                        <xs:element name="SourceIdC" type="sincro:SourceIdC"
minOccurs="0" maxOccurs="unbounded"/>
                        <xs:element name="MoreInfo" type="sincro:MoreInfo"
minOccurs="0"/>
                </xs:sequence>
        </xs:complexType>
        <xs:complexType name="NameAndSurname">
                <xs:sequence>
                        <xs:element name="FirstName" type="sincro:FirstName"/>
                        <xs:element name="LastName" type="sincro:LastName"/>
                </xs:sequence>
        </xs:complexType>
        <xs:complexType name="AgentName">
```

```
                <xs:choice>
                        <xs:element name="NameAndSurname" type="sincro:NameAndSurname"/>
                        <xs:element name="FormalName" type="sincro:FormalName"/>
                </xs:choice>
        </xs:complexType>
        <xs:complexType name="Agent">
                <xs:sequence>
                        <xs:element name="AgentName" type="sincro:AgentName"/>
                        <xs:element name="Agent_ID" type="sincro:Agent_ID" minOccurs="0"
maxOccurs="unbounded"/>
                        <xs:element name="MoreInfo" type="sincro:MoreInfo"
minOccurs="0"/>
                </xs:sequence>
                <xs:attribute ref="sincro:type" use="required"/>
                <xs:attribute ref="sincro:role" use="required"/>
                <xs:attribute ref="sincro:otherRole"/>
        </xs:complexType>
        <xs:complexType name="Process">
                <xs:sequence>
                        <xs:element name="Agent" type="sincro:Agent"
maxOccurs="unbounded"/>
                        <xs:element name="TimeReference" type="sincro:TimeReference"/>
                        <xs:element name="LawAndRegulations"
type="sincro:LawAndRegulations" minOccurs="0"/>
                        <xs:element name="MoreInfo" type="sincro:MoreInfo"
minOccurs="0"/>
                </xs:sequence>
        </xs:complexType>
        <xs:complexType name="TimeReference">
                <xs:choice>
                        <xs:element name="DetachedTimestamp"
type="sincro:DetachedTimeStamp"/>
                        <xs:element name="AttachedTimeStamp"
type="sincro:AttachedTimeStamp"/>
                        <xs:element name="TimeInfo" type="sincro:TimeInfo"/>
                </xs:choice>
        </xs:complexType>
        <xs:complexType name="AttachedTimeStamp">
                <xs:simpleContent>
                        <xs:extension base="sincro:EmptyString">
                                <xs:attribute ref="sincro:normal" use="required"/>
                        </xs:extension>
                </xs:simpleContent>
        </xs:complexType>
        <xs:complexType name="DetachedTimeStamp">
                <xs:simpleContent>
                        <xs:extension base="xs:anyURI">
                                <xs:attribute ref="sincro:normal" use="required"/>
                                <xs:attribute ref="sincro:encoding" default="binary"/>
                                <xs:attribute ref="sincro:format" use="required"/>
                        </xs:extension>
                </xs:simpleContent>
        </xs:complexType>
        <xs:complexType name="IdC">
                <xs:sequence>
                        <xs:element name="SelfDescription"
type="sincro:SelfDescription"/>
                        <xs:element name="VdC" type="sincro:VdC"/>
                        <xs:element name="FileGroup" type="sincro:FileGroup"
maxOccurs="unbounded"/>
                        <xs:element name="Process" type="sincro:Process"/>
                </xs:sequence>
                <xs:attribute ref="sincro:version"/>
                <xs:attribute ref="sincro:url"/>
        </xs:complexType>
        <xs:annotation>
                <xs:documentation xml:lang="en">Definition of root
element</xs:documentation>
        </xs:annotation>
        <xs:element name="IdC" type="sincro:IdC"/>
</xs:schema>
```

Al pacchetto d'archiviazione sono collegati i seguenti elementi "MoreInfo"

- **FileGroupMoreInfo.xsd**

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema xmlns:fgmi="http://conservazione.insiel.it/idc/filegroup/moreinfo/"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://conservazione.insiel.it/idc/filegroup/moreinfo/"
elementFormDefault="qualified" attributeFormDefault="qualified">
        <xs:element name="FileGroupMoreInfo">
                <xs:annotation>
                        <xs:documentation>idDocSgd, VersSgd, DataRegistrazione,
Riferimento al rapporto di versamento</xs:documentation>
                </xs:annotation>
                <xs:complexType>
                        <xs:choice>
                                <xs:sequence>
                                        <xs:element name="IdDocSgd" type="xs:string"/>
                                        <xs:element name="VersSgd"
type="xs:nonNegativeInteger"/>
                                        <xs:element name="DataRegistrazione"
type="xs:date"/>
                                        <xs:element name="RapportodiVersamento"
type="xs:string"/>
                                </xs:sequence>
                                <xs:element name="idRapportodiVersamento"
type="xs:string"/>
                        </xs:choice>
                </xs:complexType>
        </xs:element>
</xs:schema>
```

- **FileMoreInfo.xsd**

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:fgfmi="http://conservazione.insiel.it/idc/filegroup/file/moreinfo/"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://conservazione.insiel.it/idc/filegroup/file/moreinfo/"
elementFormDefault="qualified" attributeFormDefault="qualified">
        <xs:simpleType name="Version">
                <xs:restriction base="xs:integer"/>
        </xs:simpleType>
        <xs:simpleType name="IssuerDN">
                <xs:restriction base="xs:string"/>
        </xs:simpleType>
        <xs:simpleType name="SerialNumber">
                <xs:restriction base="xs:integer"/>
        </xs:simpleType>
        <xs:simpleType name="SubjectDN">
                <xs:restriction base="xs:string"/>
        </xs:simpleType>
        <xs:simpleType name="NotBefore">
                <xs:restriction base="xs:dateTime"/>
        </xs:simpleType>
        <xs:simpleType name="NotAfter">
                <xs:restriction base="xs:dateTime"/>
        </xs:simpleType>
        <xs:simpleType name="SigAlgName">
                <xs:restriction base="xs:string"/>
        </xs:simpleType>
        <xs:simpleType name="Nota">
                <xs:restriction base="xs:string"/>
        </xs:simpleType>
        <xs:complexType name="Firmatario">
                <xs:sequence>
                        <xs:element name="Version" type="fgfmi:Version"/>
                        <xs:element name="IssuerDN" type="fgfmi:IssuerDN"/>
                        <xs:element name="SerialNumber" type="fgfmi:SerialNumber"/>
```

```
                        <xs:element name="SubjectDN" type="fgfmi:SubjectDN"/>
                        <xs:element name="NotBefore" type="fgfmi:NotBefore"/>
                        <xs:element name="NotAfter" type="fgfmi:NotAfter"/>
                        <xs:element name="SigAlgName" type="fgfmi:SigAlgName"/>
                        <xs:element name="Nota" type="fgfmi:Nota" minOccurs="0"
maxOccurs="unbounded"/>
                        <xs:element name="Firmatario" type="fgfmi:Firmatario"
minOccurs="0" maxOccurs="unbounded"/>
                </xs:sequence>
        </xs:complexType>
        <xs:element name="FileMoreInfo">
                <xs:annotation>
                        <xs:documentation> Tipologia File (allegato, rapporto di
versamento, marca rapporto di versamento, xml dichiarativo)</xs:documentation>
                </xs:annotation>
                <xs:complexType>
                        <xs:sequence>
                                <xs:element name="TipologiaFile">
                                        <xs:simpleType>
                                                <xs:restriction base="xs:string">
                                                        <xs:enumeration
value="rapporto di versamento"/>
                                                        <xs:enumeration
value="marca rapporto di versamento"/>
                                        <xs:enumeration value="xml dichiarativo"/>
                                        <xs:enumeration value="xml anomalie"/>
                                        <xs:enumeration value="allegato"/>
                                                </xs:restriction>
                                        </xs:simpleType>
                                </xs:element>
                                <xs:element name="schemaxml" type="xs:anyURI"
minOccurs="0"/>
                                <xs:element name="Firmatario" type="fgfmi:Firmatario"
minOccurs="0" maxOccurs="unbounded"/>
                        </xs:sequence>
                </xs:complexType>
        </xs:element>
</xs:schema>
```

- **ProcessMoreInfo.xsd**

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:pmi="http://conservazione.insiel.it/idc/process/moreinfo/"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://conservazione.insiel.it/idc/process/moreinfo/"
elementFormDefault="qualified" attributeFormDefault="qualified">
        <xs:element name="ProcessMoreInfo">
                <xs:annotation>
                        <xs:documentation>DataApertura, DataChiusura,
RegolaChiusura</xs:documentation>
                </xs:annotation>
                <xs:complexType>
                        <xs:sequence>
                                <xs:element name="DataApertura" type="xs:dateTime"/>
                                <xs:element name="DataChiusura" type="xs:dateTime"/>
                                <xs:element name="RegolaChiusura">
                                        <xs:complexType>
                                                <xs:sequence>
                                                        <xs:element
name="ChiusuraPerGiorni" type="xs:string" minOccurs="0"/>
                                                        <xs:element
name="DataInizioChiusuraPerGiorni" type="xs:date" minOccurs="0"/>
                                                        <xs:element
name="ChiusuraPerDocumenti" type="xs:string" minOccurs="0"/>
                                                        <xs:element
name="ChiusuraPerDimensione" type="xs:string" minOccurs="0"/>
                                                        <xs:element
name="DataChiusuraPrevista" type="xs:date" minOccurs="0"/>
                                                        <xs:element
name="DataMassimaConservazione" type="xs:date" minOccurs="0"/>
                                                </xs:sequence>
```

```
                                                </xs:complexType>
                                        </xs:element>
                                </xs:sequence>
                        </xs:complexType>
                </xs:element>
</xs:schema>
```

- **VdCMoreInfo.xsd**

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:vdcmi="http://conservazione.insiel.it/idc/vdc/moreinfo/"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://conservazione.insiel.it/idc/vdc/moreinfo/"
elementFormDefault="qualified" attributeFormDefault="qualified">
        <xs:element name="VdCMoreInfo">
                <xs:annotation>
                        <xs:documentation>Struttura proprietaria (Ente, Area, Ufficio,
Classe, Versione), NumeroDocumenti, Dimensione</xs:documentation>
                </xs:annotation>
                <xs:complexType>
                        <xs:sequence>
                                <xs:element name="SoggettoProduttore">
                                        <xs:complexType>
                                                <xs:sequence>
                                                        <xs:element name="Ente"
type="xs:string"/>
                                                        <xs:element name="Area"
type="xs:string"/>
                                                        <xs:element name="Ufficio"
type="xs:string"/>
                                                </xs:sequence>
                                        </xs:complexType>
                                </xs:element>
                                <xs:element name="Serie">
                                        <xs:complexType>
                                                <xs:sequence>
                                                        <xs:element name="Classe"
type="xs:string"/>
                                                        <xs:element name="Versione"
type="xs:string"/>
                                                </xs:sequence>
                                        </xs:complexType>
                                </xs:element>
                                <xs:element name="NumeroDocumenti" type="xs:long"/>
                                <xs:element name="Dimensione" type="xs:long"/>
                                <xs:element name="PeriodoConservazione"
type="xs:string"/>
                        </xs:sequence>
                </xs:complexType>
        </xs:element>
</xs:schema>
```

Torna al sommario

6.3 Pacchetto di distribuzione

Il pacchetto di distribuzione selettiva è formato dai seguenti oggetti:

- Indice del pacchetto di archiviazione
- Marca temporale apposta sull'indice del pacchetto di archiviazione
- Una o più unità documentarie conservate, unitamente ai relativi metadati
- Eventuale file contenente l'elenco delle anomalie rilevate ma considerate non bloccanti dal RCE

- Rapporto di versamento
- Marca temporale del rapporto di versamento
- Visori e strumenti di verifica delle firme digitali e delle marche temporali
- Note esplicative sugli oggetti esibiti e sull'utilizzo dei visori

Eventuali personalizzazioni di tali pacchetti di distribuzione eventualmente richieste sono descritte negli allegati ai rispettivi disciplinari.

Torna al sommario

7. IL PROCESSO DI CONSERVAZIONE

Il processo di conservazione si suddivide in due fasi principali e ha inizio una volta che i sistemi documentali produttori hanno predisposto e trasmesso al sistema di conservazione i pacchetti di versamento.

Torna al sommario

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

Le modalità di acquisizione dei pacchetti di versamento vengono concordate col RCE. Per ogni classe documentale sono definite contrattualmente le tempistiche di acquisizione dei pacchetti di versamento, le verifiche sulle unità documentarie, sui formati e i visualizzatori associati.

Per ogni ente/area/ufficio/classe documentale viene configurato un processo automatico che si attiva nei tempi concordati in fase contrattuale, legge l'elenco delle richieste di conservazione pervenute, e acquisisce i relativi pacchetti di versamento in un perimetro protetto all'interno del sistema di conservazione per la loro presa in carico. I file contenenti informazioni riservate/sensibili sono criptati dal produttore che provvede a fornire anche gli strumenti idonei a garantirne la leggibilità.

La trasmissione dei pacchetti di versamento avviene in modalità SFTP all'interno della RUPAR.

Per ogni pacchetto di versamento le operazioni di presa in carico sono registrate in appositi log (denominato log_dataProvider.log) e gli esiti restituiti in tempo reale ai produttori. Qualora le verifiche sul pacchetto di versamento non vadano a buon fine, il sistema avvisa gli addetti del Servizio Conservazione mediante un messaggio di posta elettronica generato automaticamente, riportante le informazioni relative all'unità documentaria, al produttore ed alla causa della mancata presa in carico. Le richieste inevase potranno essere soddisfatte al successivo versamento dopo la rimozione del problema.

Per la descrizione più dettagliata del log si rimanda al paragrafo 8.4 "Gestione e conservazione dei log" più avanti nel documento.

Torna al sommario

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

I pacchetti di versamento vengono sottoposti ai controlli necessari a determinare la loro idoneità, integrità e congruenza con le caratteristiche predefinite per le classi documentali cui i pacchetti si riferiscono. In particolare sono effettuati controlli di:

- corretta identificazione dell'Ente di provenienza;
- univocità dell'identificativo assegnato dal produttore all'unità documentaria: il sistema di conservazione richiede l'identificazione univoca delle unità documentarie;
- presenza dei metadati obbligatori;
- idoneità dei formati sia rispetto alle regole tecniche che a quanto previsto negli allegati ai disciplinari;
- congruenza dei formati rispetto ai contenuti (es. mime type/magic number)
- integrità dei file valutando le impronta rispetto ai valori dichiarati nei metadati;
- validità delle eventuali firme e marche temporali;

Previo accordo col RCE è prevista la possibilità di trattare in modo automatico le anomalie derivanti da:

- certificati utilizzati per la firma di documenti informatici per i quali non è rilevabile un riferimento temporale opponibile a terzi e già scaduti al momento della creazione del pacchetto di versamento;
- certificati utilizzati per firma di documenti informatici non associati a certificati di certificazione pubblicati nell'elenco pubblico dei certificatori accreditati AgID (TSL);
- documenti informatici firmati, ma non completamente aderenti a quanto previsto dalle specifiche (ETSI TS 103173 v.2.2.1) previste dalla Decisione di esecuzione (UE) 2015/1506 della Commissione a cui il Regolamento (UE) 910/2014 (eIDAS) fa riferimento (es. documenti informatici della classe documentale "FLUSSO FATTURE" i cui documenti sono correttamente transitati nel Sistema d'Interscambio nazionale denominato SDI);

Le operazioni sopra descritte sono quotidianamente registrate per Ente/Area/Ufficio/classe documentale nei log di processo (denominato log_archiviatore.log) e periodicamente inviate al sistema di conservazione.

Per la descrizione più dettagliata del log si rimanda al paragrafo 8.4 "Gestione e conservazione dei log" più avanti nel documento.

Torna al sommario

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

A seguito del superamento dei controlli effettuati sui pacchetti di versamento ricevuti, il sistema

- genera un rapporto di versamento attestante l'avvenuta presa in carico;
- associa al rapporto una marca temporale di tipo detached;
- memorizza i metadati trasmessi dal produttore generando opportuni indici di ricerca.

Il rapporto di versamento può riguardare anche più pacchetti di versamento. Esso è costituito da un file in formato xml, che in particolare contiene le impronte dei documenti versati, riscontrando così al produttore l'avvenuta presa in carico delle unità documentarie in esso riferite.

Si riporta la struttura del Rapporto di versamento:

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns:rdv="http://conservazione.insiel.it/rdv/"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://conservazione.insiel.it/rdv/" elementFormDefault="qualified"
attributeFormDefault="qualified">
          <xs:annotation>
                    <xs:documentation xml:lang="en">Definition of simple
types</xs:documentation>
          </xs:annotation>
          <xs:simpleType name="Version">
                    <xs:restriction base="xs:integer"/>
          </xs:simpleType>
          <xs:simpleType name="IssuerDN">
                    <xs:restriction base="xs:string"/>
          </xs:simpleType>
          <xs:simpleType name="SerialNumber">
                    <xs:restriction base="xs:integer"/>
          </xs:simpleType>
          <xs:simpleType name="SubjectDN">
                    <xs:restriction base="xs:string"/>
          </xs:simpleType>
          <xs:simpleType name="NotBefore">
                    <xs:restriction base="xs:dateTime"/>
          </xs:simpleType>
          <xs:simpleType name="NotAfter">
                    <xs:restriction base="xs:dateTime"/>
          </xs:simpleType>
          <xs:simpleType name="SigAlgName">
                    <xs:restriction base="xs:string"/>
          </xs:simpleType>
          <xs:simpleType name="Nota">
                    <xs:restriction base="xs:string"/>
          </xs:simpleType>
          <xs:simpleType name="Label">
                    <xs:restriction base="xs:string"/>
          </xs:simpleType>
          <xs:simpleType name="Path">
                    <xs:restriction base="xs:anyURI"/>
          </xs:simpleType>
          <xs:simpleType name="TimeInfo">
                    <xs:restriction base="xs:dateTime"/>
          </xs:simpleType>
          <xs:annotation>
                    <xs:documentation xml:lang="en">Definition of attributes</xs:documentation>
          </xs:annotation>
          <xs:attribute name="version" type="xs:NMTOKEN" fixed="1.0"/>
          <xs:attribute name="url" type="xs:anyURI"
fixed="http://conservazione.insiel.it/rdv/"/>
          <xs:attribute name="scheme" type="xs:string" default="local"/>
          <xs:attribute name="function" type="xs:NMTOKEN" default="SHA-256"/>
          <xs:attribute name="extension" type="xs:NMTOKEN"/>
          <xs:attribute name="format" type="xs:string"/>
          <xs:attribute name="encoding">
                    <xs:simpleType>
                              <xs:restriction base="xs:NMTOKEN">
                                        <xs:enumeration value="7bit"/>
                                        <xs:enumeration value="8bit"/>
                                        <xs:enumeration value="base64"/>
                                        <xs:enumeration value="binary"/>
```

```
                                        <xs:enumeration value="quotedprintable"/>
                                        <xs:enumeration value="xtoken"/>
                                </xs:restriction>
                        </xs:simpleType>
                </xs:attribute>
                <xs:annotation>
                        <xs:documentation xml:lang="en">Definition of complex
types</xs:documentation>
                </xs:annotation>
                <xs:complexType name="Identifier">
                        <xs:simpleContent>
                                <xs:extension base="xs:NMTOKEN">
                                        <xs:attribute ref="rdv:scheme"/>
                                </xs:extension>
                        </xs:simpleContent>
                </xs:complexType>
                <xs:complexType name="Hash">
                        <xs:simpleContent>
                                <xs:extension base="xs:string">
                                        <xs:attribute ref="rdv:function" use="required"/>
                                </xs:extension>
                        </xs:simpleContent>
                </xs:complexType>
                <xs:complexType name="FileGroup">
                        <xs:sequence>
                                <xs:element name="Label" type="rdv:Label" minOccurs="0"/>
                                <xs:element name="File" type="rdv:File" maxOccurs="unbounded"/>
                        </xs:sequence>
                </xs:complexType>
                <xs:complexType name="File">
                        <xs:sequence>
                                <xs:element name="ID" type="rdv:Identifier"/>
                                <xs:element name="Path" type="rdv:Path" minOccurs="0"/>
                                <xs:element name="Hash" type="rdv:Hash"/>
                                <xs:element name="Firmatario" type="rdv:Firmatario" minOccurs="0"
maxOccurs="unbounded"/>
                        </xs:sequence>
                        <xs:attribute ref="rdv:encoding" default="binary"/>
                        <xs:attribute ref="rdv:extension"/>
                        <xs:attribute ref="rdv:format" use="required"/>
                </xs:complexType>
                <xs:complexType name="Firmatario">
                        <xs:sequence>
                                <xs:element name="Version" type="rdv:Version"/>
                                <xs:element name="IssuerDN" type="rdv:IssuerDN"/>
                                <xs:element name="SerialNumber" type="rdv:SerialNumber"/>
                                <xs:element name="SubjectDN" type="rdv:SubjectDN"/>
                                <xs:element name="NotBefore" type="rdv:NotBefore"/>
                                <xs:element name="NotAfter" type="rdv:NotAfter"/>
                                <xs:element name="SigAlgName" type="rdv:SigAlgName"/>
                                <xs:element name="Nota" type="rdv:Nota" minOccurs="0"
maxOccurs="unbounded"/>
                                <xs:element name="Firmatario" type="rdv:Firmatario" minOccurs="0"
maxOccurs="unbounded"/>
                        </xs:sequence>
                </xs:complexType>
                <xs:complexType name="SelfDescription">
                        <xs:sequence>
                                <xs:element name="ID" type="rdv:Identifier"/>
                        </xs:sequence>
                </xs:complexType>
                <xs:complexType name="Process">
                        <xs:sequence>
                                <xs:element name="TimeReference" type="rdv:TimeReference"/>
                        </xs:sequence>
                </xs:complexType>
                <xs:complexType name="TimeReference">
                        <xs:choice>
                                <xs:element name="TimeInfo" type="rdv:TimeInfo"/>
                        </xs:choice>
                </xs:complexType>
                <xs:complexType name="RdV">
                        <xs:sequence>
                                <xs:element name="SelfDescription" type="rdv:SelfDescription"/>
```

```
                              <xs:element name="FileGroup" type="rdv:FileGroup"
maxOccurs="unbounded"/>
                              <xs:element name="Process" type="rdv:Process"/>
                    </xs:sequence>
                    <xs:attribute ref="rdv:version"/>
                    <xs:attribute ref="rdv:url"/>
          </xs:complexType>
          <xs:annotation>
                    <xs:documentation xml:lang="en">Definition of root
element</xs:documentation>
          </xs:annotation>
          <xs:element name="RdV" type="rdv:RdV"/>
</xs:schema>
```

In questa fase si provvede inoltre, in via collaborativa, a segnalare all'Ente l'eventuale prossima scadenza dei certificati di firma verificati.

Le operazioni sopra descritte sono quotidianamente registrate per Ente/Area/Ufficio/classe documentale nei log di processo (denominato log_archiviatore.log) e periodicamente inviate al sistema di conservazione.

Per la descrizione più dettagliata del log si rimanda al paragrafo 8.4 "Gestione e conservazione dei log" più avanti nel documento.

Torna al sommario

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

A seguito del mancato superamento dei controlli, gli identificativi dei pacchetti di versamento anomali vengono registrati nel sistema di conservazione unitamente al tipo di errore rilevato e al numero di richieste di versamento. A titolo di esempio nella seguente tabella si riportano le descrizioni di alcuni degli errori rilevabili:

Descrizione
Documento rettificato assente
Impronta non valida
Xml dichiarativo non valido
Errore su controllo firma
Impossibile completare il controllo firma
Errore durante la lettura dell'xml dichiarativo
Metadato obbligatorio non trovato
Il documento non presenta alcun allegato firmato
Allegato assente
File non presente tra gli allegati
Nome allegato non univoco
Documento firmato con carta compromessa
Documento firmato con carta non attiva
Firma con certificato revocato
Firma con certificato sostituito
Lista delle CRL non disponibile
File imbustato senza estensione consentita
Mime file imbustato non corrispondente

Certificato di firma scaduto
Firma con impronta incongruente
Firma non ancora valida al signing time
Firma non conforme alla Deliberazione 45/2009
Firma non conforme alla direttiva ETSI TS 101 733
Firma non valida
Firma scaduta al signing time
Errore generico su allegato
Marca apposta dopo scadenza certificato di firma
Mime allegato non permesso
Mime non corrispondente
Mime non corrispondente con estensione
Errore su controllo marca
La marca non corrisponde al documento originale
Marca temporale assente

Le unità documentarie che presentano anomalie sono rifiutate e contestualmente il sistema genera un avviso, trasmesso mediante posta elettronica, anche certificata al RCE ed alla casella di posta elettronica del Servizio Conservazione di Insiel.

Il messaggio contiene:

- L'ente produttore
- L'area/Ufficio/classe documentale cdi competenza
- L'identificativo univoco del Pacchetto di versamento che presenta anomalie
- La descrizione delle anomalie rilevate
- riferimento temporale della comunicazione dell'anomalia

Le operazioni sopra descritte sono quotidianamente registrate per Ente/Area/Ufficio/classe documentale nei log di processo (denominato log_archiviatore.log) e periodicamente inviate al sistema di conservazione.

Per la descrizione più dettagliata del log si rimanda al paragrafo 8.4 "Gestione e conservazione dei log" più avanti nel documento.

Torna al sommario

7.5 Preparazione e gestione del pacchetto di archiviazione

La predisposizione del pacchetto di archiviazione avviene secondo modalità concordate con il RCE e può essere legata alla dimensione, al numero di documenti oppure ad una periodicità prefissata. Questi criteri sono riportati negli allegati al disciplinare di servizio tra Ente e Regione FVG.

Processi automatici, partendo dai pacchetti di versamento presi in carico e non ancora conservati, generano i pacchetti di archiviazione. Più in dettaglio l'elaborazione effettua le seguenti operazioni:

- predispone l'indice del pacchetto di archiviazione
- applica la firma digitale del RSC, o di un suo delegato, con processo automatico
- applica una marca temporale di tipo detached all'Indice
- archivia il pacchetto.
- sincronizza i tempi di conservazione per tutti i file appartenenti al pacchetto, anche se versati in tempi diversi, ovvero la data di inizio conservazione sarà la medesima per tutti gli elementi appartenenti al pacchetto di archiviazione.

Il pacchetto di archiviazione è costituito quindi da:

- Una o più unità documentarie derivate dai pacchetti di versamento, unitamente ai relativi metadati
- Uno o più rapporti di versamento e rispettive marche temporali
- Indice del pacchetto di archiviazione e rispettiva marca temporale
- Eventuale indice delle anomalie rilevate e non considerate a seguito di opportune direttive impartite dal RCE

Le operazioni sopra descritte sono quotidianamente registrate nei log di processo (denominato log_web.html) e periodicamente inviate al sistema di conservazione.

Per la descrizione più dettagliata del log si rimanda al paragrafo "Gestione e conservazione dei log" più avanti nel documento.

Torna al sommario

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

L'informazione conservata è resa disponibile alla Comunità designata, formata dai Responsabili della conservazione degli enti, dai loro eventuali delegati e dall'Autorità giudiziaria. In particolare gli RCE e loro delegati sono individuati fin dalla stipula dei disciplinari e conseguentemente registrati nel sistema di conservazione. Eventuali variazioni devono essere comunicate tramite PEC ad Insiel. L'accesso da parte di altri soggetti aventi titolo (accessi, ispezioni, verifiche o sequestri ordinati dalle autorità competenti) viene gestito dall'Ufficio legale di Insiel. Sono previste le seguenti possibilità di esibizione:

ON-LINE: nel caso in cui l'RCE abbia effettuato formale richiesta di attivazione del servizio on-line, egli o suoi delegati possono:

- collegarsi al sistema di conservazione con le proprie credenziali;
- ricercare e selezionare l'unità documentaria
- effettuare la richiesta di esibizione mediante l'apposita funzione;

Il sistema genera una One Time Password che invia all'indirizzo e-mail dichiarato dall'RCE. Tale OTP è necessaria per effettuare il download del pacchetto di distribuzione e può essere utilizzata solo nell'ambito della stessa sessione e per il solo pacchetto di distribuzione selettiva selezionato.

Tutte le operazioni svolte vengono registrate nel log si sistema, periodicamente inviato in conservazione.

ON-SITE: previa formale richiesta di accesso nei locali di Insiel, l'RCE o suoi delegati, possono recarsi nell'apposita saletta di esibizione, ove sono a disposizione postazioni di lavoro dedicate. L'accesso ai locali è normato da direttive aziendali certificate ISO 27001.

Qualora non abbia attivato la funzionalità di esibizione da remoto, l'RCE può richiedere la generazione di un pacchetto di distribuzione selettiva alla casella PEC di Insiel S.p.A. tramite la casella di PEC istituzionale dell'Ente. Gli addetti del Servizio Conservazione di Insiel prendono in carico la richiesta e provvedono alla generazione del pacchetto di distribuzione, alla sua protezione con password nonché alla sua memorizzazione su supporto non riscrivibile. La sua trasmissione all'Ente richiedente avviene tramite corriere con cui è stato stipulato un contratto le cui clausole rientrano nel perimetro della certificazione ISO 27001. Separatamente avviene la comunicazione della password d'apertura del pacchetto di distribuzione.

Per le esibizioni non on-line viene compilato un apposito verbale di esibizione firmato dal RCE o suo delegato e dal RCS di Insiel.

Il pacchetto di distribuzione selettiva viene generato mediante funzionalità disponibili nell'applicazione di gestione del servizio sviluppata da Insiel. Esso contiene almeno i seguenti oggetti:

- Indice del pacchetto di archiviazione
- Marca temporale apposta sull'indice del pacchetto di archiviazione
- Una o più unità documentarie conservate, unitamente ai relativi metadati
- Eventuale file contenente l'elenco delle anomalie rilevate ma considerate non bloccanti dal RCE
- Rapporto di versamento
- Marca temporale del rapporto di versamento
- Visori e strumenti di verifica delle firme digitali e delle marche temporali
- Note esplicative sugli oggetti esibiti e sull'utilizzo dei visori

Le operazioni sopra descritte sono quotidianamente registrate nei log di processo (denominato log_web.html) e periodicamente inviate al sistema di conservazione.

Per la descrizione più dettagliata del log si rimanda al paragrafo 8.4 "Gestione e conservazione dei log" più avanti nel documento.

Torna al sommario

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

Eventuali richieste di duplicati e copie informatiche di documenti conservati dovranno essere effettuate dal RCE al quale viene reso disponibile un pacchetto di distribuzione contenente i documenti richiesti.

Nell'ambito dei processi change management e di verifica periodica di conformità alla normativa e agli standard di riferimento, vengono considerate ed analizzate anche le possibili implicazioni derivanti dall'obsolescenza tecnologica. Qualora si rendesse necessaria la produzione di copie informatiche dei documenti conservati gli addetti del Servizio Conservazione ne daranno notizia al RCE il quale provvederà a validare le soluzioni tecnologiche proposte e ad attestane la conformità.

Insiel nei casi in cui sia previsto l'intervento di un pubblico ufficiale, assicura allo stesso l'assistenza tecnica necessaria per l'espletamento delle attività al medesimo attribuite.

Ogni risorsa, comprese quelle di natura economica, necessaria per l'espletamento delle attività attribuite al pubblico ufficiale dovranno essere garantite e sostenute dal Cliente/Ente.

Torna al sommario

7.8 Scarto dei pacchetti di archiviazione

Tra i parametri di configurazione delle classi documentali vi è anche il tempo previsto per la conservazione archivistica delle relative unità documentarie. Questo valore è riportato nell'allegato al disciplinare di servizio tra Ente e Regione Friuli Venezia Giulia.

Mediante appositi report il RCE può produrre gli elenchi di documenti scartabili entro una determinata data limite impostabile, al fine sia di valutare lo stato di conservabilità dei documenti e, conformemente alla normativa vigente, richiedere alla Soprintendenza archivistica competente l'autorizzazione allo scarto. In caso di risposta affermativa, mediante apposita interfaccia disponibile nell'applicazione web, il RCE può procedere alla selezione dei documenti scartabili ed all'invio della relativa richiesta di scarto. Il sistema di conservazione procede quindi alle conseguenti elaborazioni ed alla produzione di un rapporto di scarto che, similmente agli altri rapporti, viene conservato nel sistema di conservazione.

Torna al sommario

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

L'interoperabilità tra sistemi viene garantita dall'utilizzo dello standard UNI 11386:2010 SinCRO. Inoltre ogni singolo Manuale di conservazione dell'Ente riporterà una descrizione di tutti gli ulteriori metadati presenti nel Pacchetto di Archiviazione e specifici di ogni singolo contratto.

Torna al sommario

8. IL SISTEMA DI CONSERVAZIONE

In questo capitolo viene fornita la descrizione del sistema di conservazione, in termini di componenti logiche, tecnologiche e fisiche. Quanto descritto si riferisce principalmente al sistema di produzione ma, con alcune naturali semplificazioni, può applicarsi anche ai sistemi di sviluppo e collaudo.

Torna al sommario

8.1 Componenti Logiche

Le entità funzionali relative al sistema di conservazione sono:

Entità funzionale	Funzioni esercitate
CONSWEB Portale conservazione	Applicazione web per la configurazione ed il controllo del sistema di conservazione, articolata nei seguenti moduli: • gestore enti/aree/uffici/classi documentali • gestore utenti • gestore dei pacchetti di archiviazione • gestore verifiche manuali • gestore anomalie • gestore esibizione e pacchetti di distribuzione • interrogazioni • monitoraggio • report e log
GPC Gestore Processo Conservazione	Applicazione per la gestione dei processi di conservazione, articolata nei seguenti moduli: • gestore presa in carico pacchetti di versamento • gestore versamento dei pacchetti • gestore firme digitali e marche temporali • gestore notifiche automatiche • gestore controlli automatici integrità documenti
ADS Area Di Scambio	Area di storage a disposizione del produttore per la trasmissione dei pacchetti di versamento
ADC Area Di Conservazione	Area per la conservazione dei pacchetti di archiviazione
WS	Web services a disposizione del produttore per inoltrare le richieste di

Web Services	conservazione, nonché per il monitoraggio dell'esito delle stesse
BCK Modulo BaCKup	Entità con la funzione di produrre le copie di backup di documenti e metadati conservati
FRM	Modulo di Firma Remota Massiva

Torna al sommario

8.2 Componenti Tecnologiche

L'insieme delle componenti tecnologiche a supporto delle entità logiche dell'infrastruttura dedicata al servizio di conservazione documentale nel sito primario è rappresentato in Figura 1., mentre quello relativo al sito di Disaster Recovery è riprodotto in Figura 2.

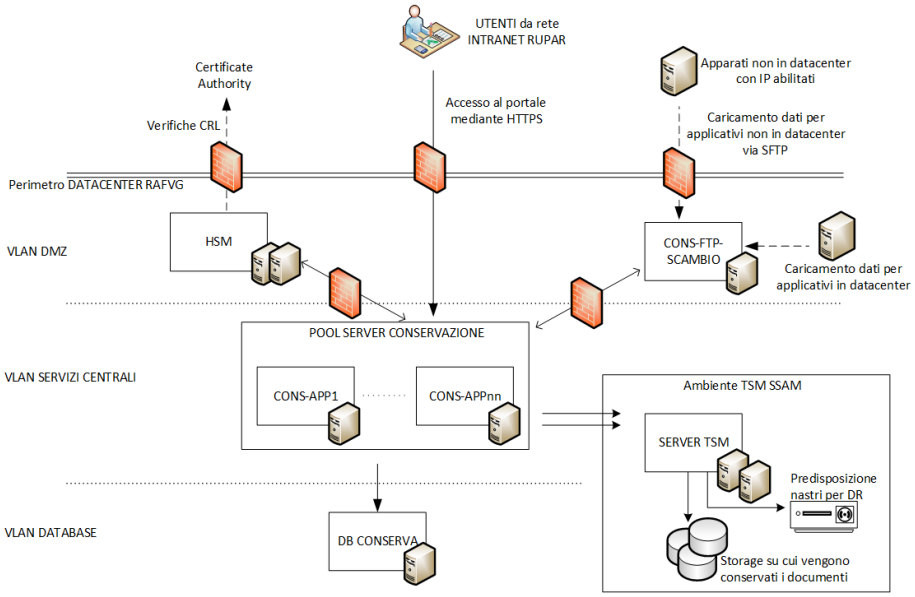

Figura 1.: Componenti tecnologiche del sistema di conservazione (sito primario)

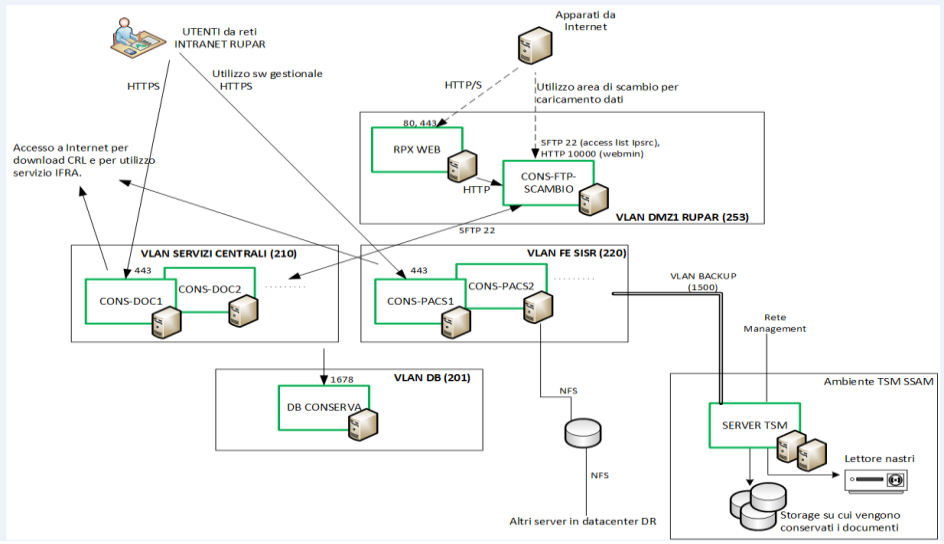

Figura 2.: Componenti tecnologiche del sito di Disaster Recovery

Il sistema di conservazione utilizza server con sistema operativo Linux, ospitati su piattaforma di virtualizzazione VMWare. Questa soluzione consente di svincolarsi dall'hardware, utilizzando al meglio le risorse dei sistemi e minimizzando i tempi di delivery. Inoltre l'impiego di una tecnologia di virtualizzazione consente di garantire l'alta affidabilità a fronte di guasti hardware e di ridurre i tempi di ripristino in caso di fault.

Il carico elaborativo dei processi di conservazione è distribuito su diverse istanze in alta affidabilità appoggiate su più server virtuali (POOL SERVER CONSERVAZIONE). Ciascun processo utilizza le API specifiche che consentono l'interfacciamento con la "IBM Spectrum Protect Suite", installata su cluster AIX, sul quale è abilitata la funzione "IBM Spectrum Protect Suite for Data Retention" per consentire l'archiviazione effettiva dei documenti su disco e successivamente su nastro mediante l'impiego di tape library.

Sono previsti la protezione e il controllo degli accessi tramite un'architettura a diverse zone di sicurezza isolate verso Internet e tra di loro da firewall. Tutta la procedura avviene nel contesto del data center, e l'accesso ai diversi apparati che concorrono all'erogazione del servizio è consentito da indirizzi IP specificamente abilitati su firewall.

Lo scambio di documenti da archiviare e conservare avviene mediante delle procedure automatiche che consentono il trasferimento di tali dati dagli indirizzi IP dei soli server gestionali abilitati. Per gli Enti che non dispongono di software produttori di documenti presso il data center regionale, lo scambio di documenti da conservare avviene in modo mediato da un server SFTP.

L'accesso al portale di amministrazione, che utilizza le piattaforme open source Apache HTTP Server e Apache Tomcat, è previsto esclusivamente via HTTPS da postazioni connesse alla RUPAR del Friuli-Venezia Giulia. Il database che sottende all'intera infrastruttura, ove sono conservati gli indici dei documenti conservati (DB CONSERVA) è Oracle.

Nella seguente tabella è riportata la corrispondenza tra componenti tecnologiche ed entità funzionali.

Componente tecnologica	Descrizione	Entità funzionali correlate
POOL SERVER CONSERVAZIONE DB CONSERVA	Server virtuali Linux e application server Apache Tomcat	CONSWEB GPC WS
CONS-FTP-SCAMBIO	Server virtuali Linux	ADS
AMBIENTE DATA RETENTION	Software IBM Spectrum Protect Suite for Data Retention per la gestione di archiviazione, conservazione e recupero dei documenti	ADC BCK
HSM	Infrastruttura hardware e software di firma remota massiva Actalis s.p.a.	FRM

Torna al sommario

8.3 Componenti Fisiche

Le componenti fisiche sono descritte nel seguito:

- **IBM Spectrum Protect Suite**

  È il sistema di memorizzazione su cui è installata l'applicazione IBM Spectrum Protect Suite for Data Retention tramite la quale vengono gestiti i documenti informatici in conservazione. Sono presenti le seguenti istanze:

  - **sviluppo**: è collegata all'application server di sviluppo, utilizzato dal servizio conservazione per lo sviluppo di nuovi processi, usando il nodo di sviluppo dedicato;

  - **collaudo**: è collegata all'application server di collaudo utilizzato dal servizio conservazione per il collaudo di nuovi processi, usando il nodo di collaudo dedicato;

  - **produzione (documenti)**: è utilizzata per la gestione dell'archiviazione, conservazione ed il recupero delle unità documentarie versate dagli Enti; essa è collegata agli application server di produzione che ospitano i gestori dei processi di conservazione e utilizza i nodi definiti sul server IBM Spectrum Protect Suite. Nelle fasi di verifica, i gestori dei processi appoggiano i dati su uno storage pool a disco IBM NetApp.

- **produzione (PACS)**: analoga all'istanza IBM Spectrum Protect Suite dei documenti, ma dedicata ai PACS prodotti dalle aziende sanitarie/ospedaliere.

- **Server sftp per il deposito di documenti provenienti dall'esterno**

  È il server che ospita l'area di interscambio dove gli Enti, tramite protocollo sftp, depositano i pacchetti di versamento da inviare in conservazione.

- **Application server per i processi di conservazione**

  Sono i server virtuali che ospitano gli application server in cui sono installate le applicazioni Java, sviluppate da Insiel, che gestiscono i processi di presa in carico e conservazione dei documenti e dei PACS.

- **DataBase Server**

  È il server che ospita la base informativa utilizzata dalle applicazioni Java che gestiscono il sistema di conservazione. Sono definiti sistemi distinti per sviluppo, collaudo e produzione.

- **Application server per i servizi web**

  È il server che ospita il web service utilizzabile dagli utenti esterni per l'interfacciamento dei propri sistemi produttori col sistema di conservazione Insiel. Sono definiti sistemi distinti per il collaudo e la produzione.

- **Storage NetApp.**

  Gli application server condividono dello spazio disco, mappato tramite NFS, su storage NetApp, per il deposito temporaneo dei documenti prima della loro archiviazione

- **Libreria Oracle Storage Tek**

  È la libreria utilizzata dall'istanza IBM Spectrum Protect Suite di produzione per la creazione delle copie di sicurezza su cassette LTO.

- **HSM**

  Infrastruttura di firma remota massiva.

A corollario si riporta il quadro riassuntivo delle componenti logiche, tecnologiche e fisiche.

Logica	Tecnologica	Fisica
CONSWEB	POOL-SERVER-CONSERVAZIONE	Server virtuali VMWARE Linux
GPC		Apache HTTP Server
WS		Apache Tomcat application server
	DB-CONSERVA	
		Oracle Database

ADS	CONS-FTP-SCAMBIO	Server virtuali VMWARE Linux
ADC	IBM PROTECT – DATA RETENTION	IBM Spectrum Protect Suite installato su cluster AIX, sul quale è abilitata la funzione DATA RETENTION
BCK	IBM PROTECT SUITE	Tape Library
FRM	HSM	HSM

Torna al sommario

8.4 Procedure di gestione e di evoluzione

L'operatività del Servizio si esplica attraverso le seguenti fasi e relative attività:

- **Personalizzazione sistema:** definizione ed attivazione del processo di carico e dei profili utente

Attività svolte	**Strutture e ruoli coinvolti**	**Input**	**Output**	**Vincoli, controlli, variabili, criticità**
Configurazione del sistema per Ente/Area/Ufficio e classe documentale	Delegato ai processi di conservazione di Insiel	AT	Applicativo Consweb e DB aggiornati	Configurazione ambiente di collaudo, test di presa in carico, configurazione ambiente di esercizio
Definizione processo di presa in carico e degli accessi, schedulazione dei lavori	Delegato ai processi di conservazione di Insiel	AT e documenti con cui l'Ente ha nominato i propri referenti (RCE e delegati)	Creazione di un nuovo processo di presa in carico Inserimento del profilo e delle credenziali di accesso	Verifica del login e del profilo

Attività svolte	Strutture e ruoli coinvolti	Input	Output	Vincoli, controlli, variabili, criticità
Comunicazione credenziali	Delegato ai processi di conservazione di Insiel RCE	Credenziali di accesso	Le credenziali vengono comunicate via e-mail (distinte per codice utente e password) Per gli enti sanitari viene seguita la procedura dedicata.	Il sistema chiede obbligatoriamente il cambio della password al primo accesso
Comunicazione all' Ente di Attivazione del processo di Conservazione tramite gestore flusso documentale e protocollo informatico	Delegato ai processi di conservazione di Insiel Responsabile della conservazione di Insiel RCE	Modello lettera comunicazione	Comunicazione ufficiale al RCE tramite PEC dell'avvenuta attivazione del Servizio di Conservazione	

Si ricorda che prerequisito è la stipula/aggiornamento del Disciplinare di Servizio tra Regione ed Ente richiedente con i relativi allegati tecnici (AT). Si riportano nel seguito maggiori dettagli su tali attività.

- **Conduzione:** attività quali generazione dei rapporti di versamento e dei pacchetti di archiviazione, verifica degli esiti, gestione delle anomalie e supporto al cliente, quotidianamente svolte dagli incaricati per l'erogazione del servizio.

Attività svolte	Strutture e ruoli coinvolti	Input	Output	Vincoli, controlli, variabili, criticità
Generazione dei pacchetti di archiviazione	Delegato ai processi di conservazione di Insiel	Pacchetti di archiviazione	Creazione, firma digitale e marcatura temporale dell'indice del pacchetto di archiviazione. Consolidamento dei documenti mediante chiamata a IBM Spectrum Protect Suite	Delega nominativa, certificato di firma digitale in corso di validità, marche temporali

Attività svolte	Strutture e ruoli coinvolti	Input	Output	Vincoli, controlli, variabili, criticità
Verifiche manuali	Delegato ai processi di conservazione di Insiel	Scelta casuale di un'unità documentaria all'interno di ogni pacchetto di archiviazione non ancora controllato	Registrazione estremi del documento ed esito controllo di integrità	Verifica di integrità
Verifiche automatiche	Delegato ai processi di conservazione di Insiel	Insieme di unità documentarie non ancora controllate	Registrazione estremi documenti ed esiti controllo di integrità	Controllo esiti della procedura automatica
Verifiche esiti presa in carico dei documenti	Delegato ai processi di conservazione di Insiel	Processi di presa in carico schedulati nella giornata	Report riassuntivo sui processi eseguiti inviato via e-mail	Verifica processi e salvataggio della e-mail
Comunicazione elenchi anomalie	Delegato ai processi di conservazione di Insiel	Unità documentarie da prendere in carico che hanno presentato anomalie durante la fase di verifica	Le anomalie intercettate e comunicate in automatico dal sistema, vengono raggruppate in elenchi contenuti in bozze già predisposte come direttiva di sanatoria ed inviate ai Responsabili della conservazione	I Responsabili della conservazione degli Enti non provvedono a sanare le anomalie nonostante le ripetute comunicazioni
Gestione anomalie	Delegato ai processi di conservazione di Insiel	Direttive dal RCE	Presa in carico o rifiuto dei documenti che presentano anomalie come da direttiva	I Responsabili della conservazione degli Enti possono verificare dal portale l'avvenuta sanatoria
Operazioni periodiche (controllo saletta esibizione, verifica normativa, simulazione restore dati)	Delegato ai processi di conservazione di Insiel	DB e HW	Verbali di verifica	Eventuali criticità vengono registrate e subito risolte

Attività svolte	Strutture e ruoli coinvolti	Input	Output	Vincoli, controlli, variabili, criticità
Supporto cliente (solo in fase di avviamento)	Delegato ai processi di conservazione di Insiel	Richieste telefoniche e richieste di assistenza via e-mail	Assistenza telefonica o via e-mail del servizio conservazione	Registrazione attività su un Issue tracking system dedicato, utilizzo CRM

- **Gestione e conservazione dei log (anche in accordo con l'ente Produttore)**

Il sistema di conservazione produce i log di tutti i lavori eseguiti. Il log giornaliero è costituito da un'unità documentaria contenente tutti i log dei singoli processi e viene trasmesso al sistema di conservazione e conservato per il periodo di un anno.

Ogni processo operante nel sistema di conservazione è definito in base all'Ente/Area/Uffici/Classe/Versione e genera propri log. In particolare vengono prodotti i seguenti log:

- **Log_Launcher.log**: log relativo al sistema di schedulazione del processo
- **Log_DataProvider.log**: log relativo alla presa in carico delle richieste di conservazione;
- **Log_Archiviatore.log**: log relativo alle verifiche ed accettazione/rifiuto dei pacchetti di versamento;
- **Log_controlloLotti.log**: log per la registrazione delle verifiche automatiche/manuali sulle unità documentarie conservate scelta e campione;
- **Log_Web.html**: log generale dei processi di generazione dei pacchetti di archiviazione, distribuzione e delle operazioni eseguite in generale dagli operatori mediante interfaccia web.

- **Monitoraggio del sistema di conservazione**

Le attività di monitoraggio riguardano sia aspetti applicativi che di infrastruttura. Le prime sono in carico al Servizio conservazione, e sono finalizzate a rilevare eventuali problemi relativi al processo di conservazione nelle sue componenti applicative. Tali attività rientrano a tutti gli effetti nell'ambito della conduzione del servizio descritta precedentemente.

Le seconde sono finalizzate alla rilevazione di problemi a livello infrastrutturale e vengono gestite da uno specifico reparto che, fra le funzioni, ha il compito di gestire gli incidenti di sicurezza.

- **Change management**

La gestione del cambiamento è in carico alle figure professionali che rivestono i vari ruoli previsti nell'ambito della conservazione. Tali figure hanno il compito di seguire le evoluzioni tecnologiche e normative, analizzare i feedback ricevuti dalle attività di monitoraggio o innescate dai processi di

incident management, e collaborare nella definizione delle soluzioni idonee a garantire che le funzionalità del sistema di conservazione siano costantemente adeguate. In queste attività essi possono anche avvalersi della consulenza di professionisti specializzati in informatica giuridica.

- **Verifica periodica di conformità a normativa e standard di riferimento.**

Insiel ha stipulato un contratto di consulenza con professionisti specializzati in informatica giuridica al fine di usufruire delle attività di monitoraggio sull'evoluzione della normativa di riferimento. L'evoluzione del software viene effettuata in base alle indicazioni dello studio in accordo con le modalità di cui al Piano della Configurazione secondo le regole previste nel sistema di Qualità Insiel certificato ISO 9001:2008 n. CERT-00652-95-AQ-VEN-SINCERT.

Torna al sommario

9. MONITORAGGIO E CONTROLLI

Torna al sommario

9.1 Procedure di monitoraggio

Le attività di monitoraggio applicative riguardano il processo di conservazione. In particolare il controllo dei processi di presa in carico viene effettuato verificando i report giornalieri generati automaticamente ed inviati a tutti i componenti il gruppo che si occupa del Servizio di Conservazione. Essi riportano in dettaglio le informazioni relative alla presa in carico dei pacchetti di versamento. Dopo la consultazione, i report vengono archiviati in cartelle su risorse di rete. Tale archiviazione costituisce evidenza di avvenuta presa visione.

Processi automatici esaminano tutti i pacchetti di archiviazione creati giornalmente. La verifica d'integrità viene effettuata estraendo un documento a campione per ciascuno dei pacchetti di archiviazione. Tali verifiche sono registrate e consultabili mediante l'applicazione web ConsWeb.

Inoltre è attivo un processo che esegue controlli automatici incrementali al fine di verificare l'integrità dell'intero patrimonio documentale conservato. Il risultato di tali controlli viene verificato ogni mattina dai delegati al Servizio.

È disponibile un cruscotto che consente di monitorare i processi di presa in carico dei pacchetti di versamento e di generazione dei pacchetti di archiviazione. Per ciascun server del POOL di conservazione è possibile verificare tempi ed esiti delle elaborazioni impostando la data d'interesse.

Le fasi con le quali sono gestiti gli eventi derivanti dalle attività di monitoraggio infrastrutturale sinteticamente sono le seguenti:

- **Rilevazione dell'evento di sicurezza**: l'evento può essere rilevato da sistemi automatici oppure da qualunque dipendente nel corso della propria attività lavorativa. Sono stati predisposti canali di comunicazione (e-mail dedicata e specifica interfaccia su intranet aziendale) per una pronta segnalazione al settore preposto.

- **Mitigazione**: in questa fase vengono interessati tutti i soggetti funzionali alla risoluzione dell'incidente. È in vigore una procedura che prevede che vengano effettuate tutte le operazioni tecniche per ridurre al minimo l'impatto dell'incidente
- **Risoluzione**: in questa fase vengono identificate, da parte del personale deputato alla gestione delle infrastrutture informatiche interessate, con il supporto del personale del settore IT Security, le azioni correttive da compiere per rimuovere gli effetti dell'incidente sulle risorse informatiche, individuarne le cause e ripristinare la normale operatività. Vengono decisi gli interventi da eseguire e contattate le persone adibite alla loro esecuzione, che provvedono prontamente con la massima diligenza ed efficienza, verificando anche l'efficacia delle operazioni fatte
- **Ripristino**: una volta risolto l'incidente di sicurezza e verificato il corretto funzionamento delle risorse informatiche, ivi compreso la risoluzione delle cause che hanno portato al verificarsi dell'incidente, viene ripristinato il servizio nella sua totalità, revocando eventuali contromisure temporanee svolte in emergenza nella fase di mitigazione
- **Spunti per il miglioramento**: In ogni fase della procedura di gestione degli incidenti di sicurezza si tiene traccia delle operazioni eseguite. Una volta ripristinato il servizio, viene terminata la compilazione del registro inserendo tutti i dettagli sull'incidente di sicurezza e sulle attività intraprese per fronteggiarlo.

Torna al sommario

9.2 Verifica dell'integrità degli archivi

Report giornalieri, inviati automaticamente a tutti i delegati, permettono di appurare la corretta esecuzione dei lavori schedulati e le eventuali anomalie riscontrate.

La verifica dell'integrità degli archivi viene realizzata secondo le seguenti modalità:

- manuale: il sistema di conservazione rende disponibile al RCE ed agli addetti al Servizio di conservazione una funzionalità che consente di verificare l'integrità di qualsiasi documento conservato compatibilmente con le abilitazioni assegnate;
- automatica su attività del giorno: il sistema di conservazione esegue la verifica d'integrità su un documento estratto a campione su ciascun pacchetto di archiviazione generato nella giornata;
- automatica su tutto l'archivio: il sistema di conservazione verifica ogni giorno l'integrità di una percentuale di documenti con lo scopo di controllare almeno una volta tutti i documenti conservati nell'arco temporale di 4 anni.

Gli esiti delle verifiche sopra elencate sono registrati nel sistema e possono essere consultati mediante specifiche funzionalità. Tutte le operazioni sono inoltre registrate nel log di sistema, conservato settimanalmente.

A cadenza mensile vengono effettuate delle verifiche documentali sui supporti di backup per verificarne la leggibilità. L'attività viene svolta da un addetto alla conservazione in collaborazione con un incaricato dal Systems Management. Al termine dell'attività viene redatto un verbale che, dopo la sottoscrizione da parte dell'addetto alla conservazione, viene registrato.

Torna al sommario

9.3 Soluzioni adottate in caso di anomalie

Nel caso in cui i processi di presa in carico e di archiviazione rilevino anomalie sui documenti elaborati, registrano l'anomalia nella base informativa permanente e generano automaticamente in alcuni casi (definibili parametricamente) delle e-mail con indicazione degli identificativi dei documenti. Il Servizio di conservazione monitora tali anomalie e, nel caso in cui il RCE non si attivi autonomamente, lo contatta, per richiedergli indicazioni sulle modalità di trattamento delle anomalie rilevate. Il RCE dovrà inviare ad Insiel una comunicazione in cui fornisce ad Insiel le opportune direttive al fine di sanare le anomalie rilevate. Il Servizio conservazione di Insiel, in via collaborativa per facilitare l'ente, può produrre delle bozze relative alle anomalie da sanare. I documenti con le direttive ricevute sono anch'essi sottoposti al processo di conservazione e correlati alle anomalie trattate.

Sono previste inoltre delle e-mail informative, sempre generate automaticamente dal sistema, che avvisano il RCE di eventuali prossime scadenze dei certificati di firmatari usuali dei documenti. E' possibile parametrizzare i destinatari di tali e-mail.

Torna al sommario