MANUALE
della
CONSERVAZIONE

Versione 1.2

Data 21 Marzo 2016

Emissione del documento

Azione	Data	Nominativo	Funzione
Redazione	15/03/2016	Gianluca Cardin	Responsabile Funzione Archivistica di Conservazione
		Andrea Rossi	Responsabile Sviluppo e Manutenzione del Sistema di Conservazione
Verifica	16/03/2016	Claudio Visigalli	Responsabile Sicurezza dei Sistemi per la Conservazione
		Mario Priori	Responsabile Sistemi Informativi per la Conservazione
Approvazione	21/03/2016	Gian Mario Canaparo	Responsabile del Servizio di Conservazione

Indice del documento

Registro delle Versioni

Versione	Data	Descrizione	Modifiche
1.0	10/02/2015	Prima redazione	-
1.1	20/01/2016	Modifiche	Apportate modifiche ed integrazioni segnalate da AgID
1.2	21/03/2016	Modifiche	Apportate modifiche ed integrazioni segnalate da AgID

Torna al sommario

Cronologia dei Responsabili del Servizio di Conservazione

Responsabile del Servizio di Conservazione			
Nominativo	email	Periodo nel ruolo	Eventuali deleghe
Gian Mario Canaparo	mario.canaparo@imaging.it	Dal 2008 (Rinnovo nel 2014)	Delega per la conduzione delle attività operative che rientrano nel processo di conservazione e per l'apposizione della firma digitale sull'IPdA. Con atto di nomina sono stati delegati: • Felice Traversa • Fabrizio Consorti

Responsabile Sicurezza dei Sistemi per la Conservazione			
Nominativo	email	Periodo nel ruolo	Eventuali deleghe
Claudio Visigalli	claudio.visigalli@imaging.it	Dal 2014	

Responsabile Funzione Archivistica di Conservazione			
Nominativo	email	Periodo nel ruolo	Eventuali deleghe
Gianluca Cardin	gianluca.cardin@imaging.it	Dal 2014	

Responsabile Trattamento Dati personali			
Nominativo	email	Periodo nel ruolo	Eventuali deleghe
Claudia Canaparo	claudia.canaparo@imaging.it	Dal 2014	

Responsabile Sistemi Informativi per la Conservazione			
Nominativo	email	Periodo nel ruolo	Eventuali deleghe
Mario Priori	mario.priori@imaging.it	Dal 2014	

Responsabile Sviluppo e Manutenzione del Sistema di Conservazione			
Nominativo	email	Periodo nel ruolo	Eventuali deleghe
Andrea Rossi	andrea.rossi@imaging.it	Dal 2014	

Torna al sommario

1 Scopo e ambito del Documento

Il presente Manuale della Conservazione (d'ora in avanti "MdC") ha come obiettivo quello di illustrare in dettaglio tutte le procedure operative e gli attori coinvolti nel processo di conservazione, al fine di ottenere un Sistema di Conservazione allineato con le normative vigenti in materia di conservazione di documenti informatici.

Il documento riporta inoltre le normative e gli standard di riferimento a cui Imaging Group SpA si attiene.

Viene quindi descritto il modello generale del processo ed inoltre:

- Le competenze, i compiti e le responsabilità del Responsabile del Servizio di Conservazione;
- Le regole e le procedure utilizzate per implementare il processo di conservazione dei documenti, originariamente analogici e/o informatici, nonché la loro riproduzione su diversi tipi di supporto;
- Gli oggetti interessati dal servizio di Conservazione;
- Le infrastrutture tecnologiche utilizzate, suddivise nelle sue componenti logiche e fisiche;
- Le procedure di gestione della sicurezza, di trattamento dei dati personali, di monitoraggio e controllo dell'intero sistema.

Il Manuale della Conservazione viene utilizzato come riferimento per il mantenimento, l'aggiornamento e lo sviluppo del sistema di gestione documentale della società. Non include informazioni riguardanti aspetti delle specifiche forniture del Servizio di Conservazione, che sono invece presentate nella documentazione "specificità del contratto".
Il presente documento è redatto in solo formato informatico e conservato secondo le norme in tema di conservazione digitale delle scritture contabili e può, su richiesta, essere fornito in copia cartacea.

Torna al sommario

1.1 Dati identificativi del soggetto conservatore

Denominazione sociale	Imaging Group SpA
Indirizzo della sede legale/operativa	C.D. Milanofiori Strada 4 Pal. A6 - 20090 Assago (MI)
Legale rappresentate	Dott.ssa Claudia Canaparo
Responsabile del Servizio di Conservazione	Sig. Gian Mario Canaparo
N° iscrizione al registro delle imprese	MI – 2036796
Partita IVA	08608200963
N° Telefono	+39 02 8246020
N° Fax	+39 02 8242990
Sito WEB	http://www.imaging.it
e-mail	imaging@imaging.it

Torna al sommario

2 Terminologia (Glossario ed Acronimi)

Di seguito si riporta il glossario dei termini e delle definizioni contenuti nell'Allegato 1 alle Regole tecniche in materia di documento informatico e gestione documentale, protocollo informatico e conservazione di documenti informatici.

Termine	Definizione
Accesso	operazione che consente a chi ne ha diritto di prendere visione ed estrarre 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
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 o in relazione alle funzioni dell'ente
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	un insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che 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
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
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

Termine	Definizione
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 di conservazione
Coordinatore della Gestione Documentale	responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 nei casi di amministrazioni che abbiano istituito più Aree Organizzative Omogenee
Copia analogica del documento informatico	documento analogico avente contenuto identico a quello del documento informatico da cui è tratto
Copia di sicurezza	copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 delle presenti regole tecniche per il sistema di conservazione
Destinatario	identifica il soggetto/sistema al quale il documento informatico è indirizzato
Duplicazione dei documenti informatici	produzione di duplicati informatici
Esibizione	operazione che consente di visualizzare un documento conservato e di ottenerne copia
Estratto per riassunto	documento nel quale si attestano in maniera sintetica ma esaustiva fatti, stati o qualità desunti da dati o documenti in possesso di soggetti pubblici
Evidenza informatica	una 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. nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del Codice.
Formato	modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
Funzionalità aggiuntive	le ulteriori componenti del sistema di protocollo informatico necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni
Funzionalità interoperative	le componenti del sistema di protocollo informatico finalizzate a rispondere almeno ai requisiti di interconnessione di cui all'articolo 60 del D.P.R. 28 dicembre 2000, n. 445
Funzionalità minima	la componente del sistema di protocollo informatico che rispetta i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445

Termine	Definizione
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
Generazione automatica di documento informatico	formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni
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
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 5 del DPCM 3/12/2013, 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
Manuale di gestione	strumento che descrive il sistema di gestione informatica dei documenti di cui all'articolo 5 delle regole tecniche del protocollo informatico ai sensi delle regole tecniche per il protocollo informatico D.P.C.M. 31 ottobre 2000 e successive modificazioni e integrazioni
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
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

Termine	Definizione
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
Piano della sicurezza del sistema di conservazione	documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza
Piano della sicurezza del sistema di gestione informatica dei documenti	documento, che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi nell'ambito dell'organizzazione di appartenenza
Piano di conservazione	strumento, integrato con il sistema di classificazione per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445
Piano generale della sicurezza	documento per la pianificazione delle attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza
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 10 delle regole tecniche del sistema di conservazione
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 particolare	registro informatico di particolari tipologie di atti o documenti; nell'ambito della pubblica amministrazione è previsto ai sensi dell'articolo 53, comma 5 del D.P.R. 28 dicembre 2000, n. 445
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
Repertorio informatico	registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche con cui si formano altri atti e documenti o indici di atti e documenti secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica

Termine	Definizione
Responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi	dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione.
Responsabile della conservazione	soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 delle regole tecniche del sistema di conservazione
Responsabile del trattamento dei dati	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali
Responsabile della sicurezza	soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di Sicurezza
Riferimento temporale	informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento
Scarto	operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale
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 D.P.R. 28 dicembre 2000, n. 445; per i privati è il sistema che consente la tenuta di un documento informatico
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
Transazione informatica	particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche della base di dati
Testo unico	decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni
Ufficio utente	riferito ad un area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico
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
Versamento agli archivi di stato	operazione con cui il responsabile della conservazione di un organo giudiziario o amministrativo dello Stato effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali

Acronimo	Definizione
AgID	Agenzia per l'Italia Digitale
CA	Certification Authority, cioè ente accreditato per l'emissione e la gestione di certificati di firma qualificata
CAD	Codice dell'Amministrazione Digitale, Decreto Legislativo 7 marzo 2005,n.82 e successive modifiche/integrazioni
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione
CRL	Certificate Revocation List, liste di certificati digitali revocati
HASH	Impronta informatica di un documento ottenuta applicando una "funzione di hash" e costituita da una sequenza di simboli binari
HTTP	Hyper Text Transfer Protocol (identificativo convenzionale per un sito)
HTTPS	Secure Hyper Text Transmission Protocol. Protocollo sviluppato allo scopo di cifrare e decifrare le pagine Web che vengono inviate dal server ai client
IPdA	Indice del Pacchetto di Archiviazione – evidenza informatica associata ad ogni pacchetto di archiviazione contenente un insieme di informazioni articolate secondo lo standard SInCRO
NAS	Network Attached Storage, dispositivi ad alta capacità, sicurezza ed affidabilità per la memorizzazione dei dati
SFTP	SSH File Transfer Protocol o SFTP è un protocollo di rete che prevede il trasferimento dei dati e funzionalità di manipolazione. È tipicamente usato con il protocollo SSH-2 che utilizza un trasferimento dei file sicuro, anche se è utilizzabile con un qualsiasi altro protocollo
PAdES-T	PDF Advanced Electronic Signature, formato standard di firma su PDF, con informazioni aggiuntive rispetto al formato base(PADES-BES) per includere la marca temporale
PdA	Pacchetto di Archiviazione
PdV	Pacchetto di Versamento
RSC	Responsabile del Servizio di Conservazione
RSSC	Responsabile Sicurezza dei Sistemi per la Conservazione
SinCRO	Supporto all'interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI11386:2010)- Standard nazionale in linguaggio xml, riguardante la struttura dell'insieme di dati a supporto del processo di conservazione
TSA	Time Stamping Authority, infrastruttura necessaria a realizzare e svolgere la funzione di timbratura temporale
UTC	Universal Time Coordinated (Misura del tempo così come stabilito dall'International Radio Consultative Committee – CCIR)
RFAC	Responsabile Funzione Archivistica di Conservazione
RTDP	Responsabile Trattamento Dati personali
RSIC	Responsabile Sistemi Informativi per la Conservazione
RSMC	Responsabile Sviluppo e Manutenzione del Sistema di Conservazione

Torna al sommario

3 Normativa e Standard di riferimento

3.1 Normative di riferimento

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

[1]	Codice Civile art.2215 bis	[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
[2]	Legge n.241 7/8/1990	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
[3]	DPR 445/2000	Decreto del Presidente della Repubblica del 28/12/2000 n. 445 – Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (G. U. n. 42 del 20/02/2001) - (sostituito per le parti non riguardanti il Protocollo Informatico dal Dlgs 82/2005)
[4]	Dlgs 196/2003	Decreto legislativo 30 Giugno 2003, n. 196 - Codice in materia di protezione dei dati personali
[5]	Dlgs 42/2004	Decreto legislativo 22 Gennaio 2004, n. 42, e successive modificazioni - Codice dei beni culturali e del paesaggio
[6]	DPCM 13/1/2004	Decreto del Presidente del Consiglio dei Ministri 13/01/2004 – Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici (G. U. N. 98 del 27/04/2004)
[7]	Dlgs 82/2005	Decreto legislativo del 07/03/2005 n. 82 – Codice dell'amministrazione digitale (G. U. N. 112 del 16/05/2005), come modificato dal Decreto legislativo N. 159 del 4 aprile 2006 – Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale. Testo in vigore dal 14-5-2006 (G. U. N. 99 del 29 Aprile 2006)
[8]	Circ. Ag.Entr 45/2005	Agenzia delle Entrate – Direzione Centrale Normativa e Contenzioso – Circolare del 19/10/2005 n. 45 – Decreto legislativo 20/02/2004, n. 52 – attuazione della direttiva 2001/115/CE che semplifica ed armonizza le modalità di fatturazione in materia di IVA
[9]	DM 9/7/2008	Decreto del Ministero del Lavoro, della Salute e delle Politiche Sociali 9 Luglio 2008 - Modalità di tenuta e conservazione del libro unico del lavoro e disciplina del relativo regime transitorio
[10]	DPCM 3/12/2013	Decreto del Presidente del Consiglio Dei Ministri 3 Dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005. (14A02098) (GU Serie Generale n.59 del 12-3-2014 - Suppl. Ordinario n. 20)

[11]	DPCM 22/2/2013	Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71
[12]	DMEF 55/2013	Decreto Ministero Economia e Finanze del 3 Aprile 2013, n. 55 - Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'art. 1, commi da 209 a 213, della legge 24 dicembre 2007. Pubblicato in G.U. n. 118 del 22 maggio 2013
[13]	DPCM 21/3/2013	Decreto del Presidente del Consiglio Dei Ministri 21 marzo 2013 - Documenti analogici originali unici per i quali permane l'obbligo della conservazione dell'originale cartaceo oppure, in caso di conservazione di documenti informatici, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico
[14]	DMEF 17/6/2014	Decreto Ministero Economia e Finanze - 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
[15]	Cir. AgID 65/2014	Circolare AgID - N. 65 del 10 aprile 2014 - 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

3.2 Standard di riferimento

[1]	ISO 14721:2012	OAIS Open Archival Information System,
[2]	ISO/IEC 27001:2013	Information technology - Security techniques - Information security management systems – Requirements
[3]	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
[4]	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
[5]	UNI 11386:2010	Sincro - Recupero degli Oggetti digitali
[6]	ISO 15836:2009	Information and documentation - The Dublin Core metadata element set

Torna al sommario

4 Ruoli e Responsabilità

Il Responsabile del Servizio di Conservazione, all'interno della propria struttura, ha definito:

- Le procedure per la conservazione della documentazione fiscale e non;
- Le funzioni delegate della conservazione che agiscono per suo conto a garanzia della continuità del processo;
- I compiti delle funzioni delegate;
- La documentazione cartacea di delega e il relativo mantenimento;
- Le procedure e i compiti in materia di protezione e salvaguardia delle informazioni.

Le deleghe sono formalizzate tramite documento apposito riportante la motivazione della delega, la data della delega, la descrizione dei compiti affidati e la durata dell'incarico.
L'incarico del delegato può essere permanente e i modi e le modalità con cui egli opera sono definiti nel documento di delega.
I riferimenti, il loro periodo nel ruolo ed eventuali deleghe di coloro che coprono i ruoli di:

- Responsabile del Servizio di Conservazione;
- Responsabile Sicurezza dei Sistemi per la Conservazione;
- Responsabile Funzione Archivistica di Conservazione;
- Responsabile Trattamento Dati personali;
- Responsabile Sistemi Informativi per la Conservazione;
- Responsabile Sviluppo e Manutenzione del Sistema di Conservazione.

sono indicati nella tabella seguente:

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo
Responsabile del Servizio di Conservazione	Gian Mario Canaparo	• Definizione delle caratteristiche e dei requisiti del Sistema di Conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente; • Gestione del processo di conservazione e garantisce nel tempo la conformità alla normativa vigente; • Generazione del Rapporto di Versamento, secondo le modalità previste dal Manuale della Conservazione; • Generazione e sottoscrizione del Pacchetto di Distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal Manuale della Conservazione; • Verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi; • Adozione di misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità. Attuazione di analoghe misure con riguardo all'obsolescenza dei formati. L'adozione	Dal 2008 (Rinnovo nel 2014)

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo
		di queste misure è atta a garantire la conservazione e l'accesso ai documenti informatici; • Gestione della duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal Manuale della Conservazione; • Monitoraggio della corretta funzionalità del Sistema di Conservazione; • Adozione delle misure necessarie per la sicurezza fisica e logica del Sistema di Conservazione ai sensi delle norme vigenti; • Predisposizione del Manuale della Conservazione e cura del suo aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti; • Controllo e garanzia della presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite; • Esecuzione, per gli organi giudiziari e amministrativi dello Stato, del versamento dei documenti conservati all'archivio centrale dello Stato e agli archivi di Stato secondo quanto previsto dalle norme vigenti; • Predisposizione, per gli organismi competenti previsti dalle norme vigenti, dell'assistenza e delle risorse necessarie per l'espletamento delle attività di verifica e di vigilanza.	
Responsabile Sicurezza dei Sistemi per la Conservazione	Claudio Visigalli	• Monitoraggio ed accertamento del Sistema di Conservazione per l'aderenza ai requisiti di sicurezza stabiliti dagli standard, dalle normative vigenti e dalle procedure interne di sicurezza del Soggetto Conservatore; • Comunicazione di eventuali non conformità al Responsabile del Servizio di Conservazione, ed identificazione e studio delle necessarie azioni correttive.	Dal 2014

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo
Responsabile Funzione Archivistica di Conservazione	Gianluca Cardin	• Definizione, direzione e monitoraggio dell'intero processo di conservazione, comprese le modalità di versamento dei documenti da parte del Produttore, l'esibizione, l'accessibilità e la fruizione degli oggetti conservati ed anche la loro esportazione dal sistema; • Gestione e definizione del processo di acquisizione, verifica di integrità dei documenti e delle aggregazioni documentali versate dal Produttore; • Definizione del set di metadati per le diverse tipologie di documenti informatici sottoposti a conservazione; • Progettazione ed analisi riguardante lo sviluppo di nuove soluzioni applicative del Sistema di Conservazione.	Dal 2014
Responsabile Trattamento Dati personali	Claudia Canaparo	• Gestione e definizione del processo relativo al trattamento dei dati per adempiere a tutto quanto necessario per il rispetto delle disposizioni vigenti ed obbligo di osservare scrupolosamente quanto in esse previsto, nonché le istruzioni impartite dal Titolare del trattamento	Dal 2014
Responsabile Sistemi Informativi per la Conservazione	Mario Priori	• Amministrazione delle componenti hardware e software costituenti il Sistema di Conservazione; • Controllo continuo del mantenimento dei livelli di servizio (SLA) concordati con l'ente Produttore; • Comunicazione di eventuali non conformità sui livelli di servizio concordati (SLA) al Responsabile del Servizio di Conservazione ed identificazione e studio delle necessarie azioni correttive; • Verifica ed accertamento dei livelli di servizio erogati da fornitori terzi, con eventuale segnalazione delle non conformità al Responsabile del Servizio di Conservazione; • Progettazione ed organizzazione dell'operatività delle infrastrutture tecnologiche, hardware e software, del Sistema di Conservazione.	Dal 2014

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo
Responsabile Sviluppo e Manutenzione del Sistema di Conservazione	Andrea Rossi	• Coordinamento con l'ente Produttore per la definizione delle modalità di trasferimento dei documenti informatici, con particolare riguardo ai formati elettronici da utilizzare, alla possibile evoluzione tecnologica hardware e software futura ed alle eventuali migrazioni verso diverse piattaforme tecnologiche; • Direzione dello sviluppo e della manutenzione delle componenti software ed hardware costituenti il Sistema di Conservazione; • Monitoraggio dei livelli di servizio (SLA) relativi alla manutenzione del Sistema di Conservazione.	Dal 2014

Torna al sommario

4.1 Produttore

Il Produttore (o Ente Produttore o Soggetto Produttore) è l'entità titolare dei documenti informatici – e delle loro aggregazioni – da conservare.
Si occupa di trasmetterli, insieme ai metadati ad essi associati, al Servizio di Conservazione.
Sottoscrive un contratto di affidamento del servizio con il soggetto conservatore, assegnandogli in outsourcing il processo di conservazione.
Il Produttore, quindi, genera il Pacchetto di Versamento (PdV) ed è responsabile del suo contenuto. E' tenuto a trasmetterlo al soggetto conservatore secondo le modalità operative allegate al contratto di affidamento del servizio.
Le tipologie di documenti ed i rispettivi metadati, oggetto della conservazione, sono concordati attraverso gli allegati tecnici che sono a corredo del contratto di affidamento del servizio.
Il Produttore garantisce l'autenticità ed integrità dei documenti, ed in particolare da garanzia che il trasferimento dei documenti informatici venga realizzato utilizzando formati compatibili con la funzione di conservazione e rispondenti a quanto previsto dalla normativa vigente.

Torna al sommario

4.2 Utente

Si identifica l'utente come una persona, ente o sistema che ha la possibilità di interagire con il Sistema di Conservazione dei documenti informatici.
Può fruire delle informazioni di suo interesse in esso contenute, sia in modo diretto che remoto, sempre nei limiti previsti dalle norme in vigore.
Il Produttore sceglie, abilita e definisce i differenti ruoli per i diversi utenti che dovranno accedere ai documenti, a tutti o solo ad alcuni di essi, seguendo le regole di visibilità specificate negli allegati tecnici al contratto di servizio.

Torna al sommario

4.3 Responsabile della conservazione

Il Responsabile della conservazione è un soggetto nominato dal Produttore ed appartenente a quest'ultimo, i cui riferimenti sono elencati nell'allegato "specificità del contratto". In questo documento sono anche definite le attività e responsabilità affidate al Responsabile del Servizio di Conservazione.
Il Responsabile del Servizio di Conservazione è un soggetto a cui è stato affidato, da parte del Produttore, il processo di conservazione dei documenti informatici, tramite un apposito contratto di servizio.

Torna al sommario

4.4 Organismo di tutela e vigilanza

Il Ministero per i beni e le attività culturali e del turismo (MiBACT) esercita funzioni di tutela e vigilanza sugli archivi degli enti pubblici territoriali e non e di enti privati dichiarati di interesse storico particolarmente importante (ai sensi dell'art. 4 e dell'art. 18 del D.Lgs. 42/2004 e successivi aggiornamenti) e autorizza le operazioni di scarto e trasferimento della documentazione conservata ai sensi del D.Lgs 42/2004.
La Soprintendenza può, in seguito a preavviso, effettuare ispezioni per accertare lo stato di conservazione e custodia degli archivi e possono emettere prescrizioni per la tutela degli archivi.

Torna al sommario

5 Struttura organizzativa per il Servizio di Conservazione

5.1 Organigramma

Il Responsabile del Servizio di Conservazione ha creato una struttura e un'organizzazione, coerente con le proprie politiche di efficienza gestionale, sia per quanto riguarda la scelta delle risorse coinvolte nel processo sia per quanto riguarda l'impostazione operativa delle attività di conservazione, che garantisce la piena osservanza dei principi stabiliti dalla legislazione fiscale e tecnica.

All'interno della società sono state individuate le seguenti figure:

- Responsabile del Servizio di Conservazione (RSC);
- Responsabile Sicurezza dei Sistemi per la Conservazione (RSSC);
- Responsabile Funzione Archivistica di Conservazione (RFAC);
- Responsabile Trattamento Dati personali (RTDP);
- Responsabile Sistemi Informativi per la Conservazione (RSIC);
- Responsabile Sviluppo e Manutenzione del Sistema di Conservazione (RSMC).

le quali fanno capo ad alcuni dipartimenti che si occupano materialmente delle attività operative.
Di seguito l'organigramma delle funzioni coinvolte nel processo di conservazione di documenti informatici:

Figura 1 - Organigramma

Torna al sommario

5.2 Strutture organizzative

Le strutture organizzative di Imaging Group SpA, coinvolte nella gestione operativa del processo del Servizio di Conservazione, sono coordinate dai rispettivi responsabili. Il Responsabile del Servizio di Conservazione opera d'intesa con il Responsabile del Trattamento dei Dati Personali, con il Responsabile Sicurezza dei Sistemi per la Conservazione e con il Responsabile dei Sistemi Informativi per la Conservazione.
Il coordinamento e la supervisione del Responsabile vengono svolte anche attraverso il diretto utilizzo dell'apporto consulenziale offerto dalle strutture legali e tecniche proposte all'erogazione e sviluppo del processo.
In relazione a ciascun contratto di servizio di conservazione, sono coinvolte le seguenti strutture con le corrispondenti attività:

Struttura organizzativa	Attività	In collaborazione con
System Admin dept.	Attivazione del servizio di conservazione (a seguito di una sottoscrizione di un contratto di servizio)	RSIC, Customer care dept.
	Acquisizione, verifica e gestione dei Pacchetti di Versamento presi in carico e generazione del Rapporto di Versamento	RFAC
	Preparazione e gestione del Pacchetto di Archiviazione	RFAC
	Preparazione e gestione del Pacchetto di Distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta	RFAC
	Scarto dei Pacchetti di Archiviazione	RFAC
	Chiusura del servizio di conservazione (al termine di un contratto)	RFAC, Customer care dept.
Development dept.	Interfaccia applicativa verso il Produttore per quanto riguarda le modalità di trasmissione ed i formati dei documenti da conservare	RSIC, Customer care dept.
Customer care dept.	Fornisce supporto ed assistenza, pre e post-vendita, al Produttore, e concorda con esso la configurazione del servizio di conservazione	RSIC, Development dept.

Per quanto riguarda le attività proprie di gestione dei sistemi informativi, le attività sono così ripartite:

Struttura organizzativa	Attività	In collaborazione con
System Admin dept.	Conduzione e manutenzione del Sistema di Conservazione	RSMC
	Monitoraggio del Sistema di Conservazione, comprese tutte le attività di backup dei documenti conservati	RSIC
	Change management, sia hardware che software, dei componenti base del Sistema di Conservazione	
Monitoring & Audit dept.	Verifica periodica di conformità a normative e standard di riferimento. Monitoraggio degli SLA concordati con il Produttore e segnalazione al RSC di eventuali discordanze	RSIC, RSC
Development dept.	Manutenzione, correttiva ed evolutiva, del software di conservazione. In caso di modifiche nelle norme o negli standard di riferimento, provvede alla rispettiva implementazione applicativa, mantenendo aggiornato il servizio di conservazione.	RSMC

Torna al sommario

6 Oggetti sottoposti a conservazione

Gli oggetti sottoposti a conservazione sono i documenti informatici, fascicoli informatici ed aggregazioni documentali informatiche, che insieme ai corrispondenti metadati, alle relative firme digitali e marche temporali vengono racchiusi in pacchetti informativi, ed in questa forma vengono gestiti dal Sistema di Conservazione.

I metadati, legati al documento conservato, costituiscono la struttura di base per la ricerca e l'individuazione del documento stesso all'interno del Sistema di Conservazione e permettono inoltre di conoscerne il formato.

I pacchetti informativi sono distinti in tre diverse tipologie: Pacchetto di Versamento, Pacchetto di Archiviazione e Pacchetto di Distribuzione, e possono contenere uno o più oggetti.

Torna al sommario

6.1 Oggetti conservati

Il Sistema di Conservazione è in grado di trattare diverse tipologie di documenti informatici.
La distinzione delle varie tipologie documentali è necessaria per impostare la corretta tempistica di conservazione e le procedure di scarto dei documenti in anomalia.
Per ognuna di queste tipologie vengono definiti i rispettivi metadati, sia minimi (o standard) che propri per ogni Produttore. La definizione di questi ultimi garantisce il regolare versamento dei documenti, facendo in modo che il Pacchetto di Versamento contenga il corretto set di metadati per la specifica classe documentale.

I metadati, sia standard che propri per ogni Produttore, vengono indicati nel documento di "Specificità del contratto".
Per i documenti informatici con rilevanza ai fini fiscali si utilizzano i metadati minimi (specificati dall'art. 3,comma 1 del D.M. 17 giugno 2014), che sono qui elencati:

- Cognome;
- Nome;
- Denominazione;
- Codice fiscale;
- Partita IVA;
- Data;
- Associazioni logiche di questi ultimi, laddove tali informazioni siano obbligatoriamente previste.

Per gli oggetti gestiti dal Sistema di Conservazione, i principali formati previsti sono conformi a quanto descritto nelle Regole tecniche – Allegato 2 – Punto 5 e qui di seguito elencati:

Formato	Visualizzatore	Versione	Oggetto	Mime type
PDF	Adobe Reader	1.4	Fattura di acquisto, Fattura di vendita, documento ad emissione e tenuta obbligatoria con valenza tributaria, documento generico per il quale si voglia mettere in atto la conservazione a norma	application/pdf
PDF/A	Adobe Reader	1.4 – 1.7	Fattura di acquisto, Fattura di vendita, documento ad emissione e tenuta obbligatoria con valenza tributaria, documento generico per il quale si voglia mettere in atto la conservazione a norma	application/pdf

Formato	Visualizzatore	Versione	Oggetto	Mime type
Email	Mozilla Thunderbird, Opera Mail, Windows Live Mail	-	PEC, email	message/rfc2822 message/rfc5322
TIFF	Irfanview, Windows Image viewer	CCITT Group 4	Fattura di acquisto, Fattura di vendita, documento ad emissione e tenuta obbligatoria con valenza tributaria, documento generico per il quale si voglia mettere in atto la conservazione a norma	image/tiff
XML	Browser internet	-	Fattura di acquisto, Fattura di vendita, documento ad emissione e tenuta obbligatoria con valenza tributaria (Fattura PA), documento generico per il quale si voglia mettere in atto la conservazione a norma, Notifiche di esito relative al Sistema Di Interscambio	application/xml e text/xml

I formati PDF e PDF/A possono essere accompagnati da firma digitale, ove la classe documentale ne richieda la presenza.
Il formato TIFF, generalmente utilizzato per i documenti cartacei forniti dal Produttore, viene sempre firmato digitalmente.
Specifiche tipologie di documenti o formati richiesti dal Produttore sono definiti anch'essi all'interno del documento di "Specificità del contratto", in cui vengono descritte anche le possibili modalità di aggiornamento di questi formati.

Per tutte le tipologie documentali, il periodo di conservazione è della durata di 10 anni, salvo che per i documenti generici e quelli specifici per ogni Produttore, per i quali la durata è variabile in base alla tipologia di documento da conservare.

Torna al sommario

6.2 Pacchetto di Versamento

E' una tipologia di pacchetto informativo, creato secondo un formato concordato con il Produttore, con il quale quest'ultimo invia gli oggetti da conservare al Sistema di Conservazione. Il pacchetto possiede una struttura dati di base comune per tutti i Produttori ed ha, al suo interno, un file contenente i metadati relativi agli oggetti presenti nel pacchetto.

L'arrivo di un Pacchetto di Versamento al Sistema origina la creazione di un Rapporto di Versamento, il quale attesta l'avvenuta presa in carico, da parte del Sistema di Conservazione, del pacchetto inviato dal Produttore. Garantisce inoltre l'esatta corrispondenza tra gli oggetti inviati dal Produttore e quelli acquisiti dal Sistema.
I diversi Rapporti di Versamento vengono univocamente identificati e conservati nel Sistema di Conservazione.
I Pacchetti di Versamento, una volta elaborati dal Sistema, generano Pacchetti di Archiviazione aderenti alle specifiche indicate nell'Allegato 4 alle Regole tecniche.

Torna al sommario

6.3 Pacchetto di Archiviazione

Pacchetto informativo nel quale il Sistema di Conservazione conserva i dati, assicurandone la rintracciabilità e l'integrità nel tempo. Il Pacchetto di Archiviazione è costituito dall'elaborazione di uno o più Pacchetti di Versamento.

I Pacchetti di Archiviazione sono conservati in archivi distinti per ogni Produttore e sono ripartiti in gruppi documentali omogenei per natura, modalità di produzione e tipologia giuridico/legale.
Il Pacchetto di Archiviazione è gestito secondo gli standard tecnici previsti dalla norma UNI 11386:2010 Standard SInCRO.

Il file Indice del Pacchetto di Archiviazione (IPdA, nello standard SInCRO denominato IdC), contenuto all'interno del PdA, racchiude tutte le informazioni identificative per ogni documento sottoposto a conservazione, ed è costruito, sempre in conformità allo Standard SInCRO prima citato, in formato XML e la cui struttura è di seguito riportata:

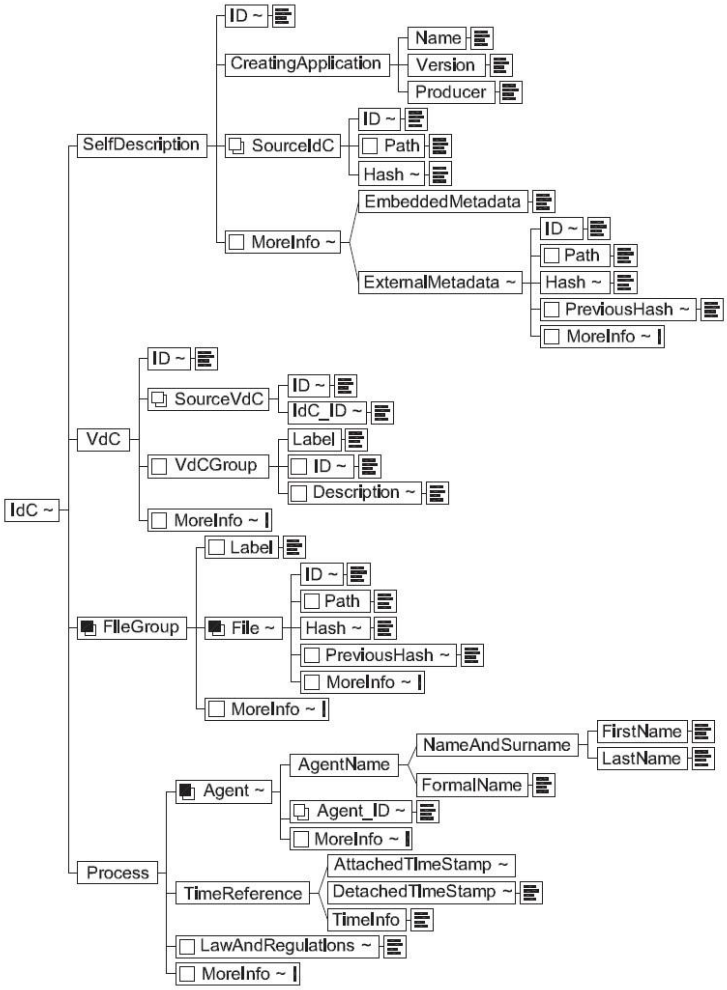

Figura 2 – Struttura dell'Indice del Pacchetto di Archiviazione (IPdA)

Nel nodo denominato *MoreInfo* - all'interno della sezione *FileGroup* - in base alla classe documentale scelta il Produttore può inserire, oltre ai metadati minimi richiesti dalla normativa ed indicati nell'Allegato 4 (Specifiche tecniche del Pacchetto di Archiviazione) delle Regole Tecniche in materia di conservazione, dei metadati aggiuntivi che sono distintivi della tipologia di documento inviato in conservazione e vengono scelti in base alle specifiche necessità di ricerca e reperibilità di questi ultimi.

Di seguito si riporta la struttura dell'elemento *docI*, contenuto nella sezione *FileGroup – MoreInfo* ed utilizzato per lo scopo sopra descritto:

```
<?xml version="1.0" encoding="UTF-8"?>
<schema xmlns="http://www.w3.org/2001/XMLSchema"
 targetNamespace="http://www.imaging.it/cos"
 xmlns:tns="http://www.imaging.it/cos" elementFormDefault="qualified">

 <element name="doc">
    <complexType>
       <sequence>
             <element name="hash">
                   <complexType>
                         <simpleContent>
                               <extension base="string">
                                     <attribute name="encoding" type="string" />
                                     <attribute name="algorithm" type="string" />
                               </extension>
                         </simpleContent>
                   </complexType>
             </element>
             <element name="detachedSign" minOccurs="0">
                   <complexType>
                         <simpleContent>
                               <extension base="string">
                                     <attribute name="encoding" type="string" />
                                     <attribute name="algorithm" type="string" />
                               </extension>
                         </simpleContent>
                   </complexType>
             </element>
             <sequence>
                   <element name="index" minOccurs="0"
                         maxOccurs="unbounded">
                         <complexType>
                               <attribute name="value" type="string"></attribute>
                               <attribute name="name" type="string"></attribute>
                         </complexType>
                   </element>
             </sequence>
       </sequence>
       <attribute name="protocollo" type="string"></attribute>
       <attribute name="filename" type="string"></attribute>
       <attribute name="byte" type="long"></attribute>
       <attribute name="tipodoc" type="string"></attribute>
       <attribute name="datarif" type="string"></attribute>
       <attribute name="action">
             <simpleType>
                   <restriction base="string">
                         <enumeration value="modify"></enumeration>
                               <enumeration value="cancel"></enumeration>
                   </restriction>
             </simpleType>
       </attribute>
       <attribute name="ref"  type="string"></attribute>
    </complexType>
 </element>

</schema>
```

Torna al sommario

6.4 Pacchetto di Distribuzione

Per assicurare l'accesso e la fruibilità della documentazione conservata a norma viene utilizzato il Pacchetto di Distribuzione (PdD). Viene inviato dal Sistema di Conservazione agli Utenti abilitati in risposta ad una loro richiesta (a fini di esibizione), e contiene, oltre ai documenti, le evidenze create durante il processo di conservazione da parte del Sistema di Conservazione.
Tramite questo pacchetto informativo è possibile permettere l'accesso, in modalità informatica, ai documenti conservati anche da remoto.

L'Indice del Pacchetto di Distribuzione possiede un tracciato dati che raccoglie tutti gli oggetti conservati e che sono stati inseriti nel PdD. Tutti gli indici caratteristici degli oggetti e le informazioni di riferimento sono stati strutturati in modo tale da poter essere facilmente interpretati anche da applicazioni esterne al Sistema di Conservazione.

Torna al sommario

7 Il processo di conservazione

Lo schema seguente illustra come avviene il Processo di Conservazione dei documenti informatici:

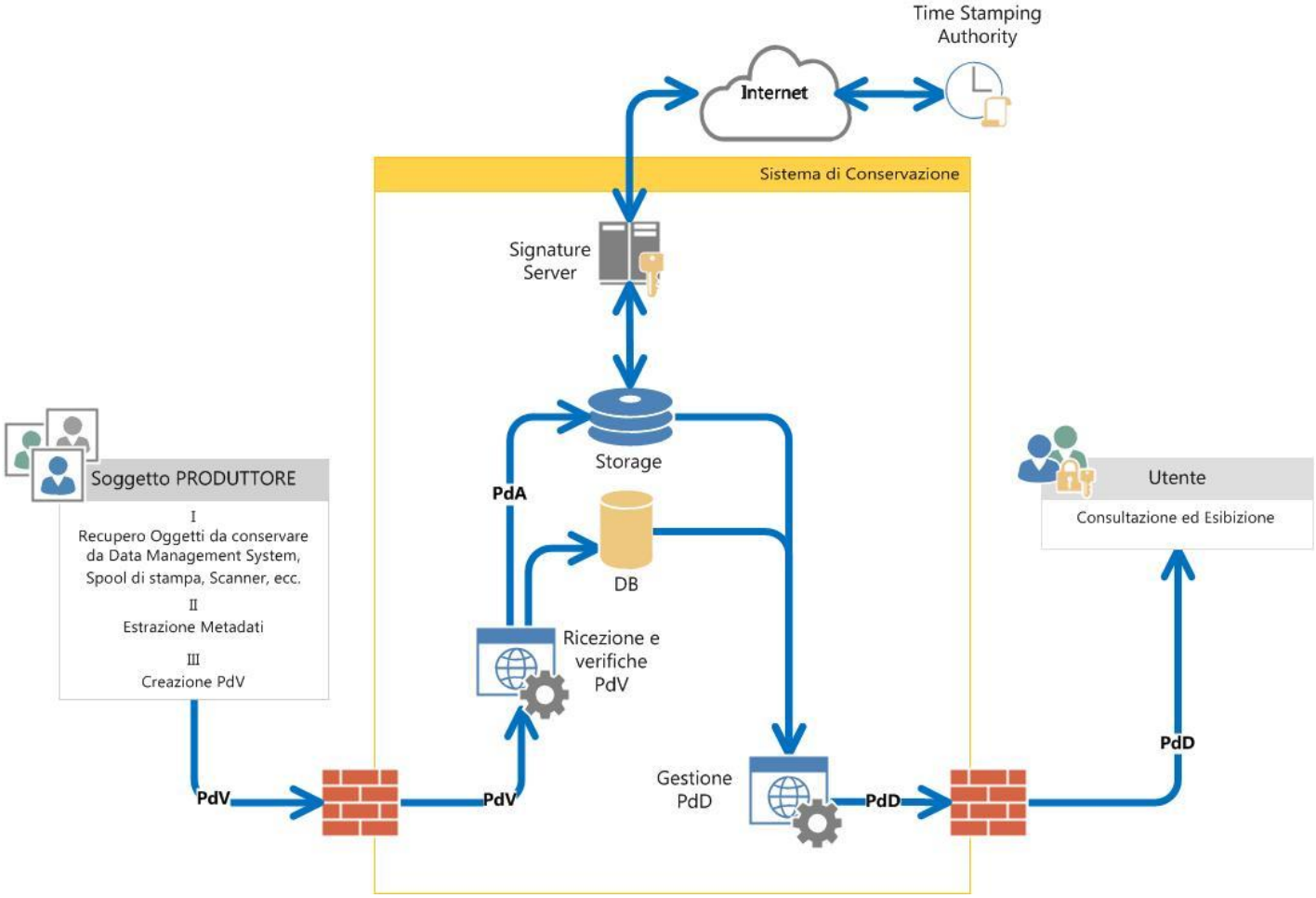

Figura 3 – Processo di conservazione

Il Processo, così composto, garantisce tutti i requisiti di integrità, autenticità dell'origine, leggibilità e disponibilità nel tempo per tutti gli oggetti sottoposti al Processo di Conservazione. Inoltre, assicura la loro rintracciabilità fino al termine del periodo di conservazione.

L'Applicazione proprietaria utilizzata da Imaging Group SpA per la gestione dell'intero processo, è LegalBunker®. Quest'ultima è stata interamente sviluppata e progettata per assicurare nel tempo la conformità alle normative vigenti ed a quanto richiesto dalle Regole tecniche (Art.9).

Lo Storage è il supporto di memorizzazione dei dati sottoposti a conservazione, ed è caratterizzato da uno o più componenti hardware, collegati tra loro per garantire la massima affidabilità e sicurezza del SdC.

Il Server di firma (Signature Server) si occupa di tutta la gestione dell'apposizione della firma sugli oggetti da conservare.

Per l'apposizione della marca temporale, sugli oggetti per cui è richiesta, viene utilizzato un sistema esterno al SdC.
Tutti i processi, coinvolti nella gestione del SdC, sono stati progettati e realizzati in modo tale da automatizzare efficacemente tutte le attività inerenti alla fornitura del servizio di conservazione, riducendo così possibili errori introdotti dall'intervento di operatori umani.

L'Ente Certificatore scelto da Imaging Group SpA per il rilascio delle firme digitali e delle marche temporali, ai fini delle procedure di conservazione di documenti informatici, è iscritto nell'Elenco Pubblico previsto dalla legge ed accreditato AgID.

Torna al sommario

7.1 Modalità di acquisizione dei Pacchetti di Versamento per la loro presa in carico

La trasmissione dei Pacchetti di Versamento da parte del Produttore avviene tramite una applicazione client appositamente sviluppata da Imaging Group. L'applicazione, denominata LegalSender®, si occupa di:

- Effettuare tutti i controlli di conformità preventivi e necessari per l'accettazione dei documenti da parte del Sistema di Conservazione;
- Creare il Pacchetto di Versamento, in formato file .zip, contenente un file indice che racchiude tutti i metadati caratteristici dei documenti che si stanno trasmettendo. Questo file viene firmato dal Produttore che ne garantisce così l'integrità e la provenienza;
- Inviare il Pacchetto di Versamento al Sistema di Conservazione, attraverso protocollo di trasferimento SFTP basato su SSH (Secure Shell - sistema di comunicazione sicuro e crittografato);
- Gestire e segnalare eventuali anomalie di comunicazione;
- Registrare in un apposito log tutte le operazioni effettuate dal Produttore.

Il Sistema di Conservazione annota, in appositi log di Sistema, il versamento dei pacchetti sui propri server SFTP, registrando tutte le informazioni necessarie per l'identificazione di ogni singolo PdV. Per questi log viene eseguito un backup su base giornaliera.
Dopo aver verificato che la trasmissione da parte del Produttore si è conclusa correttamente, viene iscritto nel Database il PdV ricevuto, inserendolo in una coda di attesa per l'elaborazione.
Tutti gli oggetti del PdV vengono quindi spostati in una area di storage sicura e da questa vengono prelevati da un processo interno al SdC ed elaborati.

Torna al sommario

7.2 Verifiche effettuate sui Pacchetti di Versamento e sugli oggetti in essi contenuti

Il processo automatico che si occupa del prelievo e dell'elaborazione dei PdV è responsabile delle seguenti verifiche:

- Corretto formato e tipologia degli oggetti trasmessi, che devono essere compresi tra quelli stabiliti negli accordi con il Produttore;
- Corrispondenza biunivoca tra quanto indicato nell'IdV e gli oggetti contenuti nel PdV;
- Presenza dei metadati obbligatori per ogni tipologia di oggetto, come indicato nel documento "Specificità del contratto";
- Validità della firma sull'IdV;
- Controllo della validità della firma apposta sugli oggetti, se questi vengono sottoscritti dal Produttore;
- Controllo dell'identità del firmatario tramite la sua firma digitale;
- Identificazione del Produttore e verifica che sia abilitato all'invio dei PdV;
- Controllo della validità della marca temporale, se sugli gli oggetti trasmessi vi è l'apposizione di un riferimento temporale opponibile a terzi;
- Integrità nella trasmissione dei dati, procedendo con l'apertura del file .zip ricevuto.

Ogni volta che il processo effettua le operazioni di verifica sui PdV ricevuti, tutti gli eventi vengono appositamente tracciati all'interno di un log di Sistema.

Questo log registra le seguenti informazioni:

- Filename del PdV;
- ID univoco del PdV;
- ID univoco del file dei metadati contenuto nel PdV;
- Descrizione dell'attività di verifica eseguita;
- Data e ora dell'attività svolta;
- Esito finale dell'operazione;

Nel caso in cui le verifiche presentino degli errori:

- Identificativo della tipologia di errore;
- Descrizione dell'errore occorso.

Torna al sommario

7.3 Accettazione dei Pacchetti di Versamento e generazione del Rapporto di Versamento di presa in carico

L'Applicazione di Conservazione ha il compito di generare il Rapporto di Versamento (RdV). L'RdV, formalizzato in un file XML, attesta l'avvenuta acquisizione e presa in carico con successo, da parte del Sistema di Conservazione, del Pacchetto di Versamento (PdV), inviato dal Produttore.
Il RdV, come stabilito dalle Regole tecniche (Art. 9, comma 1, lettere d, e) è univocamente identificato e contiene, per ogni PdV:

- Lo stato del PdV – ACCETTATO/SCARTATO;
- La Ragione Sociale del Produttore ed il suo codice univoco;
- Il Nome del File PdV;
- L'ID univoco del PdV;
- La Data di Arrivo del PdV;
- Un hash (SHA256), relativo all'intero PdV che è stato preso in carico dal Sistema di Conservazione;
- Un riferimento temporale UTC, che attesta il momento in cui è avvenuta la presa in carico del PdV.

Il sistema di log del SdC registra tutte le fasi (creazione chiavi univoche, inserimento a DB dei metadati, ecc.) dell'operazione di accettazione del PdV, aggiornando lo stato di quest'ultimo in accettato o scartato (in questo caso, annotando anche la motivazione dell'anomalia che ha portato allo scarto).
Gli RdV generati vengono sottoscritti con Firma Digitale dal RdC e sono salvati all'interno del repository di conservazione, e seguono lo stesso iter di backup del Sistema di Conservazione. Il Produttore o gli Utenti abilitati possono richiedere la loro consultazione in qualsiasi momento.

Torna al sommario

7.4 Rifiuto dei Pacchetti di Versamento e modalità di comunicazione delle anomalie

Se, a fronte di una delle verifiche (vedere punto 9.2) effettuate dal Sistema di Conservazione, il Pacchetto di Versamento risultasse errato, l'intero pacchetto viene rifiutato dal SdC ed il PdV viene archiviato come *scartato* e non viene elaborato.

Nel caso, invece, di errata ritrasmissione di un oggetto già conservato, è possibile configurare il SdC per prendere in carico solo gli oggetti validi contenuti nel PdV e segnalando gli altri come "scartati". In questo caso il PdV viene marcato come "parzialmente accettato".

Tutte queste operazioni vengono opportunamente registrate in un log di Sistema, con esplicita segnalazione della causa del rifiuto del PdV.
Vengono inoltre inviate delle email di segnalazione del rifiuto agli utenti che sono configurati nel SdC come referenti del Produttore per l'invio degli oggetti in conservazione.
A fronte di queste segnalazioni, il Produttore può richiedere ulteriori informazioni, riguardanti il rifiuto del PdV, al Responsabile del Servizio di Conservazione
Anche in caso di rifiuto, le informazioni relative al PdV vengono inserite nel RdV.

Oltre alle verifiche del punto 9.2, la cessazione o l'inadempienza del contratto da parte del Produttore possono causare il rifiuto del PdV.

Torna al sommario

7.5 Preparazione e gestione del Pacchetto di Archiviazione

Dopo che il PdV ha superato tutti i controlli e le verifiche per la presa in carico e si è proceduto con la generazione del RdV, il Sistema di Conservazione crea il Pacchetto di Archiviazione (PdA).
Il PdA, oltre a contenere esclusivamente oggetti tra loro omogenei, ha al suo interno:

- Il file Indice del Pacchetto di Archiviazione, che alla conclusione del Processo di Conservazione, viene sottoscritto con firma digitale dal RSC e marcato temporalmente;
- Un file doc.xsd, che rappresenta la struttura con cui vengono inseriti i metadati degli oggetti sottoposti a conservazione nel file IPdA.

Per assicurare l'interoperabilità nel tempo dei diversi sistemi di conservazione, il file IPdA viene formato in rispondenza alle Regole tecniche definite nella norma UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.
Tutte le operazioni effettuate dal Sistema di Conservazione in fase di preparazione del PdA, vengono registrate in un apposito file di log.

Una volta che il PdA è pronto per la conservazione, viene segnalato al RSC, il quale si occupa di apporre la propria firma digitale secondo la seguente procedura:

- Il RSC accede, attraverso l'interfaccia web, alla pagina di amministrazione del Sistema di Conservazione da cui ha evidenza di tutti i PdA che sono in attesa per la chiusura del processo di conservazione;
- Dopo aver selezionato dalla lista i PdA che interessano, il RSC appone la propria firma digitale sui file IPdA relativi;
- Il SdC provvede ad apporre la marca temporale ai file IPdA appena firmati, contattando i server della Time Stamping Autorithy, gestita da un certificatore presente nell'Elenco dei conservatori attivi accreditati presso AgID.

Si procede quindi con le copie dei PdA sui diversi repository appartenenti al SdC.
Una notifica a video ed una segnalazione via email confermano o meno l'avvenuta conclusione del processo di conservazione.
È anche possibile che la procedura sopra descritta sia eseguita in modalità mista, cioè automatizzata ma con un intervento manuale in certe fasi, utilizzando un dispositivo HSM che consenta di evitare le attività di firma locale in favore di una struttura di firma remota.

Ad intervalli pianificati, un processo automatico provvede ad effettuare una serie di verifiche sui PdA presenti nel repository di conservazione. Vengono analizzati prima i pacchetti per cui è passato maggior tempo dall'ultimo controllo con esito positivo.
Se il controllo di un pacchetto dovesse dare esito negativo, quest'ultimo avrà la priorità alla prossima esecuzione del processo.

Il controllo si suddivide in diverse fasi:

- Verifica a livello base dell'integrità del documento su file system, effettuata calcolando l'hash SHA256 del file memorizzato e confrontandolo con quello memorizzato nel database del Sistema di Conservazione in fase di accettazione del PdV;
- Verifica della validità della firma apposta su ogni documento, ove presente;
- Verifica della validità della firma e della marca temporale apposte sul file IPdA.

Questi tipi di verifiche, avendo un accesso fisico al documento in esame, forniscono adeguate garanzie sia in termini di disponibilità che di leggibilità del file.

Il Sistema di Conservazione permette la modifica e la cancellazione logica dei documenti informatici costituenti il PdA. Queste azioni sono inserite nel database applicativo e nel file di log. Si ha così la possibilità di ricostruire tutti i passaggi che hanno coinvolto uno specifico documento.
La modifica e la cancellazione logica possono essere richieste solo dal Produttore o dagli Utenti abilitati che utilizzano le funzioni rese disponibili dal Sistema.

Torna al sommario

7.6 Preparazione e gestione del Pacchetto di Distribuzione ai fini dell'esibizione

Per permettere l'accesso diretto, da parte degli Utenti abilitati del Produttore, ai propri documenti conservati, il Sistema di Conservazione dispone di una interfaccia web dedicata.
L'Utente, dopo aver completato la necessaria fase di autenticazione, utilizza l'interfaccia web che consente di ricercare e selezionare i documenti esclusivamente all'interno del proprio repository, utilizzando delle funzionalità di ricerca basate sia su campi obbligatori che concordati con il Produttore.
Una volta selezionati i documenti che andranno a comporre il Pacchetto di Distribuzione (PdD), l'Utente richiede al SdC la generazione del PdD che viene reso disponibile in formato compresso (Zip) od in formato immagine ISO.

Le attività svolte, sia dall'utente che dal Sistema, sono tutte tracciate nel file di log e restano a disposizione del Produttore per tutta la durata del contratto.

Torna al sommario

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

Gli Utenti, accreditati dal Sistema di Conservazione attraverso il modulo di controllo degli accessi, possono ottenere un duplicato dei propri documenti conservati.
La richiesta avviene in maniera totalmente autonoma – on demand – e senza limitazioni di numero di duplicati richiesti, attraverso l'interfaccia web od attraverso i metodi esposti dei web services del SdC.

In aggiunta a queste modalità, su specifica domanda dell'Utente, possono essere creati duplicati dei documenti su supporto ottico, che successivamente verrà inviato al richiedente.
Per la produzione di copie informatiche, su esplicita domanda dell'Utente, il Sistema genera il documento con l'apposizione della firma digitale del RSC.

Inoltre, ove sia richiesto, a seguito della comparazione tra il documento originale e la sua copia, viene inserita in quest'ultima l'attestazione di conformità con l'apposizione della firma digitale del notaio o di un pubblico ufficiale.

Attraverso un confronto tra l'hash del documento duplicato – o della copia – e l'hash dell'originale, si garantisce che i due oggetti siano esattamente corrispondenti.

Nei casi in cui il RSC lo ritenga necessario, ai fini di fronteggiare l'obsolescenza dei formati elettronici, è possibile effettuare il riversamento sostitutivo (copia informatica) dei documenti conservati.
Il RSC deve eseguire il riversamento sostitutivo nel caso in cui sia necessario un aggiornamento tecnologico dell'archivio informatico, in quanto non è più conveniente mantenere nel tempo il formato di rappresentazione digitale dei documenti originariamente conservati.
Il processo si conclude con l'apposizione, sull'insieme dei documenti o su una evidenza informatica contenente l'impronta o le impronte dei documenti o di insiemi di essi, del riferimento temporale e della firma digitale da parte del RSC, salvo i casi previsti dalla legge secondo i quali risulti indispensabile la presenza di un pubblico ufficiale a chiusura del processo di conservazione (ad esempio nel riversamento di documenti analogici originali unici conservati).

Tutte le attività di richiesta e fornitura di duplicati e copie vengono registrate e mantenute nel file di log di Sistema.

Torna al sommario

7.8 Scarto dei Pacchetti di Archiviazione

L'RSC, coadiuvato dal RFAC, procede, tramite interfaccia web esposta dal SdC, alla selezione dei PdA che hanno superato i termini di conservazione previsti dalle norme.
Questi termini vengono impostati in fase di configurazione del repository, ed associati ad ogni tipologia documentale conservata.

Una volta selezionati, si può procedere con l'esportazione dei PdA. Questa fase marca i PdA come *esportati* e quindi preparati per la fase successiva di scarto.
Questa sequenza ben definita di attività non permette lo scarto di PdA che non siano stati preventivamente esportati e quindi memorizzati su dispositivi esterni al Sistema.
Prima di effettuare la procedura di scarto, viene inviata una comunicazione preventiva al Produttore chiedendo un suo espresso consenso.
Nel caso in cui le procedure di scarto interessino archivi pubblici o privati di particolare interesse culturale, queste avverranno unicamente previa autorizzazione del Ministero dei Beni e delle Attività Culturali e del Turismo.

Se nel mese solare successivo il Produttore non invia una comunicazione, richiedendo esplicitamente l'estensione del periodo di conservazione dei PdA in oggetto, il Sistema provvede ad avviare la procedura di scarto, che consiste alla cancellazione fisica dallo storage dei PdA selezionati e di tutti i documenti relativi, basandosi sul principio del silenzio assenso.

Tutte le comunicazioni intercorse vengono sottoscritte dal RSC ed archiviate a Sistema.

Torna al sommario

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

Per favorire l'interoperabilità tra Sistemi di Conservazione diversi, la soluzione realizzata da Imaging Group è aderente alle regole ed agli standard seguenti:

- Allegato 2 delle Regole tecniche del DCPM 3 dicembre 2013, per la definizione dei formati accettati per gli oggetti da conservare;
- Standard UNI 11386 "SInCRO", per la creazione dei file di Indice del PdA;

- Art. 9, comma 1, lettera h delle Regole tecniche del DCPM 3 dicembre 2013, per la creazione dei PdD coincidenti con i Pacchetti di Archiviazione.

Nel caso in cui il contratto di servizio tra Imaging Group ed il Produttore dovesse terminare, l'archivio contenente tutti gli oggetti in conservazione viene reso disponibile al Produttore su di un supporto adatto alle dimensioni dell'archivio.
Il periodo per la gestione di tale procedura è previsto della durata di 30 giorni, durante i quali il Produttore dovrà richiedere la consegna dell'archivio dei file. La procedura è descritta in dettaglio nel contratto di servizio.

Torna al sommario

8 Il Sistema di Conservazione

Nel seguente capitolo vengono descritte le componenti logiche, tecnologiche e fisiche coinvolte nel Sistema di Conservazione, con particolare risalto agli aspetti di sicurezza ed alle procedure adottate per garantire la massima qualità del servizio erogato.

Torna al sommario

8.1 Componenti Logiche

Il Sistema di Conservazione si basa su 5 componenti logiche distinte ma sinergiche tra loro:

- Una applicazione client, chiamata LegalSender, che serve per gestire i dati esportati dai sistemi del Produttore e creare il Pacchetto di Versamento;
- Il processo di accettazione dei pacchetti, che ha il compito di aprire, controllare ed inserire nei Pacchetti di Archiviazione i documenti ricevuti;
- Il processo di chiusura e conservazione dei Pacchetti di Archiviazione, che effettua una serie di controlli formali per assicurarsi che i documenti in essi contenuti siano integri e conformi alle specifiche del Sistema;
- Una interfaccia web, che permette al Produttore di ricercare e consultare i documenti inviati al Sistema di Conservazione;
- Una interfaccia web di amministrazione che permette al Responsabile del Servizio di Conservazione ed ai suoi delegati, di gestire il DB di configurazione del Sistema e di monitorare e lanciare i task di verifica.

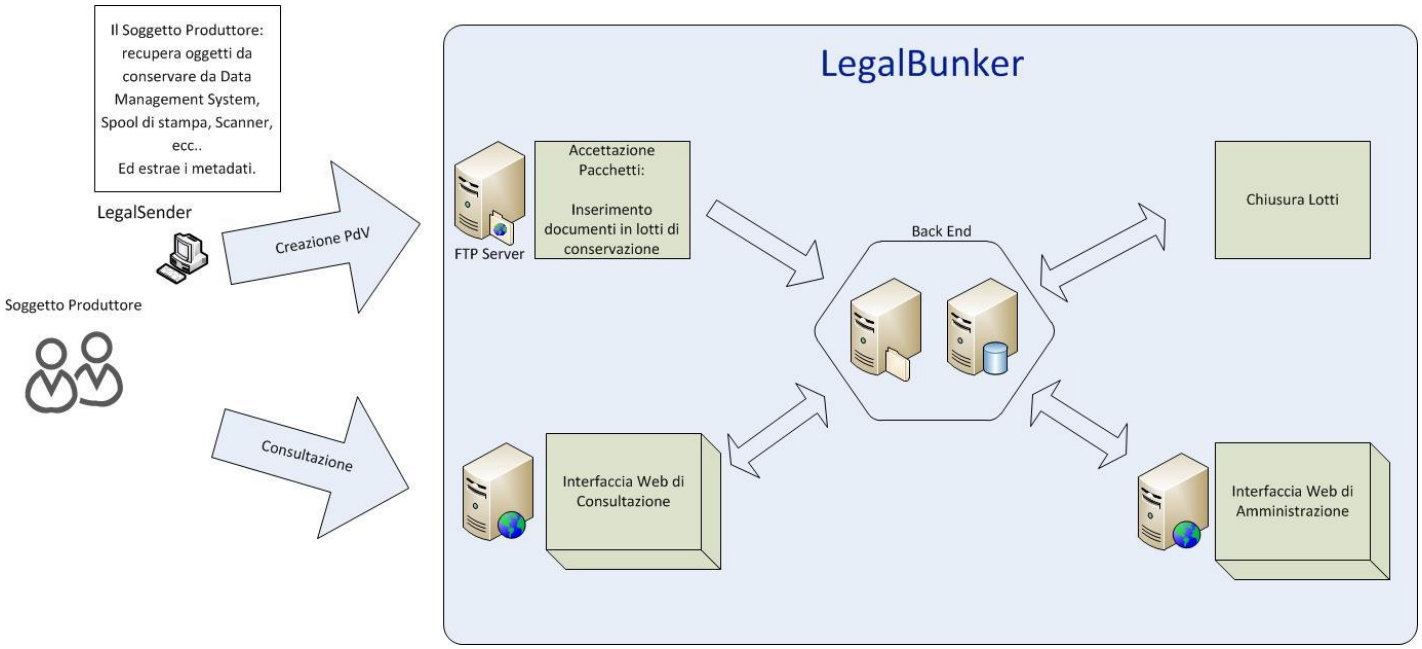

Figura 4 –Componenti logiche

Torna al sommario

8.2 Componenti Tecnologiche

Il Sistema di Conservazione è implementato da un'applicazione software, appositamente sviluppata a tale scopo interamente in Java, e da una serie di servizi di interesse generalizzato, condivisi con altre applicazioni (marca temporale, HSM, supporti di conservazione, PEC).

Per motivi di sicurezza si è fatto in modo che il Sistema non sia raggiungibile direttamente dall'esterno (da internet). Il punto di accesso al Sistema dall'esterno è una web Application dedicata, accedibile con protocollo sicuro https, denominata LegalBunker Client. Il server su cui è installata questa applicazione non è connesso alle infrastrutture di back end contenenti i dati (DB, storage,...). L'applicazione LegalBunker Client ha il compito di smistare le chiamate provenienti dall'esterno verso l'applicazione vera e propria, tramite apposite servlet. In questo modo si evita che il server esposto in internet, pur protetto da firewall con filtro sugli indirizzi IP, possa direttamente aver accesso ai documenti in conservazione. Per motivi prestazionali, tutte le attività amministrative effettuate dal RSC e dai suoi delegati vengono eseguite direttamente utilizzando l'applicazione LegalBunker, in quanto le chiamate vengono fatte all'interno della rete Imaging Group.

La crescita del numero dei documenti, vista la dimensione fisica degli oggetti, è molto importante in termini di scalabilità. Per questo motivo LegalBunker è stato sviluppato per essere indipendente dal sistema hardware che conserva i file. I documenti possono anche essere distribuiti in diversi storage in funzione della configurazione del Sistema.

Tutte le strutture dati di configurazione e di conservazione sono memorizzate in un database Oracle.
Per ogni aspetto riguardante la sicurezza delle componenti Tecnologiche e per quanto riguarda le politiche di backup si fa riferimento al "Piano della Sicurezza per attività di conservazione documentale".

Torna al sommario

8.3 Componenti Fisiche

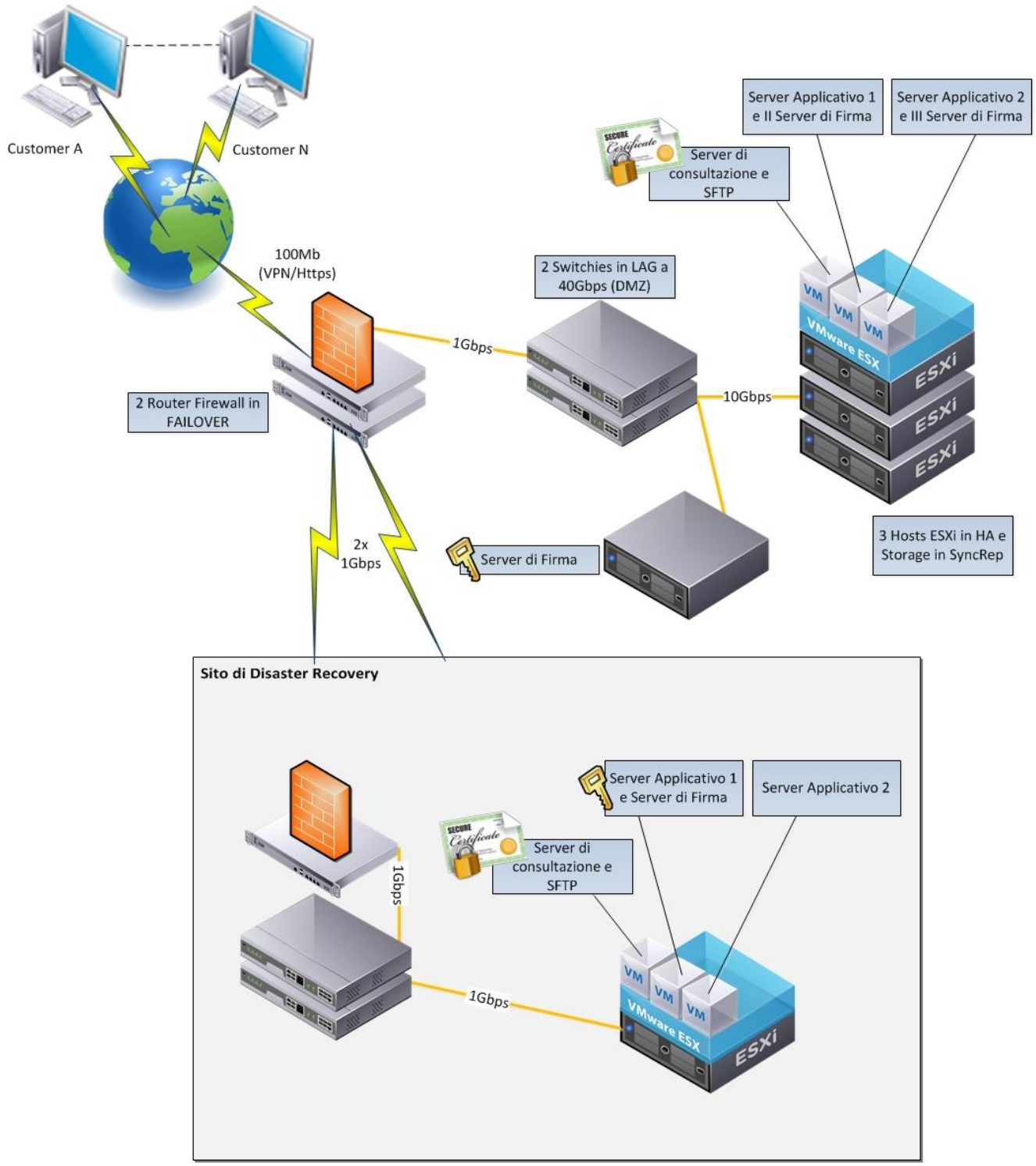

Figura 5 – Componenti fisiche

Il Sistema di Conservazione di Imaging Group in modalità SAAS è composto da:

- Due server virtuali ridondati tra loro, uno primario attivo ed uno secondario in failover. I dati dei due media vengono allineati grazie a delle logiche di replica dei dati in tempo reale. I server sono collegati tra loro con due reti distinte attestate su switch Dell Force10, una dedicata alla DMZ e una dedicata alla rete interna. e da antivirus in realtime scan aggiornati giornalmente;

- Un server virtuale per la consultazione dove i clienti si collegano tramite VPN/Https. Il server è usato anche come SFTP con certificato web SSL;
- Un server fisico per la firma dei Pacchetti di Archiviazione.

Tutto il sistema è supportato da un'infrastruttura hardware composta da:

- Due firewall CISCO in failover;
- Due switch in LAG tra loro a 40Gbs ed una velocità interna di 10Gbs;
- Tre hosts Esxi in HA e totalmente ridondati;
- Due storage totalmente ridondati e speculari in SyncRep.

L'infrastruttura software è basata su VMware VSphere.
Il backup viene effettuato tramite Veeam Backup & Replication sia su storage interno e sia su tape library. I nastri magnetici sono Ultrium Cartridge che, tramite una modalità di retention che garantisce il recupero dei dati fino ad 1 mese, vengono archiviate settimanalmente e spedite in un caveau blindato.

Sempre tramite Veeam Backup & Replication viene gestita la copia delle macchine virtuali sul sito di Disaster Recovery.

Torna al sommario

8.4 Procedure di gestione e di evoluzione

Per quel che concerne le procedure di gestione ed evoluzione, LegalBunker si attiene ai criteri previsti nell'ambito della certificazione ISO/EIC 27001.
Nello specifico esse riguardano:

- Il monitoraggio e verifiche UPS (Uninterruptable Power Supply) : PSI11 – Sicurezza fisica ed ambientale;
- Il monitoraggio dei sistemi fisici: IO07 - Gestione Alert;
- Il Business Continuity Plan: DSGI10 - Business Continuity Plan;
- Il controllo e gestione del cambiamento del sistema informatico aziendale: POLICY12.1 - Tenuta Sotto Controllo Dei Cambiamenti;
- L'Analisi del rischio: PSI04 - Analisi Dei Rischi;
- La vulnerabilità e la sicurezza nell'operatività: PSI12 - Sicurezza Delle Attivita Operative;
- La gestione degli accessi alle strutture fisiche: PSI09 - Controllo Accessi.

Il controllo dell'implementazione di queste procedure è in carico ad un team preposto con a capo il Responsabile del Servizio di Conservazione. Questo team provvede anche alla verifica dell'evoluzione normativa ed al tempestivo adeguamento delle procedure e degli strumenti tecnici e tecnologici del Sistema di Conservazione.

Le configurazioni dell'hardware di sistema e di rete, del software di sistema e di rete e del software applicativo sono documentate e tale documentazione è conservata in modo sicuro, anche presso la sede di Disaster Recovery, a cura del Responsabile del Servizio di Conservazione che ne cura la verifica periodica della corrispondenza tra le configurazioni in essere e quelle previste.

Le operazioni più delicate sui sistemi dell'hardware e software del servizio e della rete sono effettuate in regime di dual control.
Ove possibile e ragionevole, sono utilizzati dispositivi crittografici / biometrici per l'identificazione e l'autorizzazione degli addetti a operare sui sistemi. Laddove sono utilizzate userid e password, queste ultime, oltre ad essere custodite in modo riservato, devono rispettare determinati criteri di composizione (ad esempio: lunghezza minima, utilizzo di caratteri alfanumerici, caratteri speciali, punteggiatura, ecc.) e devono essere sostituite almeno ogni tre mesi. Eventuali password non personali (password di sistema e simili) sono assegnate ad uno specifico responsabile, ma una copia ne è custodita in maniera sicura e tamper-evident presso il

Responsabile del Servizio di Conservazione che, in caso di necessità, le consegna ad un eventuale sostituto registrando l'evento.

Per garantirne la continuità del Servizio di Conservazione di documenti informatici nel tempo, il RSC deve programmare un piano di manutenzione (sia per quanto riguarda il software sia per quanto riguarda l'hardware) al fine di ridurre al minimo le alterazioni del sistema informativo.
A tale scopo viene tenuto un registro di manutenzione programmata dove vengono inseriti i seguenti dati:

Sistema Operativo	Versione LegalBunker	Data manutenzione	Funzione aziendale	Descrizione intervento

Il riversamento della documentazione conservata su supporti di memorizzazione che siano, in quel momento, adeguati alla tecnologia corrente è un altro dei compiti del Responsabile del Servizio di Conservazione.
Di questo se ne tiene traccia in un registro di riversamento dove vengono riportate le informazioni di seguito:

Dispositivo riversato	Tipologia dispositivo	Nuovo dispositivo	Data	Funzione aziendale

In appositi archivi, duplicati e tempestivamente aggiornati anche presso le sedi di disaster recovery, viene conservato quanto segue:

1. Il software di base su cui sono state installate le varie versioni dei prodotti utilizzati per la conservazione di documenti informatici;
2. Il software di rete;
3. Tutte le diverse versioni dei prodotti utilizzati per la conservazione di documenti informatici;
4. I programmi di visualizzazione dei vari formati dei documenti sottoposti a conservazione di documenti informatici;
5. Ogni versione dell'applicazione LegalBunker (codici sorgenti e documentazione tecnica). Il versionamento viene gestito tramite un apposito repository SVN.

Di quanto sopra indicato l'RSC gestisce un registro che riporta, per ogni prodotto utilizzato per la conservazione:

Nome dell'Applicativo	Sistema Operativo	Versione	Data di inizio utilizzo	Versione sostituita

Torna al sommario

9 Monitoraggio e controlli

Al fine di identificare e prevedere delle criticità del Sistema di Conservazione, sono stati attivati dei meccanismi di monitoraggio e controllo particolarmente articolati, così da permettere l'implementazione di soluzioni tecniche ed operative atte alla pronta risoluzione di eventuali incidenti che dovessero occorrere.

Torna al sommario

9.1 Procedure di monitoraggio

9.1.1 Procedure di audit

Periodicamente vengono effettuati audit aziendali da parte di "terzi verificatori", in modo da poter monitorare costantemente:

- Il processo di esibizione e l'accesso alle varie tipologie documentali sottoposte alla procedura di conservazione di documenti informatici;
- I processi organizzati per rispondere ai requisiti dello standard ISO/IEC 27001:2013, del Manuale di Conservazione e quanto stabilito nel documento "Specificità del Contratto".

Durante queste ispezioni possono essere rilevate delle anomalie, che vengono annotate in un apposito registro ("Eccezione sollevate in sede di ispezione da parte dei verificatori") dove devono essere riportate tutte le seguenti informazioni:

Data Verifica	Verificatore	Descrizione Eccezione	Tipo Verifica	Azione

Questo documento viene utilizzato per:

- Avviare le azioni preventive e correttive fondamentali per evitare il reiterare delle carenze e delle problematiche riguardanti i processi od i sistemi in analisi;
- Funzioni di storicizzazione di tutte le criticità che sono emerse dalle precedenti verifiche ispettive, che devono essere verificate nelle prime fasi del successivo audit.

Il registro, essendo un documento informatico, viene sottoposto anch'esso al processo di Conservazione.

Torna al sommario

9.1.2 Monitoraggio della validità dei certificati di firma

Il Sistema di Conservazione verifica, in modalità totalmente automatica, la validità dei certificati di firma sui documenti informatici che devono essere portati in conservazione.
Inoltre, provvede al controllo dei certificati relativi alla TSA, nel momento dell'apposizione della marca temporale sugli IPdA.

Torna al sommario

9.1.3 Monitoraggio delle attività attraverso i file di log

La gestione dei log applicativi e di sistema è stata implementata da Imaging Group per ottenere i seguenti obiettivi:

- Un report di tutte le attività di accesso e disconnessione al sistema da parte dei vari Soggetti Utente;
- Una registrazione delle azioni svolte nell'ambito dei vari work-flow operativi;
- Inalterabilità, tramite firma elettronica, e possibilità di accertamento dell'integrità dei file di log;
- Conservazione dei file di log con un Data Retention Time di almeno 1 anno.

I file di log con le suddette caratteristiche posseggono tutte le informazioni indispensabili per ricostruire a posteriori i comportamenti dei sistemi e dei suoi utilizzatori.

Torna al sommario

9.1.4 Monitoraggio delle componenti fisiche costituenti il SdC

Come specificato nel documento "Piano della Sicurezza per attività di conservazione documentale", tutte le operazioni di controllo e monitoraggio sono volte a valutare ed analizzare periodicamente le prestazioni del Sistema di Conservazione.

Ogni parte componente l'infrastruttura del SDC – dagli Application Server ai DB – dove sia stata installata una applicazione o servizio afferente il Sistema di Conservazione, viene controllata costantemente da un software di network monitoring, che attraverso opportune probes, ne verifica il funzionamento.
Questa applicazione :

- supporta i protocolli SNMP, ICMP, DNS e TCP, e li utilizza in base alla tipologia di sistema che è sotto controllo;
- possiede un archivio storico degli stati delle singole componenti monitorate che può essere consultato attraverso una opportuna interfaccia;
- allerta gli addetti di riferimento in caso di occorrenza di anomalie.

In aggiunta ai controlli precedenti, sono attivi dei processi di alert, che a seguito di particolari condizioni di criticità su di ogni singolo componente del sistema, inviano una segnalazione al personale addetto alla gestione delle anomalie.

Torna al sommario

9.1.5 Controllo sulla gestione della Privacy

I delegati al processo di conservazione sono stati adeguatamente formati in merito alla normativa attualmente in vigore in materia di protezione dei dati personali e sono stati preventivamente incaricati al trattamento dei dati personali di natura fiscale e contabile.

Tutte le procedure di gestione della privacy, nel pieno rispetto della normativa attualmente in vigore, sono compiutamente descritte nella documentazione redatta nell'ambito della certificazione ISO/EIC 27001, alla quale si rimanda.

Torna al sommario

9.1.6 Security policy e gestione incidenti di sicurezza

Imaging Group, adottando un sistema di gestione della sicurezza delle informazioni conforme alla norma ISO IEC 27001:2013, implementa tutte le procedure interne necessarie al fine di prevenire i rischi associati al trattamento delle informazioni e di tutelare il patrimonio informativo aziendale e dei suoi Clienti.

Sono in essere security policy che definiscono le misure di sicurezza strategiche e quelle di dettaglio in vigore per i vari sistemi. Tali policy prevedono anche le modalità di reporting e le procedure da seguire da parte degli addetti al verificarsi di incidenti di sicurezza dei vari livelli di gravità, fino ai casi in cui il Responsabile del Servizio di Conservazione o un suo delegato dichiarano lo stato di disastro che comporta lo spostamento delle operazioni presso il sito di Disaster Recovery.

Al verificarsi di incidenti di sicurezza di entità non trascurabile e quando lo decide il Responsabile del Servizio di Conservazione, le security policy e le succitate procedure vengono riviste, almeno per quanto relativo agli incidenti che si siano verificati. Una completa revisione viene eseguita almeno una volta l'anno.

Torna al sommario

9.2 Verifica dell'integrità degli archivi

Il Sistema di Conservazione opera in modalità automatica dei severi controlli, ad intervalli regolari, sull'integrità dei file contenuti all'interno del Sistema.
L'esito di queste verifiche viene segnalato tempestivamente al RSC e viene salvato all'interno del Sistema di Conservazione.

Inoltre, il Responsabile del Servizio di Conservazione o suo delegato, verifica periodicamente, con cadenza non superiore a tre anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti.

Questa verifica viene effettuata selezionando a campione diversi documenti conservati (almeno uno per ognuna classe documentale).
Dopo averli scaricati dal Sistema di Conservazione, si procede con la loro apertura, attraverso un programma specifico per ogni tipologia di file.
La regolare apertura dei file e la corretta lettura delle informazioni contenute garantiscono l'effettiva leggibilità del documento conservato.

Qualora venisse identificato un supporto non più leggibile, si provvederà ad effettuare un riversamento del suo contenuto su altro supporto con l'ausilio della copia di sicurezza secondaria e/o dei backup.

In particolare, per quanto riguarda la leggibilità dei supporti, il RSC od uno dei suoi delegati, effettua le seguenti verifiche:

- Verifica a campione dell'hash di un documento informatico conservato;
- Verifica a campione della firma digitale e del riferimento temporale apposto sul singolo documento conservato;
- Verifica a campione della firma digitale e della marca temporale apposta sull'evidenza informatica conservata.

ed attesta l'effettuazione di queste ultime ed il relativo esito su di un registro informatico, da lui firmato e marcato temporalmente, custodito nei vari siti di Imaging Group SpA.

Questo registro, che riporta quindi la storia delle verifiche periodiche, contiene le seguenti informazioni:

Data Verifica	Verificatore	Documenti verificati	Scritture contabili e altri documenti verificati	Esito verifica

Il RSC deve inoltre aggiornare il registro che riporta le scadenze delle verifiche periodiche che dovranno essere effettuate, e più precisamente contiene le seguenti informazioni:

Data prossima verifica	Documenti da verificare (Ciclo passivo di fatturazione)	Documenti da verificare (Ciclo attivo di fatturazione)	Documenti da verificare (Scritture contabili e similari)	Verificatore

Torna al sommario

9.3 Soluzioni adottate in caso di anomalie

Nonostante tutte le precauzioni adottate, potrebbero verificarsi casi di anomalie, in cui i documenti non possano essere portati in conservazione entro i tempi previsti oppure qualora le verifiche effettuate presso ogni sito di conservazione mostrino delle discordanze tra gli oggetti conservati ed i corrispondenti metadati. Tali situazioni potrebbero verificarsi nei seguenti casi:

- Guasto ai sistemi di Imaging Group SpA che rendano temporaneamente inutilizzabili le procedure di Conservazione di documenti informatici;
- Guasto ai sistemi del Cliente di Imaging Group SpA che non gli consenta di inviare i file da conservare entro i tempi previsti;
- Guasto od indisponibilità delle linee di comunicazione;
- Guasti od indisponibilità della Time Stamping Authority a fornire la marcatura entro i tempi previsti;
- Blackout prolungato;
- Incendio o distruzione degli edifici contenenti i sistemi informativi;
- Eventi naturali;
- Altre cause non predeterminabili.

In questi casi viene tenuta traccia dell'anomalia verificatasi in un apposito documento elettronico denominato "Registro degli Incidenti di Sicurezza" o nel "Registro delle non Conformità", in osservanza delle procedure previste dalla certificazione ISO/EIC 27001:2013 e ISO 9001:2008.
Tale documento conterrà le seguenti informazioni:

- Data di inizio dell'anomalia riscontrata;
- Descrizione dell'anomalia riscontrata, della causa che l'ha generata e del suo impatto sul Sistema di Conservazione;
- Precauzioni e rimedi adottati;
- Data di fine anomalia.

Tale documento, ove di tipo informatico, sarà digitalmente firmato dal RSC, o da un suo delegato, e sarà sottoposto a marcatura temporale in modo da renderlo opponibile a terzi e verrà conservato unitamente ai PdA. Ove di tipo cartaceo sarà prodotto in più copie conservate presso il sito di Disaster Recovery e presso quello di storage backup.

Esiste una procedura di "incident reporting" che qualsiasi persona di Imaging Group SpA è tenuta a rispettare qualora rilevi una situazione anomala onde segnalare l'incidente.
Il Responsabile del Servizio di Conservazione è la persona deputata a valutare l'entità dell'incidente e, nel caso, a dichiarare lo stato di disastro. In tal caso entra in funzione la procedura di Disaster Recovery

Qualora il RSC dichiari lo stato di disastro, il personale abilitato si trasferisce preso la sede di Disaster Recovery ove esegue le operazioni, indicate in apposita procedura il cui contenuto è riservato, che comprendono anche quanto indicato ai precedenti paragrafi del capitolo Le attività di conservazione possono quindi riprendere entro un lasso di tempo massimo di 4 ore, a meno di eventi catastrofici.

A seconda dei casi, l'operatività normale sarà riportata presso la sede principale o presso una sede sostitutiva secondo i piani e le procedure di recovery redatti nel documento "Piano della Sicurezza per attività di conservazione documentale".

Torna al sommario