La conservazione a norma dei documenti in Insiel – compiti dell'outsourcer e descrizione del processo – (Manuale del Responsabile del procedimento di conservazione)

Compilato: L.Semolic (Delegato al Servizio CS)

Rivisto: C.Otti (RQ Responsabile Qualità)
E. Bombardieri (Responsabile del Servizio CS)
M. Ferrara (Responsabile dell'Ufficio Legale)

Autorizzato: L.Pozza (Presidente)

Versione: 6
Variante: 0

Compendio: Il presente documento descrive dettagliatamente le modalità organizzative ed operative con cui viene applicato il processo di archiviazione e conservazione a norma dei documenti informatici secondo le disposizioni vigenti in materia.

Principali riferimenti normativi:

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"

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"*

Decreto Legislativo. n. 159 del 4 aprile 2006 - *"Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82 recante codice dell'amministrazione digitale"*

Decreto Legislativo. n. 235 del 30 dicembre 2010 - *" Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69".*

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 verifi ca delle fi rme elettroniche avanzate, qualifi cate 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.*

Versione	Data	Principali modifiche rispetto alla versione precedente
1.0	22.07.2009	Prima versione. Le modifiche apportate nel tempo al contenuto del presente manuale sono referenziate nell'apposito *"Registro delle versioni del manuale IIT-CS-MP-01"* (IIT-CS-RG-06).
2.0	28.10.2010	Seconda versione. Le modifiche apportate nel tempo al contenuto del presente manuale sono referenziate nell'apposito *"Registro delle versioni del manuale IIT-CS-MP-01"* (IIT-CS-RG-06).
3.0	20.12.2011	Terza versione. Le modifiche apportate nel tempo al contenuto del presente manuale sono referenziate nell'apposito *"Registro delle versioni del manuale IIT-CS-MP-01"* (IIT-CS-RG-06)
4.0	12/10/2012	Quarta versione Le modifiche apportate nel tempo al contenuto del presente manuale sono referenziate nell'apposito *"Registro delle versioni del manuale IIT-CS-MP-01"* (IIT-CS-RG-06)
5.0	17/07/2013	Quinta versione Le modifiche apportate nel tempo al contenuto del presente manuale sono referenziate nell'apposito *"Registro delle versioni del manuale IIT-CS-MP-01"* (IIT-CS-RG-06)
6.0	30/05/2014	Sesta versione Le modifiche apportate nel tempo al contenuto del presente manuale sono referenziate nell'apposito *"Registro delle versioni del manuale IIT-CS-MP-01"* (IIT-CS-RG-06)

INDICE

1. Introduzione

1.1. Premessa

Nel presente manuale sono descritte le modalità operative e l'organizzazione per mezzo delle quali Insiel, in qualità di outsourcer delegato, gestisce il processo di archiviazione e conservazione dei documenti informatici, secondo le disposizioni vigenti in materia.

1.2. Abbreviazioni e definizioni

AIPA	Autorità per l'informatica nella Pubblica Amministrazione ora Agenzia per l'Italia Digitale
CA	Certification Authority (indica l'Autorità di certificazione di un dispositivo di firma digitale)
CAD	Codice dell'amministrazione digitale
CS	Conservazione a norma dei documenti
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione ora Agenzia per l'Italia Digitale
CTOSIR	Conduzione Tecnica e Operativa di Sistemi Informativi e Reti di telecomunicazione
DIT	Dipartimento per l'Innovazione e le Tecnologie
DPCM	Decreto Presidente del Consiglio dei Ministri
DGR	Deliberazioni della Giunta Regionale
DPR	Decreto Presidente della Repubblica
HTTP	Hyper Text Transfer Protocol (identificativo convenzionale per un sito)
HTTPS	Secure Hyper Text Transmission Protocol. Protocollo sviluppato allo scopo di cifrare e decifrare le pagine Web che vengono inviate dal server ai client
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
RCO	Responsabile della Conservazione dell'Outsourcer
RdC	Responsabile della Conservazione
SAQ	Servizio Assicurazione Qualità
SQI	Sistema Qualità Insiel
SSL	Secure Socket Layer. Protocollo che consente, grazie a tecniche di crittografia, il trasferimento di dati tramite la rete Internet in modo sicuro.
TSA	Time Stamping Authority
URL	Uniform Resource Locator (indica la modalità per individuare univocamente un sito Internet)
UTC	Universal Time Coordinated (Misura del tempo così come stabilito dall'International Radio Consultative Committee -CCIR)
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
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
disponibilità	requisito di sicurezza che esprime la certezza di poter utilizzare un'informazione o risorsa. Le informazioni devono sempre essere accessibili a chi ne ha diritto nei tempi e nei modi previsti. La disponibilità delle informazioni va assicurata in base ad un livello di servizio concordato,

	ovvero secondo modalità predefinite
dispositivo di firma sicuro	particolare componente hardware (smart card o dispositivo HSM) 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
documento analogico	rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti
documento informatico	rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
documento statico non modificabile	documento informatico redatto in modo tale per cui il contenuto risulti non alterabile durante le fasi di accesso e di conservazione nonché immutabile nel tempo; a tal fine il documento informatico non deve contenere macroistruzioni o codice eseguibile, tali da attivare funzionalità che ne modifichino il contenuto
evidenza informatica	sequenza di simboli binari (bit) che viene prodotta da una procedura informatica
firma digitale	particolare firma elettronica qualificata basata su un certificato qualificato e 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.
firma elettronica	insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica
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.
firma elettronica qualificata	firma elettronica avanzata, basata su un certificato elettronico qualificato e creata mediante un dispositivo di firma sicuro

funzione di hash	funzione matematica che genera, a partire da una generica sequenza di simboli binari, un'impronta da cui risulti di fatto impossibile, determinare la sequenza di simboli binari (bit) originaria e tale per cui sia estremamente improbabile che due messaggi differenti, anche se simili, abbiano lo stesso hash
impronta	sequenza alfanumerica o stringa di simboli binari (bit) di lunghezza predefinita che identifica un certo file; viene generata mediante l'applicazione al file di un'opportuna funzione di hash.
Integrità di un documento informatico	requisito di sicurezza che assicura che non vi siano state modificazioni, anche accidentali, sul documento
marca temporale	il riferimento temporale che consente la validazione temporale ed è generato in appositi sistemi di validazione temporale garantiti da terze parti.
riferimento temporale	informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici;
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.
riversamento diretto	processo che trasferisce uno o più documenti conservati da un supporto di memorizzazione a un altro non alterandone la rappresentazione informatica. E' una attività tipica, ammessa dalla normativa, per produrre le copie di sicurezza.
riversamento sostitutivo	processo che trasferisce uno o più documenti conservati da un supporto di memorizzazione a un altro alterandone la rappresentazione informatica. E' una attività tipica, ammessa dalla normativa, nel caso in cui si intenda aggiornare l'archivio al fine di garantire l'esibizione dei documenti anche a fronte di innovazioni tecnologiche.
sottoscrizione elettronica	apposizione della firma elettronica qualificata, generata attraverso l'utilizzo di un dispositivo di firma sicuro.

1.3. Gestione del documento

E' responsabilità del RCO, anche per tramite dei suoi delegati, di provvedere alla gestione del presente documento secondo le modalità indicate in *"Gestione della documentazione del sistema Qualità"* (IAQ-AQ-MP-06).

2. Approfondimenti tecnici

Prima di descrivere le attività e i processi implementati da Insiel SpA, per garantire un servizio di conservazione legale, è opportuno soffermarsi su alcuni concetti che stanno alla base della conservazione medesima; in particolare sono di seguito approfonditi gli aspetti relativi:

- documento informatico e utilizzo di chiavi crittografate
- caratteristiche di un certificato qualificato
- requisiti dei soggetti in grado di rilasciare certificati qualificati
- utilizzo della marcatura temporale

2.1. Documento informatico e chiavi crittografate

Per proteggere un documento informatico è possibile utilizzare un software di cifratura che, mediante un algoritmo matematico che utilizza un codice Kc, denominato chiave di codifica, lo trasforma in una configurazione binaria diversa da quella originaria, illeggibile con qualsiasi software ovvero applica ad un testo in chiaro le regole del cifrario per produrre un testo illeggibile.

Il processo inverso si realizza con un software che applica al file cifrato un altro algoritmo matematico il quale, utilizzando un codice Kd, denominato chiave di decodifica, riporta il file nella configurazione originaria.

Quando la chiave di codifica è uguale a quella di decodifica si parla di crittografia a chiavi simmetriche; se le due chiavi sono diverse si parla di crittografia a chiavi asimmetriche. La crittografia a chiavi simmetriche è un processo che sotto il profilo pratico operativo è molto efficiente e veloce, tuttavia presenta due peculiarità che in alcuni casi costituiscono un limite:

1. i soggetti che si scambiano il documento, devono utilizzare la medesima chiave, il che non rappresenta un problema se essi si conoscono e hanno stipulato un accordo preventivo (è il caso di una banca che offre ai suoi clienti servizi on line con comunicazioni riservate); se invece i due soggetti sono, ad esempio, degli utenti di Internet entrati casualmente in contatto, le cose si complicano;

2. il meccanismo di crittografia a chiavi simmetriche non può essere utilizzato per la generazione di firme elettroniche in quanto almeno due soggetti possiedono la stessa chiave e quindi sono in grado, a partire da un documento informatico, di generare la stessa firma.

La crittografia a chiavi asimmetriche richiede che ogni soggetto sia dotato di una coppia di chiavi: una segreta Ks, nota solo al suo possessore, e una pubblica Kp,conosciuta da tutti, ulteriori requisiti sono:

1. ciascuna coppia di chiavi deve essere univoca.

2. dalla chiave pubblica Kp non si deve poter risalire alla chiave segreta Ks.

3. se un file viene cifrato con una chiave segreta, l'operazione inversa di decodifica deve potersi eseguire solo utilizzando la chiave pubblica appartenente alla medesima coppia.

Ciò premesso, se un soggetto A volesse inviare un messaggio riservato a un soggetto B, dovrebbe cifrarlo con la chiave pubblica di B, infatti soltanto B potrebbe decodificarlo, in quanto possiede la chiave segreta (l'altra chiave della stessa coppia).

Gli algoritmi di crittografia a chiavi asimmetriche più utilizzati sono l'algoritmo RSA (dai nomi degli inventori Rivest, Shamir e Adleman) e l'algoritmo DSA (Digital Signature Algorithm). La lunghezza delle chiavi può variare: tanto più sono lunghe, tanto più è difficile violare i messaggi che con esse vengono cifrati.

La crittografia a chiavi asimmetriche viene utilizzata per generare la firma elettronica qualificata (di cui la firma digitale ne è una particolare specie) allo scopo di garantire la autenticità e l'integrità di un documento informatico.

2.2. Caratteristiche di un certificato qualificato

Un certificato qualificato deve riportare almeno le seguenti informazioni (CAD art.28, comma 1) :

1. l'indicazione che il certificato elettronico è un certificato qualificato,

2. il numero di serie o altro codice identificativo del certificato,

3. il nome, la ragione o la denominazione sociale del certificatore e lo Stato nel quale è stabilito,

4. il nome, il cognome e il codice fiscale del titolare del certificato o uno pseudonimo chiaramente identificato come tale,

5. i dati per la verifica della firma, cioè i dati peculiari, come codici o chiavi crittografiche pubbliche, utilizzati per verificare la firma elettronica corrispondenti ai dati per la creazione della stessa in possesso del titolare,

6. l'indicazione del termine iniziale e finale del periodo di validità del certificato,

7. la firma elettronica del certificatore che ha rilasciato il certificato, realizzata in conformità alle regole tecniche ed idonea a garantire l'integrità e la vericidità di tutte le informazioni contenute nel certificato medesimo.

Oltre alle precedenti informazioni, per i titolari residenti all'estero, il certificato deve riportare il codice fiscale rilasciato dal Paese di residenza ovvero il codice di sicurezza sociale o altro identificativo generale. (CAD art.28, comma 2)

A titolo opzionale, il certificato può contenere anche le seguenti informazioni (CAD art.28, comma 3):

8. le qualifiche specifiche del titolare, quali l'appartenenza ad ordini o collegi professionali, la qualifica di Pubblico Ufficiale, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, nonché poteri di rappresentanza,

9. i limiti d'uso del certificato, ove applicabili,

10. i limiti del valore degli atti unilaterali e dei contratti per i quali il certificato può essere usato, ove applicabili.

2.3. Requisiti dei certificatori

I prestatori di servizi di certificazione che rilasciano certificati qualificati devono (CAD art.27, comma 2):

1. dimostrare l'affidabilità organizzativa, tecnica e finanziaria necessaria per fornire servizi di certificazione.

2. utilizzare personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie a svolgere i servizi forniti

3. applicare procedure e metodi amministrativi e di gestione adeguati e conformi a tecniche consolidate

4. utilizzare sistemi affidabili e prodotti di firma protetti da alterazioni

5. adottare adeguate misure di sicurezza contro la contraffazione dei certificati e garantire la riservatezza, l'integrità e la sicurezza nella generazione delle chiavi

2.4. La marcatura temporale

Le marche temporali garantiscono un riferimento temporale opponibile a terzi (data/ora riferite alla scala di tempo UTC, con una differenza non superiore ad un minuto primo) e vengono fornite da un ente terzo detto Time Stamping Authority (normalmente un certificatore qualificato) attraverso una rete di telecomunicazione.

La Time Stamping Authority (TSA), usualmente, espone in rete un servizio ed i passi per richiedere la marcatura temporale di un documento sono:

1. dopo aver calcolato l'impronta di un documento mediante opportuni strumenti software, la si invia al server della TSA,

2. il server della TSA firma digitalmente data/ora corrente e impronta ricevuta e restituisce la marca temporale al richiedente.

2.5. I compiti del Responsabile della conservazione

Il Responsabile della Conservazione (RdC) ha l'onere di stabilire le caratteristiche e i requisiti del sistema di conservazione a norma nonchè la responsabilità di verificarne il corretto funzionamento.

Come precedentemente disposto dall'art. 5 (comma 1) della Deliberazione CNIPA n. 11 del 19 febbraio 2004, e successivamente ribadito dal DPCM 3 dicembre 2013, il Responsabile della Conservazione:

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

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

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

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

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

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

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

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

i) adotta le misure necessarie per la sicurezza fi sica e logica del sistema di conservazione ai sensi dell'art. 12 del DPCM 3 dicembre 2013;

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

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

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

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

La stessa Deliberazione citata (art. 5 comma 3) prevedeva la possibilità di affidare, in tutto o in parte il processo di conservazione, ad altri soggetti, pubblici o privati;la medesima possibilità è ora ribadita dal DPCM del 3 dicembre 2013 (art 6, comma 8)

Rispetto al quadro normativo precedente, le nuove regole tecniche in materia di conservazione prevedono che le pubbliche amministrazioni affidino i processi di conservazione a conservatori accreditati, pubblici o privati (art 5 comma 3 del DPCM del 3 dicembre 2013). Insiel, ha già iniziato il percorso per ottemperare a tale obbligo e le attività correlate dovranno tassativamente concludersi entro il 12 aprile 2017; fino al completamento del processo restano validi i sistemi realizzati ai sensi della Deliberazione CNIPA n. 11/2004 (art 14 del DPCM del 3 dicembre 2013)

3. Ripartizione dei compiti nel processo di conservazione a norma

La Regione Friuli Venezia Giulia e tutte le Aziende e gli Enti che intendono avvalersi dei servizi di conservazione in outsourcing erogati da Insiel SpA, nominano al proprio interno un Responsabile della Conservazione (RCE), redigono un proprio "Manuale della Conservazione " ai sensi dell'articolo 8 del DPCM 3 dicembre 2013, in esso specificano le attività che intendono delegare alla Regione FVG e, per tramite di quest'ultima, a Insiel SpA. Appositi disciplinari vengono redatti e sottoscritti tra le parti al fine di stabilire i ruoli e responsabilità, nonché le attività delegate e le caratteristiche del servizio fornito.

3.1. Compiti del Responsabile della Conservazione dell'Ente

L'RCE definisce le classi documentali e i metadati specifici, le caratteristiche, la periodicità di invio in conservazione, la frequenza di generazione dei pacchetti di archiviazione, il periodo di conservazione; ogni qualvolta emerga la necessità di variare il sistema di conservazione, l'RCE concorda con la Regione Friuli Venezia Giulia e con l'outsourcer nuove modalità operative.

Dopo l'attivazione del servizio da parte dell'outsourcer, l'RCE verifica la presa in carico dei documenti ovvero segnala al produttore del documento eventuali anomalie riscontrate durante tali fasi e vigila che il procedimento di conservazione si svolga in conformità alla normativa vigente e con le modalità concordate. A tal scopo e con finalità meramente ispettive può richiedere l'esibizione di documenti registrando gli esiti in un verbale sottoscritto congiuntamente all'RCO.

L'RCE opera d'intesa con il Responsabile del servizio di tenuta del protocollo informatico verifica che il sistema di conservazione assicuri il rispetto delle misure di sicurezza previste dagli articoli 31-36 del Decreto Legislativo n° 196 del 30/6/2003 *"Codice in materia di protezione dei dati personali"* e dal disciplinare tecnico pubblicato in allegato B.

3.2. Compiti dell'outsourcer

Analogamente a quanto avviene per i soggetti committenti anche Insiel, in qualità di outsourcer, nomina un proprio Responsabile della Conservazione (RCO), che ha responsabilità sulle fasi del procedimento di conservazione a norma ad essa affidate.

L'RCO, in accordo con il Conservatore (Regione FVG) e l'RCE, predispone ed eroga le seguenti attività previste all'art 9 del DPCM 3 dicembre 2013:

- realizza ed esegue procedure informatiche che permettano l'acquisizione e la presa in carico del pacchetto di versamento;

- verifica che gli oggetti contenuti nel pacchetto di versamento siano conformi alle regole definite nel Manuale di Conservazione dell'Ente e, in caso contrario, genera automaticamente delle notifiche via e-mail, indirizzate all'RCE, specificando le anomalie riscontrate;

- genera automaticamente il rapporto di versamento e vi appone una marca temporale;
- predispone il pacchetto di archiviazione, lo firma digitalmente e vi appone una marca temporale;
- realizza procedure per la preparazione dei pacchetti di distribuzione che rende disponibili, al momento, presso una saletta di esibizione allestita presso la propria sede;

L'RCO inoltre

- attraverso un rigido assetto organizzativo, protegge il sistema da eventuali intrusioni di personale non autorizzato;
- traccia le attività correlate ai processi di conservazione;
- aggiorna il proprio dispositivo di firma digitale seguendo i dettami del Certificatore Qualificato che gli ha rilasciato il certificato,
- tiene aggiornata la documentazione relativa al servizio di conservazione in cui evidenzia gli aspetti organizzativi, quali ruoli e iter procedurali, nonché quelli tecnologici.

I dati identificativi del Responsabile della Conservazione a norma della società Insiel SpA e dei suoi eventuali delegati sono reperibili nel "Registro dei delegati alla conservazione" (IIT-CS-RG-01).

Al fine di monitorare e garantire il corretto funzionamento del procedimento di conservazione dei documenti, l'azienda ha costituito al suo interno, un apposito Servizio di Conservazione dei documenti (Servizio CS) che opera sotto la supervisione dell'RCO e di concerto con gli altri servizi e strutture societarie; esso si occupa di garantire:

- la gestione tecnica dell'infrastruttura hardware e software del sistema di conservazione, mediante l'adozione di misure atte ad assicurare la sicurezza logica e l'integrità fisica dei supporti di memorizzazione utilizzati;
- la manutenzione dei programmi utilizzati nel processo di conservazione e la verifica della loro corretta archiviazione, in accordo alle normative vigenti e alle disposizioni dello SQI;
- la gestione operativa ovvero:
  - la generazione e la schedulazione di processi di presa in carico per le classi documentali previste nei Manuali di conservazione degli Enti;
  - la predisposizione di procedure informatizzate che consentano la verifica di conformità dei pacchetti di versamento ai requisiti predefiniti e la notifica automatica agli RCE di eventuali anomalie rilevate;

- l'attivazione di procedure/applicazioni che consentono agli RCE (o ai loro delegati) il controllo, l'esibizione e la riproduzione di documenti che abbiano completato il processo di conservazione

- l'esecuzione e controllo dell'esito delle procedure che generano le copie di sicurezza

- lo stoccaggio dei dispositivi di memorizzazione contenenti le copie di sicurezza anche in luoghi geograficamente differenti

- l'esecuzione di controlli periodici sia a campione che massivi, in conformità alle disposizioni legislative vigenti, atti a garantire l'integrità e la leggibilità dei documenti posti in conservazione, con eventuale riversamento diretto o sostitutivo, ove necessario.

L'RCO ha il compito di intervenire personalmente nei confronti di tutte le strutture societarie coinvolte nel processo affinché eventuali malfunzionamenti emersi siano corretti e rimossi nel più breve tempo possibile ed ha facoltà, senza alcun preavviso, di effettuare personalmente, o far svolgere da altri soggetti preposti, le verifiche funzionali ritenute necessarie a garanzia del corretto svolgimento del processo con particolare riguardo all'applicazione puntuale delle norme. Gli esiti dei controlli (integrità dei documenti e dei supporti, anomalie dei documenti...) vengono registrati in appositi registri, anche informatici e gli accessi al sistema vengono tracciati in appositi log sottoposti, anch'essi, a processo di conservazione.

4. Aspetti operativi e procedurali.

Il processo di conservazione si applica a documenti informatici; essi vengono controllati, raggruppati e trasferiti su un supporto idoneo alla loro conservazione; l'apposizione della firma da parte dell'RCO (o dei suoi delegati) e della marca temporale sull'indice di archiviazione contenente le impronte di tutti i documenti del pacchetto permettono di garantirne l'immodificabilità e verificare nel tempo la loro integrità.

4.1. L'organizzazione del lavoro.

Il processo di Conservazione viene eseguito in collaborazione con le altre strutture gestionali operanti nel contesto del Servizio CTOSIR mediante l'utilizzo di procedure informatiche la cui operatività è garantita dal Servizio CS.

I singoli processi si applicano a documenti, omogenei per tipologia ed Ente di appartenenza, e sono schedulati automaticamente con la frequenza richiesta dai Responsabili della Conservazione degli Enti committenti.

Ogni processo è costituito dalle seguenti fasi principali:

1. presa in carico dei documenti da parte del sistema di conservazione

2. controllo dell'integrità e della rispondenza dei documenti ai requisiti prefissati per la classe, registrazione dei metadati nel DataBase e generazione del rapporto di versamento ovvero segnalazione di eventuali anomalie riscontrate

3. archiviazione dei documenti nei dispositivi di memorizzazione non riscrivibili del sistema di conservazione

4. generazione del pacchetto di archiviazione, apposizione della firma dell'RCO (o dei suoi delegati) e della marca temporale: tali attività sanciscono l'inizio della fase di conservazione vera e propria.

4.2. Collocazione dei documenti da prendere in carico.

Le procedure di presa in carico vengono concordate con l'RCE committente e differiscono a seconda del sistema gestionale del cliente e dalla sua collocazione.

Possiamo avere infatti:

1. enti che utilizzano applicazioni Insiel e che si avvalgono della Server Farm Insiel

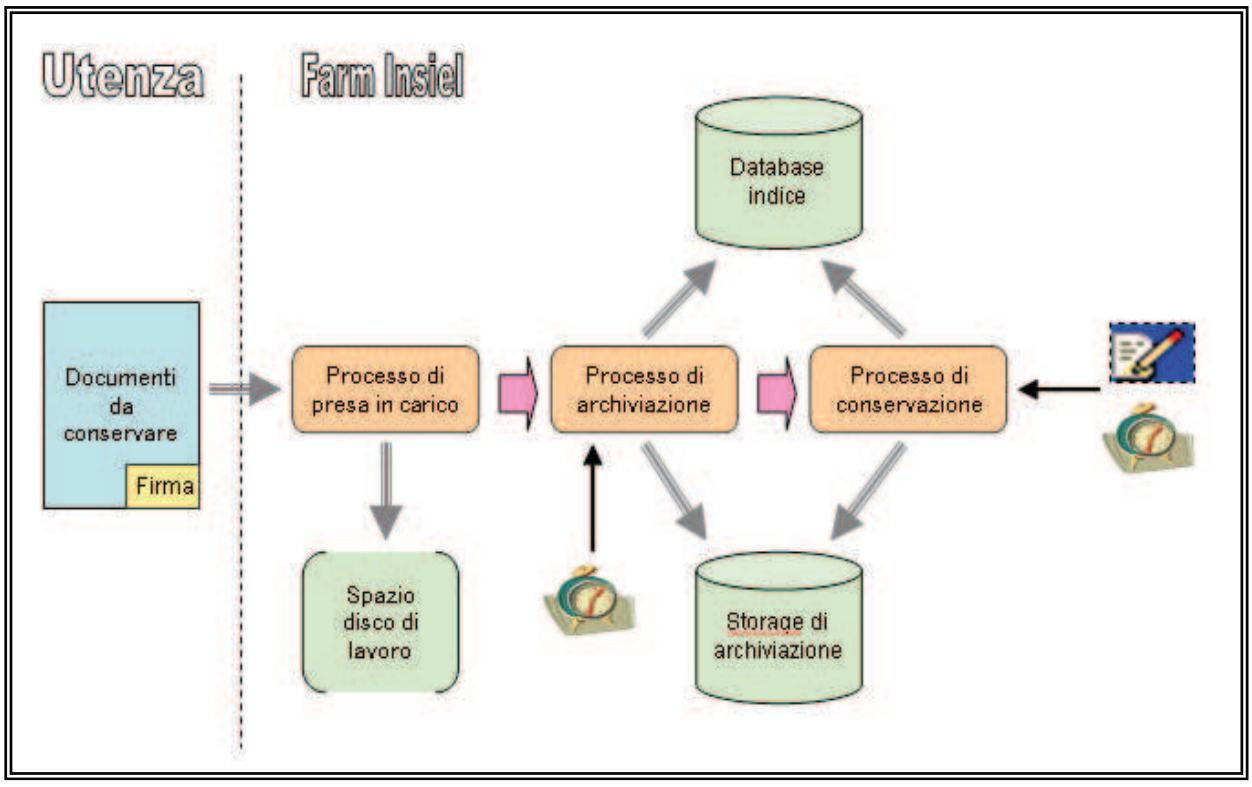
2. enti che utilizzano applicazioni Insiel ma che gestiscono esternamente alla Server Farm Insiel le basi di dati

3. enti che utilizzano applicazioni non Insiel e le cui basi di dati sono memorizzate su infrastrutture dell'Ente stesso

La predisposizione delle liste di documenti da portare in conservazione rimane in carico alle applicazioni gestionali che generano e gestiscono il flusso documentale. La procedura di presa in carico in conservazione può essere personalizzata a seconda della collocazione degli elenchi e dei documenti da elaborare, ed è in grado, se necessario, di generare essa stessa files XML di metadati sulla base di specifiche tecniche concordate (XSD).

4.3. Definizione del processo di conservazione.

Lo schema di seguito riportato riassume per blocchi funzionali la sequenza operativa della procedura di conservazione:



Nello schema vengono evidenziati anche lo spazio temporaneo utilizzato dai processi come area di lavoro, i dispositivi di memorizzazione (storage) dove vengono archiviati e conservati i documenti e il "database indice" contenente i metadati necessari alle ricerche dei documenti nonché tutte le informazioni di dettaglio che consentono di gestire i processi.

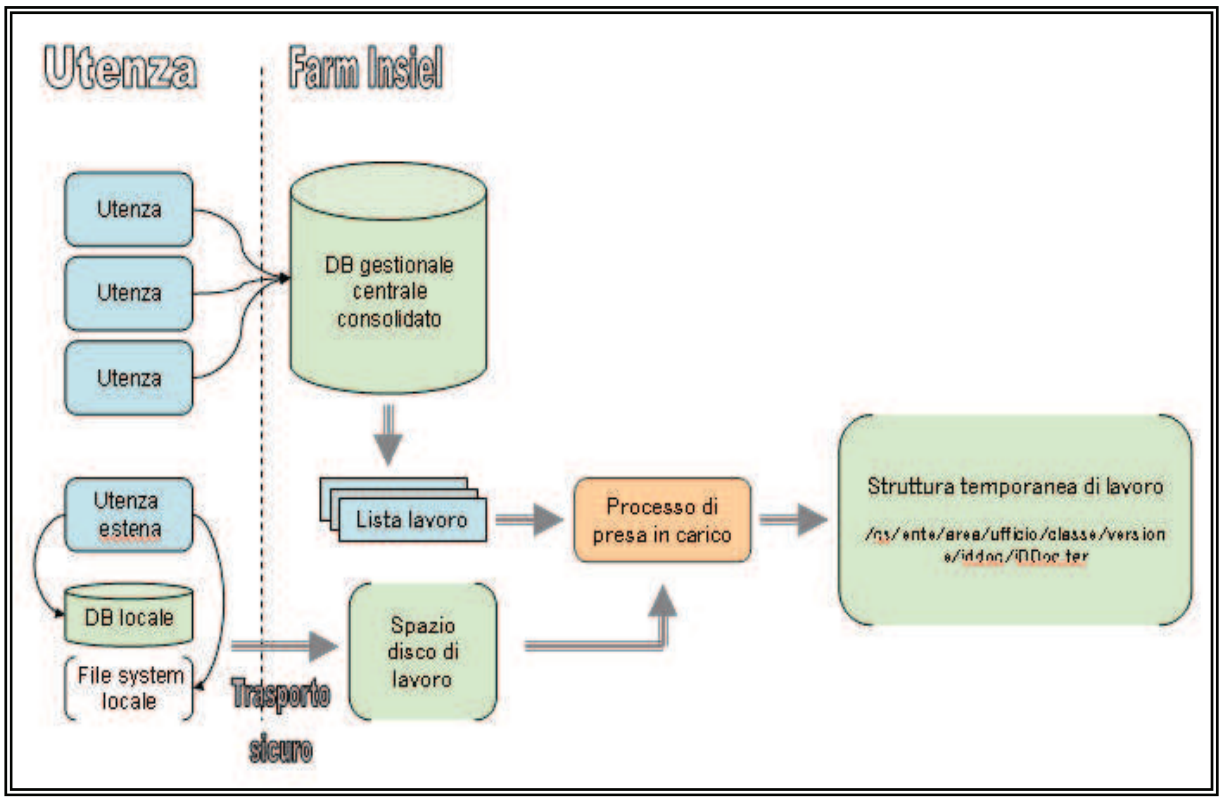
La durata del periodo di conservazione non potrà essere inferiore a quello dichiarato, per ogni singola classe documentale, sul manuale della conservazione, adottato dagli Enti, in vigore al momento della

presa in carico. Eventuali prolungamenti dovranno essere concordati successivamente e comunque non prima della scadenza della marca temporale.

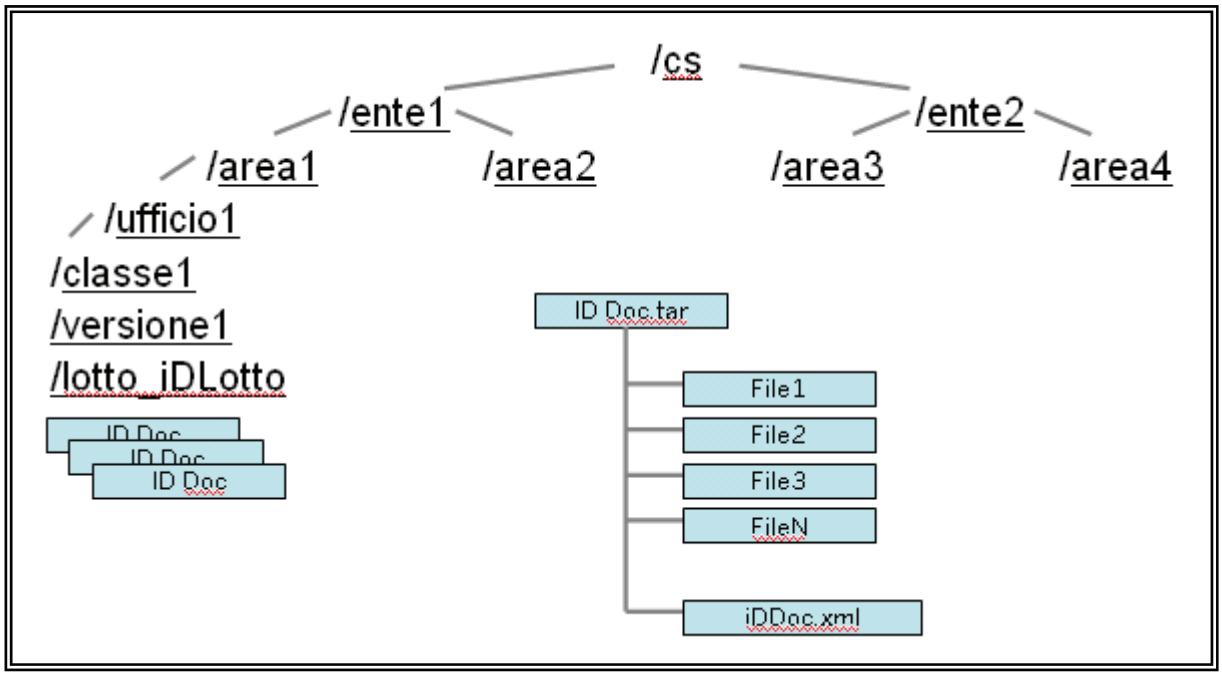
Per quanto attiene i lotti di documenti appartenenti a classi documentali per le quali il periodo di conservazione, dichiarato dall'Ente, risulta illimitato o superiore alla durata massima di validità della marca temporale applicata (attualmente 20 anni prolungabili su richiesta – art. 53 DPCM 22 febbraio 2013), Insiel provvederà a richiedere il prolungamento della validità della marca temporale ovvero ad effettuare tutte le operazioni che si rendessero necessarie a consolidare ulteriormente la conservazione.

4.3.1. Il processo di presa in carico.

Rappresenta il passo iniziale del procedimento: i documenti da conservare, presenti nell'elenco messo a disposizione dal sistema gestionale vengono copiati, unitamente ai loro metadati strutturati in base alle specifiche concordate con i committenti (XSD), su un'area temporanea di lavoro e resi disponibili alle elaborazioni successive.



Il risultato di questa prima fase elaborativa sull'area temporanea di lavoro è rappresentato da una struttura di cartelle nidificate la cui foglia finale contiene un file, denominato "tarfile" in cui sono presenti, in formato compresso, il documento e i suoi allegati, un file di tipo "xml", chiamato "xml dichiarativo", contenente i metadati e le evidenze informatiche dei tutti i files, ed eventuali marche temporali associate.



4.3.2. Il processo di archiviazione.

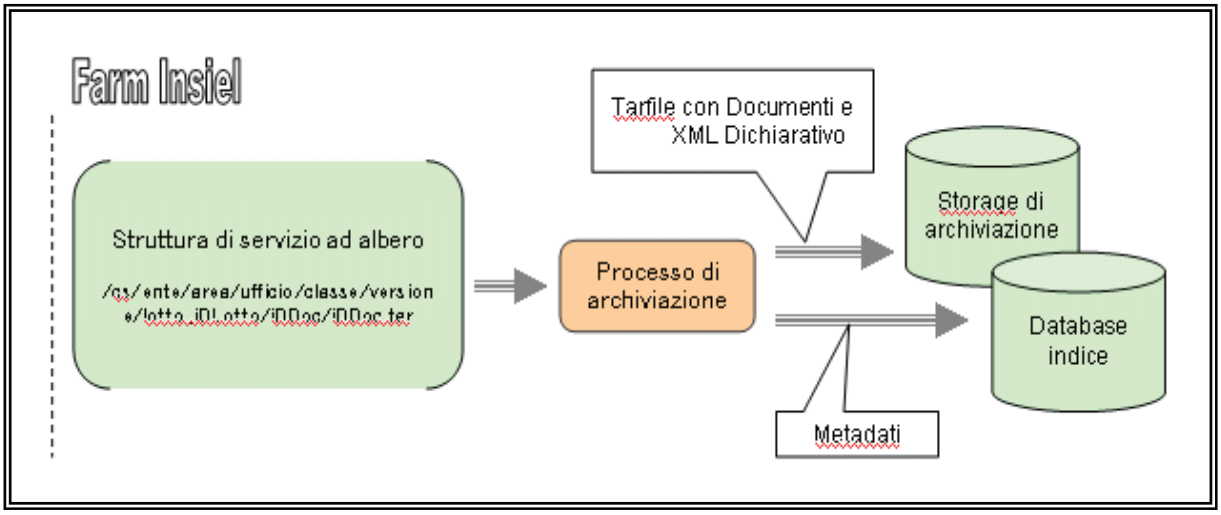
In questa fase i documenti vengono sottoposti a tutti i controlli preliminari necessari a determinare la loro idoneità, integrità e congruenza con le caratteristiche predefinite a livello di classe documentale.

Sono effettuati controlli di:

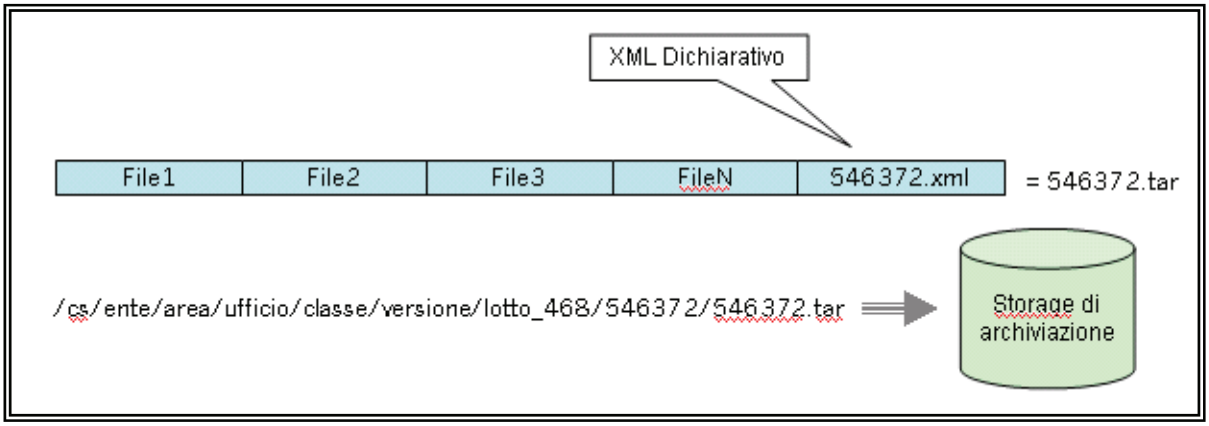
1. validità della firma e della eventuale marca temporale,
2. correttezza dell'impronta (se già disponibile),
3. presenza dei metadati obbligatori,
4. Idoneità dei formati.

I documenti invalidi o non rispondenti ai requisiti vengono scartati e contestualmente il sistema avvisa via e-mail l'RCE e il Servizio CS di Insiel delle anomalie riscontrate.

In questa fase si provvede inoltre a segnalare all'Ente interessato l'eventuale prossima scadenza dei certificati digitali di autenticazione, affinché si possa provvedere per tempo al loro rinnovo.



Il dispositivo ed il processo di archiviazione utilizzati garantiscono fin da subito l'immodificabilità dei documenti anche se la data di inizio conservazione verrà consolidata solamente nella successiva fase di conservazione.



Un pacchetto di archiviazione può essere formato da documenti archiviati in fasi successive e, al fine di consolidare immediatamente la validità del certificato di firma, ad ogni archiviazione viene generato anche un file di tipo xml, detto lotto parziale o rapporto di versamento, sul quale viene applicata la marca temporale; tale file contiene le impronte dei documenti archiviati nella singola fase e garantisce fin da subito il prolungamento di validità del certificato di firma dei documenti coinvolti.

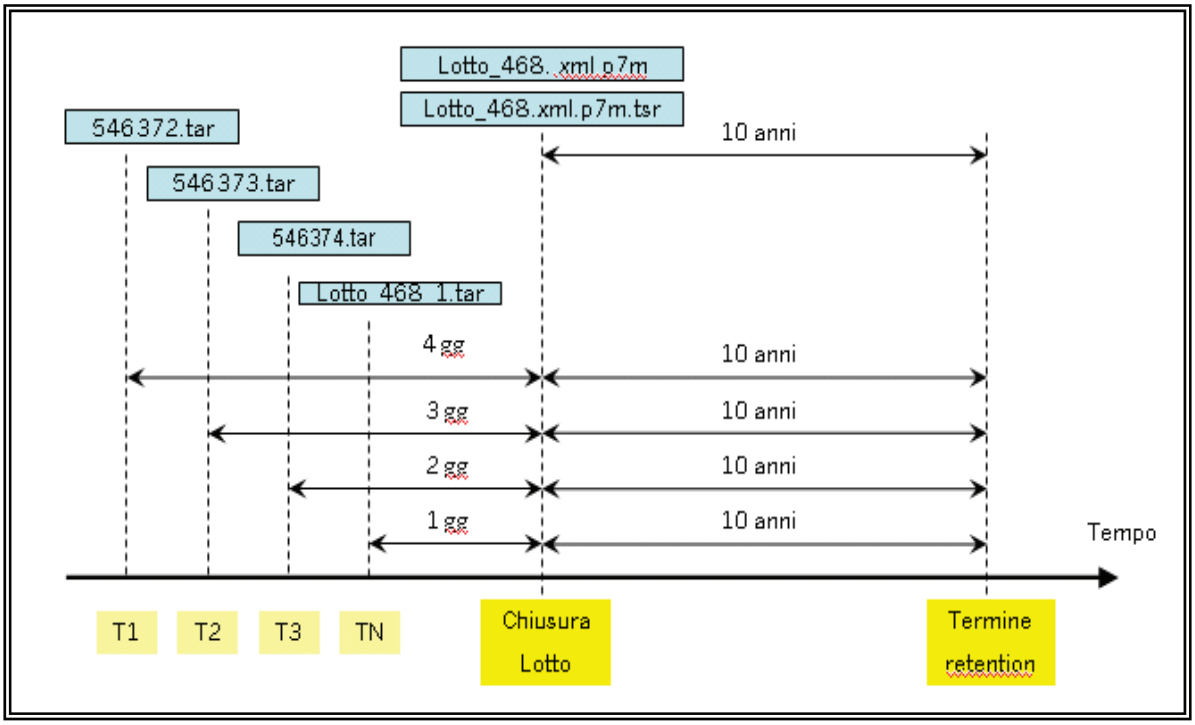
4.3.3. Il processo di conservazione.

Il processo viene attivato secondo le modalità concordate con il RCE e può essere legato alla dimensione o o al numero di documenti del lotto oppure ancora ad una periodicità prefissata.

Essendo i documenti appartenenti al lotto già archiviati, la predisposizione del pacchetto di archiviazione consiste nella preparazione di un file di tipo xml, detto "xml di chiusura lotto", riportante le evidenze informatiche di tutti i documenti archiviati nei lotti parziali; esso viene firmato dal Responsabile della Conservazione dell'Outsourcer (o da un suo delegato) e marcato temporalmente e quindi conservato con le policy previste per la classe documentale a cui i documenti appartengono.

La firma del Responsabile della Conservazione dell'Outsourcer (o da un suo delegato) può essere apposta anche mediante funzionalità di firma massiva.

L'ultimo passo del processo di conservazione, consiste nella sincronizzazione dei tempi di ritenzione per tutti i file appartenenti al lotto, anche se archiviati in tempi diversi, ovvero la data di inizio conservazione sarà la medesima per tutti gli elementi appartenenti al lotto.



4.4. Gestione della privacy

Gli accordi fra Regione Friuli Venezia Giulia ed Insiel, prevedono per la società dei precisi obblighi di riservatezza ed richiedono l'applicazione del Decreto legislativo 196/03, denominato "Codice in materia di protezione dei dati personali" .

Regione Friuli Venezia Giulia, in qualità di titolare dei trattamenti dei dati personali oggetto dei servizi, ai sensi e per gli effetti del citato decreto legislativo, nomina Insiel quale Responsabile dei predetti trattamenti.

Nelle more del citato ruolo di "Responsabile del Trattamento", Insiel SpA che mantiene aggiornati le applicazioni, i servizi e le infrastrutture nel rispetto della normativa citata, con particolare riferimento a quanto stabilito nel Titolo V ("Sicurezza dei dati e dei sistemi"), Capo I ("Misure di sicurezza") e Capo II ("Misure minime di sicurezza") e nel "Disciplinare Tecnico in materia di misure minime di sicurezza" (allegato B).

Annualmente Insiel SpA predispone, in qualità di "Responsabile Trattamento", il Documento Programmatico sulla Sicurezza (DPS) che provvede formalmente a consegnare alla Regione Friuli Venezia Giulia ad alle Aziende Sanitarie che aderiscono al Sistema Informativo Socio Sanitario Regionale (SISSR).

Nell'ambito del DPS vengono dettagliati:

- la distribuzione dei compiti e delle responsabilità,
- l'analisi dei rischi incombenti sui dati
- le misure di protezione adottate,
- i criteri e le modalità di ripristino della disponibilità dei dati,
- gli interventi formativi correlati.

4.5. Controllo degli accessi fisici e logici

Per quanto attiene il controllo degli accessi, Insiel SpA ha predisposto una specifica procedura secondo la quale vengono dettagliatamente elencate le responsabilità e descritti i criteri per la gestione accessi delle credenziali e dei permessi di accesso ai contenuti informativi.

Per la gestione della sicurezza, vengono presi in considerazione i seguenti aspetti:

- identificazione - atto con cui un soggetto dichiara la propria identità (è il primo passo dell'autenticazione),

- autenticazione - processo di verifica dell'identità dichiarata dal soggetto (è correlata all'identificazione),
- autorizzazione - concessione dei diritti di accesso al soggetto dopo la sua identificazione e autenticazione,
- tracciabilità - registrazione delle azioni svolte dal soggetto precedentemente identificato in modo univoco.

I diritti di accesso dipendono dal ruolo assegnato e consentono la visibilità dei soli dati di competenza.

4.6. Gestione delle password.

Insiel SpA ha inoltre stabilito le modalità per la registrazione e la cancellazione delle credenziali di accesso e quelle di assegnazione delle password e dei relativi privilegi. Periodicamente, e comunque almeno semestralmente, viene effettuato un processo formale di revisione dei diritti di accesso.

I soggetti abilitati vengono comunque forzati a cambiare trimestralmente le password di login rispettando per esse le seguenti caratteristiche:

- lunghezza minima 8 caratteri
- combinazione di caratteri alfanumerici, minuscoli e maiuscoli
- unicità a livello di sistema
- non visibilità in fase di inserimento nelle sessioni di logon
- Inoltre ogni sessione di lavoro viene chiusa dopo 30 minuti di inattività.

4.7. La manutenzione.

Il sistema preposto alla conservazione documentale a norma può essere variato a fronte di:

- necessità di adeguamento a nuove disposizioni normative,
- richieste di implementazione da parte dei RCE,
- correzione di errori,
- manutenzione ordinaria dell'infrastruttura hardware e software,
- adeguamenti tecnologici dell'infrastruttura hardware e software.

Ogni modifica alla configurazione del sistema verrà opportunamente pianificata di concerto ai RCE, in modo da ridurre al minimo l'impatto verso l'utenza e sarà opportunamente registrata secondo le modalità previste dal SQI. In particolare gli interventi effettuati sul sistema operativo o sui componenti sw non applicativi utilizzati dai server del sistema di conservazione verranno registrati anche tramite l'uso di un apposito registro delle manutenzioni programmate (IIT-CS-RG-04). Nel caso in cui le modifiche della configurazione introdotte comportino la necessità di effettuare un riversamento dei documenti in conservazione, si provvederà alla registrazione di tale operazione sul registro dei riversamenti (IIT-CS-RG-05). Le modifiche apportate ai programmi applicativi verranno registrate in base a quanto previsto dal sistema qualità aziendale.

Tutte le modifiche alla configurazione del sistema di erogazione del servizio devono essere preventivamente sottoposte al vaglio dell'RCO o dei suoi delegati.

5. Procedure di gestione delle copie di sicurezza.

5.1. Produzione dei backup.

Nelle politiche di backup notevole importanza rivestono le copie di sicurezza ottenute tramite i salvataggi su nastro magnetico, che costituiscono una ulteriore garanzia di protezione contro potenziali eventi che potrebbero invalidare i dati in conservazione, oltre a rappresentare un indispensabile strumento nell'ambito del disaster recovery.

La politica di backup implementata da Insiel per il progetto di conservazione a norma si basa sull'utilizzo di componenti software che gestiscono l'automazione delle operazioni di salvataggio dei dati; tali operazioni sono effettuate tramite l'impiego di una tape library costituita da un sistema modulare, composto da frame individuali in grado di utilizzare supporti magnetici di tipo WORM (Write Once, Read Many) conformi ai requisiti normativi richiesti per l'archiviazione dei dati.

Tutti i dispositivi utilizzati e le componenti di accesso agli stessi, compresi i sistemi di controllo della libreria, sono ridondati in modo tale da assicurare la continuità del servizio anche in condizioni di guasto su alcune componenti hardware del sistema.

La memorizzazione dei dati su cassetta ai fini di backup viene gestita in base a specifici criteri; i dati che risiedono nello storage primario di archiviazione (su disco) vengono salvati automaticamente in condizioni che garantiscono di operare su una struttura congruente e definita (non in fase di aggiornamento). Dopo il salvo iniziale solo i dati inseriti successivamente nella struttura considerata vengono salvati (backup incrementale).

I salvataggi effettuati copiano i dati inseriti nella struttura successivamente all'ultimo backup; i dati salvati vengono mantenuti on-line nella tape library su supporti di tipo WORM per un eventuale e rapido ripristino mirato su disco mentre copie dell'intero storage pool della conservazione vengono giornalmente archiviate ai fini del disaster recovery, secondo le modalità descritte nel documento "*Modello: Disaster Recovery Conservazione Sostitutiva Documenti* " (IOF-CS-GO-01 Allegato-disaster recovery) allegato alla Guida Operativa (IOF-CS-GO-01 Guida operativa.doc).

Si hanno quindi a disposizione, su supporti fisici stoccati in locali protetti, set di cassette a partire dai quali è possibile ricostruire, all'occorrenza, la base informativa della conservazione a norma. Le varie fasi di questo processo vengono controllate per verificarne la regolare conclusione.

5.2. Archiviazione dei supporti di backup.

I supporti creati dalle procedure di backup vengono immagazzinati e custoditi in luoghi geografici differenti, al fine di salvaguardare i dati da danni provocati da calamità.

I locali destinati allo stoccaggio hanno le seguenti caratteristiche:

- impianto anti-intrusione,
- impianto antincendio,
- requisiti di sicurezza negli ambienti di lavoro, come da legge n° 626/94 e successive,
- sistemi impiantistici e strutture immobiliari conformi, per quanto attiene alle tipologie di costruzione, alle norme CEI ed UNI in materia.

5.3. Procedure di verifica dei supporti di backup.

La policy di backup adottata prevede l'esecuzione di controlli periodici sui dispositivi di memorizzazione WORM usati per il salvo dei dati in conservazione; lo scopo è quello di verificare l'integrità e la leggibilità dei supporti utilizzati. Sono previste delle procedure di recupero a campione di singoli documenti e di intere strutture documentali che vengono copiate dai dispositivi di backup e rese temporaneamente disponibili per le operazioni di controllo in un apposito ambiente di lavoro, distinto da quello originale di conservazione. L'esito delle verifiche sui documenti recuperati viene registrato in uno specifico verbale in cui vengono descritte le verifiche effettuate; al termine delle stesse si procede alla soppressione dell'ambiente temporaneo di lavoro.

In caso di rilevata difettosità del supporto di backup di tipo WORM viene eseguita la medesima procedura sul dispositivo contenente il salvo più recente dello storage pool della conservazione; successivamente si provvede a effettuare un nuovo salvataggio dell'intero storage pool su cassette WORM (che va in sostituzione di quello precedente costituito da supporti magnetici di cui si è evidenziata la parziale difettosità).

6. Procedure di gestione degli eventi catastrofici.

Questo paragrafo descrive, nelle sue linee generali, le modalità adottate per fronteggiare le ripercussioni sul servizio di conservazione a norma che potrebbero essere causate dal manifestarsi di eventi eccezionali e catastrofici, focalizzando l'attenzione sulla continuità del servizio.

6.1. Continuità del business.

Insiel S.p.A., a seguito di una attenta valutazione del rischio, ha predisposto un piano teso al raggiungimento di una sempre maggior garanzia della continuità del business. Ciò ha comportato una verifica dei processi aziendali e l'identificazione degli eventi che possono costituire possibili cause di interruzione all'erogazione del servizio.

Il piano di recovery per la conservazione documentale è stato predisposto utilizzando appositi componenti software che consentono anche la gestione di supporti di memorizzazione immagazzinati in sede diversa e il ripristino del server di controllo dell'ambiente di conservazione nel caso in cui esso risulti completamente inutilizzabile.

In esso si considerano:

- l'identificazione delle responsabilità e delle procedure di emergenza.
- l'implementazione delle procedure d'emergenza per il ripristino operativo nei tempi previsti.
- la documentazione delle procedure e dei processi previsti.
- la formazione del personale coinvolto nelle procedure d'emergenza.
- la verifica dei piani di emergenza che necessitano di prove e di revisioni periodiche ai fini della loro efficacia attuativa.

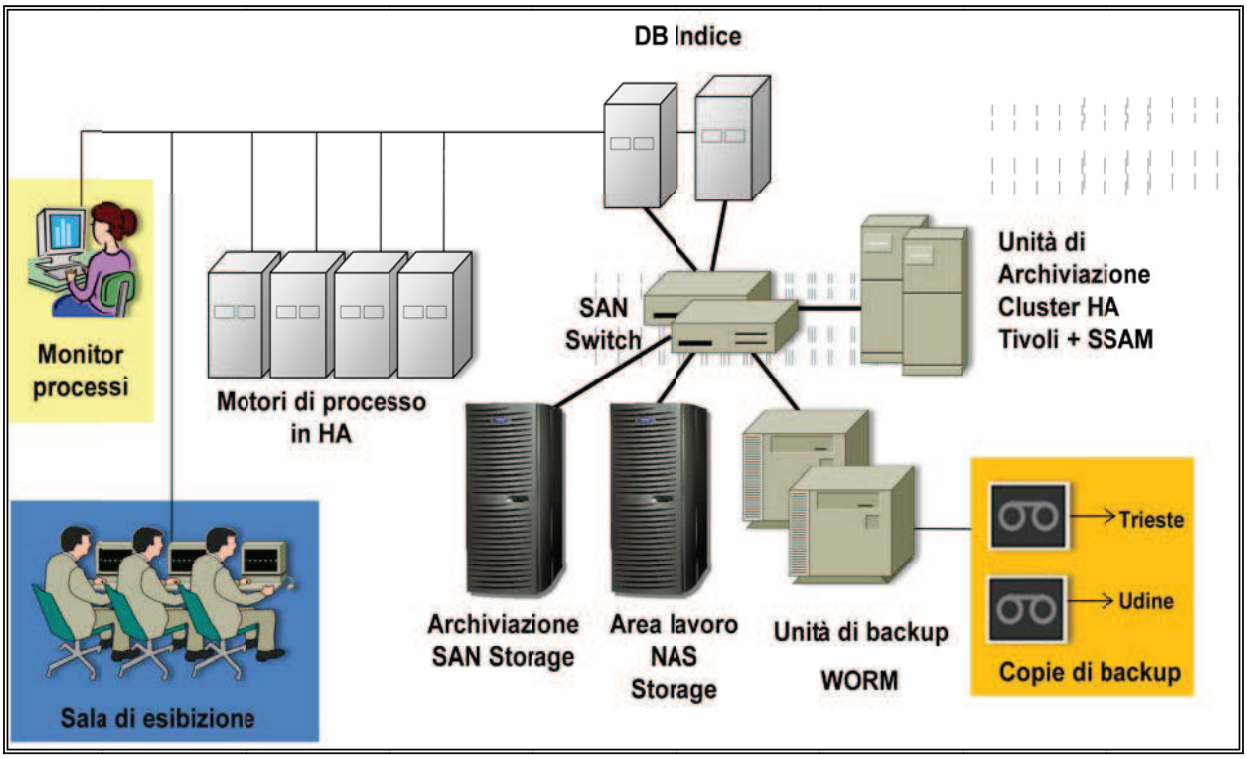
6.2. Guasti ai sistemi di elaborazione

L'ambiente operativo utilizzato, in accordo con le politiche aziendali in essere, è stato strutturato in modo tale da fornire ampie garanzie di sicurezza per l'integrità e la disponibilità dei dati anche a fronte di guasti improvvisi agli elaboratori utilizzati. Il sistema di conservazione si appoggia a server aziendali tecnologicamente avanzati e opportunamente ridondati (server mirrorati e dotati di gruppi di continuità). I dispositivi vengono ridondati in base alla numerosità dei dati da trattare ed ai carichi di lavoro previsti, in modo da garantire il più possibile sia le prestazioni che la continuità di servizio a fronte di eventuali guasti.

A seconda della tipologia di componenti l'alta affidabilità (HA) è stata realizzata utilizzando le tecnologie più adeguate e di seguito riportate:

- Database (attraverso l'utilizzo di sistemi clusterizzati multinodo su cui viene resa disponibile la base dati d'indicizzazione).
- Storage (attraverso l'utilizzo di dispositivi con hardware ridondato).
- sistema di archiviazione (attraverso l'utilizzo di sistemi clusterizzati multinodo).
- application server (attraverso l'utilizzo parallelo di più motori di processo su sistemi diversi).
- unità a nastro (attraverso l'utilizzo anche parallelo di più unità di scrittura).
- collegamenti di rete nella Server Farm Insiel (attraverso l'uso di apparecchiature di switch ridondate).

L'infrastruttura predisposta è in grado di garantire la continuità del servizio anche a fronte di guasto del singolo apparato ridondato.



Situazioni più complesse che coinvolgono l'infrastruttura in cui la ridondanza non è sufficiente a far fronte al disservizio, vengono governate in base ai piani di ripristino predisposti.

6.3. Compromissione del software.

In caso di malfunzionamento dei programmi utilizzati nelle procedure di conservazione si può ripristinare l'uso della versione precedente a partire dai backup aziendali dei repository del software.

6.4. Guasto al dispositivo di firma.

In caso di guasto al dispositivo di firma del Responsabile della Conservazione questi può essere sostituito nell'apposizione della firma digitale da personale opportunamente delegato munito di analogo dispositivo funzionante.

6.5. Compromissione del sito della Certification Authority.

La compromissione del sito della Certification Authority per il rilascio della marca temporale da apporre sul flusso dei documenti in conservazione per la certificazione della presenza alla data, è un evento ragionevolmente remoto. Vi è da sottolineare che la Certification Authority implementa politiche di continuità di erogazione del servizio con SLA di altissimo livello per cui questo è un evento da considerarsi piuttosto remoto.

7. Verifiche periodiche.

7.1. Generalità.

Oltre alle verifiche previste dalle disposizioni di legge e dalla normativa vigente (art. 5 comma 1 lettera h della Deliberazione CNIPA nr 11/2004 del 19 febbraio 2004 e DPCM 3 dicembre 2013, art.7, comma 1, lettera f), l'RCO ha disposto ulteriori controlli funzionali sui processi di conservazione.

Una procedura automatica verifica ogni giorno l'integrità dei documenti, garantendo il controllo di ogni singolo documento in un periodo non superiore ai 4 anni dalla sua conservazione e registrandone l'esito sul database indice consultabile mediante specifiche funzionalità, quotidianamente, inoltre, un soggetto preposto verifica manualmente l'integrità di almeno un documento per singolo pacchetto di archiviazione generato alla data e l'esito di tale operazione viene anch'esso registrato.

Report giornalieri, inviati automaticamente a tutti i delegati, permettono di appurare l'effettiva esecuzione dei lavori schedulati, il numero di documenti presi in carico ed archiviati e le eventuali anomalie riscontrate.

A cadenza mensile vengono effettuate delle verifiche sull'integrità e la "leggibilità dei supporti di memorizzazione allo scopo di intercettare, con l'ausilio di software appropriati, eventuali difettosità e provvedendo, se necessario, alla loro sostituzione. Gli esiti di tali verifiche (automatiche o manuali) vengono riportati, assieme alle eventuali notazioni, su appositi registri .

Secondo un calendario annuale, gli incaricati del Gruppo Assicurazione Qualità (GAQ) interni e gli ispettori esterni inviati dalla Società di certificazione ISO 9001 effettuano visite ispettive, allo scopo di verificare che i processi gestionali del Servizio CS:

- rispettino, nella prassi, i dettami stabiliti nella documentazione specifica del Servizio
- siano conformi ai requisiti di sicurezza.
- rispettino i regolamenti e le procedure del Sistema Qualità Insiel per i Servizi.

Le relative registrazioni sono effettuate in base a quanto stabilito dalla normativa ISO 9001 e dal SQI per i Servizi.

8. Esibizione dei documenti conservati.

L'esibizione è l'operazione che consente di visualizzare un documento conservato ed ottenerne copia (art.1, co.1, lett. m delibera CNIPA n.11/04).

Tale operazione può avvenire solo su richiesta dell'Ente proprietario del documento o, qualora normativamente previsto, di un'autorità superiore. Ogni Ente deve definire al proprio interno le modalità organizzative per la dichiarazione di conformità di un documento, nel caso in cui esso sia esibito su supporto cartaceo fuori dall'ambiente in cui è installato il sistema di conservazione.

Tranne casi eccezionali, la richiesta di esibizione dovrà essere indirizzata all'RCO (casella PEC di Insiel SpA) dalla casella PEC dell'Ente. Sarà cura dell'RCO provvedere al soddisfacimento della richiesta mettendo a disposizione il documento nei locali predisposti allo scopo presso la propria sede oppure attraverso la PEC aziendale.

9. Elenco dei Registri.

- *"Registro dei delegati alla conservazione"* (IIT-CS-RG-01)
- *"Registro delle verifiche documentali"* (IIT-CS-RG-02)
- *"Registro delle verifiche documentali sui supporti di backup"* (IIT-CS-RG-03)
- *"Registro delle manutenzioni programmate"* (IIT-CS-RG-04)
- *"Registro dei riversamenti"* (IIT-CS-RG-05)
- *"Registro delle versioni del documento IIT-CS-MP-01"* (IIT-CS-RG-06)
- *"Verbale di verifica" (IIT-CS-MD-01)*
- *"Verbale di esibizione" (IIT-CS-MD-01)*

Elenco firmatari

ATTO SOTTOSCRITTO DIGITALMENTE AI SENSI DEL D.P.R. 445/2000 E DEL D.LGS. 82/2005 E SUCCESSIVE MODIFICHE E INTEGRAZIONI

Questo documento è stato firmato da:

NOME: ANGELA ZANELLO
CODICE FISCALE: ZNLNGL63T57F756T
DATA FIRMA: 12/10/2015 15:32:16
IMPRONTA: 4044BB28F8BD3ACEF4E411FBD265DDF64C3E584950A6AA433B12C39544D52C4D
4C3E584950A6AA433B12C39544D52C4D968909C7F0FA82331181BF99E4D71B14
968909C7F0FA82331181BF99E4D71B14753331B8A7FF964EE9088E76E49D5CA9
753331B8A7FF964EE9088E76E49D5CA9D7D3FA22E24C961304FE70F009AD36D8

NOME: LUCA MARCHESI
CODICE FISCALE: MRCLCU65S03F205I
DATA FIRMA: 12/10/2015 15:35:23
IMPRONTA: C16BFE774B9005D87526D2A312404DA383E90839EEBD2CA76A5EC14FAA421948
83E90839EEBD2CA76A5EC14FAA4219485400F189088692717815D996803B7774
5400F189088692717815D996803B77743DDC5FA14175D214E1F8BD9CF83901DA
3DDC5FA14175D214E1F8BD9CF83901DA696901953E273F659AA0C264C4981B81

NOME: LUCA MARCHESI
CODICE FISCALE: MRCLCU65S03F205I
DATA FIRMA: 12/10/2015 15:36:43
IMPRONTA: AA35D31F9A2D21E462F4DBA943700EA786419AB44902B654B681836183F17149
86419AB44902B654B681836183F17149D5FC6EA6AE157AF770463E777EDBB452
D5FC6EA6AE157AF770463E777EDBB45222848AD05D98844245975928B2C3D627
22848AD05D98844245975928B2C3D6274B1846B122880A3A12EEF535C6846C9F