Manuale di Conservazione

di Iccrea Banca S.p.A.

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione		Aldo Bucci	*Responsabile del servizio di Conservazione*
Verifica		Giancarlo Castorina	Responsabile UO Sicurezza delle Informazioni
Verifica		Davide Pascuttini	Responsabile UO Applicazioni Gestionali e Direzionali
Verifica		Antonio Zattera	Responsabile UO Data Center
Approvazione		Vittorio Marogna	Responsabile UO Incassi e Pagamenti

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
1.0	17 /06/2012	Creazione documento	n.a.
1.1	29/07/2013	Creazione nuova classe documentale: Buste di cassa	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.
3.0	31/03/2015	Esecuzione del piano di adeguamento previsto	n.a.
3.1	07/05/2015	Interventi di fine tuning a seguito dell’esecuzione del piano di adeguamento.	n.a.
4.0	01/3/2016	Adeguamento allo schema previsto da AGID	n.a.

INDICE DEL DOCUMENTO

1 Scopo e ambito del documento

Il presente documento è il manuale della Conservazione di Iccrea Banca S.p.A., 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 Banca S.p.A. effettua il servizio di Conservazione per i propri documenti e in outsourcing per i documenti delle Banche (di Credito Cooperativo o altre Banche tramitate) o per la Pubblica Amministrazione centrale e locale (di seguito Pubblica Amministrazione) mediante la stipula di un apposito contratto.

Le Banche e la Pubblica Amministrazione al proprio interno nominano un Responsabile della Conservazione.

Le Banche possono fornire anche alla propria clientela il servizio di Conservazione.

Il manuale di 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:
  - 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:
  - 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:
  - 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;
  - 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; ad oggi viene rilasciata una 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:

- l'elenco delle Classi documentali da portare in conservazione;
- gli indici delle Classi documentali

Le indicazioni contenute nel presente documento hanno validità nell'adempimento di quanto previsto nei contratti:

a) "Affidamento in outsourcing di servizi di Conservazione e altri servizi accessori" fra Iccrea Banca S.p.A. e la Banca e/o la Pubblica Amministrazione;
b) "Fornitura di servizi di gestione, smistamento e Conservazione di documenti" fra la Banca e il Cliente.

La mancata applicazione di quanto indicato dal presente manuale potrà essere sanzionata secondo quanto previsto dal contratto.

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 Banca S.p.A.;
    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 dal sistema di conservazione comprese le funzionalità di presa visione ed estrazione copia dei documenti informatici.
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
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.
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
Certificatore accreditato	soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, dall' Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza.
Ciclo di gestione	arco temporale di esistenza del documento informatico, del fascicolo

	informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo.
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
Conservazione	insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione.
Copia 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 immagine 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'articolo 12 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 da r) 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	sono tutti quei dati che sono identificativi del soggetto fisico, giuridico ,di ente o associazione e, quindi, come tali, anche i dati anagrafici, o addirittura un eventuale indicazione numerica identificativa della persona.
Dati Sensibili	i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo

	stato di salute e la vita sessuale (Decreto Legislativo 30 giugno 2003, n.196 - Codice in materia di protezione dei dati personali Art. 4 comma 1 d)).
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	la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti come definito dal Codice dell'Amministrazione Digitale.
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 elettronica avanzata, risultato della procedura informatica (validazione), basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore 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, utilizzati come metodo di identificazione.
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 che sia basata su un certificato qualificato e creata mediante un dispositivo sicuro per la creazione della firma.
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	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.
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 di 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 di conservazione.
Pacchetto di distribuzione	pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta
Pacchetto di versamento	pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di

	conservazione
Pacchetto informativo	contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare
Presa in carico	accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione.
Processo di conservazione	insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 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 8, comma 1 del DPCM 3/12/2013.
Responsabile del trattamento dei dati	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.
Responsabile della sicurezza	soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza
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	strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e 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
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], articolo 2215 bis - Documentazione informatica;
- **Legge 7 agosto 1990, n. 241 e s.m.i**. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- **Decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000**, e successive modificazioni, recante «Regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica 20 ottobre 1998, n. 428».
- **Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445**, recante «Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa".
- **D. Legislativo 30 giugno 2003, n.196 "**Codice in materia di protezione dei dati personali" (Legge delega n. 127/2001) (Supplemento Ordinario alla n.123 alla GU n. 174 del 29 Luglio 2003 e successive modificazioni).
- **D. Legislativo 22 gennaio 2004, n. 42,** e successive modificazioni, recante «Codice dei beni culturali e del paesaggio, ai sensi dell'art. 10 della legge 6 luglio 2002, n. 137».
- **D. Legislativo 20 febbraio 2004, n.52 "**Attuazione della direttiva 2001/115/CE che semplifica ed armonizza le modalità di fatturazione in materia di IVA". (Gazzetta Ufficiale N. 49 del 28 Febbraio 2004).
- **D. 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.**
- **Circolare Agenzia delle Entrate n.45/E del 19 ottobre 2005.**
- **Circolare 36/E dell'Agenzia delle Entrate dicembre 2006.**
- **Art. 2215 bis Codice Civile.**
- Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (**G.U. n. 300 del 24 dicembre 2008**) e successive modificazioni
- **Decreto Legislativo 1° dicembre 2009, n. 177,** recante «Riorganizzazione del Centro nazionale per l'informatica nella pubblica amministrazione, a norma dell'art. 24 della legge 18 giugno 2009, n. 69».
- **Deliberazione CNIPA n. 45 del 21 maggio 2009** "Regole per il riconoscimento e la verifica del documento informatico".
- **Provvedimento Agenzia delle Entrate del 25 ottobre 2010** "Provvedimento attuativo della comunicazione dell'impronta relativa ai documenti informatici rilevanti ai fini tributari, ai sensi dell'articolo 5 del decreto 23 gennaio 2004 (provvedimento del Direttore dell'Agenzia delle Entrate, prot. Nr 2010/143663)".
- **Decreto-Legge 22 giugno 2012, n. 83**, convertito, con modificazioni, dalla legge 7 agosto 2012, n. 134, recante «Misure urgenti per la crescita del Paese», con cui stato soppresso DigitPA e le funzioni sono state attribuite all'Agenzia per l'Italia digitale.

- **Decreto Presidente Consiglio dei Ministri 22 febbraio 2013. "**Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali". Pubblicato nella Gazzetta Uff. 21 maggio 2013, n. 117.
- **Decreto Presidente Consiglio dei Ministri del 3 dicembre 2013.** "Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005". Pubblicato nella Gazzetta Ufficiale n.59 del 12-3-2014 - Supplemento Ordinario n. 20).
- **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 13-11-2014** 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 eIDAS**

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 1o ottobre 2014:

- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- ETSI TR 101 533-2 V1.3.1 (2012-04)Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

Torna al sommario

4 Ruoli e Responsabilità

Nella tabella che segue sono indicati i ruoli e le responsabilità assegnati in conformità a quanto previsto dal DPCM del 3 dicembre 2013. I commi da a) a l) si riferiscono alle attività previste dall'art. 8.

ruoli	nominativo	attività di competenza	periodo nel ruolo	eventuali deleghe
Responsabile del servizio di conservazione	Aldo Bucci	a) definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale provvede a tenere evidenza, in conformità alla normativa vigente; b) gestisce il processo di conservazione e garantirne nel tempo la conformità alla normativa vigente; c) genera il "rapporto di versamento", secondo le modalità previste dal manuale di conservazione; d) genera e sottoscrive il "pacchetto di distribuzione" con firma digitale, nei casi previsti dal manuale di conservazione; e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione; f) assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi; g) al fine di garantire la conservazione e l'accesso ai documenti informatici, concorre ad assicurare misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità. Concorrere, inoltre, ad assicurare l'adozione di analoghe misure con riguardo all'obsolescenza dei formati; h) assicura la duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal "manuale di conservazione"; i) concorre all'adozione delle misure necessarie per la sicurezza fisica e logica del sistema di conservazione; j) assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per	Dal marzo del 2012 alla data attuale	

		l'espletamento delle attività al medesimo attribuite; k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza; l) predispone il manuale di conservazione e curarne l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.		
Responsabile Sicurezza dei sistemi per la conservazione	Giancarlo Castorina	Ha la responsabilità di definire le Politiche in tema di sicurezza delle informazioni. Valuta e monitora i rischi connessi alla sicurezza delle informazioni provvedendo a coordinare le iniziative ed attività circa gli interventi progettuali connessi. E' responsabile del Sistema di Gestione della Sicurezza delle Informazioni. Assicura la funzione di "chief information security officer" (CISO). Coadiuva il Responsabile del servizio di Conservazione per gli aspetti di competenza in particolare per lo svolgimento dei compiti di cui alla lettere a) e l).	Dal marzo del 2012 alla data attuale	
Responsabile funzione archivistica di conservazione	Elena Lisi	Coadiuva il Responsabile del servizio di Conservazione per gli aspetti di competenza. In particolare concorre: - alla 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; - alla definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici; - al monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione.	Da maggio 2016.	
Responsabile trattamento	Vittorio Marogna	Garantisce il rispetto delle vigenti disposizioni in materia di trattamento dei dati personali ai sensi delle	Dal marzo del 2012 alla data attuale	

dati personali		normativa interna di Iccrea Banca S.p.A. in materia di Privacy[1]. Garantisce che il trattamento dei dati affidati dai clienti avviene nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza. Coadiuva il Responsabile del servizio di Conservazione per gli aspetti di competenza.		
Responsabile sistemi informativi per la conservazione	Antonio Zattera	Ha il compito di curare la gestione e lo sviluppo dei sistemi di elaborazione e di collaborare allo sviluppo dei sistemi di sicurezza dati dell'Istituto e di eventuali utenti esterni (in qualità di "Incaricato Specializzato Tecnologie"), in conformità alle politiche di qualità e sicurezza emanate dagli Organi competenti. Assicura la corretta funzionalità delle procedure prese in carico controllando il buon esito dei lavori e fornendo la necessaria assistenza tecnica agli utenti interni/esterni. E' responsabile del coordinamento della ricerca tecnologica. Responsabile dell'U.O. Data Center è responsabile del sottosistema Disaster Recovery Plan (DRP) della Continuità Operativa. Coadiuva il Responsabile del servizio di Conservazione per gli aspetti di competenza in particolare per lo svolgimento dei compiti di cui alla lettere a), e), h), g) e i).	Da ottobre del 2014 alla data attuale	
Responsabile sviluppo e manutenzione del sistema di conservazione	Davide Pascuttini	Assicura, in accordo con la pianificazione definita, lo sviluppo e la manutenzione delle procedure e dei servizi informatici di competenza sulla base degli indirizzi strategici ed operativi aziendali definiti, garantendo l'adeguatezza degli interventi agli obiettivi fissati. Coadiuva il Responsabile del servizio di Conservazione per gli aspetti di competenza in particolare per lo svolgimento dei compiti di cui alla lettera a).	Da Aprile 2015 alla data attuale	

Inoltre la Struttura organizzativa funzionale di Iccrea Banca S.p.A. e del Gruppo Bancario Iccrea prevede che il Responsabile del servizio di Conservazione sia coadiuvato dai Responsabili:

- della UO Sicurezza del Lavoro e delle Aree Operative e della UO Sicurezza Logica per ciò che attiene

[1] Iccrea Banca S.p.A. ha ritenuto di individuare come Responsabili Interni del trattamento i Responsabili delle singole Unità Organizzative ed i Ruoli Funzionali in relazione ai trattamenti di dati personali svolti nell'ambito della UO di competenza.

lo svolgimento dei compiti di cui alla lettera i);
- della UO Rischi Operativi, Compliance e Antiriciclaggio per ciò che attiene lo svolgimento dei compiti di cui alla lettere b) e l);
- della UO Processi e Procedure di Iccrea Holding S.p.A. per ciò che attiene lo svolgimento dei compiti di cui alla lettera l).

Torna al sommario

5 Struttura organizzativa per il servizio di Conservazione

5.1 Organigramma

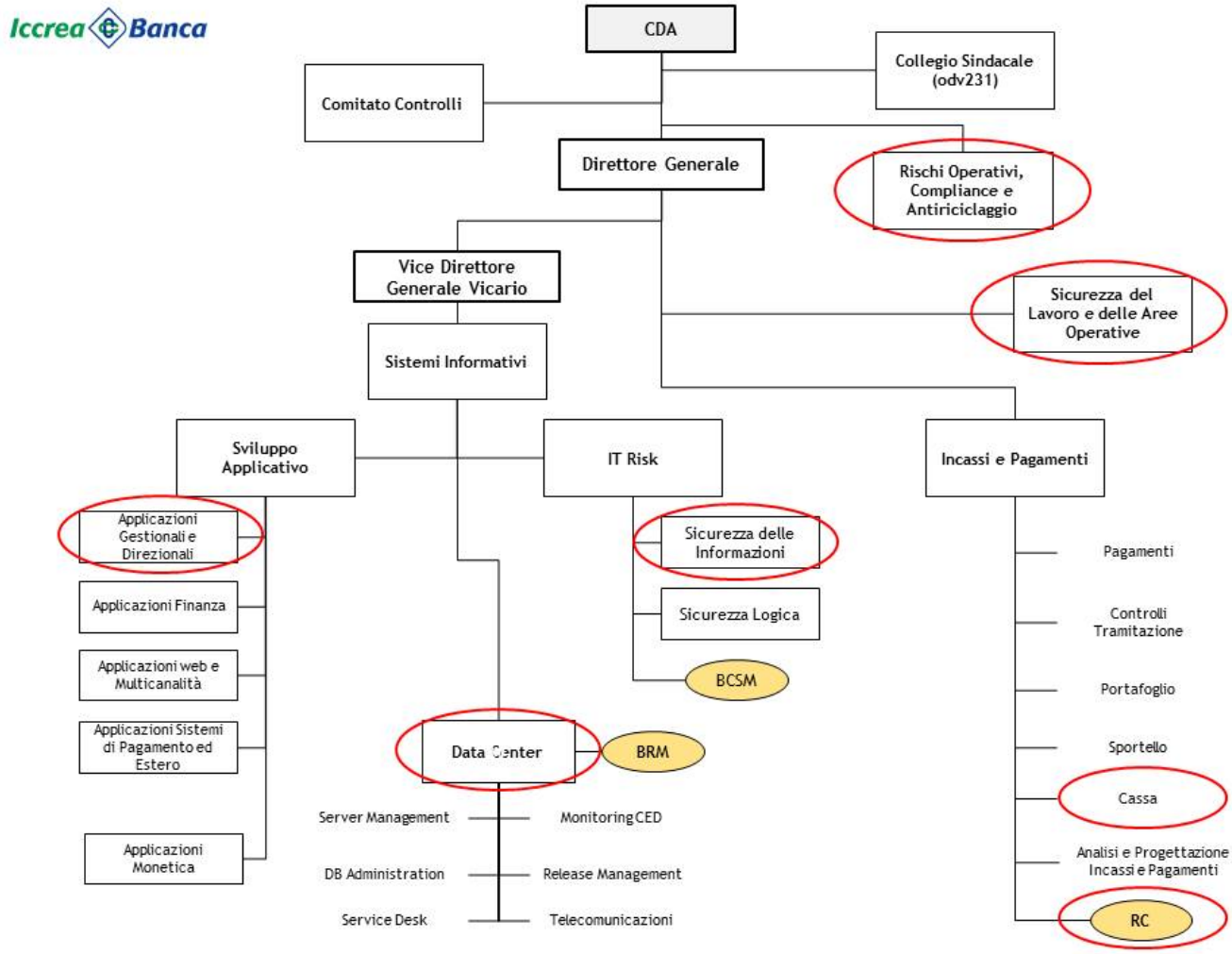

Figura 1 Organigramma per il servizio di Conservazione

Torna al sommario

5.2 Strutture Organizzative

Con un provvedimento interno il Consiglio di Amministrazione di Iccrea Banca S.p.A. 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 Banca S.p.A. ha costituito il Ruolo Funzionale di Responsabile della Conservazione dei propri documenti e di quelli della propria clientela situato all'interno dell'Unità Organizzativa Incassi e Pagamenti

(figura 1). La medesima risorsa svolge anche il ruolo di Responsabile del servizio di Conservazione per conto delle Banche o della Pubblica Amministrazione.

Il Responsabile del servizio di Conservazione di Iccrea Banca S.p.A. espleta in particolare i processi di apposizione di firme digitali e marche temporali. Per svolgere tale attività può avvalersi di altra risorsa di Iccrea Banca S.p.A. situata anch'essa nell'Unità Organizzativa Incassi e Pagamenti, Il Responsabile del servizio di conservazione coadiuvato dai delegati interviene nelle funzioni sotto indicate:

- attivazione del servizio di conservazione (a seguito della sottoscrizione di un contratto);
- acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento;
- preparazione e gestione del pacchetto di archiviazione;
- preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta;
- scarto dei pacchetti di archiviazione;
- chiusura del servizio di conservazione (al termine di un contratto).

Iccrea Banca S.p.A. ha inoltre individuato all'interno del proprio organigramma, oltre ai Ruoli e Responsabilità indicati nel precedente paragrafo, le Unità Organizzative dei Sistemi Informativi che coadiuvano il Responsabile del servizio di Conservazione ad ottemperare agli obblighi contrattuali e normativi, in particolare:

- UO Applicazioni Direzionali e Gestionali: assicura la conduzione e manutenzione del sistema di conservazione. Coadiuva 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();
- UO Data Center: monitora il sistema di conservazione. Coadiuva 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 ;
- UO Sistemi Informativi ha la responsabilità di 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;
- UO Sicurezza delle Informazioni: valuta e monitora i rischi connessi alla sicurezza delle informazioni provvedendo a coordinare le iniziative ed attività circa gli interventi progettuali connessi. Provvede alla verifica periodica di conformità a normativa e standard di riferimento in coordinamento con la U.O. Rischi Operativi, Compliance e Antiriciclaggio.
- UO Sicurezza Logica: cura la progettazione , lo sviluppo e la gestione dei sistemi di sicurezza logica per l'accesso a dati e sistemi.

Torna al sommario

6 Oggetti sottoposti a conservazione

6.1 Oggetti conservati

Il servizio di conservazione coerentemente con quanto previsto dagli articoli 3, 4 e 9 del DPCM del 3/12/2013 assicura, dalla presa in carico dal produttore fino all'eventuale scarto, la conservazione, tramite l'adozione di regole, procedure e tecnologie, degli oggetti di seguito elencati che saranno conservati, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità:

- i documenti informatici[2]:
  a. riferiti alle classi documentali di cui all'allegato "Specificità del contratto" del presente manuale;
  b. con i metadati ad essi associati di cui all'allegato "Specificità del contratto" del presente manuale;
  c. con i riferimenti ai visualizzatori relativi alle tipologie di documenti gestiti di cui all'allegato "Specificità del contratto" del presente manuale;

Gli oggetti della conservazione sono trattati dal "sistema di conservazione" in "pacchetti informativi" che si distinguono in: 1) "pacchetti di versamento", 2) "pacchetti di archiviazione", 3) "pacchetti di distribuzione".

Torna al sommario

6.2 Pacchetto di versamento

Il pacchetto di versamento è rappresentato da una serie di parametri passati all'interno della chiamata al servizio esposto dal sistema di conservazione.
La struttura della chiamata è descritta nel seguente file wsdl (web service description language):

```
            <xs:element name="addDocuments">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element maxOccurs="unbounded" minOccurs="0" name="docInfos"
nillable="true" type="ns1:DocInfo"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>

            <xs:complexType name="DocInfo">
                <xs:sequence>
                    <xs:element minOccurs="0" name="classId" type="xs:int"/>
                    <xs:element minOccurs="0" name="companyId" type="xs:int"/>
                    <xs:element minOccurs="0" name="docFile" nillable="true"
type="xs:base64Binary"/>
                    <xs:element minOccurs="0" name="docId" type="xs:int"/>
                    <xs:element minOccurs="0" name="fileName" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="0" name="filePath" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="0" name="indexes" nillable="true"
type="ns:IndexList"/>
                    <xs:element minOccurs="0" name="logDiskId" type="xs:int"/>
                </xs:sequence>
            </xs:complexType>
            <xs:complexType name="IndexList">
                <xs:sequence>
                    <xs:element maxOccurs="unbounded" minOccurs="0" name="index"
nillable="true" type="ns:IndexType"/>
                </xs:sequence>
            </xs:complexType>
            <xs:complexType name="IndexType">
                <xs:sequence>
                    <xs:element minOccurs="0" name="label" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="0" name="name" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="0" name="type" type="xs:int"/>
                    <xs:element minOccurs="0" name="value" nillable="true"
type="xs:string"/>
                </xs:sequence>
            </xs:complexType>
```

Figura 2 struttura del pacchetto di versamento

Elemento	Descrizione
classId	codice identificativo di sistema della classe documentale configurata sul sistema Paperless
companyId	codice identificativo di sistema della persona (giuridica o fisica) configurata sul sistema Paperless
docFile	Rappresentazione in byte transcodificata in base 64 del file documento
fileName	Nome del file
indexes	Lista degli indici

Elemento	Descrizione
label	Label dell'indice
name	Nome dell'indice
type	Tipo di dato dell'indice
value	Valore dell'indice

Figura 3 dettaglio degli elementi valorizzati

Torna al sommario

6.3 Pacchetto di archiviazione

Il processo di conservazione e del trattamento dei pacchetti di archiviazione si compone delle seguenti attività:

1. Preparazione del pacchetto di archiviazione
2. Chiusura del pacchetto di archiviazione
3. Conservazione (o archiviazione) del pacchetto di archiviazione

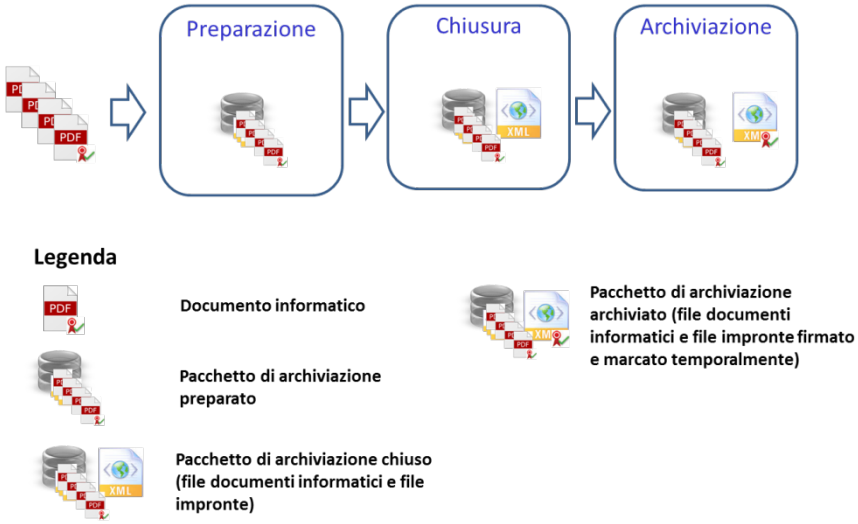

Figura 4 Pacchetto di Archiviazione

Di seguito si descrive in modo puntuale ciascuna delle attività sopra elencate e le funzionalità della piattaforma a supporto delle stesse.
Il pacchetto di archiviazione, generato secondo il processo descritto al paragrafo 7.5, è conservato è strutturato come segue:

- Una folder DOCS contenente i documenti informatici oggetto di conservazione elettronica
- Una folder INDEX contenente un file indice (formato xml) contenente i metadati dei documenti inclusi nella folder DOCS
- il file di impronte dei documenti secondo formato UNI SINCRO
- il file di impronte di cui al punto precedente ma firmato dal RdC
- il file di impronte di cui al punto precedente ma con marca temporale.

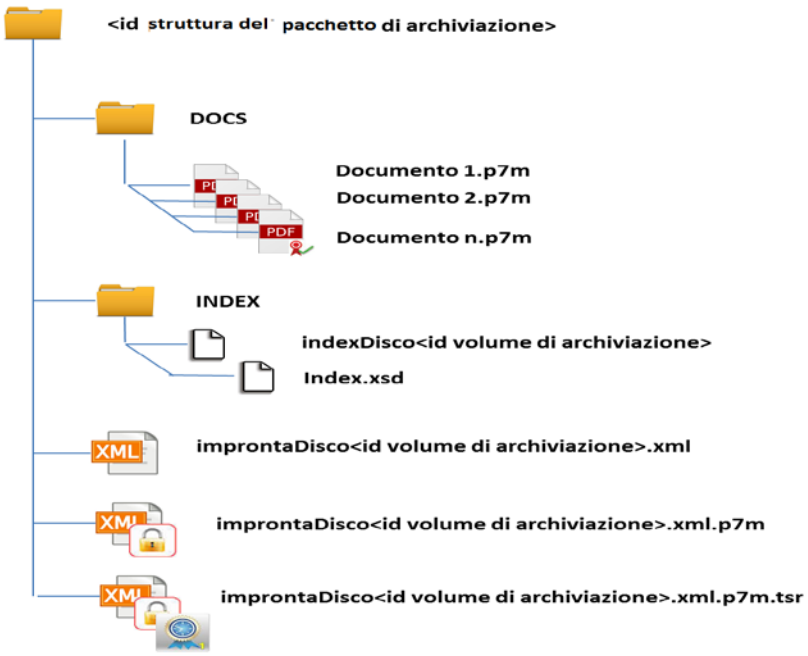

Figura 5 Struttura pacchetti di Archiviazione

All'interno del file impronte, all'interno del nodo VdC sono riportate le indicazioni relative alla struttura collegata IndexDisco. In particolare:

- il path dello schema XML (`IndexDisco.xsd`) della struttura di metadati custom adottata per descrivere le fatture;
- il suddetto Schema XML istanziato (`IndexDisco.xml`), contenente le informazioni strutturate dell'elemento <MoreInfo>.

```
<ns1:VdC>
    <ns1:ID ns1:scheme="Paperless">217</ns1:ID>
    <ns1:MoreInfo ns1:XMLScheme="INDEX/index.xsd">
        <ns1:ExternalMetadata ns1:format="text/xml">
            <ns1:ID ns1:scheme="Paperless">indexDisco217.xml</ns1:ID>
            <ns1:Path>INDEX/indexDisco217.xml</ns1:Path>
            <ns1:Hash ns1:function="SHA-256">0ad5fca2fc09b8a6e7a06181314c03767cfa4c08caae94002277e54c541cfc20</ns1:Hash>
        </ns1:ExternalMetadata>
    </ns1:MoreInfo>
</ns1:VdC>
```

Figura 6 Esempio di un file di impronte

Torna al sommario

6.4 pacchetto di distribuzione

Il responsabile del servizio di Conservazione, mediante specifica funzionalità, può predisporre pacchetti di distribuzione da rilasciare ai fini dell'esibizione dei documenti archiviati.

Tramite specifica funzionalità, è possibile generare dei file immagine (ISO) a loro volta masterizzabili su supporti esterni (ad esempio CD e DVD) contenenti i file dei documenti, i relativi a pacchetti di archiviazione ed un tool applicativo che dispone di funzionalità analoghe alla versione on line (ricerca, visualizzazione, verifica della firma di emissione, della firma del responsabile di conservazione e della marcatura temporale).
La struttura del pacchetto di distribuzione è la seguente:

- una folder dischiLogici con i pacchetti di archiviazione selezionati
- una folder Tools con il tool di consultazione del pacchetto di distribuzione
- un file autorun.inf contenente dati di configurazione necessari all'avvio del tool di consultazione
- un file avvia.bat contenente le istruzioni per l'avvio del tool di consultazione

La folder dischiLogici assume la medesima struttura del pacchetto di archiviazione ma in aggiunta al pacchetto di archiviazione e in funzione delle dimensioni del supporto su cui viene salvato il pacchetto di distribuzione possono essere inseriti uno o più pacchetti di archiviazione.

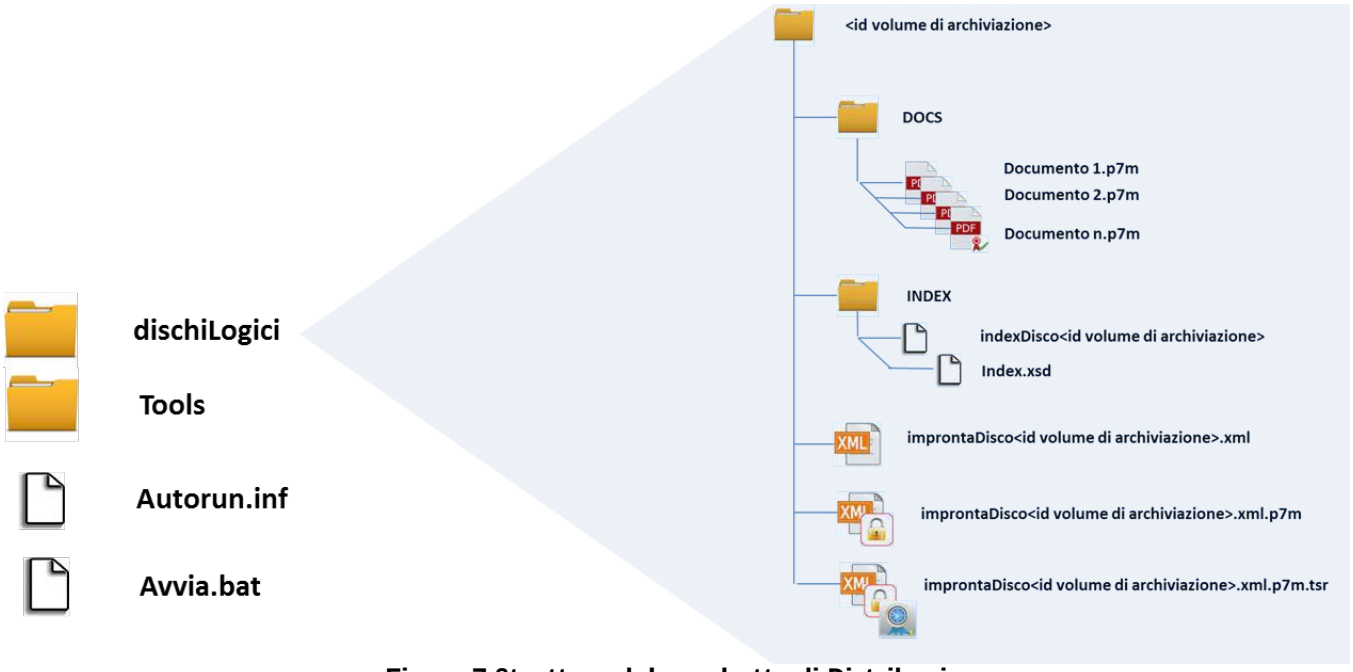

Figura 7 Struttura del pacchetto di Distribuzione

Torna al sommario

7 Processo di Conservazione

La realizzazione del servizio di Conservazione permette di gestire le attività sinteticamente descritte di seguito.

1. Il cliente accede ad un'interfaccia WEB caricando il proprio documento firmato digitalmente e mediante apposita procedura (compresa nell'Home Banking per la Pubblica Amministrazione e clientela, piattaforma dedicata per le BCC e Banche) crea il pacchetto di versamento da inviare in Conservazione,
2. verifica che il "pacchetto di versamento" e gli oggetti contenuti siano coerenti con le modalità previste dal presente manuale e con i formati indicati nell'allegato "Specificità del contratto";
3. rifiuto, a mezzo di invio tramite collegamento telematico, del "pacchetto di versamento", nel caso in cui le verifiche di cui al punto precedente abbiano evidenziato delle anomalie;
4. acquisizione del "pacchetto di versamento" attraverso un collegamento telematico;
5. generazione e messa a disposizione del cliente tramite collegamento telematico del "rapporto di versamento" relativo ad uno o più pacchetti di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo universale coordinato (UTC), e una o più' impronte, calcolate sull'intero contenuto del pacchetto di versamento, secondo le modalità descritte nel presente manuale;
6. la preparazione, la sottoscrizione e la gestione del "pacchetto di archiviazione" in particolare:
    a. generazione dell'impronta (*hash)* dei Documenti,
    b. memorizzazione dell'impronta del pacchetto di Documenti nel "pacchetto di archiviazione",
    c. apposizione della Firma Digitale al pacchetto di archiviazione ,
    d. richiesta di una Marca Temporale associata al pacchetto di archiviazione firmato,
    e. memorizzazione del pacchetto di Documenti, del pacchetto di archiviazione firmato digitalmente e della Marca Temporale su supporto con caratteristiche di alta affidabilità e alta permanenza del dato, per un periodo temporale previsto dalla legge o concordato con il cliente,
7. preparazione del "pacchetto di distribuzione", coincidente con il "pacchetto di archiviazione" sottoscritto con firma digitale ai fini dell'esibizione richiesta dall'utente (Banca, Pubblica Amministrazione o Cliente);
8. realizzazione di un'apposita interfaccia che, con riferimento al pacchetto di distribuzione, permetta alla Banca, alla Pubblica Amministrazione o al Cliente di:
    a. effettuare ricerche all'interno del repository documentale, sulla base degli indici definiti,
    b. visualizzare i risultati della ricerca,
    c. visualizzare il documento risultante dalla ricerca effettuata,
    d. effettuare il download di uno o di tutti i documenti risultanti dalla ricerca effettuata, in conformità a quanto previsto dalle regole tecniche in materia di formazione del documento informatico

e. verificare, in caso di esibizione dei documenti, la Marca Temporale e la Firma Digitale del pacchetto di documenti in cui ogni documento è stato inserito;

9. lo scarto del "pacchetto di archiviazione" dal sistema di conservazione alla scadenza dei termini di conservazione previsti, dandone informativa al produttore.

Torna al sommario

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

La fase di versamento è costituita dalle seguenti attività:

- Predisposizione dei documenti da versare da parte dell'azienda
- Caricamento singolo o massivo attraverso:
  - upload dei documenti tramite funzione on line del sistema di front end
  - web services esposti dal sistema di front end

Le modalità di trasmissione del pacchetto di versamento sul sistema di conservazione viene effettuato attraverso un servizio (web services) utilizzando una connessione su canale criptato (https), specificando le seguenti informazioni:

- l'azienda di competenza
- la classe documentale di competenza
- i metadati specifici del documento
- il codice binario trascodificato in base-64 del documento informatico

Il complesso delle informazioni di cui sopra costituisce il pacchetto di versamento verso il sistema di conservazione.

Tutte le operazioni di presa in carico dei pacchetti di versamento sono tracciate:

- su log applicativo, che permette di individuare per ogni evento: data, ora, operazione, dati di dettaglio accessibile solo dagli amministratori del sistema
- su tabella di tracking, per la registrazione di tutti gli eventi significativi occorsi, le informazioni registrate sono: l'operazione, l'autore, l'ID della sessione oltre che la data e l'ora, consultabile da interfaccia utente, accessibile solo dagli amministratori del sistema

I file di log e il tracking di processo vengono sottoposti a periodici processi di back-up e sono mantenuti per tutto il periodo di conservazione.

Torna al sommario

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

Il cliente, la BCC o la Pubblica Amministrazione accedono alla piattaforma di Iccrea Banca, tramite un sistema di strong authentication finalizzato all'identificazione certa del soggetto.

In sede di upload del documento, il sistema effettua specifici controlli sui pacchetti di versamento.

I controlli si svolgono in maniera sincrona all'elaborazione dei pacchetti di versamento e riguardano l'integrità dei dati, la coerenza e conformità dei metadati trasferiti dal Produttore all'interno di ciascun PdV. Nello specifico, la piattaforma di conservazione a norma è in grado di assegnare, in fase di configurazione del servizio, a ciascun metadato un controllo specifico secondo il seguente schema:

- Incrementale: verifica che il valore associato al documento in verifica sia maggiore o uguale al valore dell'ultimo documento caricato;
- Ordinato: permette di ordinare i documenti per i valori associati all'indice configurato;
- Elapsed: verifica che la data relativa all'indice selezionato più il numero di giorni stabilito in fase di configurazione come valore di riferimento, sia maggiore della data attuale. Questo controllo è utilizzabile solo per indici di tipo data.
- Obbligatorio: verifica che l'indice selezionato sia sempre valorizzato.
- Sequenziale: verifica che il valore associato al documento in verifica sia immediatamente successivo al valore dell'ultimo documento caricato.

Tali controlli sono effettuati se e solo se configurati sulla specifica classe documentale, sulla fase di caricamento…

Nel caso in cui i controlli abbiano esito positivo, il servizio di trasmissione del pacchetto di versamento risponde con un codice di esito positivo mentre in caso contrario risponde con un codice di esito negativo riportando altresì il motivo del rifiuto.

Al completamento dell'operazione, il PdV sarà pronto per la fase di preparazione del pacchetto di archiviazione.

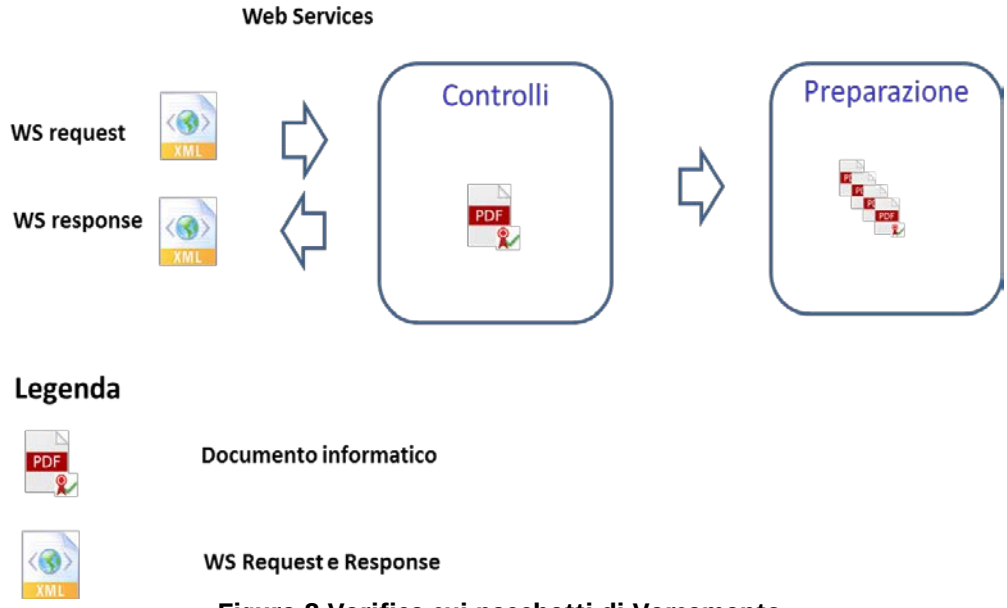

Figura 8 Verifica sui pacchetti di Versamento

Su tutti i documenti entranti è apposta una firma digitale che identifica univocamente il soggetto produttore. L'ente produttore è identificato dal parametro *CompanyId* associato in modo univoco ad ogni ente produttore configurato nel sistema.
Tutte le operazioni di verifica sono tracciate:

- su log applicativo, che permette di individuare per ogni evento: data, ora, operazione, dati di dettaglio accessibile solo dagli amministratori di sistema
- su tabella di tracking, per la registrazione di tutti gli eventi significativi occorsi, le informazioni registrate sono: l'operazione, l'autore, l'ID della sessione oltre che la data e l'ora, consultabile da interfaccia utente, accessibile solo dagli amministratori di sistema

I file di log e il tracking di processo vengono sottoposti a periodici processi di back-up e sono mantenuti per tutto il periodo di conservazione.

Torna al sommario

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

Il rapporto di versamento è un file che viene prodotto dal sistema di conservazione elettronica contestualmente alla operazione di caricamento di un pacchetto di versamento e restituito al produttore, attraverso il medesimo canale utilizzato per il versamento dello stesso.
Il rapporto di versamento è restituito dunque attraverso le seguenti modalità:

1. depositandolo sulla directory timestamp di input nel caso di caricamento del pacchetto di versamento tramite file system,
2. restituendolo mediante risposta del web service di upload nel caso sia utilizzato il rispettivo servizio.

Il rapporto di versamento viene inoltre mantenuto in un'apposita directory di sistema a scopo di conservazione del file prodotto. La nomenclatura del file è la seguente:

IR_<progressivo numerico>.xml

Es: IR_1424450980244.xml

rapporto di versamento è un file in formato xml che assume la struttura documentata nel seguente file xsd (si veda il file xsd allegato al presente documento):

```
<?xml version="1.0"?>
- <xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified" attributeFormDefault="unqualified">
  - <xs:element name="InflowReport">
    - <xs:complexType>
      - <xs:sequence>
        - <xs:element name="Documents">
          - <xs:complexType>
            - <xs:sequence>
              - <xs:element name="Document" minOccurs="0" maxOccurs="unbounded">
                - <xs:complexType>
                  - <xs:sequence>
                    - <xs:element name="Indexes">
                      - <xs:complexType>
                        - <xs:sequence>
                          - <xs:element name="Index" minOccurs="0" maxOccurs="unbounded">
                            - <xs:complexType>
                              - <xs:simpleContent>
                                - <xs:extension base="xs:string">
                                    <xs:attribute name="indexName" use="required" type="xs:string"/>
                                    <xs:attribute name="error" use="optional" type="xs:string"/>
                                    <xs:attribute name="description" use="optional" type="xs:string"/>
                                  </xs:extension>
                                </xs:simpleContent>
                              </xs:complexType>
                            </xs:element>
                          </xs:sequence>
                        </xs:complexType>
                      </xs:element>
                    </xs:sequence>
                    <xs:attribute name="fileName" use="required" type="xs:string"/>
                    <xs:attribute name="documentId" use="required" type="xs:string"/>
                    <xs:attribute name="companyId" use="required" type="xs:string"/>
                    <xs:attribute name="classId" use="required" type="xs:string"/>
                  </xs:complexType>
                </xs:element>
              </xs:sequence>
            </xs:complexType>
          </xs:element>
          <xs:element name="Result" type="xs:string"/>
          <xs:element name="ErrorMessage" type="xs:string"/>
          <xs:element name="Timestamp" type="xs:string"/>
        </xs:sequence>
      </xs:complexType>
    </xs:element>
  </xs:schema>
```

Figura 9 struttura del rapporto di versamento

Il rapporto di versamento contiene:

Percorso	Elemento	Descrizione
InflowReport\Documents\Document	classId	codice identificativo di sistema della classe documentale configurata sul sistema Paperless
InflowReport\Documents\Document	companyId	codice identificativo di sistema della persona (giuridica o fisica) configurata sul sistema Paperless
InflowReport\Documents\Document	documentId	codice identificativo univoco assegnato al documento qualora l'esito dei controlli effettuati ai fini del caricamento siano andati a buon fine o un codice di errore quando il documento viene scartato
InflowReport\Documents\Docum	Name	Nome del metadato e valore del

ent\indexes\index		metadato
InflowReport\Documents\Document	Hash	Impronta del file calcolata con algoritmo SHA-256
InflowReport\Documents	Result	Risultato dell'operazione di caricamento (OK, KO)
InflowReport\Documents	ErrorMessage	Descrizione dell'errore nel caso di esito dell'operazione (resultmessage) negativo
InflowReport\Documents	Timestamp	Riferimento temporale, specificato con riferimento al Tempo universale coordinato (UTC)

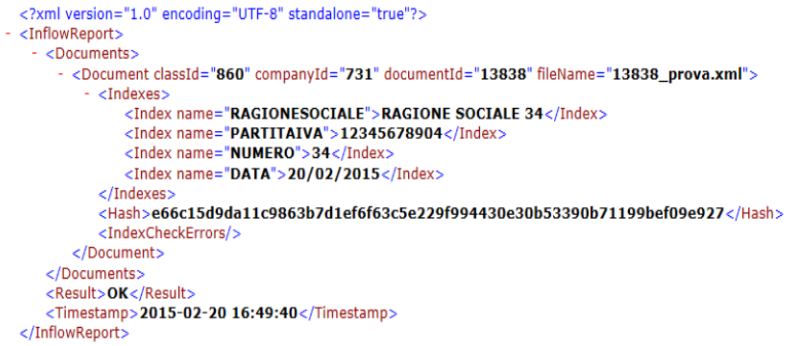

Figura 10 esempio rapporto di versamento

Torna al sommario

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

La gestione del rifiuto dei pacchetti di versamento, cambia secondo il tipo di errore:

- errore di integrità del documento, l'elaborazione si ferma ed è necessario annullare il PdV e ricevere un pacchetto corretto dal Produttore
- errore di validazione. Le condizioni che causano l'errore sono diverse:
  - manca un Documento che invece è presente negli indici
    - il PdV deve essere rinviato
  - il formato dei documenti non è corretto
    - il PdV deve essere rinviato
  - un indice ha un formato non conforme con la configurazione
    - il PdV deve essere rinviato.
  - un indice obbligatorio non è presente

- il PdV deve essere rinviato.

Nel caso in cui la classe documentale preveda la verifica di sequenzialità (es. classi documentali a valore tributario) verranno elaborati tutti i PdV fino al primo che presenta un'anomalia (es. buco di numerazione o mancato rispetto dell'ordine cronologico). Tutti i PdV successivi, anche completi, rimarranno anch'essi bloccati fino ad integrazione/correzione da parte del produttore con invii successivi.

Le comunicazioni al soggetto produttore, nel caso in cui le verifiche effettuate sul pacchetto di versamento abbiano evidenziato delle anomalie, vengono restituite all'interno del rapporto di versamento, in cui sono presenti oltre ai dati di versamento e riferimento temporale (cfr. anche 7.3) anche le motivazioni del rifiuto (cfr. anche 7.2).

Tutte le operazioni dei pacchetti di versamento rifiutati sono tracciate:

- su log applicativo, che permette di individuare per ogni evento: data, ora, operazione, dati di dettaglio accessibile solo dagli amministratori di sistema
- su tabella di tracking, per la registrazione di tutti gli eventi significativi occorsi, le informazioni registrate sono: l'operazione, l'autore, l'ID della sessione oltre che la data e l'ora, consultabile da interfaccia utente, accessibile solo dagli amministratori di sistema

I file di log e il tracking di processo vengono sottoposti a periodici processi di back-up e sono mantenuti per tutto il periodo di conservazione.

Torna al sommario

7.5 Preparazione dei pacchetti di archiviazione

Dopo l'acquisizione dei pacchetti di versamento, il responsabile del servizio di conservazione o suo delegato procede alla preparazione dei pacchetti di archiviazione. Durante l'esecuzione di tale attività il sistema effettua in automatico una serie di controlli volti a garantire sia la corretta formazione dei pacchetti di archiviazione (ad esempio controlli sulla progressività della numerazione dei documenti all'interno del pacchetto, controlli sulla sequenzialità delle date dei documenti all'interno dei pacchetti, ecc..) sia il corretto dimensionamento dei pacchetti stessi in termini di numero e dimensione dei documenti.
Al completamento della preparazione dei pacchetti di archiviazione, in modalità manuale o automatica, il responsabile del servizio di conservazione provvede alla chiusura dei pacchetti stessi: tale operazione determina la produzione automatica dell'impronta dei documenti contenuti all'interno dei pacchetti e l'esecuzione di un controllo puntuale dei documenti inclusi all'interno del pacchetto stesso ed il relativo hash inserito nell'impronta.
Al completamento della chiusura dei pacchetti di archiviazione, il responsabile del servizio di conservazione a provvede all'archiviazione dei pacchetti di archiviazione preparati e chiusi nelle due attività precedenti. La

rispettiva funzionalità avvia il processo di firma dell'impronta e di marcatura temporale della stessa a garanzia dell'integrità dei pacchetti di archiviazione.
Anche tale fase, oltre a prevedere un meccanismo di *Strong Authentication* per l'attivazione della firma, è oggetto di controlli sulla validità della firma e della marca temporale apposte.
Il completamento di tale attività determina lo spostamento del pacchetto di archiviazione generato dalla directory di lavoro del sistema di conservazione alla directory di conservazione configurata per la specifica classe documentale oggetto del processo.
I pacchetti di archiviazione conservati sono sottoposti a periodici controlli a campione per la verifica dell'integrità e la leggibilità dei documenti.
In caso dovessero verificarsi casi di corruzione o perdita dei dati, si procede a:

- Recupero delle copie di backup dei dati corrotti;
- Verifica puntuale dell'integrità e della leggibilità dei dati recuperati;
- Ripristino dei dati recuperati;
- Tracciatura della operazione di ripristino;
- Repentina notifica al soggetto produttore;

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

La procedura di esibizione permette di generare un pacchetto di distribuzione per un documento di cui sia completata la procedura di conservazione e generato il corrispondente pacchetto di archiviazione.
Il processo aggrega tutte le informazioni che qualificano il processo di conservazione a cui il documento è stato sottoposto costituendone il pacchetto di distribuzione composto da:

- Il documento
- Il file indice del PdA (.xml),.xml.p7m,.xml.p7m.tsr)
- Il file indice del PdA firmato dal RC (.xml.p7m)
- Il file indice del PdA firmato e maracto temporalmente (.xml.p7m.tsr)

La distribuzione può avvenire, da remoto, tramite interrogazione diretta al sistema di conservazione.
In alternativa, il Responsabile del sistema di conservazione può procedere alla generazione di un pacchetto di distribuzione tramite riversamento su supporto rimovibile (CD, DVD) di specifici pacchetti di archiviazione presenti sul sistema stesso .
La fase di invio viene effettuata tenendo presente le modalità di trasmissione che Iccrea Banca S.p.A. utilizza per l'invio di valori di immediata spendita (tramite corrieri specializzati che garantiscono la tracciabilità della spedizione). Inoltre i dati vengono protetti da sistemi crittografici.
Per ogni Pacchetto di Distribuzione, l'utente ha la possibilità di:

- Visualizzare i documenti contenuti

- Verificare, con apposita funzione, che il file di indice ed i documenti contenuti all'interno del pacchetto selezionato siano conformi ed effettuare la verifica della firma e della marca temporale sul file di indice
- Utilizzare una funzione mediante la quale scaricare il file di indice relativa al PdD.

Utilizzando la funzione di verifica del file delle impronte potrà essere verificata:

- l'integrità della firma
- la validità dell'intervallo firma
- la validità del certificato utilizzato
- lo stato del certificato.

Eventuali segnalazioni di errore da parte dell'utente, ricevute tramite uno qualunque dei canali di contatto previsti dalla banca, vengono indirizzate al sistema di incident management del servizio di conservazione per la corretta gestione.

Torna al sommario

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

La procedura di produzione di duplicati o copie dei documenti, analogamente al processo di generazione del pacchetto di distribuzione, si compone delle seguenti attività:

1. Ricerca, consultazione e download di copia del documento
2. Preparazione del pacchetto di distribuzione e riversamento su supporto

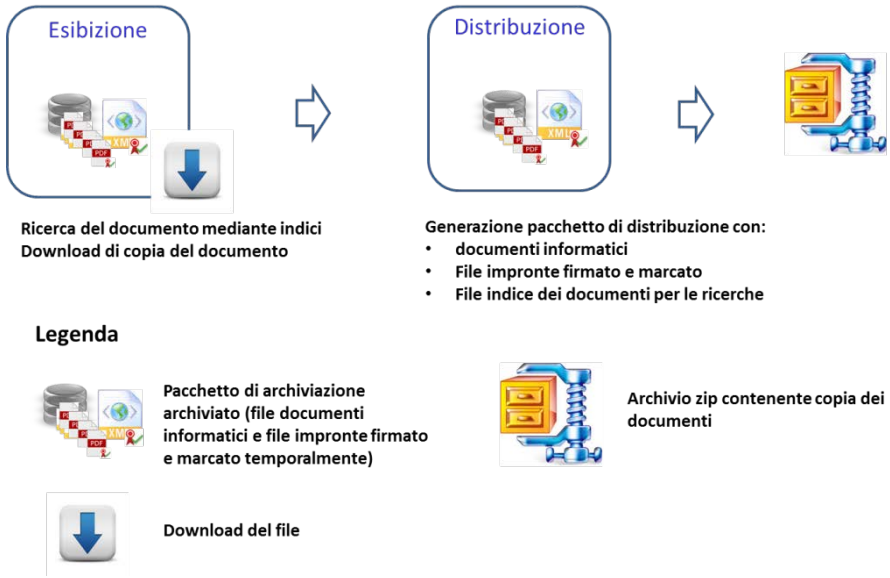

Figura 11 Produzione dei duplicati

Con le stese modalità della preparazione dei pacchetti di distribuzione l'utente può predisporre delle copie dei documenti da rilasciare a fini di consultazione.
Questa funzionalità consente di generare degli archivi in formato .zip contenenti i documenti informatici ed il file di impronte firmato dal Responsabile del servizio di Conservazione e con marca temporale.
A differenza della funzionalità di generazione del pacchetto di distribuzione, la funzionalità in oggetto non include il tool di consultazione dei documenti.
Il file archivio generato è strutturato come segue:

- Una folder DOCS contenente i documenti informatici oggetto di conservazione elettronica
- Una folder INDEX contenente un file indice (formato xml) contenente i metadati dei documenti inclusi nella folder DOCS
- il file di impronte dei documenti secondo formato UNI SINCRO
- il file di impronte di cui al punto precedente ma firmato dal RdC

- il file di impronte di cui al punto precedente ma con marca temporale.

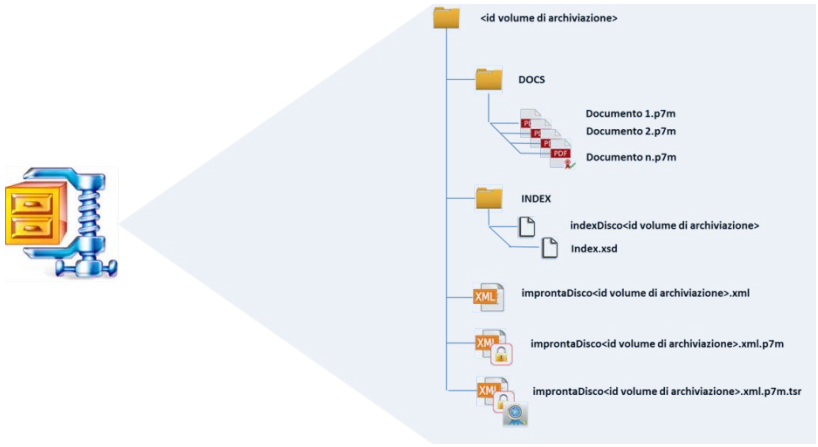

Figura 12 Struttura dell'archivio ZIP

Il responsabile del servizio diConservazione, nei casi previsti dalla legge, si occupa di contattare ed assistere un Pubblico Ufficiale che attesti la correttezza del processo.
Il Pubblico Ufficiale viene scelto nell'alveo dei professionisti solitamente utilizzati da Iccrea Banca S.p.A..
In caso di verifiche, controlli o ispezioni, i documenti informatici rilevanti ai fini tributari conservati sono esibiti secondo le seguenti modalità:

- il documento è reso leggibile e, a richiesta, disponibile su supporto cartaceo e informatico presso il luogo di Conservazione delle scritture (ovvero la sede di Iccrea Banca S.p.A.). Iccrea Banca S.p.A., provvede a renderlo leggibile in qualunque momento presso il sistema di Conservazione e disponibile, a richiesta, su supporto cartaceo;
- su richiesta, il documento conservato potrà anche essere esibito per via telematica secondo le indicazioni di volta in volta fornite dall'Agenzia delle Entrate.

Torna al sommario

7.8 Scarto dei pacchetti di archiviazione

Alla scadenza del contratto con cui vengono affidate le funzioni di Responsabile del procedimento di Conservazione, Iccrea Banca S.p.A. rimuove gli archivi interessati dallo storage e li pone "offline".
Gli archivi tolti dallo storage vengono preventivamente riversati anche su altro supporto idoneo affinché Iccrea Banca S.p.A. possa sempre mantenere una duplice copia degli archivi non più disponibili sullo storage accessibile online. La produzione dei supporti idonei alla Conservazione è una funzione controllata da Iccrea Banca S.p.A. e prevede le seguenti fasi:

- selezione dei segmenti di archivi da riversare su supporto ottico. La selezione è manuale da parte dell'operatore e permette di aggregare sullo stesso supporto segmenti anche appartenenti a diversi

archivi;

- riversamento diretto dei segmenti di archivi da supporto magnetico a supporto ottico o altro supporto idoneo;
- produzione dei supporti in duplice copia;
- conservazione di una copia presso Iccrea Banca S.p.A., invio dell'altra copia di backup alla Banca o al Cliente secondo le modalità previste contrattualmente e le policy sulla sicurezza di Iccrea Banca S.p.A..

Alla fine del processo il sistema opera una verifica automatica dei supporti utilizzati in modo che Iccrea Banca S.p.A. possa avere certezza che i dispositivi utilizzati siano esenti da difetti e pronti per la Conservazione nei locali destinati al loro stoccaggio.

Ai sensi del decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013, art. 9, c. 1, lett. c, nel caso di archivi pubblici o privati, che rivestono interesse storico particolarmente importante, lo scarto del pacchetto di archiviazione avviene previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo rilasciata al produttore secondo quanto previsto dalla normativa vigente in materia.

Torna al sommario

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

Alla scadenza del contratto o in caso di cessazione dello stesso, Iccrea Banca S.p.A., disattiva i servizi e consegna alla Banca i supporti informatici (CD, DVD) contenenti documenti conservati ed ottenuti attraverso la procedura di conservazione.

Iccrea Banca S.p.A. mantiene l' archivio fino alla conclusione del riversamento e dopo che i controlli effettuati abbiano dato esito positivo.

La struttura dell'indice del pacchetto di archiviazione garantisce lo standard "*Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali*", (c.d.UNI SInCRO). In tal modo viene preservata l'interoperabilità e l'eventuale trasferibilità degli oggetti conservati ad altri conservatori, nonché la possibilità di accogliere clienti che provengono da altri sistemi di conservazione.

Torna al sommario

8 Sistema di Conservazione

Il sistema di Conservazione di Iccrea Banca è implementato nella piattaforma Iccrea di Fatturazione Elettronica e Conservazione che integra diverse componenti tecnologiche, di seguito descritte, al fine di fornire servizi documentali alle banche del gruppo ed ai relativi utenti.

L'intera piattaforma è realizzata nel rispetto delle Policy di Sicurezza di Iccrea Banca S.p.A. che, 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.

8.1 Componenti Logiche

La piattaforma ICCREA di Fatturazione Elettronica e Conservazione è composta da diverse componenti che si integrano tra loro e, nel complesso, con l'infrastruttura del gruppo bancario al fine di erogare, in sicurezza, i servizi agli utenti finali.

Le principali componenti interne della piattaforma sono:

1. il portale SDC che orchestra i servizi erogati costituendo in punto di accesso logico alla piattaforma;
2. il prodotto di Conservazione con cui SDC è integrato;
3. la piattaforma di interscambio multicanale per la gestione dei flussi documentali in entrata ed uscita dalla piattaforma;

Il principali sistemi con cui la piattaforma interagisce sono:

- il sistema di firma digitale remota basato su HSM (Hardware Security Module);
- Certification/TimeStamp Authority per l'apposizione di marche temporali e verifiche della validità delle firme digitali;
- il sistema di Autenticazione ed Autorizzazione della banca;
- i sistemi informatici delle strutture tecniche a supporto delle banche del gruppo che veicolano i documenti verso la piattaforma.

Il disegno dell'architettura logica del sistema è riportato nel seguente diagramma.

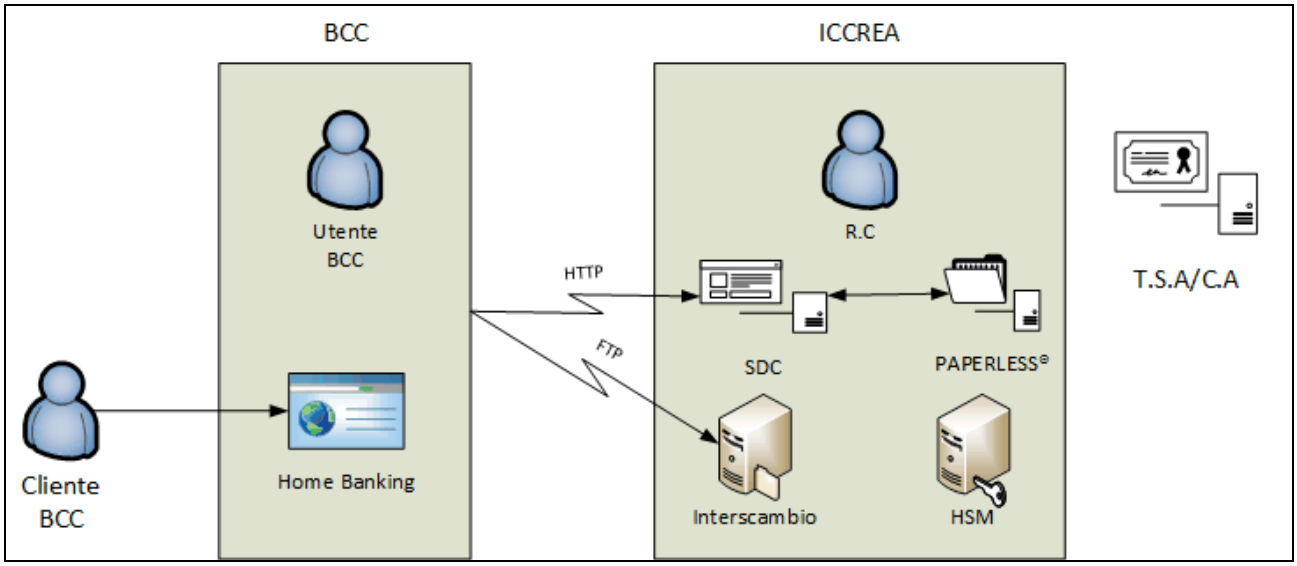

Figura 13 Componenti Logiche

8.2 Componenti Tecnologiche

La Piattaforma Iccrea di Fatturazione Elettronica e Conservazione integra diverse componenti tecnologiche per erogare i servizi secondo i requisiti di affidabilità e sicurezza. In base alle esigenze sono impiegate soluzioni custom o di mercato, sia open source che proprietarie. Di seguito sono riportate le principali caratteristiche tecnologiche della piattaforma.

- I servizi agli utenti sono erogati tramite il portale web SDC, costruito con tecnologia Java (JEE) ed installato su server Linux.
- Le pagine web ed i Web Services sono filtrati da un Web Server (Apache) di front end con funzioni di proxy applicativo.
- Il controllo degli accessi è implementato:
  - Dal sistema centralizzato di controllo accessi della banca per tutti gli utenti delle banche del gruppo che accedono tramite intranet;
  - Dai sistemi di strong authentication degli applicativi di *home banking* per i clienti delle banche che hanno aderito al servizio.
- I flussi massivi di documenti inviati alla piattaforma, viaggiano tramite i canali di *secure file transfer* della banca e transitano per il sistema custom di interscambio multicanale costruito con tecnologia JAVA. Tutti i processi di gestione dei flussi documentali sono monitorati e schedulati dal sistema di monitoraggio centralizzato della Banca (Control-M).
- Il servizio di firma digitale dei documenti in entrata e dei pacchetti di archiviazione si appoggia su HSM (Hardware security module) COSign di Arx (certificato C.C. EAL4+). Nel rispetto del security target della certificazione Common Criteria, l'accesso ai servizi di firma è effettuato con l'ausilio di *One Time Password (otp).*
- I servizi di apposizione delle marche temporali si appoggiano a Timestamp Authority accreditate.
- Il prodotto di conservazione a norma (prodotto proprietario) non è esposto direttamente agli utenti con l'esclusione del solo Responsabile della Conservazione (e dei suoi delegati). A quest'ultimo, il prodotto espone una console web (J2EE) per la gestione dei propri compiti di operatività e controllo. Tutti gli altri servizi di conservazione sono erogati tramite il portale SDC che dialoga con il prodotto di conservazione tramite WebServices.
- Tutti i componenti interni della piattaforma appoggiano la propria base dati su database Oracle della banca.
- I file sono conservati su storage centralizzato della banca.

Per i dettagli si rimanda alle schede tecniche delle tecnologie e prodotti utilizzati.

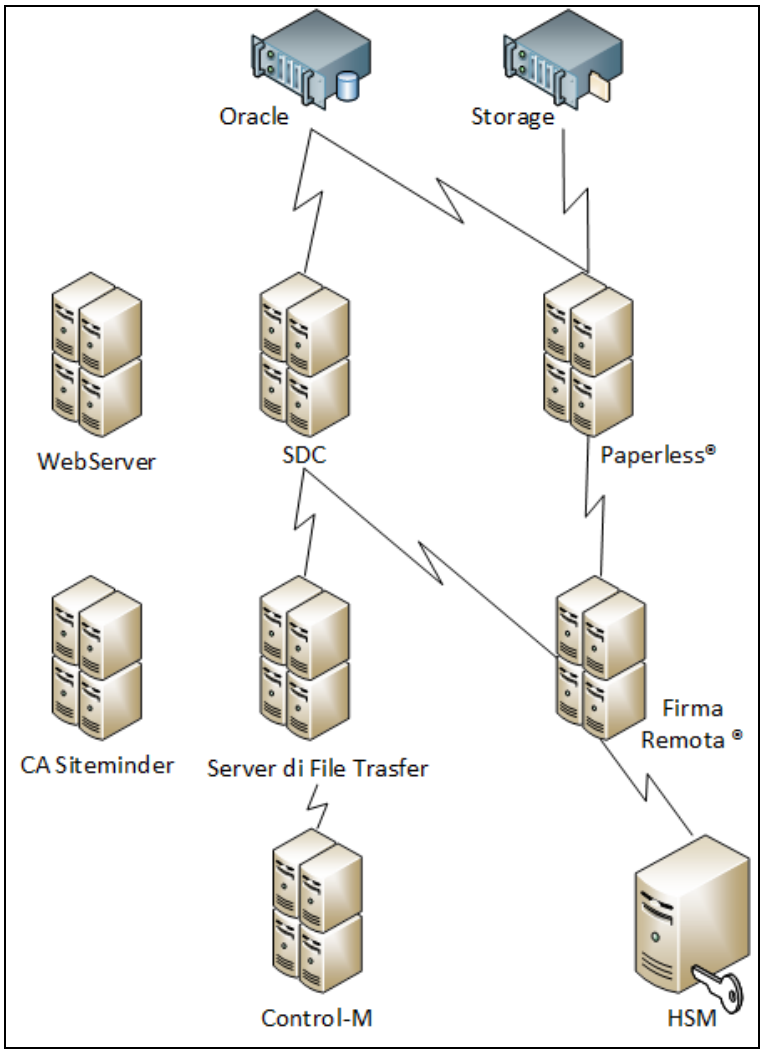

Figura 14 Componenti Tecnologiche

8.3 Componenti Fisiche

L'architettura fisica della Piattaforma Iccrea di Fatturazione Elettronica e Conservazione, in conformità con le Policy in tema di Sicurezza di Iccrea Banca S.p.A., si distribuisce in un sito primario localizzato nella sede di Via Lucrezia Romana e nel sito di Disaster Recovery localizzato nei locali di Via Giacomo Peroni.

Nel sito primario sono presenti le seguenti componenti fisiche principali:

- Web Server di front end per l'accesso alla piattaforma dall'esterno;
- Application Server che ospita la soluzione SdC;
- Application Server che ospita il prodotto di conservazione Paperless®;
- Server di File Transfer Multicanale;
- Server di Firma Remota (Server di Enrollment e Server di Firma);
- HSM (Cosign);
- Database Oracle;

- SAN.

Tutte le componenti fisiche sono replicate nel sito di Disaster Recovery di Via Giacomo Peroni.

Per gli approfondimenti ed il dettaglio in relazione alle componenti fisiche ed alla continuità operativa si rimanda alla documentazione relativa al Manuale Tecnico della Piattaforma di Conservazione e alle Policy in tema di Sicurezza di Iccrea Banca S.p.A.

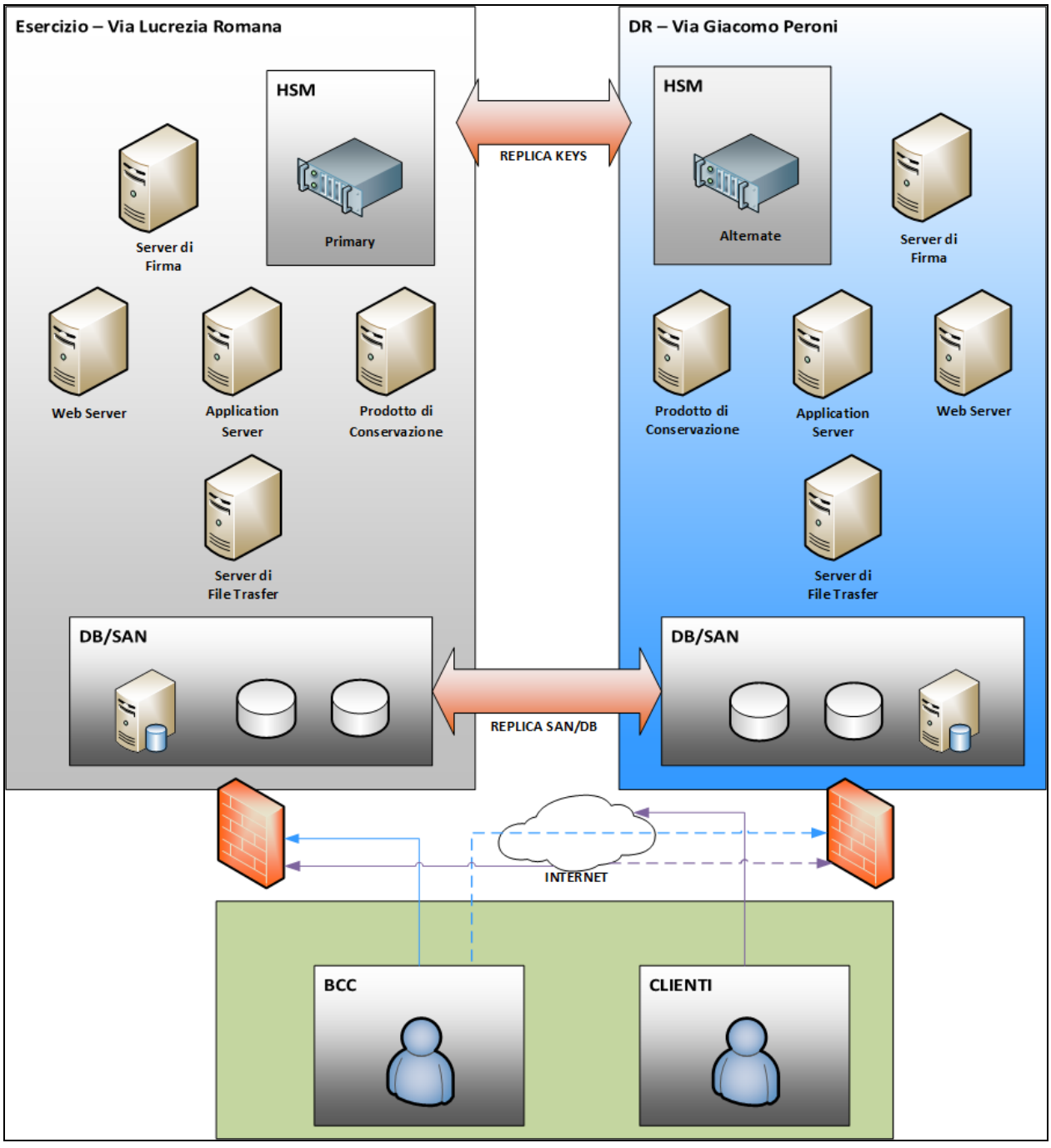

Figura 15 Componenti Fisiche

8.4 Procedure di Gestione ed Evoluzione

Iccrea Banca S.p.A. 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.

Alla manutenzione della piattaforma ICCREA di Fatturazione Elettronica e Conservazione, la banca ha dedicato un team di risorse con competenze sull'intera architettura implementata. Il team di application management si occupa principalmente di:

- Attività di *problem determination* e *bug fixing* in caso di *incident* secondo gli *sla* di servizio concordati;
- Attività di aggiornamento degli applicativi che implementano la piattaforma;
- Attività di supporto di secondo livello per la gestione delle segnalazioni degli utenti;
- Supporto al Responsabile della Conservazione per lo svolgimento delle attività pertinenti;
- Cooperazione con le altre unità organizzative della Banca che contribuiscono alla manutenzione complessiva della piattaforma.

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

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 Banca S.p.A., 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 Banca S.p.A. 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 un proprio file di log nel quale sono tracciate tutte le operazioni eseguite dal componente 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 Banca S.p.A. 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 informative 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).

La documentazione prevista dalle attività deve essere a disposizione del personale autorizzato, risultare facilmente consultabile, adeguatamente protetta e storicizzata.

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)

9 Monitoraggio e controlli

9.1 Procedure di monitoraggio

Iccrea Banca per mezzo del Responsabile del servizio di Conservazione, supportato e coadiuvato dalle competenti Unita Organizzative, esegue con cadenza annuale un controllo a campione 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 Banca S.p.A. provvede al riversamento diretto a partire dalla copia di sicurezza realizzata, oppure ripristinando un backup del supporto magnetico.

Iccrea Banca S.p.A.:

- 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 e dei suoi delegati all'apposizione della firma digitale;
  - 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 il corretto funzionamento delle procedure di sicurezza utilizzate per garantire l'apposizione del riferimento temporale;
- 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 auditing 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.

Per quanto riguarda l'accesso ai dati da parte di personale Iccrea Banca S.p.A. si fa riferimento alle procedure di gestione della privacy presenti nella documentazione ufficiale della società coerente ai dettami del D LGS 196/2003 "Codice in materia di protezione dei dati personali".

9.2 Verifica dell'integrità degli archivi

I controlli (di leggibilità e di integrità) vengono effettuati in modalità campionaria, sulla base di percentuali non superiori all'8% per ogni singola classe portata in Conservazione, entro 5 anni dalla data di caricamento dei file. Le verifiche e il loro esito vengono riportati nel libro dei verbali.

Tutte le procedure di verifica, gli eventuali interventi sul software applicativo, le modifiche delle configurazioni, l'assegnazione delle deleghe a svolgere opportune operazioni, nonché tutti gli avvenimenti importanti o ritenuti tali dal Responsabile del servizio di Conservazione ai fini del corretto svolgimento del processo di Conservazione saranno opportunamente tracciati su un apposito Libro dei Verbali. Le componenti infrastrutturali facenti parte del sistema di conservazione vengono monitorate attraverso specifiche sonde che verificano costantemente lo stato dei sistemi e dei loro componenti. Al sopravvenire di uno stato di criticità, il sistema di monitoraggio emette degli alert che sono costantemente monitorati dal personale di presidio. Qualora il personale di presidio non sia in grado di risolvere autonomamente la situazione venutasi a creare, vengono chiamati in causa i team di specialisti di secondo livello (sistemistici o applicativi).

Il monitoraggio è strutturato sui seguenti strati:

- Infrastruttura di rete: monitoraggio dei livelli di traffico, di possibili intrusioni (attraverso l'utilizzo di IPS attivi su tutti i segmenti di rete, interni ed esterni);
- Infrastruttura di sicurezza: monitoraggio degli accessi e delle violazioni di accesso;
- Infrastruttura sistemistica: monitoraggio dello stato dei componenti di sistema (connettività di rete, servizi attivi, CPU, file system);
- Infrastruttura applicativa: monitoraggio dello stato dei componenti applicativi;
- Infrastruttura logistica: monitoraggio dello stato dei locali CED (temperatura, alimentazione, ecc.) e dell'impiantistica."

9.3 Soluzioni adottate in caso di anomalie

In caso di evento catastrofico 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 alla Banca, alla Pubblica Amministrazione o al Cliente e registrati sul Libro dei Verbali.