# Manuale di Conservazione

# Iccrea Banca S.p.A.

**EMISSIONE DEL DOCUMENTO**

| Azione | Data | Nominativo | Funzione |
|---|---|---|---|
| *Redazione* | 23/12/2019 | Caterina Pompei | *Responsabile del servizio di Conservazione* |
| *Verifica* | 27/12/2019 | Marco Palazzesi | Responsabile ad interim UO ICT Security |
| *Verifica* | 27/12/2019 | Fabio Stefanutti | Responsabile UO Applicazioni Gestionali e Direzionali |
| *Verifica* | 27/12/2019 | Giuseppe Cardillo | Responsabile UO Open Systems |
| *Approvazione* | 27/12/2019 | Vittorio Marogna | Responsabile UO Incassi e Pagamenti |

**REGISTRO DELLE VERSIONI**

| N°Ver/Rev/Bozza | Data emissione | Modifiche apportate | Osservazioni |
|---|---|---|---|
| 5.3 | 27/12/2019 | Adeguamento a seguito delle modifiche della struttura organizzativa di Iccrea Banca<br>Aggiornamento del capitolo Termination Plan | n.a |
| 5.2 | 13/06/2019 | Integrazione compiti del Responsabile della Conservazione<br>Aggiornamento del capitolo Sistema di Storage<br>Aggiornamento del capitolo Sincronizzazione dei Sistemi | n.a. |
| 5.1 | 02/05/2019 | Aggiornamento Termination Plan<br>Aggiornamento Ruolo | n.a. |
| 5.0 | 09/10/2018 | Adeguamento a seguito delle modifiche della struttura organizzativa di Iccrea Banca e avvio della nuova piattaforma operativa. | n.a. |
| 4.0 | 01/03/2016 | Adeguamento allo schema previsto da AGID | n.a. |
| 3.1 | 07/05/2015 | Interventi di fine tuning a seguito dell'esecuzione del piano di adeguamento. | n.a. |
| 3.0 | 31/03/2015 | Esecuzione del piano di adeguamento previsto | n.a. |
| 2.0 | 15/10/2014 | Adeguamento al Decreto del Presidente del Consiglio dei Ministri del 3/12/2013 "Regole Tecniche in materia di sistema di conservazione" | n.a. |
| 1.1 | 29/07/2013 | Creazione nuova classe documentale: Buste di cassa | n.a. |
| 1.0 | 17 /06/2012 | Creazione documento | n.a. |

*SOMMARIO*

# 1 Scopo e ambito del documento

Il presente documento è il Manuale della Conservazione di Iccrea Banca S.p.A. (di seguito Iccrea), la quale, nell'ambito della sua attività, ha sviluppato una piattaforma tecnologica in grado di gestire il processo di Conservazione digitale di documenti (di seguito "Conservazione").

Iccrea effettua il servizio di Conservazione per i propri documenti e in outsourcing assumendo il ruolo di Responsabile del Servizio di Conservazione per i Clienti.

Tutti i Clienti nominano un Responsabile della Conservazione interno.

Il Manuale della Conservazione con riferimento al sistema di conservazione illustra dettagliatamente (cfr. art. 8 Decreto del Presidente del Consiglio dei Ministri del 3/12/2013):

- l'organizzazione ed in particolare:
  - o la struttura organizzativa comprensiva delle funzioni, delle responsabilità e degli obblighi dei diversi soggetti che intervengono nel processo di conservazione;
- i soggetti coinvolti e i ruoli svolti dagli stessi ed in particolare:
  - o i dati dei soggetti che nel tempo hanno assunto la responsabilità del sistema di conservazione, descrivendo in modo puntuale, in caso di delega, i soggetti, le funzioni e gli ambiti oggetto della delega stessa;
- il modello di funzionamento ed in particolare:
  - o la descrizione delle tipologie degli oggetti sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di documenti e delle eventuali eccezioni;
  - o i tempi entro i quali le diverse tipologie di documenti devono essere scartate ovvero trasferite in conservazione;

    i casi in cui è previsto l'intervento di un Pubblico Ufficiale e le modalità con cui viene richiesta la sua presenza;
- la descrizione del processo ed in particolare:
  - la descrizione delle modalità di presa in carico di uno o più pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento;
  - la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione;
  - la modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;
  - la descrizione delle procedure per la produzione di duplicati o copie
  - la descrizione delle architetture e delle infrastrutture utilizzate ed in particolare:

- la descrizione del sistema di conservazione, comprensivo di tutte le componenti tecnologiche, fisiche e logiche, opportunamente documentate e delle procedure di gestione e di evoluzione delle medesime;

- le misure di sicurezza adottate ed in particolare:

la descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie.

Il presente documento è completato dall'allegato "Specificità del contratto" dove sono riportati:

1. l'elenco delle Classi documentali da portare in conservazione e relativi metadati per la conservazione;
2. le specifiche tecniche del servizio.

Torna al sommario

## 1.1 Struttura del documento

Per una efficace gestione del documento il Manuale è diviso in 9 capitoli riferiti a tre principali aree tematiche:

- **Introduttiva** che esplicita scopo e ambito del documento, terminologia e Normativa e standard di riferimento;
  1. Scopo e ambito del documento;
  2. Terminologia (glossario ed acronimi);
  3. Normativa e standard di riferimento;
- **Organizzativa** dove sono descritti i ruoli e le responsabilità assegnate nel servizio di Conservazione di Iccrea;
  4. Ruoli e Responsabilità;
  5. Strutture Organizzative;
- **Tecnico/Operativa** afferente la descrizione degli oggetti sottoposti a conservazione, delle modalità di svolgimento del Processo di Conservazione, del Sistema di Conservazione in tutte le sue componenti e delle modalità di svolgimento delle procedure di Monitoraggio e di controllo;
  6. Oggetti conservati;
  7. Processo di Conservazione;
  8. Sistema di Conservazione;
  9. Monitoraggio e Controlli.

Torna al Sommario

# 2 Terminologia (glossario ed acronimi)

| | |
|---|---|
| **ACCESSO** | Operazione che da il permesso di usufruire delle funzionalità erogate da sistema di conservazione comprese le funzionalità di presa visione ed estrazione copia dei documenti informatici. |
| **ACCREDITAMENTO** | Riconoscimento, da parte dell'Agenzia per l'Italia digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione. |
| **AFFIDABILITÀ** | Caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico. |
| **AGID** | Agenzia per l'Italia Digitale |
| **AGGREGAZIONE DOCUMENTALE INFORMATICA** | Aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia |
| **ARCHIVIAZIONE** | Processo di trattamento e gestione dei documenti di uso corrente e/o nel medio lungo periodo. È passo propedeutico alla conservazione, per il quale non sono previsti particolari obblighi di legge. |
| **ARCHIVIO** | Complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività. |
| **ARCHIVIO INFORMATICO** | Archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico. |
| **AREA ORGANIZZATIVA OMOGENEA** | Insieme di funzioni e di strutture, individuate dall'amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445.Documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445. |
| **ASP** | Application Service Provider. |
| **ATTESTAZIONE DI CONFORMITÀ DELLE COPIE PER IMMAGINE SU SUPPORTO INFORMATICO DI UN DOCUMENTO ANALOGICO** | Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico. |
| **AUTENTICITÀ** | Caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico. |
| **BASE DI DATI** | Collezione di dati registrati e correlati tra loro |
| **CA** | Certification Authority |
| **CAD** | Codice Amministrazione Digitale D.lgs. 82 del 7 marzo 2005 e successive modifiche. |
| **CAS** | Content Addressed Storage. |

| | |
|---|---|
| **CICLO DI GESTIONE** | Arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo. |
| **CLASSIFICAZIONE** | Attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati. |
| **CODICE** | Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni. |
| **CODICE ESEGUIBILE** | Insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici |
| **CONSERVATORE ACCREDITATO** | Soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, dall'Agenzia per l'Italia Digitale. |
| **CONSERVAZIONE** | Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel Manuale della Conservazione. |
| **COPIA ANALOGICA DEL DOCUMENTO INFORMATICO** | Documento analogico avente contenuto identico a quello del documento informatico da cui è tratto. |
| **COPIA INFORMATICA DI DOCUMENTO ANALOGICO**: | Il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto. |
| **COPIA PER IMMAGINE SU SUPPORTO INFORMATICO DI DOCUMENTO ANALOGICO** | Il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari. |
| **COPIA INFORMATICA DI DOCUMENTO INFORMATICO** | Il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari |
| **COPIA DI SICUREZZA:** | Copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell'articolo12 del DPCM 3 dicembre 2013. |
| **DATI GIUDIZIARI** | Dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e dar) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale. (Decreto Legislativo 30 giugno 2003, n.196 - Codice in materia di protezione dei dati personali Art. 4 comma 1 e)). |
| **DATI PERSONALI** | Dato personale è qualsiasi informazione (es. nome) concernente una **persona fisica identificata o identificabile** (art. 4 GDPR), anche indirettamente, oppure informazioni (es. codice fiscale, impronta digitale, traffico telefonico, immagine, voce) riguardanti una persona la cui identità può comunque essere accertata mediante informazioni supplementari. |
| **DATI GENETICI** | Sono i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione. |
| **DATI BIOMETRICI** | I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici. |

| | |
|---|---|
| **DATI RELATIVI ALLA SALUTE** | Il responsabile del trattamento (nel Regolamento UE 2016/679 data processor) è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento (art. 4, par. 1, n. 8 GDPR.) |
| **DESTINATARIO** | Identifica il soggetto/sistema al quale il documento informatico è indirizzato |
| **DISPONIBILITÀ** | Protezione dall'impossibilità di utilizzo di una informazione che deve essere sempre accessibile agli utilizzatori che ne hanno diritto, nei tempi e nei modi previsti dal livello di servizio concordato tra la Banca e il Cliente |
| **DOCUMENTO ANALOGICO** | La rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti |
| **DOCUMENTO ANALOGICO ORIGINALE** | S'intende un documento analogico che può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la Conservazione, anche se in possesso di terzi. |
| **DOCUMENTO INFORMATICO** | Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dato giuridicamente rilevanti |
| **DOCUMENTO STATICO E 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 possano modificare gli atti, i fatti o i dati nello stesso rappresentati. |
| **DUPLICATO INFORMATICO** | Il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario |
| **ESIBIZIONE** | Operazione che consente di visualizzare e rendere leggibile un documento conservato attraverso la visualizzazione e la stampa. |
| **EVIDENZA INFORMATICA** | Sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica. |
| **FASCICOLO INFORMATICO** | Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. |
| **FIRMA DIGITALE** | Un particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici. |
| **FIRMA ELETTRONICA** | L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare. |
| **FIRMA ELETTRONICA AVANZATA** | Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati. |

| | |
|---|---|
| **FIRMA ELETTRONICA QUALIFICATA** | Firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche |
| **FORMATO** | Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file. |
| **FTP SERVER** | Programma che permette di accettare connessioni in entrata e di comunicare con un Client attraverso il protocollo FTP |
| **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 |
| **HSM** | Hardware Security Module, Dispositivo sicuro in grado di impedire un accesso abusivo ai certificati di firma contenuti al suo interno. Può ospitare un elevato numero di certificati di firma e relative chiavi, è in grado di essere attivato da remoto e |
| **IDENTIFICATIVO UNIVOCO (DI SEGUITO DETTO TOKEN)** | Sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione. |
| **IDP** | Strumento per rilasciare le informazioni di identificazione di tutti i soggetti che cercano di interagire con un Sistema; ciò si ottiene tramite un modulo di autenticazione che verifica un token di sicurezza come alternativa all'autenticazione esplicita di un utente all'interno di un ambito di sicurezza. |
| **IMMODIFICABILITÀ** | Caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso |
| **IMPRONTA** | La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash. |
| | |
| **INSIEME MINIMO DI METADATI DEL DOCUMENTO INFORMATICO** | Complesso dei metadati, la cui struttura è descritta nell'allegato "Specificità del contratto" del presente manuale, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta. |
| **INTEGRITÀ** | Insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato. |
| **INTEROPERABILITÀ** | Capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi. |
| **LEGALDOC** | Software di InfoCert spa per l'implementazione dei sistemi di conservazione utilizzato da Iccrea per l'erogazione del servizio di conservazione digitale. |
| **LEGGIBILITÀ** | Insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti |
| **LOG DI SISTEMA** | Registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati. |
| **MANUALE DELLA CONSERVAZIONE** | Strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 delle regole tecniche del sistema di conservazione (DPCM del 3/12/2013). |

| | |
|---|---|
| **MARCA TEMPORALE** | Evidenza di tipo informatico che consente di rendere certa ed opponibile a terzi una determinata data. L'apposizione sull'insieme dei documenti deve essere effettuata a cura del Responsabile del servizio di Conservazione. Con l'apposizione della marca temporale si ottiene la certezza che il procedimento di Conservazione dei documenti sia stato completato in una determinata data e ora. |
| **MEMORIZZAZIONE** | Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici. |
| **METADATI** | Insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 del DPCM 3/12/2013. |
| **OAIS** | ISO 14721:2012; Open Archival Information System |
| **PACCHETTO DI ARCHIVIAZIONE** | Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del DPCM 3/12/2013 e secondo le modalità riportate nel Manuale della Conservazione. |
| **PACCHETTO DI DISTRIBUZIONE** | Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta |
| **PACCHETTO DI VERSAMENTO** | Pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel Manuale della Conservazione |
| **PACCHETTO INFORMATIVO** | Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare |
| **PRESA IN CARICO** | Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal Manuale della Conservazione. |
| **PROCESSO DI CONSERVAZIONE** | Insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 9 del DPCM 3/12/2013. |
| **PRODUTTORE** | Persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale. |
| **RAPPORTO DI VERSAMENTO** | Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore. |
| **REGISTRAZIONE INFORMATICA** | Insieme delle informazioni risultanti da transazioni informatiche o dalla presentazione in via telematica di dati attraverso moduli o formulari resi disponibili in vario modo all'utente |
| **REGISTRO DI PROTOCOLLO** | Registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti. |
| **RESPONSABILE DELLA CONSERVAZIONE** | Soggetto responsabile dell'insieme delle attività elencate nell'articolo 7,comma 1 del DPCM 3/12/2013. |

| | |
|---|---|
| **RESPONSABILE DEL SERVIZIO DI CONSERVAZIONE** | Risorsa di Iccrea, che, su delega del Responsabile della Conservazione, gestisce le politiche generali del sistema di conservazione, nel rispetto del modello organizzativo esplicitato nel presente Manuale e di quanto previsto nel contratto |
| **RESPONSABILE DEL TRATTAMENTO DEI DATI** | Il responsabile del trattamento (nel Regolamento UE 2016/679 data processor) è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento (art. 4, par. 1, n. 8 GDPR.) |
| **RESPONSABILE DELLA SICUREZZA INFORMATICA** | Soggetto al quale compete la definizione delle soluzioni tecniche ed Organizzative in attuazione delle disposizioni in materia di sicurezza |
| **RICEVUTA** | Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione del documento inviato dal produttore |
| **RIFERIMENTO TEMPORALE** | Informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento |
| **RISERVATEZZA** | Protezione da divulgazione non autorizzata delle informazioni, le quali devono essere accessibili direttamente o indirettamente solo alle persone che ne hanno diritto e che sono espressamente autorizzate a conoscerle |
| **SCARTO** | Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale. |
| **SEGMENTO DI ARCHIVIO** | Sottoinsieme di una parte dell'archivio di documenti informatici, firma e marca temporale, che costituiscono l'implementazione della Conservazione a norma di legge. Un archivio è creato in modo incrementale attraverso la Conservazione di segmenti di archivio definiti in ragione del volume massimo occupabile da un singolo segmento e della periodicità dell'emissione. |
| **SISTEMA DI CLASSIFICAZIONE** | Quadro di classificazione (Titolario) di riferimento, articolato in titoli e classi ed eventualmente in ulteriori sotto-partizioni, in base al quale i documenti dell'archivio corrente vengono raggruppati secondo un ordine logico, con riferimento alle funzioni alle attività dell'amministrazione interessata |
| **SISTEMA DI CONSERVAZIONE** | Sistema di conservazione dei documenti informatici di cui all'articolo 44 del codice |
| **SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI** | Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del DPR 28 dicembre 2000, n. 445; per i privati è il sistema che consente la tenuta di un documento informatico |
| **SOTTOSCRIZIONE ELETTRONICA** | L'apposizione della firma elettronica qualificata. La firma verrà generata attraverso l'utilizzo di un dispositivo di firma sicuro. |
| **STATICITÀ** | Caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione |
| **TESTO UNICO** | Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni |
| **TITOLARE** | La persona fisica o giuridica o altro tipo di società o ente che è giuridicamente responsabile della formazione dei documenti da conservare formati in proprio ovvero formati da terzi in suo/loro nome, conto e interesse. |
| **TRANSAZIONE INFORMATICA** | Particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche della base di dati. |

| | |
|---|---|
| **TSA TIME STAMPING AUTHORITY** | Ente terzo che emette i certificati di marcatura temporale |
| **TSS TIME STAMPING SERVICE** | Servizio di marcatura temporale che emette marche temporali utilizzando il certificato emesso da una TSA |
| **UTENTE** | Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse |

Torna al sommario

# 3 Normativa e standard di riferimento

## 3.1 Normativa di riferimento

**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],

**Legge 7 agosto 1990, n. 241 e s.m.i**. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;

**Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013,** "Regole tecniche per il protocollo informatico (D.P.C.M.)

**Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445**, recante «Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa" (D.P.R.)

**Decreto Legislativo 30 giugno 2003, n.196 "**Codice in materia di protezione dei dati personali"

**Decreto Legislativo 22 gennaio 2004, n. 42,** e s.m.i., recante «Codice dei beni culturali e del paesaggio, ai sensi dell'art. 10 della legge 6 luglio 2002, n. 137».

**Decreto Legislativo 7 marzo 2005, n.82 "**Codice dell'amministrazione digitale (CAD)" modificato in ultima istanza dal **Decreto legislativo 30 dicembre 2010, n. 235, e dal decreto legge 13 agosto 2011, n. 138.**

**Decreto Legge 24 aprile 2014, n. 66**, Misure urgenti per la competitività e la giustizia sociale, art. 42

**Decreto Ministero dell'Economia e delle Finanze, 3 aprile 2013, n. 55** "Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'articolo 1, commi da 209 a 213, della legge 24 dicembre 2007, n. 244"

**Circolare Agenzia delle Entrate n.45/E del 19 ottobre 2005.**

**Circolare 36/E dell'Agenzia delle Entrate dicembre 2006.**

**Decreto Presidente Consiglio dei Ministri 22 febbraio 2013. "**Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali"

**Decreto Presidente Consiglio dei Ministri del 3 dicembre 2013.** "Regole tecniche in materia di sistema di conservazione"

**Circolare AgID 10 aprile 2014, n. 65** - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.

**Decreto del Ministero dell'Economia e delle Finanze 17 giugno 2014**. Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto – articolo 21, comma 5, del decreto legislativo n. 82/2005

**Provvedimento generale prescrittivo in tema di biometria -** 12 novembre 2014 (Pubblicato sulla Gazzetta Ufficiale n. 280 del 2 dicembre 2014)

**Decreto Presidente Consiglio dei Ministri 13 novembre 2014, "**Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici"

**Regolamento Europeo n. 910/2014 e IDAS**

**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

Torna al sommario

## 3.2 Standard di riferimento

Si riportano di seguito gli standard di riferimento elencati nell'allegato 3 delle Regole Tecniche in materia di Sistema di conservazione con indicazione delle versioni aggiornate al 10 ottobre 2014:

ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;

UNI EN *ISO 9001*:2008− Quality management systems – Requirements;

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

Si riportano di seguito le figure di Responsabilità legate al servizio di conservazione e le rispettive attività di competenza che si sono susseguite nel tempo in Iccrea

| RUOLI | NOMINATIVO | ATTIVITA' DI COMPETENZA | PERIODO NEL RUOLO | EVENTUALI DELEGHE |
|---|---|---|---|---|
| *Responsabile del servizio di conservazione* | Caterina Pompei | Definizione e attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione;<br>- definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente;<br>- corretta erogazione del servizio di conservazione all'ente produttore;<br>- gestione delle convenzioni, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione. | Dal marzo del 2018 alla data attuale. Il ruolo era precedentemente assegnato ad Aldo Bucci da marzo del 2012. | |
| *Responsabile Sicurezza dei sistemi per la conservazione* | Marco Palazzesi | - Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza;<br>- segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive. | Da dicembre 2019 alla data attuale.<br>Il ruolo era precedentemente attribuito a Giorgio Crosina da luglio 2018 e ancor prima Giancarlo Castorina da marzo del 2012. | |
| *Responsabile funzione archivistica di conservazione* | Valeria Anna Uccelli | Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato;<br>- definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici;<br>- monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione;<br>- collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza. | Da ottobre 2018.<br>Precedentemente il ruolo era attribuito a Elena Lisi da maggio 2016. | |

| | | | | |
|---|---|---|---|---|
| *Responsabile Trattamento dati personali* | Vittorio Marogna | - Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali;<br>- garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza | Dal marzo del 2012 alla data attuale | |
| *Responsabile sistemi informativi per la conservazione* | Giuseppe Cardillo | - Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione;<br>- monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore;<br>- segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive;<br>- pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione;<br>- controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione. | Dal 1 maggio 2019 alla data attuale<br>Fino ad aprile 2019 il ruolo era ricoperto da Riccardo Leonori da luglio 2018. precedentemente attribuito ad Antonio Zattera da ottobre del 2014. | |
| *Responsabile sviluppo e manutenzione del sistema di conservazione* | Fabio Stefanutti | - Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione;<br>- pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione;<br>- monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione;<br>- interfaccia con l'ente produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche;<br>- gestione dello sviluppo di siti web e portali connessi al servizio di conservazione. | Dal luglio 2018 alla data attuale. Il ruolo era precedentemente attribuito a Davide Pascuttini da aprile del 2015. | |

Inoltre, il Funzionigramma di Iccrea e del Gruppo Bancario Iccrea prevede che il Responsabile del servizio di Conservazione sia coadiuvato dai Responsabili delle: UO Cassa, UO Sicurezza del Lavoro e delle Aree Operative, Funzione Compliance, Funzione Antiriciclaggio, UO Operational e IT Risk Management e UO Organizzazione.

Torna al sommario

# 5 Struttura organizzativa per il servizio di Conservazione

Iccrea Banca ha lo scopo di rendere più completa, intensa ed efficace l'attività delle Banche di Credito Cooperativo/ Casse Rurali e Artigiane (BCC/CRA), sostenendone e potenziandone l'azione mediante lo svolgimento di funzioni creditizie, di intermediazione tecnica e di assistenza finanziaria in ogni forma e mediante ogni altra idonea iniziativa consentita in materia dalle leggi vigenti e volta al perseguimento di fini di interesse della categoria del- le BCC/CRA. In tale contesto Iccrea Banca offre il servizio di Conservazione.
La comunità di riferimento del servizio di Conservazione digitale di Iccrea è un gruppo identificato di clienti e di potenziali utenti in grado di comprendere un determinato set di informazioni: si tratta di un'unica comunità, ben definita.

## 5.1 Organigramma

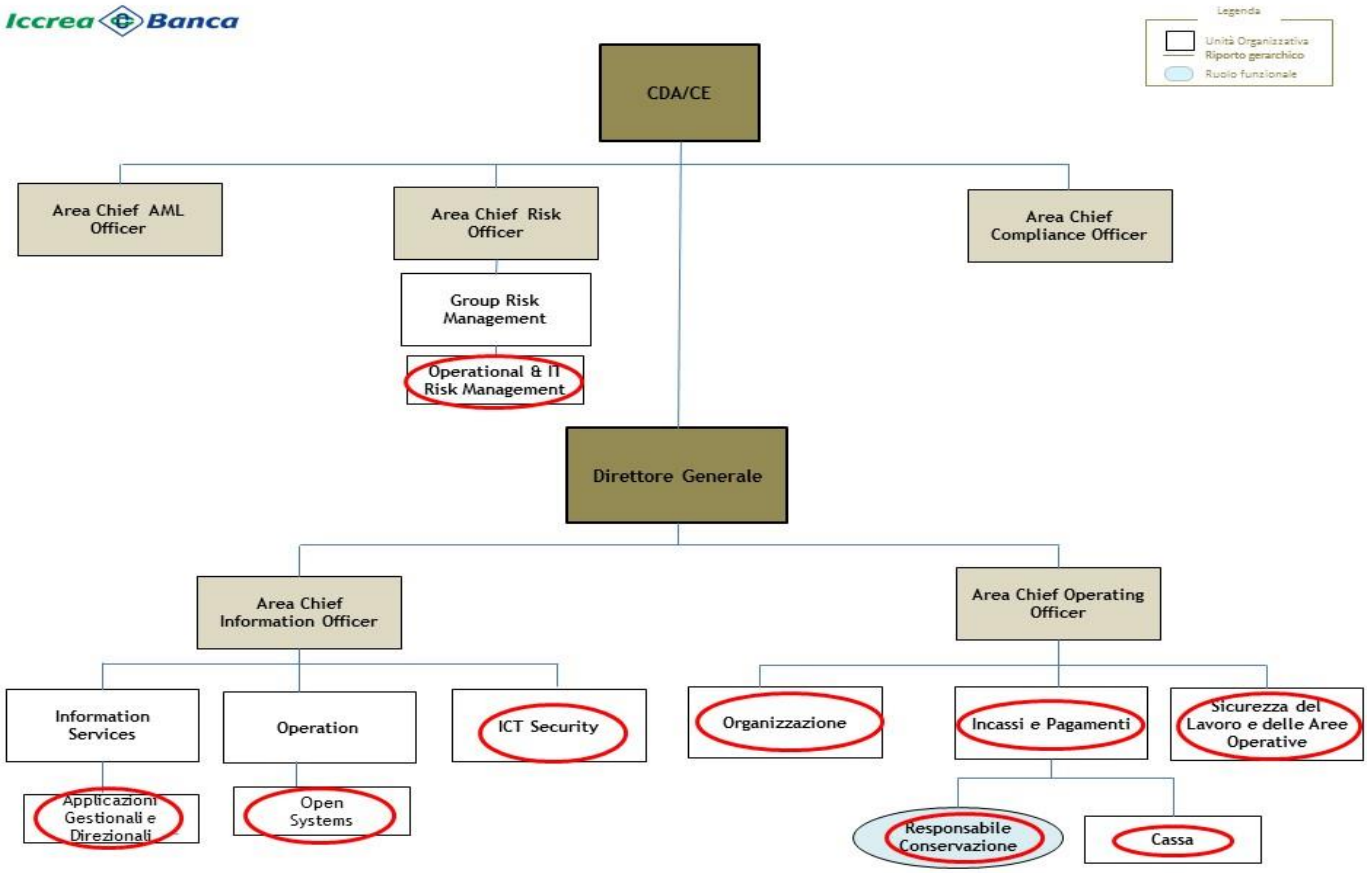


**Figura 1 Estratto Organigramma con evidenza delle principali strutture /ruoli funzionali che intervengono nel servizio di Conservazione**

Torna al sommario

## 5.2 Strutture Organizzative

Con un provvedimento interno il Consiglio di Amministrazione di Iccrea ha provveduto a individuare all'interno del proprio organigramma le persone che per competenza ed esperienza garantiscono la corretta esecuzione delle operazioni ad esse affidate, nell'ambito dei processi di Conservazione.

In particolare, Iccrea ha costituito il Ruolo Funzionale di Responsabile della Conservazione dei propri documenti situato all'interno dell'Unità Organizzativa Incassi e Pagamenti

La medesima risorsa svolge anche il ruolo di Responsabile del servizio di Conservazione per conto dei Clienti.

Il Responsabile del servizio di Conservazione coadiuvato dai delegati garantisce il corretto svolgimento dei seguenti processi:

- verifica 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.

Iccrea ha inoltre individuato, oltre ai Ruoli e Responsabilità indicati nel precedente paragrafo, le attività, svolte all'interno del proprio organigramma da Unità Organizzative dell'Area Chief Information Officer, che servono a coadiuvare il Responsabile del servizio di Conservazione ad ottemperare agli obblighi contrattuali e normativi. In particolare, si fa riferimento alle attività volte ad:

- assicurare la conduzione e manutenzione del sistema di conservazione. Coadiuvando il Responsabile del servizio di Conservazione per ciò che attiene la definizione delle caratteristiche e i requisiti del sistema di conservazione in funzione dei documenti da conservare;
- monitorare il sistema di conservazione. Coadiuvando il Responsabile del servizio di Conservazione per assicurare la corretta funzionalità delle procedure, rilevare tempestivamente eventuale degrado dei sistemi di memorizzazione e ripristinare la corretta funzionalità;
- garantire il funzionamento dei sistemi informativi e informatici, gestendo e rendendo disponibile il patrimonio di dati aziendali, assicurandone il corretto aggiornamento e il processo di change management informatico;
- valutare e monitorare i rischi connessi alla sicurezza delle informazioni provvedendo a coordinare le iniziative ed attività circa gli interventi progettuali connessi. Provvedere alla verifica periodica di conformità a normativa e standard di riferimento in coordinamento con la Funzione Compliance.
- curare la progettazione, lo sviluppo e la gestione dei sistemi di sicurezza logica per l'accesso a dati e sistemi.
- comunicare entro il ventesimo giorno, ogni eventuale variazione rispetto quanto risultante dai documenti presentati all'Agenzia (Manuale della Conservazione, Piano della Sicurezza, Piano di Cessazione, Polizza di Assicurazione)
- inviare il rapporto quadrimestrale entro il quindicesimo giorno lavorativo successivo al quadrimestre di riferimento.

Iccrea ha inoltre nella propria struttura organizzativa l'Area Chief Audit Executive che assicura, sull'intera operatività della Banca, sulla base della propria pianificazione periodica le verifiche di terzo livello circa la completezza, l'adeguatezza, la funzionalità, l'affidabilità delle componenti del sistema dei controlli interni e del sistema informativo, del processo di gestione dei rischi, del c.d. Risk Appetite Framework.

Torna al sommario

# 6 Oggetti sottoposti a conservazione

In generale si definisce “pacchetto informativo” un contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche).

I pacchetti (versamento/archiviazione/distribuzione) sono contrattualizzati con il Soggetto Produttore e si basano sulle tipologie documentali che fanno parte delle “Specificità del contratto”.

Per “pacchetto di versamento” si intende l’insieme di documenti completi di metadati che il Sistema di conservazione riceve dal Soggetto produttore tramite l’ausilio delle interfacce applicative fornite da Iccrea.

Per “pacchetto di archiviazione” si intende un pacchetto composto dalla trasformazione di pacchetti di versamento e depositato nei data center Iccrea. Ad ogni documento il Sistema di conservazione associa un file XML, detto Indice del Pacchetto di Archiviazione (IPdA, definito “Indice di Conservazione” nello standard UNI SInCRO). L’insieme degli Indici del Pacchetto di Archiviazione associati ai file componenti un pacchetto di versamento è detto Rapporto di Versamento.

Per “pacchetto di distribuzione” si intende un pacchetto informativo inviato dal sistema di conservazione all'utente in risposta a una sua richiesta, ovvero è la risposta alla ricerca effettuata dall’Utente tramite interfaccia disponibile, che porta all'esibizione del documento conservato. Il documento da esibire è accompagnato sempre dall’IPdA.

Nel sistema il “pacchetto di distribuzione” coincide con il “pacchetto di archiviazione”.

Torna al sommario

## 6.1 Oggetti conservati

Tipologie documentali, metadati e formati accettati sono elencati nell’Allegato “Specificità del contratto”.

I visualizzatori dei formati standard, previsti nell’allegato 2 del DPCM 3 dicembre 2013, sono gestiti da Iccrea che mantiene nel sistema i visualizzatori associati ai formati. Tutti i documenti inviati in conservazione saranno associati al visualizzatore configurato per il particolare formato.

Torna al sommario

## 6.2 Pacchetto di versamento

Il pacchetto di versamento è un pacchetto informativo composto da una o più aggregazioni dei seguenti tre file digitali:

- ***il file di dati***, ossia il file che si vuole versare nel sistema di conservazione;
- ***il file di indici del documento***, un file XML di indici di ricerca contenente l’indicazione della classe documentale e gli indici del documento;
- ***il file dei parametri di conservazione***, un file XML descrittivo contenente i parametri utili al versamento.

Nella piattaforma di Conservazione, tale aggregazione si definisce *documento* e rappresenta l’unità minima di elaborazione.

Il **file di indici** del documento è un file XML contenente:

- il nome della classe documentale cui il documento afferisce
- l'insieme dei metadati descrittivi del documento concordati con il Soggetto Produttore.

Si riporta un esempio di struttura del file di indici

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<legaldocIndex documentClass="ae_fata" label="Fatture emesse">
 <field name="denominazione_s">Denominazione Azienda</field>
 <field name="codice_fiscale_s" label="Codice fiscale">SNITMS82T27G224S</field>
 <field name="partita_iva_s">01032450072</field>
 <field name="via_s">Corso Stati Uniti</field>
 <field name="localita_s">Padova</field>
 <field name="provincia_s">PD</field>
 <field name="email_destinatario_em">assistenza.legaldoc@legalmail.it</field>
 <field name="totale_importo_d">550</field>
 <field name="numero_registrazione_i">1</field>
 <field name="__numero_documento_l">2</field>
 <field name="__serie_s">S1</field>
 <field name="__data_inizio_numerazione_dt">01-01-2012</field>
 <field name="__data_documento_dt">15-05-2012</field>
 <field name="data_di_presa_in_carico_dt">09-05-2012 23:39:00</field>
 <field name="__anno_fiscale_i">2012</field>
 <field name="note_s">note</field>
 <field name="boolean_index_b">true</field>
 <field name="double_index_d">.254</field>
 <field name="float_index_f">2.34</field>
 <field name="location_index_p">-12.524, 35.245</field>
 <field name="__indice_fascicolo_s">pratica-01</field>
</legaldocIndex>
```

| ***TAG*** | ***Significato*** | ***Attributo*** | ***Significato*** | ***Obbligatorietà*** |
|---|---|---|---|---|
| *legaldocIndex* | *Tag radice del file di indice* | *documentClass, label* | *documentClass: (attributo obbligatorio) identifica la classe documentale descritta dai campi di ricerca. Tale valore viene fornito all'utente in fase di contrattuale. label: (attributo facoltativo) nome logico della classe documentale* | *S* |
| *field* | *Descrive un campo di ricerca* | *name, label* | *name: (attributo obbligatorio) nome del campo di ricerca, Obbligatorio. label: (attributo facoltativo) nome logico del campo di ricerca* | *N* |

Il **file dei parametri** è un file XML contenente le seguenti principali informazioni:

- Il nome del file di dati che si vuole conservare. E' il nome con cui verrà conservato il file in LegaldDoc
- il mimetype del file di dati che si vuole conservare
- l'hash calcolato con metodo SHA-256 del file di dati
- Il nome del file di indici che si vuole conservare. E' il nome con cui verrà conservato il file in LegaldDoc
- il mimetype del file di indici che si vuole conservare
- l'hash calcolato con metodo SHA-256 del file di indici
- Il codice della Policy con cui si vuole conservare il documento

Il sistema LegalDoc prevede le definizioni di una o più policy di versamento. Una policy è un insieme di regole che definiscono il trattamento che il documento riceve all'interno al sistema di conservazione.

Le regole associate alla policy definiscono:

- i mimetype assegnabili ad un file di dati nell'apposito tag <data_mimetype> presente nel file xml dei parametri (i valori possibili sono comunicati tramite l'apposito file di configurazione che si riceve all'atto dell'attivazione)
- il periodo di retention del documento
- le classi documentali assegnabili al documento

Si riporta un esempio del file di parametri

```
<?xml version="1.0" encoding="UTF-8"?>
<parameters>
 <policy_id>P1</policy_id>
 <index_file>
  <index_name>index.xml</index_name>
  <index_hash>f2b24e7f9caa38329b954bd12ed924289620ddbaa24734646536702237673f8b</index_hash>
    <index_mimetype>text/xml;1.0</index_mimetype>
 </index_file>
 <data_file>
  <data_name>testDataFile.pdf</data_name>
  <data_hash>37fac9829dbd79a7fa8d792ceceda509649807238839c0bbd6184227cc2ba145</data_hash>
  <data_mimetype>application/pdf;1.4</data_mimetype>
 </data_file>
 <path>/fatture/2012</path>
 <encrypted_by_owner></encrypted_by_owner>
</parameters>
```

Di seguito sono riportati i tag necessari

| ***TAG*** | ***Significato*** | ***Attributo*** | ***Significato*** | ***Obbligatorietà*** |
|---|---|---|---|---|
| *parameters* | *Tag radice per la richiesta di conservazione* | | | *S* |
| *policy_id* | *Il codice della Policy con cui si vuole conservare il documento* | | | *S* |

| TAG | Significato | Attributo | Significato | Obbligatorietà |
|---|---|---|---|---|
| *index_file* | *Tag contenente le informazioni sul file di indici che si vuole conservare* | | | *S* |
| *index_name* | *Il nome del file di indice che si vuole conservare. E' il nome con cui verrà conservato il file in LegaldDoc* | | | *S* |
| *index_hash* | *E' l'hash calcolato con metodo SHA-256 del file di indice* | | | *S* |
| *index_mimetype* | *Indica il mimetype del file di indice che si vuole conservare* | | | *S* |
| *data_file* | *Tag contenente le informazioni sul file di dati che si vuole conservare* | | | *S* |
| *data_name* | *Il nome del file di dati che si vuole conservare. E' il nome con cui verrà conservato il file in LegaldDoc* | | | *S* |
| *data_hash* | *E' l'hash calcolato con metodo SHA-256 del file di dati* | | | *S* |
| *data_mimetype* | *Indica il mimetype del file di dati che si vuole conservare* | | | *S* |
| *path* | *E' il percorso logico dove si vuole salvare il proprio file di dati* | | | *S* |
| *encrypted_by_owner* | *Indica se il documento è stato cifrato dal Cliente prima dell'invio in conservazione. Valori ammessi "S" (è cifrato) o "N". Se valorizzato a "S" si solleva Iccrea Banca da qualsiasi controllo sulla visualizzazione* [1] | | | *N (se non indicato, il valore di default è "N")* |

Per il dettaglio degli schemi XML dei file che costituiscono il pacchetto di versamento, si rimanda all'allegato "Specificità del contratto".

Torna al sommario

## 6.3 Pacchetto di archiviazione

Il pacchetto di archiviazione è composto da:

- un *documento,* inteso come aggregazione dei tre file: file di dati, fil di indici, file di parametri di conservazione*;*

[1] Se impostato a S, il Cliente si impegna a mantenere gli strumenti necessari per la visualizzazione del documento

- l'indice del pacchetto di Archiviazione (IPdA).

L'Indice del Pacchetto di Archiviazione è un file in formato XML, marcato temporalmente e firmato digitalmente dal Responsabile del servizio della Conservazione, generato dal sistema, che contiene i metadati in formato UNI SInCRO e le informazioni di conservazione del documento e viene con esso conservato.

In particolare, nel file sono riportati:

- informazioni sull'applicazione che ha generato l'IPdA;
- il token del documento (ovvero il suo identificativo univoco);
- l'operazione eseguita (conservazione, rettifica, scarto e cancellazione);
- l'ambiente di conservazione associato al Soggetto Produttore e la policy utilizzata;
- il nome dei file che compongono il pacchetto, incluso il file dei parametri di conservazione ed il file di indici, e le rispettive impronte;
- eventuali informazioni relative al documento rettificante e rettificato;
- il tempo di creazione (timestamp) del file IPdA;
- l'impronta di Hash del documento.

Il file IPdA è reso disponibile con il documento di riferimento ad ogni operazione di conservazione e richiesta di esibizione. Viene di seguito riportato un esempio di file IPdA

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<IdC>
 <SelfDescription>
  <ID>TD330A311A4749C1B1C3F3A87EF533280A47DD5CE35F4C40095274D484038CF11</ID>
            <CreatingApplication>
             <Name>Legaldoc</Name>
             <Version>1.0</Version>
             <Producer>Infocert</Producer>
            </CreatingApplication>
 </SelfDescription>
 <VdC>
  <ID>TD330A311A4749C1B1C3F3A87EF533280A47DD5CE35F4C40095274D484038CF11</ID>
  <MoreInfo>
   <EmbeddMetadata>
    <additionalInfo key="token">
                    TD330A311A4749C1B1C3F3A87EF533280A47DD5CE35F4C40095274D484038CF11
            </additionalInfo>
      <additionalInfo key="bucket">B1</additionalInfo>
      <additionalInfo key="policy">P1</additionalInfo>
      <additionalInfo key="operation">C</additionalInfo>
      <additionalInfo key="IDPdV">
        PDV1c85f515533a0da59d4ee162b2df6ca66408e488
      </additionalInfo>
          </EmbeddMetadata>
  </MoreInfo>
```

```
 </VdC>
 <FileGroup>
            <File>
                        <ID>1</ID>
                        <Hash>02de3f5576b2e9b3f1eb45cc7d629e782c1078aeb6db4b5b7f8924449405efc6</Hash>
                        <MoreInfo>
                                    <EmbeddMetadata>conserve.xml</EmbeddMetadata>
                        </MoreInfo>
            </File>
            <File>
                        <ID>2</ID>
                        <Hash>717dd3622f71f029e5c05b01a5ffc412fbb6ce646195b9b0ededb870c92c7dcd</Hash>
                        <MoreInfo>
                                    <EmbeddMetadata>index.xml</EmbeddMetadata>
                        </MoreInfo>
            </File>
            <File>
                        <ID>3</ID>
                        <Hash>ea3b1238a38f72b330aac53364bd0a0481946b93fc757dde7314ce3319f1840e</Hash>
                        <MoreInfo>
                                    <EmbeddMetadata>testDataFile.pdf</EmbeddMetadata>
                        </MoreInfo>
            </File>
   </FileGroup>
  <Process>
   <TimeReference>
    <TimeInfo>2013-05-15T16:09:37+0200</TimeInfo>
   </TimeReference>
  </Process>
</IdC>
```

In particolare, ecco il significato dei tag presenti:

| ***TAG*** | ***Significato*** | ***Attributo*** | ***Significato*** |
|---|---|---|---|
| *IdC* | *Radice del file xml* | | |
| *SelfDescription* | *Informazioni relative all'indice di conservazione stesso* | | |
| *ID* | *Identificativo univoco (token) assegnato al documento dal sistema di conservazione LegalDoc* | | |

| TAG | Significato | Attributo | Significato |
|---|---|---|---|
| CreatingApplication | Informazioni sull'applicazione che ha generato l'IdC | | |
| Name | Nome dell'applicazione che ha generato l'IdC | | |
| Version | Versione dell'applicazione che ha generato l'IdC | | |
| Producer | Nome del produttore dell'applicazione che ha generato l'IdC | | |
| VdC | Informazioni relative al volume di conservazione | | |
| ID | Identificativo univoco (token) assegnato al documento dal sistema di conservazione LegalDoc | | |
| MoreInfo | Informazioni ulteriori relative al VdC | | |
| EmbeddedMetadata | Le informazioni dell'elemento <MoreInfo> strutturate nel formato XML | | |
| additionalInfo | Contenitore delle informazioni ulteriori | key="token" | Contiene il token del documento assegnatogli da LegalDoc |
| additionalInfo | Contenitore delle informazioni ulteriori | key="bucket" | ID del bucket a cui il documento appartiene così come indicato nell'url del servizio di conservazione |
| additionalInfo | Contenitore delle informazioni ulteriori | key="policy" | ID della policy associata al documento così come indicata nel file dei parametri |
| additionalInfo | Contenitore delle informazioni ulteriori | key="operation" | Tipo di operazione richiesta al sistema di conservazione LegalDoc (conservazione, rettifica, cancellazione) |
| additionalInfo | Contenitore delle informazioni ulteriori | key="IDPdV" | ID del Pacchetto di Versamento |
| FileGroup | Elemento di aggregazione di più file oggetto di conservazione | | |
| File | Informazioni relative al file oggetto di conservazione | | |
| ID | Identificatore univoco del file descritto | | |
| Hash | Informazioni sull'impronta del file cui l'elemento si riferisce | | |
| MoreInfo | Informazioni ulteriori relative al file cui l'elemento si riferisce | | |
| EmbeddMetadata | Nome del file cui l'elemento si riferisce | | |

| TAG | Significato | Attributo | Significato |
|---|---|---|---|
| *Process* | *Informazioni relative alle modalità di svolgimento del processo di conservazione* | | |
| *TimeReference* | *Informazioni relative alla data e ora di realizzazione dell'indice di conservazione* | | |
| *TimeInfo* | *Generico riferimento temporale nel formato UNI ISO 8601:2010* | | |

Le specifiche XML del file IPdA sono descritti nell'allegato "Specificità del contratto".

Torna al Sommario

## 6.4 Pacchetto di distribuzione

Il pacchetto di distribuzione è composto dallo stesso insieme di file costituenti il pacchetto di archiviazione. E' e da un'attestazione di corretta conservazione firmato dal responsabile del servizio di conservazione e marcato temporalmente.

Il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, al documento informatico conservato, attraverso la produzione di un pacchetto di distribuzione.

Non è possibile esibire parti singole di documento.

L'esibizione del pacchetto di distribuzione ottenuto tramite interrogazione al sistema di conservazione rappresenta un'esibizione completa, legalmente valida ai sensi del secondo comma dell'articolo 10 del DPCM del 03 dicembre 2013 e dell'articolo 5 del DMEF del 17 giugno 2014.

Attraverso i servizi web messi a disposizione dei sistemi applicativi chiamanti, il pacchetto di distribuzione può essere ottenuto con le seguenti strutture contenenti tutti i file del documento:

- Un file zip (*content-type = application/zip)*
- Un pacchetto http multipart (*content-type = multipart/mixed)*

Le specifiche tecniche relative ai servizi di esibizione sono descritte nell'allegato "Specificità del contratto".

Torna al sommario

# 7 Il Processo di Conservazione

Il sistema di conservazione permette di mantenere e garantire nel tempo l'integrità, la leggibilità e la validità legale di un documento informatico, nel rispetto della normativa vigente.

Il sistema consente le funzionalità di:

- **accettazione del pacchetto di versamento**, formato dal documento da conservare e dai metadati ad esso associati;
- **conservazione del pacchetto di archiviazione**: il documento, ricevuto nei Data Center di Iccrea in formato digitale, viene conservato a norma di legge per tutta la durata prevista ed è contenuto in un pacchetto di archiviazione;
- **scarto/cancellazione del pacchetto di archiviazione:** per la cancellazione di pacchetti di archiviazione ritenuti privi di valore amministrativo e di interesse storico-culturale dal Produttore, occorre formulare apposita richiesta a Iccrea. (scarto archivistico);
- **ricerca dei documenti conservati**: l'utente autorizzato può eseguire una ricerca tra i documenti conservati, utilizzando uno o più metadati popolati in fase di caricamento;
- **esibizione del pacchetto di distribuzione:** il documento richiesto viene richiamato direttamente dal sistema di conservazione digitale ed esibito, con garanzia della sua opponibilità a terzi; attraverso i servizi web di esibizione, gli applicativi che integrano i servizi di conservazione possono permettere di visualizzare e scaricare sia il documento conservato che gli altri documenti a corredo della corretta conservazione (file di indici, file di parametri, Indice del Pacchetto di Archiviazione); il responsabile del servizio di conservazione può ricercare e visualizzare i documenti conservati tramite l'applicativo web dedicato.

Il Soggetto Produttore, in base alle proprie esigenze, accede alle funzionalità di conservazione tramite uno o più applicativi esterni che orchestrano i servizi web esposti dal sistema.

Torna al sommario

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

Il sistema di conservazione di Iccrea Banca prevede due modalità di acquisizione dei pacchetti di versamento:

1. tramite i servizi web esposti da LegalDoc ed integrati dai sistemi gestionali chiamanti che offrono le interfacce ai Soggetti Produttori;
2. tramite l'interfaccia web di LegalDoc ad uso esclusivo del Responsabile del Servizio di Conservazione.

Nel primo caso, il processo di versamento prevede i seguenti passi:

- autenticazione al sistema LegalDoc mediante credenziali univoche assegnate al sistema gestionale. Il canale di comunicazione è protetto da protocollo sicuro (https) e da specifiche regole di firewall che vincolano l'accesso ai soli sistemi autorizzati;
- apertura di una sessione di versamento tramite l'operazione di login;
- versamento dei documenti, intesi come aggregazione di file di dati, file di indici, file di parametri di conservazione;

- chiusura della sessione di versamento tramite l'operazione di logout;

Le specifiche tecniche dei servizi esposti da LegalDoc, ed utilizzati dal sistema gestionale chiamante, sono dettagliate nell'allegato Specificità del Contratto.

Tutte le attività di presa in carico dei pacchetti di versamento sono tracciate su log applicativo, che permette di individuare per ogni evento: data, ora, operazione, identificativo della sessione di versamento, dati di dettaglio; accessibile solo da amministratori di sistema

Torna al sommario

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

Sul pacchetto di versamento acquisito vengono eseguite le seguenti operazioni:

- Generazione dell'impronta di ogni file costituente il documento e confronto con la corrispondente impronta inviata dal Produttore, a garanzia dell'integrità del documento ricevuto.
- In caso di esito negativo delle verifiche, rigetto del documento con invio al sistema chiamante dell'errore intercorso. In questo caso, termine del flusso.
- Controllo dei valori indicati dal Produttore nel file dei parametri di conservazione:
    - verifica della policy dichiarata,
    - verifica della congruenza dei tipi di file inviati (mimetype),
    - verifica dell'univocità del file all'interno del path (cartella) indicato.
- Controllo dei valori indicati dal Soggetto Produttore nel file di indici del documento:
    - validazione dei tracciati dei file di indice,
    - verifica della correttezza della classe documentale,
    - verifica della compatibilità fra policy dichiarate e policy configurate,
    - verifica degli indici obbligatori (esistenza, valorizzazione, non duplicazione, correttezza del tipo di file, controllo numerico).
    - i valori espressi nel file di indici vengono confrontati con la configurazione presente nelle apposite tabelle presenti nel database legaldoc.
    - il database del sistema di conservazione viene aggiornato con i dati relativi al documento e ai file che lo compongono per il mantenimento della tracciabilità delle operazioni

Le attività di verifica sui pacchetti di versamento sono tracciate su log applicativo, che permette di individuare per ogni evento: data, ora, operazione, identificativo della sessione di versamento, dati di dettaglio; accessibile solo da amministratori di sistema.

Torna al sommario

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

Il DPCM del 3 dicembre 2013 “Regole tecniche in materia di sistema di conservazione”, (art. 9 comma 1 lettere d ed e), introduce l’obbligo di generare il Rapporto di Versamento.

Il Rapoprto di Versamento è costituito dall’insieme degli Indici del Pacchetto di Archiviazione associati ai file componenti un pacchetto di versamento.

Il Rapporto di Versamento attesta l'avvenuta presa in carico da parte del sistema di conservazione del pacchetto di versamento inviato dal Produttore ed è l’insieme degli Indici dei Pacchetti di Archiviazione prodotti per ogni singolo documento oggetto di versamento (per i dettagli tecnici si rimanda “Specificità del contratto”).

A fronte di un pacchetto di versamento correttamente verificato, le fasi di accettazione dei pacchetti di versamento e di generazione del rapporto di versamento sono le seguenti:

1. Generazione del pacchetto di archiviazione
    a. Creazione del file XML IPdA (Indice del Pacchetto di Archiviazione) contenente: le informazioni sul processo di conservazione (in particolare sul software LegalDoc), le policy e l’area di conservazione utilizzati, il nome e le impronte dei file costituenti il documento e l'identificativo
    b. Marcatura e firma da parte del Responsabile del servizio della Conservazione del file IPdA. Copia del file sul supporto primario.
    c. Indicizzazione del documento conservato al fine di poter reperire lo stesso in seguito.
    d. Aggiornamento del database del sistema interessato alle modifiche di cui sopra.
2. Memorizzazione del pacchetto di archiviazione
    a. Memorizzazione del pacchetto di archiviazione sul sistema di storage ad alta affidabilità di Iccrea
    b. Inserimento nelle tabelle di interfaccia del sistema di archiviazione permanente delle informazioni di puntamento dei file, al fine di poter reperire gli stessi in seguito
    c. La procedura di creazione della copia di sicurezza avviene in maniera automatica e gestita dal sistema di Storage
3. Restituzione del Rapporto di versamento al sistema chiamante
    a. Restituzione dell'esito positivo del versamento con l’invio del Rapporto di versamento sotto forma del file IPdA al sistema chiamante utilizzato.

Le attività sono tracciate su log applicativo, che permette di individuare per ogni evento: data, ora, operazione, identificativo della sessione di versamento, dati di dettaglio; accessibile solo da amministratori di sistema.

Torna al sommario

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

In seguito a situazioni che impediscono la corretta e completa esecuzione del servizio richiesto, LegalDoc restituisce una segnalazione di errore con le seguenti informazioni:

- Codice di errore - codifica abbreviata dell'errore avvenuto
- Messaggio di errore - breve descrizione dell'errore avvenuto

campi codice e descrizione vengono restituiti al sistema chiamante nella risposta http al servizio di versamento con un messaggio composto con il seguente formato di esempio.

```
<error>
    <code>LD_XXNNN</code>
    <description>Breve descrizione del problema.</description>
</error>
```

Il tag <code> indica il codice associato all'errore, mentre il tag <description> restituisce una breve descrizione del problema.

I dettaglio dei codici di errori restituiti dal sistema è riportato nell'allegato "Specificità del contratto".

I casi di errore sono mantenuti nei log applicativi del sistema di conservazione.

Torna al sommario

## 7.5 Preparazione e gestione del pacchetto di archiviazione

La preparazione e la gestione del pacchetto archiviazione prevedono le seguenti fasi:

1. Verifica del pacchetto di versamento
    a. Generazione dell'impronta di ogni file costituente il documento e confronto con la corrispondente impronta inviata a garanzia dell'integrità del documento ricevuto. In caso di esito negativo delle verifiche, rigetto del documento con invio all'applicativo chiamante dell'errore intercorso. In questo caso, termine del flusso.
    b. Controllo dei valori indicati nel file dei parametri di conservazione: verifica della policy dichiarata, verifica della congruenza dei tipi di file inviati (mimetype), verifica dell'univocità del file all'interno del path (cartella) indicato.
    c. Controllo dei valori indicati nel file di indici del documento: validazione dei tracciati dei file di indice, verifica della correttezza della classe documentale, verifica della compatibilità fra policy dichiarate e policy configurate, verifica degli indici obbligatori (esistenza, valorizzazione, non duplicazione, correttezza del tipo di file, controllo numerico). I valori espressi nel file di indici vengono confrontati con la configurazione presente nelle apposite tabelle presenti nel database LegalDoc.

d. Aggiornamento dei database del sistema con i dati relativi al documento e ai file che lo compongono per il mantenimento della tracciabilità delle operazioni.

2. Formazione del pacchetto di archiviazione
    a. Creazione del file XML IPdA (Indice del Pacchetto di Archiviazione) contenente: le informazioni sul processo di conservazione (in particolare sul software LegalDoc), le policy e l'area di conservazione utilizzati, il nome e le impronte dei file costituenti il documento e l'identificativo assegnato al documento,
    b. Marcatura e firma da parte del Responsabile del servizio di Conservazione del file IPdA.
    c. Indicizzazione del documento conservato al fine di poter reperire lo stesso in seguito.
    d. Aggiornamento del database del sistema interessato alle modifiche di cui sopra.
3. Memorizzazione del pacchetto di archiviazione
    a. Memorizzazione del pacchetto di archiviazione sul sistema di storage ad alta affidabilità di Iccrea
    b. Inserimento nelle tabelle di interfaccia del sistema di archiviazione permanente delle informazioni di puntamento dei file, al fine di poter reperire gli stessi in seguito
    c. La procedura di creazione della copia di sicurezza avviene in maniera automatica e gestita dal sistema di Storage

Torna al sommario

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

La preparazione e la gestione del pacchetto di distribuzione ai fini dell'esibizione prevedono le seguenti fasi:

1. Ricerca del documento da esibire
    a. Tramite i servizi esposti dal sistema di conservazione, dal sistema di gestione chiamante viene eseguita la ricerca degli identificativi univoci (token) relativi al documento da esibire.
    b. Restituzione del token corretto.
2. Richiesta di esibizione da parte dell'utente
    a. Invocazione del servizio di esibizione del sistema di conservazione secondo le modalità descritte nell'allegato "Specificità del contratto" per l'integrazione di LegalDoc. In questa chiamata viene utilizzato il token ricavato in precedenza.
3. Accettazione della richiesta da parte del sistema di conservazione
    a. Ricezione della richiesta di esibizione del documento
    b. Controllo di corrispondenza tra il token inviato dall'Utente e quelli dei documenti conservati
4. Risposta del sistema di conservazione ed esibizione del documento
    a. Ricerca dei file costituenti il documento e dei file attestanti il processo di conservazione corrispondenti al token inviato e preparazione del pacchetto di distribuzione.
    b. Invio della risposta al sistema dell'Utente.

Torna al sommario

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

Per duplicato si intende il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario.

Per copia si intende il documento informatico avente contenuto identico al documento da cui è tratto, ma con forma diversa.

La conservazione avviene su supporto primario e su supporto secondario, quindi con duplicazione automatica. Come descritto in seguito, tali supporti sono ad alte capacità e performance, che garantiscono la ridondanza interna del dato. È inoltre eseguito un backup periodico.

La creazione di copie informatiche, invece, in caso di adeguamento del formato rispetto all'evoluzione tecnologica sarà presa in carico dal Responsabile del servizio della Conservazione e dalle figure professionali coinvolte nel processo di conservazione in base alle specifiche del formato in questione e alle competenze tecnologiche a disposizione.

L'intervento di un Pubblico Ufficiale per attestare la conformità di una copia all'originale avviene secondo quanto previsto dagli articoli 22 e 23 del Codice e dalle Regole Tecniche del DPCM del 13 novembre 2014 - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

Torna al sommario

## 7.8 Scarto dei pacchetti di archiviazione

LegalDoc prevede l'eliminazione di un pacchetto di archiviazione e di qualsiasi duplicato prodotto durante le attività di conservazione, per cessata rilevanza ai fini amministrativi, legali o di ricerca storica, ai sensi del Regolamento Privacy e del Codice dei beni culturali. Questa attività è espressamente richiesta a Iccrea dal Soggetto Produttore che produce, inoltre, una lista, debitamente firmata, dei documenti che intende scartare.

Per gli enti pubblici e per gli archivi privati dichiarati di notevole interesse storico, le proposte di scarto sono sottoposte a nulla osta delle soprintendenze archivistiche o delle commissioni di sorveglianza di competenza. La stesura di 'Piani di Conservazione' (detti anche 'Massimari di selezione e scarto'), la selezione dei documenti da scartare e la procedura di sdemanializzazione e approvazione ministeriale sono in capo al Soggetto Produttore, che può avvalersi del supporto di Iccrea.

Iccrea, in quanto Conservatore, attiva la procedura di scarto sempre per richiesta e approvazione del Soggetto Produttore.

La distruzione degli eventuali supporti ottici rimovibili di back-up è effettuata mediante strumentazione adeguata e seguendo le procedure definite per lo smaltimento dei rifiuti prodotti.

Il Responsabile del servizio della Conservazione mantiene traccia delle richieste di scarto ricevute e correttamente eseguite, con l'indicazione a margine di eventuali errori occorsi durante lo svolgimento del processo, dei rimedi attuati e delle altre informazioni che ritiene meritevoli di annotazione.

Per ulteriori dettagli si rimanda all'apposito documento interno "Procedura di Scarto Handover".

Torna al sommario

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

Nel caso il Soggetto Produttore decida di rescindere o interrompere il contratto di affidamento del servizio di conservazione, il Responsabile del servizio della Conservazione provvede a comunicare al Soggetto Produttore la lista dei pacchetti di archiviazione conservati.

Il Soggetto Produttore può effettuare il download dei propri Pacchetti di Distribuzione, attraverso la procedura di esibizione, o richiedendo il servizio di restituzione a Iccrea.

Al termine della procedura di trasferibilità verso il nuovo Conservatore per rescissione o risoluzione del contratto di servizio, i pacchetti conservati verranno cancellati da LegalDoc.

Insieme ai veri e propri documenti conservati, sono rese disponibili anche le informazioni e i documenti a corredo della corretta conservazione.

Gli indici di conservazione generati dal sistema Iccrea sono conformi allo standard di interoperabilità UNI SInCRO: l'interrogazione di tali archivi restituisce le informazioni secondo il suddetto standard.

Per ulteriori dettagli si rimanda all'apposito documento interno "Procedura di Scarto Handover e Termination Plan".

Torna al sommario

## 7.10 Termination Plan

Il Termination Plan descrive le operazioni previste da Iccrea in caso di cessazione, sospensione o revoca del servizio fiduciario di Conservazione.

La cessazione del servizio di conservazione comporta in Iccrea l'individuazione di un Project Manager per la gestione di un progetto apposito, al fine di stabilire le attività da effettuarsi per garantire la restituzione dei documenti in conservazione ai rispettivi Soggetti produttori.

Il Project Manager incaricato di eseguire il Termination Plan, in collaborazione con il Responsabile del servizio di conservazione coadiuvato e supportato da tutte le strutture interessate, provvederà ad assicurarsi che siano portate a termine le seguenti operazioni:

1) Individuazione del Conservatore subentrante e formalizzazione degli accordi necessari. Previo accordo tra le parti, è prevista la restituzione dei pacchetti allo stesso soggetto produttore.
2) Comunicazione a tutte le parti coinvolte a vario titolo nel servizio.
3) Migrazione dei Pacchetti di Distribuzione al Conservatore subentrante.
4) Scarto dei Pacchetti di Distribuzione e di tutti i suoi duplicati.
5) Cessazione Operativa del servizio e dei sistemi a supporto della erogazione del servizio.

Il nuovo Conservatore dovrà essere iscritto nell'elenco dei Conservatori Accreditati pubblicato da AgID e rispettare la normativa volta per volta vigente in materia di Conservazione.

Per ulteriori dettagli si rimanda all'apposito documento interno "Piano di cessazione".

Torna al sommario

# 8 Il Sistema di Conservazione

Il sistema di conservazione è implementato dall'applicativo LegalDoc di InfoCert appositamente installato sui sistemi di Iccrea.

Il sistema utilizza i servizi di Firma Digitale e Marcatura Temporale, qualificati a norma eIdAS, erogati da remoto dalla CA accreditata di InfoCert.

Il sistema espone servizi web orchestrati dagli applicativi che Iccrea utilizza per erogare i propri servizi agli utenti del Soggetto Produttore secondo le modalità con concordate.

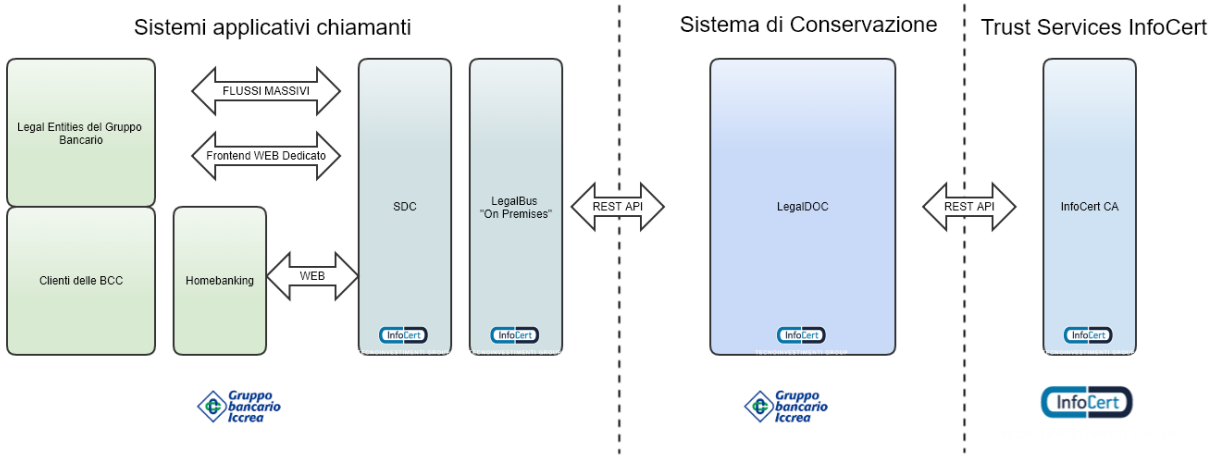


**Figura 2 : Rappresentazione del servizio**

I Web Services di LegalDoc sono implementati secondo architettura REST su protocollo HTTPS.

LegalDoc è dotato anche di un'interfaccia (LegalDoc WEB) utilizzata dal Responsabile del Servizio della Conservazione per il controllo dei documenti conservati.

L'applicazione permette di:

- estrarre un documento e visualizzarlo a video;
- produrre copia cartacea o su altro supporto informatico del documento;
- estrarre i visualizzatori memorizzati nel sistema di conservazione permettendone l'installazione sulla stazione dove si sta svolgendo il controllo;
- prendere visione dei file a corredo che formano il pacchetto di distribuzione e che qualificano il processo di conservazione attestandone il corretto svolgimento (Indice di Conservazione UNI SINCRO, altrimenti detto Indice del Pacchetto di Archiviazione, File di parametri, File di indici, File di dati, Attestato di conservazione);
- verificare la validità delle firme digitali e delle marche temporali apposte nel processo di conservazione;
- verificare l'integrità del documento.

Il sistema è protetto da firewall ed implementa un sistema di back-up dei dati memorizzati.

Torna al sommario

## 8.1 Componenti Logiche

Il sistema di conservazione è costituito dalle componenti applicative del prodotto LegalDoc di InfoCert installato sui sistemi di Iccrea. LegalDoc accede ai servizi di firma digitale e marcatura temporale esposti da InfoCert, CA accreditata presso AgID.

Torna al sommario

## 8.2 Componenti Tecnologiche

### 8.2.1 Firewall

I firewall assicurano la difesa del perimetro di sicurezza tra il sistema e il mondo esterno, nonché tra i sistemi dedicati all'erogazione del sistema e i sistemi che interfacciano i dispositivi sicuri per la generazione della firma digitale.

I firewall sono configurati in alta affidabilità e costantemente aggiornati per assicurare i massimi livelli di

Torna al sommario

### 8.2.2 Back-up

L'intero sistema di conservazione viene interessato periodicamente da processi di back-up completo dei documenti, delle evidenze qualificanti il processo, dei database di gestione del sistema e di ogni altra informazione necessaria per la sicurezza.

Torna al sommario

### 8.2.3 Servizio di marcatura temporale

Per l'emissione delle marche temporali il sistema si avvale del servizio di marcatura di InfoCert, Certification Authority accreditata, compliant eIDAS. Il Piano per la Sicurezza del Certificatore è depositato presso AgID.

La marca temporale viene richiesta al TSS (Time Stamping Service) che la restituisce firmata con un certificato emesso dalla TSA (Time Stamping Authority) di InfoCert. Il root-certificate della TSA è depositato presso AgID.

Il TSS è sincronizzato via radio con l'I.N.RI.M di Torino (Istituto Nazionale di Ricerca Metrologica, già Istituto Elettrotecnico Nazionale “Galileo Ferraris”) ed è protetto contro la manomissione della sincronizzazione mediante misure fisiche e logiche, nel pieno rispetto delle norme di legge.

Torna al sommario

### 8.2.4 Servizio di firma digitale

Per la firma digitale dei pacchetti di archiviazione, il sistema si avvale del servizio di firma digitale remota di InfoCert, Certification Authority accreditata, compliant eIDAS. Il Piano per la Sicurezza del Certificatore è depositato presso AgID.

La firma digitale viene apposta tramite ICSS (InfoCert Sign Server) che utilizza un certificato di firma automatica ad alte prestazioni emesso dalla Root CA. Il root-certificate della CA è depositato presso AgID.

Torna al sommario

## 8.3 Componenti Fisiche

### 8.3.1 Sistema Storage

Il sistema di conservazione di Iccrea utilizza storage ad alte performance come sistema primario e secondario per la memorizzazione dei dati. Tali storage, scelti tra i primari fornitori di tecnologie presenti sul mercato, garantiscono adeguati requisiti di affidabilità e di ridondanza interna del dato.

I sistemi di storage sono stati valutati da Iccrea e dai suoi partner tecnologici sotto molteplici profili e, in virtù delle loro caratteristiche fisiche e architetturali, sono ritenuti idonei ad essere utilizzati nel sistema di conservazione.

Nell'ambito del sistema di conservazione, lo storage rappresenta sia il supporto primario di conservazione posto fisicamente presso la sede primaria, sia il supporto secondario posto nel sito di disaster recovery. I due sistemi sono interconnessi mediante collegamenti ad alta velocità dedicati, completamente ridondati e protetti da misure di sicurezza. I collegamenti consentono la replicazione dei dati conservati eliminando il rischio di distruzione di tutte le copie delle informazioni in caso di danno irreparabile a livello di sito.

Questo secondo sistema funge anche da copia di sicurezza.

Torna al sommario

### 8.3.2 Sincronizzazione dei sistemi

Tutti i server di Iccrea sono sincronizzati attraverso il protocollo NTP (Network Time Protocol). La sincronizzazione è protetta da misure di sicurezza fisiche e logiche documentate per impedirne la manomissione.

Il meccanismo di allineamento temporale tra i sistemi fornisce la certezza della successione temporale degli avvenimenti nel sistema. La sincronizzazione delle macchine infatti, genera dei file di log temporalmente omogenei tra loro, che permettono di ricostruire con certezza l'ordine di accadimento degli eventi intervenuti a tutti i livelli del sistema, e di individuare la sequenza di svolgimento delle varie operazioni.

Nel piano di sicurezza sono descritti eventuali variazioni di Time zone nella generazione di log applicativi.

Torna al sommario

## 8.4 Procedure di gestione e di evoluzione

Iccrea, quale Responsabile del servizio di Conservazione è garante dell'adozione di tutte le misure necessarie per la sicurezza fisica, logica e ambientale dei dati e del sistema preposto alla loro Conservazione. Il tutto, al fine di proteggere le informazioni da possibili violazioni in termini di riservatezza, integrità e disponibilità delle informazioni.

Per l'implementazione del sistema di conservazione, Iccrea ha selezionato il prodotto LegalDoc di InfoCert che garantisce un processo di miglioramento continuo al fine di giungere all'erogazione di un sistema affidabile, sicuro e pienamente conforme alle norme.

InfoCert è costantemente impegnata nell'attività di evoluzione del prodotto al fine di garantire la conformità del prodotto.

Iccrea ha istituito un team, a supporto del Responsabile del Servizio della Conservazione, dedicato al monitoraggio e l'evoluzione del proprio sistema di conservazione.

La sicurezza fisica e logica fa riferimento alla sicurezza dei sistemi e delle reti di Iccrea e nel rispetto di quanto riportato nelle Policy in tema di Sicurezza di Iccrea

I controlli e le contromisure messi in atto per garantire la sicurezza delle informazioni vengono stabiliti a seguito di un'accurata analisi del rischio che consente di identificare e valutare il danno causabile dalla combinazione di minacce e vulnerabilità del sistema e sono finalizzati ad assicurare che gli strumenti informatici in dotazione siano protetti secondo criteri aggiornati con la tecnologia e coerenti con la normativa di tutela della privacy, per garantire il corretto funzionamento contro il cosiddetto malicious code (virus hacker, spamming, etc.), ma anche contro gli accessi non autorizzati sia logici che fisici.

Nella normativa interna di Iccrea, sono stabilite precise indicazioni atte a presidiare l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni anche al fine di ripristinare la corretta funzionalità. Inoltre il servizio di Conservazione è ricompreso nel sistema di Continuità Operativa di Iccrea che ha il compito di proteggere l'esercizio dei processi e delle informazioni aziendali – quindi delle connesse risorse umane, informatiche, logistiche, e di relazione con i soggetti esterni - in modo conforme alle normative vigenti e alle disposizioni Banca d'Italia relative alle "Linee guida per la continuità di servizio delle infrastrutture qualificate dei sistemi di pagamento".

Tutte le componenti del sistema sono dotate di propri file di log nel quale sono tracciate tutte le operazioni eseguite e le altre informazioni che permettono di tenere traccia delle attività svolte e facilitare la diagnosi di eventuali anomalie e/o incident.

I processi di *change management* con impatti sulla piattaforma sono gestiti secondo le metodologie standard di service management adottate da Iccrea al cui interno sono definiti compiti e responsabilità delle strutture competenti.

In particolare, il processo di gestione dei cambiamenti di natura informatica comprende sia i rilasci o le modifiche apportate alle applicazioni che l'aggiornamento delle infrastrutture tecnologiche (ad es. sistemi, reti, database).

Lo svolgimento del processo assicura il rispetto dei seguenti principi:

1. qualunque progetto di modifica deve essere formalmente identificato (finalità, responsabilità di svolgimento, suddivisione in interventi di modifica con identificazione, per ciascuno, di asset impattati sia direttamente che indirettamente, rischi associati e tempi di esecuzione), segnalato e autorizzato;

2. ove possibile, vanno svolti test in ambienti o condizioni non critici per la produzione;
3. gli interventi di modifica devono essere pianificati ed autorizzati, dopo aver consultato i responsabili delle applicazioni e dei servizi erogati impattati ed eventualmente il BRM di competenza;
4. ove applicabile, ogni intervento di modifica deve essere accompagnato dal piano di ripristino della situazione precedente, da eseguire in caso di problemi durante la modifica;
5. l'inizio di qualunque intervento di modifica deve essere segnalato formalmente ed avviene sotto la responsabilità del responsabile del Progetto di Modifica e sotto la supervisione del responsabile dell'intervento di modifica.
6. la chiusura degli interventi di modifica e dell'intero Progetto di Modifica deve essere segnalata formalmente comunicando i tempi dell'intervento, l'esito dell'intervento, eventuali problemi riscontrati con relative cause e soluzioni.

Nel caso di iniziative di ampio impatto per il sistema, sono previste idonee misure, tecniche, organizzative e procedurali, volte a garantire un avvio in esercizio controllato e con limitati impatti sui servizi forniti alla clientela (ad es., implementazione per stadi successivi, periodi di esercizio in parallelo con la precedente procedura, procedure di fallback e contingency).

L'infrastruttura contempla, per il corretto esercizio della piattaforma, la presenza di:

- Ambiente di sviluppo;
- Ambiente di test;
- Ambiente di collaudo/pre-produzione;
- Ambiente di produzione.

La modifica di ogni *configuration item* della piattaforma viene quindi sottoposta, ai fini del rilascio in produzione, ad un completo ciclo di collaudo e test di regressione.

Maggiori informazioni sono contenute nel documento riservato di Iccrea, Piano di sicurezza del sistema di Conservazione sulle tematiche:

- le procedure di gestione e conservazione dei log (paragrafo7.2)
- monitoraggio del sistema di conservazione, (paragrafo 7.1)
- verifica periodica di conformità. (paragrafo 6)

Torna al sommario

# 9 MONITORAGGIO E CONTROLLI

Iccrea, per mezzo del Responsabile del servizio di Conservazione, supportato e coadiuvato dalle competenti Unità Organizzative, esegue controlli sugli archivi conservati al fine di verificare l'integrità dei supporti utilizzati e la leggibilità dei documenti conservati secondo i criteri previsti dalla legge.

In caso di necessità Iccrea provvede al riversamento diretto a partire dalla copia di sicurezza realizzata, oppure ripristinando un backup del supporto magnetico.

Torna al sommario

## 9.1 Procedure di monitoraggio

Iccrea:

- verifica la capacità di esibizione dei documenti conservati attraverso il sistema di Conservazione.
- verifica che il sistema di Conservazione archivi e renda disponibile, relativamente ad ogni supporto di memorizzazione, quanto segue:
  - descrizione del contenuto dell'insieme dei documenti;
  - estremi identificativi del Responsabile del servizio di Conservazione;
  - indicazione delle copie di sicurezza;
- mantiene e rende accessibile un archivio del software dei programmi in gestione nelle eventuali diverse versioni;
- verifica la corretta funzionalità del sistema e dei programmi in gestione;
- verifica le misure adottate per la sicurezza fisica e logica del sistema preposto al processo di Conservazione e delle copie di sicurezza dei supporti di memorizzazione;
- verifica periodicamente, con cadenza non superiore a cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti;
- partecipa a visite ispettive e audit di tutti i processi coinvolti nel servizio di Conservazione al fine di individuare interventi migliorativi o correttivi;
- verifica l'adeguamento del sistema di Conservazione all'evoluzione normativa;
- provvede a tenere aggiornato il presente manuale della Conservazione a fronte di eventi di cui si deve tenere traccia, quali adeguamenti normativi, evoluzioni tecnologiche, variazioni nell'assegnazione delle responsabilità, evoluzioni tecnologiche e software, etc.

InfoCert supporta Iccrea nella gestione della piattaforma LegalDoc attivando la propria soluzione di monitoraggio remoto denominato TMS.

TMS si occupa di monitorare e misurare le componenti tecnologiche usate per erogare il servizio LegalDoc, offrendo ad Iccrea uno strumento fondamentale per individuare tempestivamente eventuali anomalie sui servizi erogati e dove andare a concentrare l'azione correttiva per una rapida risoluzione degli incident.

Torna al sommario

## 9.2 Verifica dell'integrità degli archivi

Il Responsabile del servizio della Conservazione, come descritto nell'art. 7 comma 1 lettera f) "assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità" dei documenti conservati con procedure automatiche e manuali, al fine di prevenire il rischio che i documenti non possano essere visualizzabili, inficiando il mantenimento della loro validità legale nel tempo.

La piattaforma LegalDoc fornisce una procedura, detta verificatore, che esegue il test di leggibilità binaria mediante il continuo calcolo delle impronte dei documenti conservati, con successivo confronto con l'hash del documento contenuto nel file delle direttive della conservazione inviato dal Soggetto Produttore. Se la procedura non registra differenze tra i due hash, il documento è inalterato rispetto a quanto trasmesso dal Produttore.

La procedura esegue i seguenti passi operativi:

- verifica della validità della firma digitale e della marcatura temporale apposte all'atto della conservazione dal Responsabile del servizio della Conservazione sul file IPdA e, se presenti, verifica della firma digitale e della marcatura temporale del documento;
- calcolo dell'impronta del documento e confronto con quella contenuta all'interno del file IPdA;
- generazione di un report che viene automaticamente sottoposto alla conservazione nell'area dedicata al Responsabile del servizio della Conservazione (quindi a sua volta firmato e marcato temporalmente dal Responsabile del servizio della Conservazione stesso).

In caso di anomalie, se il documento risulta corrotto, viene inviato un alert al Responsabile del servizio della Conservazione, che tenterà il ripristino manuale partendo da un'altra sorgente di backup. Se nessuna sorgente è disponibile viene redatto un verbale di incidente, sottoscritto e conservato dal Responsabile del servizio della Conservazione per attestare la situazione rilevata. Analoga procedura viene applicata in caso di perdita di tutte le copie del dato.

Periodicamente, il sistema produce dei report di sintesi dell'attività di verifica svolta.

In aggiunta alla verifica automatica dell'integrità binaria, il Responsabile del servizio della Conservazione e i suoi delegati sono dotati di apposita strumentazione (detta CORE, Console del Responsabile), con credenziali dedicate, con la quale procedono manualmente e periodicamente ad una verifica campionaria di leggibilità dell'archivio documentale conservato, scegliendo ed esibendo casualmente un campione di documenti presenti nel sistema di conservazione.

Viene poi redatto automaticamente un verbale che attesta l'elenco dei documenti visualizzati, successivamente sottoscritto e conservato dal Responsabile del servizio della Conservazione nell'area appositamente creata nel sistema di conservazione.

Torna al sommario

## 9.3 Controlli

Oltre ai monitoraggi appena descritti, il sistema di conservazione implementa numerosi sotto-processi dediti al controllo del corretto svolgimento dei processi, segnalando eventuali errori o anomalie al Soggetto Produttore ed al personale incaricato dell'amministrazione del sistema.

In fase di versamento dei pacchetti in LegalDoc vengono automaticamente eseguiti dei controlli, preventivamente concordati con il soggetto Produttore nell'allegato "Specificità del contratto" all'attivazione del servizio:

- Correttezza della struttura del file di Parametri (contenente le informazioni per la leggibilità nel tempo del documento da conservare);
- Correttezza della struttura del file di Indici;
- Presenza in conservazione sul medesimo path di un documento con lo stesso nome-file del documento da conservare;
- Dimensione massima del documento da conservare (di default 256 megabyte);

I controlli si riferiscono esclusivamente ai formati previsti contrattualmente, ossia la conservazione a norma è garantita soltanto per quei formati di documenti prescritti dalla normativa e concordati.

La Piattaforma NON effettua controlli sull'eventuale presenza di virus nei pacchetti di versamento.

Torna al sommario

## 9.4 Soluzioni adottate in caso di anomalie

Periodicamente, il Responsabile del servizio della Conservazione effettua un riesame generale del sistema insieme ai soggetti incaricati, al fine di accertare la conformità del sistema al livello atteso, analizzare le cause di eventuali incidenti o disservizi e promuovere attività di prevenzione o miglioramento.

Qualora necessario, una riunione di riesame può essere indetta a fronte di particolari eventi (ad esempio, a titolo non esaustivo, cambi tecnologici, normativi o di requisiti funzionali, stagionalità di carico elaborativo, arrivo consistente e non pianificato di nuova clientela, ecc.).

In caso di evento che pregiudichi, in tutto o in parte, il repository primario dei dati sottoposti a Conservazione, è prevista una procedura di back up che:

• assicuri nel continuo la disponibilità delle informazioni e la continuità delle attività di elaborazione dati;

• garantisca la possibilità di ripristino delle informazioni e dell'intero ambiente applicativo nel sito secondario;

• garantisca il mantenimento dei requisiti di confidenzialità ed integrità delle informazioni salvate o archiviate.

Il verificarsi dell'evento catastrofico e l'esecuzione della procedura di ripristino dell'archivio saranno tempestivamente notificati ai Clienti.

Torna al sommario