Manuale del Sistema di Conservazione

eWitness Italia Srl
Via Turati 29
20121 Milano (MI)
P. IVA e C.F. 06044690961

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	27.01.2019	Stefano Tazzi	CTO, RSM, RSSI
Verifica	28.01.2019	Patrizia Sormani Simone Diodati	Legal Advisor RSI
Approvazione	12.02.2019	Eleonora Giardino Stefano Tazzi Patrizia Sormani Riccardo Genghini	AD CTO Legal Advisor RdC, RSC

REGISTRO DELLE VERSIONI

N° Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
1.0	28.03.2015		
1.1	04.06.2015	Integrazioni ai punti 7.1, 7.2, 7.3, 7.4, 7.6, 7.7.2, 7.9	
2.0	30.05.2016	Adeguamenti formali secondo quanto previsto dallo "*Schema di manuale di conservazione v.2*"	Inserito il link "Torna al sommario"; inserita didascalia delle figure presenti; aggiornamento elenchi puntati.
2.1	26.10.2016	Aggiornamento responsabili di funzione, in seguito alle variazioni societarie	
2.2	12.02.2019	Inserimento cariche privacy (punti 2 e 4) Aggiornamento normativa per privacy (punti 1.2 e 8.4) e fatturazione elettronica (punto 3) Inserimento registro delle cariche (4.3) Precisazioni in merito alla gestione dei PdD (punto 4 par. 5.2). Specifica del supporto anche dei	In generale, sono stati sistemati diversi refusi ed elementi di formattazione, non riportati nel dettaglio in quanto non costituiscono modifiche sostanziali. In generale, in tutto il documento, dove si faceva riferimento al solo canale di acquisizione FTP è stato inserito anche il canale web service.

		web service per l'acquisizione dei PdV (par. 6.2), con il passaggio dell'IPdV da PDF/A ad XML. Aggiornamento formato IPdV. Aggiornamento formato file fatture elettroniche nel PdA (par. 6.3); aggiornamento delle specifiche dei metadati per il PdA. Inserimento punti 7.1.2, 7.2.1, 7.10, 8.5 e 9.2 Modifica alla gestione delle comunicazioni dei rifiuti dei PdV: prevista PEC (par. 7.4) Riferimento alla versione 2015 della ISO 9001 (par. 8.4)	

SOMMARIO

1 SCOPO E AMBITO DEL DOCUMENTO 6
1.1 Contesto di riferimento 7
1.2 Processo di affidamento del servizio di Conservazione del Responsabile della Conservazione 7
2 TERMINOLOGIA (GLOSSARIO, ACRONIMI) 8
3 NORMATIVA E STANDARD DI RIFERIMENTO 11
3.1 Normativa di riferimento 11
3.2 Standard di riferimento 12
4 RUOLI E RESPONSABILITÀ 13
4.1 Responsabile della Conservazione 17
4.2 Team Privacy 17
4.3 Registro delle cariche 19
5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE 20
5.1 Organigramma 20
5.2 Strutture organizzative 21
5.3 Attivazione del servizio di Conservazione 22
6 OGGETTI SOTTOPOSTI A CONSERVAZIONE 23
6.1 Oggetti conservati 23
6.2 Pacchetto di versamento (PdV) 31
6.3 Pacchetto di archiviazione (PdA) 32
6.4 Pacchetto di distribuzione (PdD) 40
7 IL PROCESSO DI CONSERVAZIONE 41
7.1 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico 43
7.1.1 Copie informatiche di documenti analogici originali anche unici 44
7.1.2 Aggiunta opzionale di una marca temporale detached 45
7.2 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti 45
7.2.1 Gestione dei virus 46
7.3 Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico 47
7.4 Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie 47
7.5 Preparazione e gestione del pacchetto di archiviazione 48
7.6 Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione 48
7.7 Produzione di duplicati e copie informatiche 49
7.7.1 Duplicati informatici 49
7.7.2 Copie informatiche 49
7.8 Scarto dei pacchetti di archiviazione 50
7.9 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori 50
7.10 Procedura di distruzione dei PdV dal Sistema eWitness 51
8 IL SISTEMA DI CONSERVAZIONE 53
8.1 Componenti Logiche 53
8.2 Componenti Tecnologiche 54

8.3 Componenti Fisiche 54
8.4 Procedure di gestione 55
8.5 Procedure di evoluzione e change management 56
9 MONITORAGGIO E CONTROLLI 57
9.1 Procedure di monitoraggio 57
9.2 Verifica dell'integrità degli archivi 58
9.3 Soluzioni adottate in caso di anomalie 59

1 SCOPO E AMBITO DEL DOCUMENTO

Il presente Manuale descrive, dal punto di vista organizzativo, tecnico ed operativo, il *sistema di conservazione* dei documenti informatici che la società eWitness Italia s.r.l. (di seguito anche solo eWitness) ha realizzato, gestisce e controlla al fine di realizzare un servizio di Conservazione a norma in favore dei propri clienti.

Il presente Manuale, in particolare:

a) individua il modello organizzativo definito da eWitness per il *sistema di conservazione*;
b) definisce le competenze, i ruoli e le responsabilità degli attori coinvolti nel processo di conservazione dei documenti;
c) elenca le 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;
d) illustra le procedure atte ad assicurare la conservazione dei documenti informatici prodotti e ricevuti dai singoli clienti, nonché dei fascicoli informatici, garantendone le caratteristiche di **autenticità, integrità, affidabilità, leggibilità e reperibilità**;
e) descrive il trattamento dell'intero ciclo di gestione dell'oggetto conservato nell'ambito del processo di conservazione;
f) descrive le modalità di accesso ai documenti e ai fascicoli conservati, per il periodo prescritto dalla norma, indipendentemente dall'evolversi del contesto tecnologico e la modalità di svolgimento del processo di esibizione e di esportazione dal *sistema di conservazione* con la produzione del **pacchetto di distribuzione**;
g) definisce le 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;
h) precisa le procedure per la produzione di *duplicati* o *copie* ai sensi del D.lgs. n. 82/2005 e s.m.i. (Codice dell'Amministrazione Digitale – di seguito anche solo CAD);
i) indica i tempi entro i quali le diverse tipologie di documenti devono essere scartate ovvero trasferite in conservazione, ove, nel caso delle pubbliche amministrazioni, non già presenti nel manuale di gestione.

Il presente Manuale recepisce appieno le disposizioni contenute nel CAD, oltre alle ulteriori norme e indicazioni riportate nei provvedimenti di legge o di prassi, anche amministrativa, richiamati nel capitolo "*normativa e standard di riferimento*".

Il presente Manuale è reso pubblico in formato PDF firmato digitalmente dal legale rappresentante di eWitness.

Il Cliente, in qualità di Titolare nonché Responsabile della conservazione (cfr. §4.1):

- è tenuto a consultare con la massima diligenza e attenzione il presente Manuale

predisposto da eWitness;

- approva facendo propri i contenuti del presente Manuale.

Torna al sommario

1.1 Contesto di riferimento

Il servizio di Conservazione erogato in outsourcing è supportato dall'articolo 44 del CAD in base al quale la conservazione può essere svolta affidandola, in modo totale o parziale, ad altri soggetti, pubblici o privati che offrono idonee garanzie organizzative e tecnologiche, anche accreditati come conservatori presso l'Agenzia per l'Italia digitale.

I clienti che ne hanno necessità affidano a eWitness la conservazione dei loro documenti secondo il modello organizzativo previsto dall'art 5 comma 2 lett. b) del DPCM 3 dicembre 2013 recante le regole tecniche in materia di sistema di conservazione.

Torna al sommario

1.2 Processo di affidamento del servizio di Conservazione del Responsabile della Conservazione

Ai sensi di quanto previsto dall'articolo 6 comma 7 del DPCM 3 dicembre 2013, la conservazione sarà affidata a eWitness attraverso un apposito contratto nel quale sarà previsto l'obbligo del rispetto del manuale della conservazione predisposto dal responsabile della stessa. In seguito a tale affidamento eWitness assumerà il ruolo di responsabile esterno del trattamento dei dati personali ai sensi dell'art. 28 del Regolamento UE 679/2016 (GDPR).

Torna al sommario

2 TERMINOLOGIA (GLOSSARIO, ACRONIMI)

In riferimento alla terminologia utilizzata nel presente Manuale si richiama integralmente il Glossario contenuto nell'allegato 1 alle Regole tecniche in tema di conservazione di cui al DPCM 3 dicembre 2013 e sue successive modifiche e/o integrazioni.

Si riportano, in ogni caso, le seguenti definizioni utili alla lettura e comprensione del presente Manuale.

Cliente: è il Titolare, unico e legittimo proprietario degli oggetti, dati, documenti inviati al sistema di conservazione; è, inoltre, il soggetto giuridicamente titolato alla sottoscrizione e accettazione del Contratto per l'affidamento in outsourcing del servizio di Conservazione digitale di documenti informatici;

Codice o CAD: decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni;

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 presente Manuale;

Contratto: è il documento per l'affidamento del servizio di Conservazione digitale di documenti informatici, sottoscritto da eWitness e il Cliente. Il Contratto regola gli aspetti generali dell'erogazione del servizio di Conservazione digitale dei documenti informatici di proprietà del Cliente;

Copia informatica di documento analogico: il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto;

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;

Documento analogico: la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti;

Documento analogico originale: 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 analogico originale unico: è quel documento analogico il cui contenuto non può essere desunto da altre scritture o documenti di cui sia obbligatoria la tenuta e che non presenta nessuna delle condizioni elencate precedente definizione;

Documento informatico: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;

Duplicato Informatico: documento informatico ottenuto mediante la memorizzazione, sullo stesso supporto o su supporti diversi, della medesima sequenza di valori binari del documento

originario;

Firma digitale: un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;

IdPdV: Indice del Pacchetto di Versamento;

Impronta: la sequenza di simboli binari di lunghezza predefinita generata mediante l'applicazione alla prima di un'opportuna funzione di hash;

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 stessi;

Marca temporale: evidenza informatica che consente di rendere opponibile a terzi un riferimento temporale; la marca temporale prova l'esistenza in un certo momento di una determinata informazione, sotto forma di struttura dati firmata da una Time Stamping Authority;

Metadati: insieme di dati associati a un documento informatico, o a un fascicolo informatico, o a 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;

Documenti analogici originali non unici: i documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi;

Pacchetto di archiviazione (PdA): pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche e le modalità riportate nel presente Manuale;

Pacchetto di distribuzione (PdD): pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta;

Pacchetto di versamento (PdV): pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel presente Manuale;

Pacchetto informativo: contenitore che racchiude uno o più oggetti da conservare, oppure anche i soli metadati riferiti agli oggetti da conservare;

Processo di conservazione: insieme delle attività finalizzate alla conservazione dei documenti informatici;

Produttore: persona fisica o giuridica responsabile del contenuto del PdV;

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che tratta dati personali per conto del titolare del trattamento;

Sistema di conservazione: insieme di hardware, software, politiche, procedure, linee guida, regolamenti, infrastrutture fisiche, logiche e organizzative, volto ad assicurare la conservazione elettronica dei documenti informatici del Cliente, per il periodo di tempo specificato nel Contratto;

Titolare del trattamento: persona fisica, giuridica, pubblica amministrazione o qualsiasi altro ente cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

Utente: è il soggetto che richiede al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge.

Per ogni altra definizione si fa riferimento al glossario contenuto nell'allegato 1 alle regole tecniche di cui all'art 71 del CAD in materia di documento informatico e sistema di conservazione dei documenti informatici.

Nella seguente tabella si riportano gli acronimi relativi alle funzioni aziendali definite nel presente documento:

Ruolo	**Acronimo**
Responsabile della Conservazione	RdC
Responsabile del Servizio di Conservazione	RSC
Responsabile della Sicurezza dei Sistemi per la Conservazione	RSSI
Responsabile della Funzione Archivistica di Conservazione	RFA
Responsabile del Trattamento Dati Personali	RTD
Responsabile della Protezione dei Dati	DPO
Responsabile dei Sistemi Informativi per la Conservazione	RSI
Responsabile dello Sviluppo e della Manutenzione del Sistema di Conservazione	RSM

Torna al sommario

3 NORMATIVA E STANDARD DI RIFERIMENTO

3.1 Normativa di riferimento

Di seguito viene individuata la principale normativa di riferimento per l'attività di conservazione a livello nazionale, nei luoghi dove sono conservati i documenti e quella specifica relativa alle diverse tipologie di documenti riguardanti i servizi di conservazione erogati da eWitness in favore dei propri clienti.

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

- Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- D.lgs. del 20/02/04 n.52 - attuazione della direttiva 2001/115/CE che semplifica ed armonizza le modalità di fatturazione in materia di IVA. Deve essere integrato con la specifica circolare dell'Agenzia delle Entrate (45/E del 2005);
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Deliberazione Cnipa del 21 maggio 2009, n. 45 (come modificata dalla determinazione dirigenziale DigitPA n. 69/2010). Regole per la creazione dei certificati di firma e di marca che quelle per il loro utilizzo, riconoscimento e verifica;
- 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;

- Regolamento (UE) n. 910/2014 - Regolamento europeo per l'identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (abbreviato in eIDAS, acronimo di electronic IDentification, Authentication and trust Services);
- 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;
- Regolamento UE 2016/679 e successivo Decreto n.101/18 del 10 agosto 2018 (GDPR - General Data Protection Regulation).

Torna al sommario

3.2 Standard di riferimento

Nella predisposizione del proprio sistema di conservazione eWitness ha adeguato le proprie infrastrutture, i propri processi e le proprie procedure agli standard elencati nell'allegato 3 del DPCM 3 Dicembre 2013 (Regole Tecniche in materia di Sistema di conservazione) con indicazione delle versioni aggiornate al giorno 1ottobre 2014 e di seguito riportati:

- 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

Di seguito sono indicate le attività svolte e i nominativi delle persone che ricoprono i ruoli principali – come specificati nel documento "*Profili professionali*" reso disponibile da AgID – all'interno dell'organizzazione deputata alla gestione del sistema di conservazione realizzato da eWitness.

Ruolo: Responsabile del Servizio di Conservazione (RSC)	
Nominativo	Notaio Riccardo Genghini
Attività di competenza	• Definizione e attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione • Definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente • Corretta erogazione del servizio di Conservazione all'ente produttore • Gestione delle convenzioni, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione. • Gestione dell'esercizio delle componenti software del sistema di conservazione
Periodo nel ruolo	Dal 2006 ad oggi
Eventuali deleghe	Nessuna
Rapporto con eWitness	Componente CdA

Ruolo: Responsabile della Sicurezza dei Sistemi per la Conservazione (RSSI)	
Nominativo	Dott. Ing. Stefano Tazzi
Attività di competenza	• Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza. • Segnalazione delle eventuali difformità al Responsabile del servizio di Conservazione e individuazione e pianificazione delle necessarie azioni correttive.
Periodo nel ruolo	Da marzo 2016 ad oggi
Eventuali deleghe	Nessuna
Rapporto con eWitness	Libero professionista con mandato professionale triennale
Ruolo: Responsabile della Funzione Archivistica di Conservazione (RFA)	
Nominativo	Notaio Riccardo Genghini
Attività di competenza	• 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. • Definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici. • Monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione. • Collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.
Periodo nel ruolo	Dal 2006 ad oggi
Eventuali deleghe	Nessuna
Rapporto con eWitness	Componente CdA

Ruolo: Responsabile del Trattamento Dati Personali (RTD)	
Nominativo	Notaio Riccardo Genghini
Attività di competenza	• Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali. • Garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.
Periodo nel ruolo	Dal 2006 ad oggi
Eventuali deleghe	Nessuna
Rapporto con eWitness	Componente CdA
Ruolo: Responsabile della Protezione dei Dati (DPO)	
Nominativo	Avv. Andrea Lisi
Attività di competenza	• informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati; • sorvegliare l'osservanza del GDPR e di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; • fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35; • cooperare con l'autorità di controllo; • fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.
Periodo nel ruolo	Dal 2018 ad oggi
Eventuali deleghe	Nessuna
Rapporto con eWitness	Consulente esterno

Ruolo: Responsabile dei Sistemi Informativi per la Conservazione (RSI)	
Nominativo	Sig. Simone Diodati
Attività di competenza	• Gestione dell'esercizio delle componenti hardware del sistema di conservazione. • Monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore. • Segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di Conservazione e individuazione e pianificazione delle necessarie azioni correttive. • Pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione • Controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di Conservazione.
Periodo nel ruolo	Da agosto 2016 ad oggi.
Eventuali deleghe	Nessuna
Rapporto con eWitness	Dipendente tempo indeterminato
Ruolo: Responsabile dello Sviluppo e della Manutenzione del Sistema di Conservazione (RSM)	
Nominativo	Ing. Stefano Tazzi
Attività di competenza	• Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione. • Pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione. • Monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione. • Interfaccia con l'ente produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche. • Gestione dello sviluppo di siti web e portali connessi al servizio di Conservazione.
Periodo nel ruolo	Da agosto 2016 ad oggi
Eventuali deleghe	Nessuna
Rapporto con eWitness	Libero professionista con mandato professionale triennale

Torna al sommario

4.1 Responsabile della Conservazione

Il Responsabile della Conservazione è il Cliente - nella persona fisica formalmente nominata all'interno dell'Azienda titolare dei documenti oggetto di conservazione - quale responsabile dell'insieme delle attività finalizzate alla conservazione a norma dei documenti informatici nell'ambito del contratto di outsourcing verso eWitness.

In qualità di Titolare dei documenti informatici oggetto di conservazione, il Cliente, attraverso il proprio RdC, definisce e attua le politiche complessive del sistema di conservazione governandone quindi la gestione con piena responsabilità e autonomia, in relazione al modello organizzativo esplicitato nel Manuale della Conservazione. Tale Manuale verrà condiviso con il conservatore eWitness che nelle "*CONDIZIONI GENERALI PER LA FORNITURA DI SERVIZI ED INFRASTRUTTURE TECNOLOGICHE PER LA CONSERVAZIONE A NORMA*" si impegnerà a rispettarlo.

Il RdC, all'interno della propria organizzazione aziendale, opera d'intesa con il Responsabile esterno del trattamento dei dati personali, con il Responsabile della sicurezza e con il Responsabile dei sistemi informativi oltre che con il Responsabile della funzione archivistica di conservazione.

Pertanto, ai fini del presente Manuale, i ruoli di Titolare e di Responsabile della Conservazione sono ricoperti dal Cliente, mentre i ruoli di Responsabile del servizio di Conservazione, Produttore e Responsabile esterno del trattamento dei dati sono ricoperti da eWitness.

Torna al sommario

4.2 Team Privacy

Con l'introduzione del GDPR la gestione dei dati personali (privacy) e, più in generale, la gestione della protezione dei dati richiede un approccio multidisciplinare. A tal proposito, è costituito in eWitness un Team Privacy che opera di concerto con il Responsabile della Protezione dei Dati e con il Responsabile del Trattamento dei Dati Personali.

Il Team Privacy e di seguito descritto.

Team Privacy	
Nominativi	Eleonora Giardino Stefano Tazzi Patrizia Sormani Valentina Folli
Attività di competenza	Eleonora Giardino: qualora la società sia Titolare del trattamento è responsabile della gestione dei dati verso i dipendenti. Stefano Tazzi: qualora la società è Responsabile esterno o altro responsabile – è responsabile dell'implementazione di tutte le policy e di tutte le procedure per essere conformi al GDPR. Patrizia Sormani: sia in caso di Titolare che di Responsabile esterno o altro responsabile, è responsabile del rispetto della conformità prevista dalla normativa vigente. Valentina Folli: sia in caso di Titolare che di Responsabile esterno o altro responsabile è responsabile dell'approntamento di tutta la documentazione necessaria nonché è responsabile della gestione del sito aziendale e dei suoi contenuti in armonia alle previsioni legislative.
Periodo nel ruolo	Dal 2018 ad oggi
Eventuali deleghe	Nessuna
Rapporto con eWitness	Eleonora Giardino – Amministratore Delegato Stefano Tazzi – Libero Professionista con mandato professionale triennale Patrizia Sormani – Componente CdA Valentina Folli – Dipendente tempo indeterminato

Torna al sommario

4.3 Registro delle cariche

Cariche	Nominativo	Periodo	Versione del manuale
Responsabile del Servizio di Conservazione (RSC)	Riccardo Genghini	Dal 2006 ad oggi	Dalla versione 1.0 alla versione 2.2
Responsabile Sicurezza dei Sistemi per la Conservazione (RSSI)	Michele Brusoni	Dal 2010, con nomina del 4/03/2015, fino ad Agosto 2016	Dalla versione 1.0 alla versione 2.0
	Stefano Tazzi	Da agosto 2016, con nomina di marzo 2016 fino ad oggi	Dalla versione 2.1 alla versione 2.2
Responsabile della Funzione Archivista di Conservazione (RFA)	Riccardo Genghini	Dal 2006 ad oggi	Dalla versione 1.0 alla versione 2.2
Ruolo Responsabile del Trattamento dei Dati Personali (RTD)	Riccardo Genghini	Dal 2006 ad oggi	Dalla versione 1.0 alla versione 2.2
Responsabile dei Sistemi Informativi per la Conservazione (RSI)	Andrea Fumagalli	Dal 2009, con nomina del 4/03/2015 fino ad agosto 2016	Dalla versione 1.0 alla versione 2.0
	Simone Diodati	Da agosto 2016 ad oggi	Dalla versione 2.1 alla versione 2.2
Responsabile dello Sviluppo e della Manutenzione del Sistema di Conservazione (RSM)	Andrea Fumagalli	Dal 2009, con nomina del 4/03/2015 fino ad agosto 2016	Dalla versione 1.0 alla versione 2.0
	Stefano Tazzi	Da agosto 2016 fino ad oggi	Dalla versione 2.1 alla versione 2.2
Ruolo Responsabile della Protezione dei Dati	Andrea Lisi	Dal 2018 fino ad oggi	Dalla versione 2.2

Torna al sommario

5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Organigramma

Il Cliente affida in outsourcing il servizio di Conservazione a eWitness che assume il ruolo di Conservatore. Sarà onere del Conservatore svolgere tutte le attività necessarie alla corretta conservazione dei documenti informatici ad esso affidati così come previste dalle regole tecniche di cui al DPCM del 3 dicembre 2013 e dagli standard tecnici ivi richiamati. In particolare il conservatore curerà la corretta esecuzione delle attività ad esso delegate dal Cliente che gli affida la conservazione dei propri documenti informatici. All'interno del servizio di Conservazione eWitness, il Responsabile del servizio di Conservazione è sempre un Notaio Pubblico Ufficiale. Tutti i soggetti coinvolti nel servizio di Conservazione sono stati incaricati al trattamento dei dati per l'attività di conservazione.

Di seguito riporta l'organigramma della struttura organizzativa coinvolta nel servizio di Conservazione:

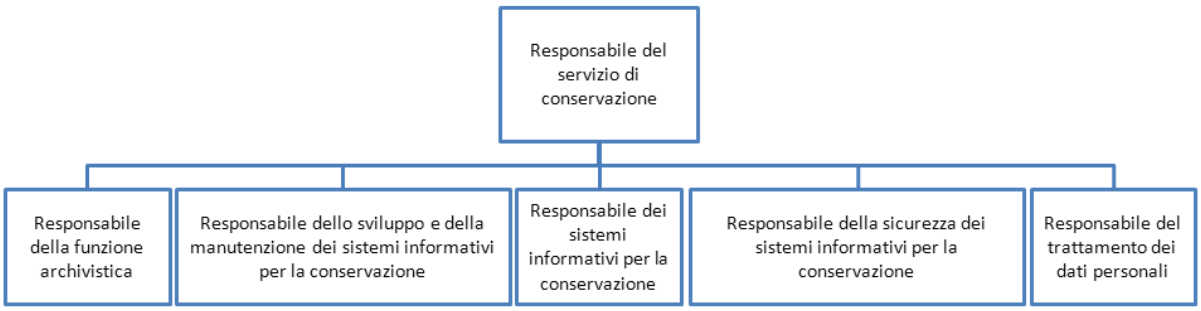


Figura 1- Organigramma struttura organizzativa eWitness Italia s.r.l.

Torna al sommario

5.2 Strutture organizzative

Nel presente paragrafo vengono descritte in modo schematico le fasi del processo di conservazione, le attività di gestione dei sistemi informativi con i relativi soggetti responsabili.

Attività proprie di ciascun soggetto coinvolto nel servizio di Conservazione			
Stato	**Attività**	**Descrizione**	**Responsabile**
1	Attivazione del servizio di Conservazione (a seguito della sottoscrizione del contratto).	Il Cliente richiede al Conservatore l'attivazione del servizio, mediante la contrattualizzazione dell'attività in outsourcing.	• RdC • RTD • RFA • RSM • RSC
2	Acquisizione, verifica e gestione dei Pacchetti di versamento e generazione del Rapporto di versamento.	Sui PdV vengono effettuate verifiche circa l'identificazione certa del soggetto, la firma digitale, formati e metadati. In caso di verifiche andate a buon fine viene generato il RdV, altrimenti viene generata la Comunicazione delle anomalie.	• RFA • RSC
3	Preparazione e gestione dei Pacchetti di archiviazione.	Gli oggetti versati vengono trasformati in PdA, i quali dovranno contenere, oltre agli oggetti da conservare, l'IdPA formato secondo le regole dello standard SInCRO. L'IdPA viene sottoscritto con firma digitale dal RdC e viene marcato temporalmente.	• RFA • RTD • RSC
4	Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta.	I PdD, vengono creati in base alle richieste del Cliente. Possono esibiti mediante web service (caso non standard, per procedure automatizzate e per PdA di piccola dimensione), tramite memorizzazione su supporto ottico non riscrivibile o tramite memorizzazione su supporto mobile riscrivibile.	• RFA • RTD • RSC
6	Conduzione e manutenzione del sistema di conservazione.	Le attività di manutenzione vengono svolte sia sui processi che sulle strutture hardware e software. Quotidianamente vengono verificate le attività sulle infrastrutture, oltre a una pianificazione delle eventuali procedure straordinarie	• RSM • RSSI

		per il caso di anomalie.	
7	Monitoraggio del sistema di conservazione.	Monitoraggio del sistema di Log per la registrazione degli accessi e degli eventi. Vengono anche monitorate le attività di verifica dell'integrità degli archivi e la gestione delle anomalie.	• RdC • RFA • RSSI • RSC
8	Change management.	Sono definite le politiche, le priorità e le tempistiche di adeguamento all'evoluzione tecnologica per far sì che il sistema di conservazione garantisca nel tempo l'integrità, la disponibilità e la sicurezza del sistema medesimo.	• RFA • RSI
9	Verifica periodica di conformità a normativa e standard di riferimento.	La conformità all'evoluzione normativa e agli standard in materia di conservazione di lungo periodo, è costantemente monitorata ed eventualmente aggiornata grazie al lavoro di supervisione svolto dal RdC.	• RdC • RSSI • RSC

Torna al sommario

5.3 Attivazione del servizio di Conservazione

Per l'attivazione del servizio di Conservazione sono state definite le seguenti attività:

a) individuazione e definizione delle classi documentali da inviare in conservazione;
b) definizione dei dati o attributi specifici da correlare a ciascuna classe documentale;
c) definizione, controllo e verifica degli strumenti software di visualizzazione, delle versioni e dei formati dei documenti;
d) definizione dei tempi di conservazione;
e) definizione dell'anagrafica dei documenti ossia dell'area organizzativa e dell'ufficio proprietario dei documenti da inviare in conservazione;
f) definizione della periodicità di invio dei documenti al sistema di conservazione ossia definizione dell'intervallo di tempo intercorrente fra due distinte prese in carico dei documenti da parte del sistema di conservazione;
g) definizione dell'intervallo di tempo intercorrente tra la presa in carico e la chiusura del pacchetto (la chiusura di un pacchetto rappresenta l'attività conclusiva del processo di conservazione al termine del quale può essere effettuata l'esibizione dei documenti);
h) definizione operativa per il consolidamento dei documenti (marcatura temporale);
i) definizione operativa per la gestione dei documenti per i quali i certificati di firma risultano non validi o scaduti.

Torna al sommario

6 OGGETTI SOTTOPOSTI A CONSERVAZIONE

Attraverso il sistema di conservazione realizzato da eWitness sarà possibile conservare sia documenti informatici che documenti amministrativi informatici unitamente ai metadati ad essi associati di cui all'allegato 5 delle Regole tecniche. Il sistema, inoltre, è in grado di conservare anche i fascicoli informatici ovvero le aggregazioni documentali informatiche con i metadati ad essi associati e contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che appartengono al fascicolo o all'aggregazione documentale.

Il sistema di conservazione, in attuazione di quanto previsto dall'art. 44, comma 1, del CAD, assicura la conservazione dei suddetti oggetti conservati dalla presa in carico fino all'eventuale scarto, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità.

Gli oggetti della conservazione sono trattati dal sistema di conservazione in **pacchetti informativi** ai sensi di quanto previsto dall'articolo 4 delle Regole tecniche[1] e dalle relative specifiche tecniche ivi allegate.

Torna al sommario

6.1 Oggetti conservati

Nel presente paragrafo sono elencate le tipologie relative ai soli documenti informatici a rilevanza tributaria e sottoposti al servizio di Conservazione eWitness. Tale elenco, da ritenersi esemplificativo e non tassativo, non tiene conto delle ulteriori specifiche tipologie concordate e contrattualizzate con il Cliente, ivi compresa l'acquisizione di documenti analogici originali anche unici.

[1] I pacchetti informativi sono distinti in:
a) pacchetti di versamento;
b) pacchetti di archiviazione;
c) pacchetti di distribuzione.

Tipologia documentale conservata: Fatture emesse	
Descrizione	Fatture di vendita: Documentazione a rilevanza tributaria emessa da soggetti IVA
Periodicità di invio in conservazione	Annuale. L'invio in conservazione deve avvenire entro tre mesi dal termine di presentazione della dichiarazione dei redditi
Periodo di durata della conservazione	Dieci anni
Formato dei file previsti	Tutti i formati previsti
Riferimenti normativi	• Circolare n. 45/2005 dell'Agenzia delle Entrate • Legge 24 dicembre 2007, n. 244 • Decreto 7 marzo 2008 del Ministero dell'Economia e delle Finanze • Direttiva UE 45/2010 • Legge di stabilità 2013 • DPCM 22 febbraio 2013 • Decreto 3 aprile 2013, n. 55 del Ministero dell'Economia e delle Finanze • DPCM 3 dicembre 2013 • Circolare 31 marzo 2014, n. 1 del Ministero dell'Economia e delle Finanze • Decreto legge 24 aprile 2014, n. 66 • Decreto 17 giugno 2014 del Ministero dell'Economia e delle Finanze • Circolare n. 18e/2014 dell'Agenzia delle Entrate • Circolare n. 1, 9 marzo 2015 del Ministero dell'Economia e delle Finanze

Tipologia documentale conservata: Fatture ricevute	
Descrizione	Fatture di acquisto - Documentazione a rilevanza tributaria ricevuta da soggetti passivi d'imposta
Periodicità di invio in conservazione	Annuale. L'invio in conservazione deve avvenire entro tre mesi dal termine di presentazione della dichiarazione dei redditi
Periodo di durata della conservazione	Dieci anni
Formato dei file previsti	Tutti i formati previsti
Riferimenti normativi	• Circolare n. 45/2005 dell'Agenzia delle Entrate • Legge 24 dicembre 2007, n. 244 • Decreto 7 marzo 2008 del Ministero dell'Economia e delle Finanze • Direttiva UE 45/2010 • Legge di stabilità 2013 • DPCM 22 febbraio 2013 • Decreto 3 aprile 2013, n. 55 del Ministero dell'Economia e delle Finanze • DPCM 3 dicembre 2013 • Circolare 31 marzo 2014, n. 1 del Ministero dell'Economia e delle Finanze • Decreto legge 24 aprile 2014, n. 66 • Decreto 17 giugno 2014 del Ministero dell'Economia e delle Finanze • Circolare n. 18e/2014 dell'Agenzia delle Entrate • Circolare n. 1, 9 marzo 2015 del Ministero dell'Economia e delle Finanze

Tipologia documentale conservata: Ricevute e notifiche SdI	
Descrizione	Messaggi e notifiche di esito che il Sistema di Interscambio (SdI), gestito dall'Agenzia delle Entrate (AE) invia al trasmittente delle fatture
Periodicità di invio in conservazione	Annuale. L'invio in conservazione avviene contestualmente alla conservazione della fattura a cui si riferiscono
Periodo di durata della conservazione	Dieci anni
Formato del file	Formato XML
Riferimenti normativi	• Circolare n. 45/2005 dell'Agenzia delle Entrate • Legge 24 dicembre 2007, n. 244 • Decreto 7 marzo 2008 del Ministero dell'Economia e delle Finanze • Direttiva UE 45/2010 • Legge di stabilità 2013 • DPCM 22 febbraio 2013 • Decreto 3 aprile 2013, n. 55 del Ministero dell'Economia e delle Finanze • DPCM 3 dicembre 2013 • Circolare 31 marzo 2014, n. 1 del Ministero dell'Economia e delle Finanze • Decreto legge 24 aprile 2014, n. 66 • Decreto 17 giugno 2014 del Ministero dell'Economia e delle Finanze • Circolare n. 18e/2014 dell'Agenzia delle Entrate • Circolare n. 1, 9 marzo 2015 del Ministero dell'Economia e delle Finanze

<table>
<tr><th colspan="3">Tipologia documentale conservata: Libri e registri contabili</th></tr>
<tr><td>Descrizione</td><td colspan="2">Documentazione a rilevanza tributaria richiesta dalla norma codicistica e dalla natura e dimensione dell’impresa per la corretta tenuta della contabilità
Libro Giornale
Libro Inventari
Libro Mastro
Registro Cronologico
Libro Cespiti
Registro Irpef
Registro Fatture Acquisto
Registro Acquisti Agenzie Viaggio
Registro Fatture Emesse
Registro Fatture In Sospeso
Registro Corrispettivi
Giornale Fondo
Registro Riepilogativo Iva
Registro Sezionale Iva Acquisiti Intra Ue
Registro Acquisti Intra Ue Non Comm
Registro Trasferimenti Intra Ue
Registro Dich Intenti Emesse
Registro Dich Intenti Ricevute
Registro Omaggi
Registro Memoria Prod Contrassegno
Registro Lavorazione Prod Contrassegno
Registro Carico Prod Contrassegno
Registro Scarico Centri Elab Dati
Registro Somme Ricevute Deposito
Registro Editori</td><td>Registro Corrispettivi Agenzie Viaggio
Registro Emergenza Iva
Bollettario
Registro Prima Nota
Registro Unico Iva
Altri Registri
Registro Scarico Prod Contrassegno
Registro Beni In Deposito
Registro Beni In Conto Lavorazione
Registro Beni Comodato
Registro Beni Prova
Registro Sezionale Iva Interno
Registro Carico Stampati Fiscali
Registro Soc Controllanti Controllate
Registro Carico Scarico Regime Margine Metodo Analitico
Registro Acquisti Regime Margine Metodo Globale
Registro Vendite Regime Margine Metodo Globale
Registro Carico Centri Elab Dati</td></tr>
<tr><td>Periodicità di invio in conservazione</td><td colspan="2">Annuale. L’invio in conservazione deve avvenire entro tre mesi dal termine di presentazione della dichiarazione dei redditi</td></tr>
<tr><td>Periodo di durata della conservazione</td><td colspan="2">Dieci anni</td></tr>
<tr><td>Formato dei file previsti</td><td colspan="2">Tutti i formati previsti</td></tr>
<tr><td>Riferimenti normativi</td><td colspan="2">Art. 2214 c.c.
Art. 2215 c.c.
Art. 2215-bis c.c.
Art. 2216 c.c.
Art. 2217 c.c.
Art. 2219 c.c.
Art. 2220 c.c.
Art. 2423 c.c.
Art. 2709 c.c.
Art. 2711 c.c.</td></tr>
</table>

Tipologia documentale conservata: Libri sociali	
Descrizione	• Documentazione obbligatoria per norma codicistica attestante la vita sociale dell'impresa • Libro Soci • Libro Obbligazioni • Libro Adunanze Deliberazioni Assemblee • Libro Adunanze Deliberazioni Consiglio Amministrazione • Libro Adunanze Deliberazioni Collegio Sindacale • Libro Adunanze Deliberazioni Comitato Esecutivo • Libro Adunanze Deliberazioni Assemblee Azionisti • Altri Libri Sociali
Periodicità di invio in conservazione	Annuale
Periodo di durata della conservazione	Dieci anni
Formati dei file permessi	Tutti i formati previsti
Riferimenti normativi	• Art. 2214 c.c. • Art. 2421 c.c. • Art. 2447-ter c.c. • Art 2447-sexies c.c.

Tipologia documentale conservata: Dichiarazioni fiscali	
Descrizione	• Anagrafe dei rapporti • Anagrafe tributaria rapporti • Beni in godimento ai soci • Contratti di locazione • Certificazione Unica • Codice fiscale e tessera sanitaria (Modello AA4/8, modello AA5/6) • Cessioni quote • Comunicazione per chiedere l'iscrizione nell'anagrafe unica delle Onlus • Comunicazione annuale dati IVA • Comunicazione anagrafe tributaria • Comunicazione opzione IRAP • Comunicazione strutture sanitarie • Comunicazione da parte di enti associativi (modello Eas) • Comunicazione per la ricezione dei modelli 730-4 • Comunicazione - Operazioni con paesi blacklist • Comunicazione polivalente (spesometro) • Dichiarazione IVA • Dichiarazione dell'imposta di bollo assolta in modo virtuale • Deleghe INPS, MOD. 730, altre deleghe fiscali • INTRASTAT • Iscrizione elenco cinque per mille (istanza per chiedere il beneficio) • Istanza IPEC • Istanza rimborso IRPEF - IRES • Istanza rimborso tassa unità da riporto • Modello DSU-ISEE • Modello 730 • Modello 770 • Modello Unico PF • Modello Unico SP • Modello Unico SC • Modello Unico enti non commerciali • Modello IRAP (PF, SP e SC) • Modello Intrastat • Modello Consolidato Nazionale e Mondiale • Modello F24 • Modello RED • Modelli Invalidi Civili (ICRIC, ICLAV o ACCAS/PS) • Partita Iva (Modello AA9/11, modello AA7/10, Modello ANR/3) • Questionari studi di settore • Richiesta di accesso alla procedura di collaborazione volontaria • Rimborsi (Accredito, rimborso trimestrale Iva, rimborsi Ue • Oggetti residenti e non, rimborso Irap, ecc.)
Periodicità di invio in conservazione	Annuale
Periodo di durata della conservazione	Dieci anni
Formati dei file permessi	Tutti i formati previsti

Tipologia documentale conservata: Messaggi ed evidenze di Posta Elettronica Certificata (PEC)	
Descrizione	Documentazione attestante il corretto invio e ricezione di messaggi di posta elettronica certificata
Periodicità di invio in conservazione	Annuale
Periodo di durata della conservazione	Dieci
Formati dei file permessi	Formato EML
Riferimenti normativi	• DPR 11 febbraio 2005, n. 31 • D. Lgs. 7 marzo 2005, n. 82 • DM 2 novembre 2005 • Circolare CNIPA CR/49 24 novembre 2005 • Legge 28 gennaio 2009, n. 2 • DPCM 6 maggio 2009

I periodi di conservazione indicati potrebbero, su richiesta del Responsabile della Conservazione, essere prorogati. Ciò potrebbe accadere, ad esempio, in caso di accertamento fiscale in corso o di contenzioso avente ad oggetto i documenti conservati o fatti in essi richiamati.

Il sistema di conservazione eWitness accetta i seguenti formati:

- Formato PDF e PDF/A (estensione .pdf) MIME type: application/pdf
  Visualizzatore: Adobe Reader
  Proprietario/Produttore: Adobe Systems
  Standard: ISO32000-1, ISO 19005-1:2005 (vers. PDF 1.4), ISO 19005-2:2011 (vers. PDF 1.7)

- Formato TIFF (estensione .tiff o .tif)
  MIME type: image/tiff
  Visualizzatore: Imagemagick o altri visualizzatori immagini

- Formato XML (estensione .xml) MIME type: application/xml o text/xml
  Proprietario/Produttore: W3C
  Visualizzatore: Editor testuali

- Formato TXT (estensioni varie) MIME type: application/text

Visualizzatore: Editor testuali

- Formato firma digitale CAdES (estensione .p7m) MIME type: application/pkcs7-mime
  Visualizzatore: Software di firma digitale
  Standard: ETSI TS 101 733 Electronic Signature and Infrastructure (ESI) – CMS Advanced Electronic Signature (CAdES)

- Formato EML (estensione .eml) MIME type: message/rfc822
  Standard: RFC2822
  Visualizzatore: Software per la gestione posta elttrovnica (es. Mozilla Thunderbird)

Torna al sommario

6.2 Pacchetto di versamento (PdV)

I documenti acquisiti massivamente dal sistema di conservazione, a prescindere dalla loro tipologia, vanno a formare un pacchetto di versamento giornaliero suddiviso per Produttore. L'attività di acquisizione avviene tramite protocollo FTP o tramite web service su canale VPN (IPSec o SSL) con autenticazione mediante certificati X509.

Durante la fase di acquisizione del dato vengono rilevate e/o calcolate le grandezze informatiche tra cui l'hash del documento, il riferimento temporale del momento di acquisizione, il nome e la dimensione del file ricevuto. Tali grandezze informatiche andranno a costituire, alla mezzanotte di ogni giorno, l'Indice dei pacchetti di versamento (IPdV) relativo ad un singolo Produttore e alla giornata lavorativa precedente. L'IPdV è costituito da un file XML.

L'indice dei pacchetti di versamento (IPdV) è identificato in modo univoco secondo la seguente naming convention prestabilita (per canale FTP e web service, rispettivamente):

yyyy-MM-dd#DAILY-LOG-FTP-NOTARY-CUSTOMER.xml

yyyy-MM-dd#DAILY-LOG-WS-NOTARY-CUSTOMER.xml

Una nota di convenzione: NOTARY è il nome del notaio cui il Daily Log fa riferimento; CUSTOMER è il codice cliente.

Di seguito è riportata la struttura e la definizione dell'IPdV:

- è presente una testata che contiene la versione del IPdV, il canale di accesso cui l'IPdV fa riferimento e il nome del notaio responsabile del servizio di conservazione;

seguono quindi le informazioni vere e proprie relative ai pacchetti di versamento:

- *Daily transaction count: ID univoco della transizione (univoco progressivo assoluto) - tipo Long int*
- *Timestamp: riferimento temporale corrispondente al momento in cui il file è stato archiviato (secondo il formato yyyy-MM-dd HH:mm:ss.fff)*

- *Etichetta che identifica l'azione tracciata (Start Upload, End Upload, ecc. sino a Preserved – azione di rilievo ai fini della conservazione)*
- *Customer ID: chiave univoca identificativa del cliente nella tabella corrispondete - tipo INT*
- *Customer name: Stringa descrittiva del cliente*
- *Username auth: Account/Username utilizzato per il trasferimento FTP o web service*
- *Customer IP: Indirizzo IP univoco e identificativo del cliente da cui provengono i trasferimenti FTP o web service*
- *File name: filename (con estensione)*
- *File size: dimensione in byte*
- *File hash (SHA-256): Impronta calcolata con algoritmo SHA-256 del file archiviato*

Torna al sommario

6.3 Pacchetto di archiviazione (PdA)

Ai fini del presente Manuale, il pacchetto di archiviazione (PdA) è composto dal documento (o dal fascicolo documentale) oggetto del processo di conservazione e da un file XML strutturato secondo lo standard SinCRO UNI 11386:2010 (IdPA) firmato e marcato digitalmente (XADES-T) dal Responsabile del Servizio di Conservazione o da un suo delegato.

Il PdA può essere il risultato dell'aggregazione di più pacchetti di versamento, eventualmente trasformati coerentemente alle specificità di contratto, secondo la tipologia documentale contenuta.

L'indice del pacchetto di archiviazione (IPdA) contiene le impronte informatiche dei documenti informatici suddivisi per tipologia omogenea, arricchite dai metadati propri della tipologia rappresentata e richiesti dalla rispettiva normativa vigente.

L'IPdA potrà contenere metadati aggiuntivi secondo le specificità di Contratto.

Viene di seguito descritta la struttura degli elementi "More Info" prevista per l'IPdA:

***More Info* PdA**

```
Indice dei documenti in archivio

<xs:element name="IndiceDocumentiInArchivio">
      <xs:complexType>
            <xs:sequence>
                  <xs:element name="Numero" type="xs:int"/>
                  <xs:element name="DataInizio" type="xs:string"/>
                  <xs:element name="DataFine" type="xs:string"/>
            </xs:sequence>
            <xs:attribute name="xmlns" type="xs:string"/>
            <xs:attribute name="xmlns:ns2" type="xs:string"/>
      </xs:complexType>
```

Dati titolare contabilità

```
<xs:element name="DatiTitolareContabilita">
<xs:complexType>
	<xs:sequence>
		<xs:element name="CodFisc"></xs:element>
		<xs:element name="Denominazione" type="xs:string"></xs:element>
		<xs:element name="DomFiscaleSedeLegale">
			<xs:complexType>
			<xs:sequence>
				<xs:element name="ComuneStato"></xs:element>
				<xs:element name="SiglaProvincia"></xs:element>
				<xs:element name="Indirizzo">
				<xs:complexType>
					<xs:sequence>
						<xs:element name="FrazioneVia"></xs:element>
						<xs:element name="Cap"></xs:element>
					</xs:sequence>
				</xs:complexType>
				</xs:element>
			</xs:sequence>
			</xs:complexType>
		</xs:element>
	</xs:sequence>
	<xs:attribute name="xmlns" type="xs:string"></xs:attribute>
	<xs:attribute name="xmlns:ns2" type="xs:string"></xs:attribute>
</xs:complexType>
</xs:element>
```

Dati del Responsabile del Servizio di Conservazione

```
<xs:element name="DatiResponsabileServizioConservazione">
<xs:complexType>
<xs:sequence>
       <xs:element name="CodFisc" type="xs:string"></xs:element>
       <xs:element name="DatiPersonaFisica">
              <xs:complexType>
              <xs:sequence>
              <xs:element name="Cognome" type="xs:string"></xs:element>
              <xs:element name="Nome" type="xs:string"></xs:element>
              <xs:element name="Sesso" type="xs:string"></xs:element>
              <xs:element name="DatiNascita">
              <xs:complexType>
              <xs:sequence>
                     <xs:element name="ComuneStato" type="xs:string"></xs:element>
                     <xs:element name="SiglaProvincia" type="xs:string"></xs:element>
              <xs:element name="Data">
              <xs:complexType>
              <xs:sequence>
                     <xs:element name="Giorno" type="xs:int"></xs:element>
                     <xs:element name="Mese" type="xs:int"></xs:element>
                     <xs:element name="Anno" type="xs:int"></xs:element>
              </xs:sequence>
              </xs:complexType>
              </xs:element>
              </xs:sequence>
              </xs:complexType>
              </xs:element>
              </xs:sequence>
              </xs:complexType>
       </xs:element>

       <xs:element name="DomFiscaleSedeLegale">
       <xs:complexType>
       <xs:sequence>
              <xs:element name="ComuneStato" type="xs:string"></xs:element>
              <xs:element name="SiglaProvincia" type="xs:string"></xs:element>
              <xs:element name="Indirizzo">
              <xs:complexType>
              <xs:sequence>
                     <xs:element name="FrazioneVia" type="xs:string"></xs:element>
                     <xs:element name="NumeroCivico" type="xs:int"></xs:element>
                     <xs:element name="Cap" type="xs:int"></xs:element>
              </xs:sequence>
              </xs:complexType>
              </xs:element>
              </xs:sequence>
              </xs:complexType>
              </xs:element>
       </xs:sequence>
       <xs:attribute name="xmlns" type="xs:string"></xs:attribute>
       <xs:attribute name="xmlns:ns2" type="xs:string"></xs:attribute>
       </xs:complexType>
</xs:element>
```

Seguono *Specifiche per tipologia documentale*

More Info documento informatico

Fatture emesse:

```
<xs:element name="EmbeddedMetadata">
<xs:complexType>
<xs:sequence>
      <xs:element name="cliente_codice_fiscale" type="xs:int">
      <xs:complexType>
            <xs:attribute name="xmlns" type="xs:string"></xs:attribute>
            <xs:attribute name="xmlns:ns2" type="xs:string"></xs:attribute>
      </xs:complexType>
      </xs:element>
      <xs:element name="cliente_partita_iva" type="xs:int">
            <xs:complexType>
      </xs:element>
      <xs:element name="fattura_sezionale" type="xs:string">
            <xs:complexType>
      </xs:element>
      <xs:element name="cliente_codice" type="xs:int">
            <xs:complexType>
      </xs:element>
      <xs:element name="cliente_ragione_sociale" type="xs:string">
            <xs:complexType>
      </xs:element>
      <xs:element name="fattura_anno" type="xs:int">
            <xs:complexType>
      </xs:element>
      <xs:element name="fattura_progressivo" type="xs:int">
            <xs:complexType>
      </xs:element>
      <xs:element name="fattura_data" type="xs:string">
            <xs:complexType>
      </xs:element>
      <xs:element name="fattura_numero" type="xs:int">
            <xs:complexType>
      </xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
```

Fatture ricevute:

```
<xs:element name="EmbeddedMetadata">
<xs:complexType>
<xs:sequence>
       <xs:element name="cliente_codice_fiscale" type="xs:int">
       <xs:complexType>
              <xs:attribute name="xmlns" type="xs:string"></xs:attribute>
              <xs:attribute name="xmlns:ns2" type="xs:string"></xs:attribute>
       </xs:complexType>
       </xs:element>
       <xs:element name="documento_data" type="xs:int">
              <xs:complexType>
       </xs:element>
       <xs:element name="documento_protocollo " type="xs:string">
              <xs:complexType>
       </xs:element>
       <xs:element name="cliente_partita_iva" type="xs:int">
              <xs:complexType>
       </xs:element>
       <xs:element name="documento_riferimento" type="xs:string">
              <xs:complexType>
       </xs:element>
       <xs:element name="cliente_codice" type="xs:int">
              <xs:complexType>
       </xs:element>
       <xs:element name="documento_registrazione" type="xs:int">
              <xs:complexType>
       </xs:element>
       <xs:element name="documento_anno" type="xs:string">
              <xs:complexType>
       </xs:element>
       <xs:element name="cliente_ragione_sociale" type="xs:int">
              <xs:complexType>
       </xs:element>
       <xs:element name="documento_sezionale" type="xs:int">
              <xs:complexType>
       </xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
```

Gli schemi successivi non sono More Info del PdA; vengono tuttavia riportati per completezza in quanto sono lo schema di riferimento per l'archiviazione delle fatture elettroniche. Il primo schema è attivo per le fatture elettroniche unitamente alle relative ricevute conservate dall'entrata in vigore dell'obbligo della fatturazione elettronica. Il secondo schema è attivo per i precedenti anni per le fatture elettroniche verso la Pubblica Amministrazione.

Formato del File (FileGroup) per le fatture elettroniche:

```
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified">
<xs:element name="pacchettoFatturaElettronica">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="fattura" type="xs:string"></xs:element>

      <xs:element name="ricevute">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="ricevuta" maxOccurs="unbounded" type="xs:string"></xs:element>
          </xs:sequence>
        </xs:complexType>
      </xs:element>

      <xs:element name="allegati">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="allegato" maxOccurs="unbounded" type="xs:string"></xs:element>
          </xs:sequence>
        </xs:complexType>
      </xs:element>

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

Fatture Elettroniche Pubblica Amministrazione:

```
<xs:element name="EmbeddedMetadata">
<xs:complexType>
<xs:sequence>
       <xs:element name="evidence_DT">
       <xs:complexType>
       <xs:sequence>
              <xs:element name="progressivo_id" type="xs:string"></xs:element>
              <xs:element name="sdi_message" type="xs:string"></xs:element>
              <xs:element name="cliente_cod_ufficioPA" type="xs:string"></xs:element>
              <xs:element name="type_docs_desc" type="xs:string"></xs:element>
       </xs:sequence>
       <xs:attribute name="xmlns" type="xs:string"></xs:attribute>
       <xs:attribute name="xmlns:ns2" type="xs:string"></xs:attribute>
       </xs:complexType>
       </xs:element>

       <xs:element name="evidence_RC">
       <xs:complexType>
       <xs:sequence>
              <xs:element name="progressivo_id" type="xs:string"></xs:element>
              <xs:element name="sdi_message" type="xs:string"></xs:element>
              <xs:element name="cliente_cod_ufficioPA" type="xs:string"></xs:element>
              <xs:element name="type_docs_desc" type="xs:string"></xs:element>
       </xs:sequence>
       <xs:attribute name="xmlns" type="xs:string"></xs:attribute>
       <xs:attribute name="xmlns:ns2" type="xs:string"></xs:attribute>
       </xs:complexType>
       </xs:element>

       <xs:element name="cliente_ragione_sociale" type="xs:string">
              <xs:complexType>
       </xs:element>
       <xs:element name="progressivo_id" type="xs:string">
              <xs:complexType>
       </xs:element>
       <xs:element name="cliente_partita_iva" type="xs:int">
              <xs:complexType>
       </xs:element>
       <xs:element name="fattura_data" type="xs:date">
              <xs:complexType>
       </xs:element>
       <xs:element name="fattura_numero" type="xs:string">
              <xs:complexType>
       </xs:element>
       <xs:element name="cliente_cod_ufficioPA" type="xs:string">
              <xs:complexType>
       </xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
```

Libri e registri contabili, libri sociali:

```
<xs:element name="EmbeddedMetadata">
<xs:complexType>
<xs:sequence>
	<xs:element name="libro_data_inizio" type="xs:string">
	<xs:complexType>
		<xs:attribute name="xmlns" type="xs:string"></xs:attribute>
		<xs:attribute name="xmlns:ns2" type="xs:string"></xs:attribute>
	</xs:complexType>
	</xs:element>
	<xs:element name="libro_type_group" type="xs:string">
		<xs:complexType>
	</xs:element>
	<xs:element name="libro_anno_fiscale" type="xs:int">
		<xs:complexType>
	</xs:element>
	<xs:element name="libro_progressivo" type="xs:int">
		<xs:complexType>
	</xs:element>
	<xs:element name="libro_type_text" type="xs:string">
		<xs:complexType>
	</xs:element>
	<xs:element name="libro_data_fine" type="xs:string">
		<xs:complexType>
	</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
```

Dichiarativi fiscali:

```
<xs:element name="EmbeddedMetadata">
<xs:complexType>
<xs:sequence>
	<xs:element name="CodiceFiscaleDichiarante" type="xs:string">
	<xs:complexType>
		<xs:attribute name="xmlns" type="xs:string"></xs:attribute>
		<xs:attribute name="xmlns:ns2" type="xs:string"></xs:attribute>
	</xs:complexType>
	</xs:element>
	<xs:element name="PartitaIvaDichiarante" type="xs:string">
		<xs:complexType>
	</xs:element>
	<xs:element name="ProgressivoInvio" type="xs:int">
		<xs:complexType>
	</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
```

Messaggi ed evidenze PEC:

```
<xs:element name="EmbeddedMetadata">
<xs:complexType>
<xs:sequence>
	<xs:element name="IdentificativoMessaggio" type="xs:string">
	<xs:complexType>
		<xs:attribute name="xmlns" type="xs:string"></xs:attribute>
		<xs:attribute name="xmlns:ns2" type="xs:string"></xs:attribute>
	</xs:complexType>
	</xs:element>
	<xs:element name="MessageAddressFrom" type="xs:string">
		<xs:complexType>
	</xs:element>
	<xs:element name="MessageAddressTo" type="xs:int">
		<xs:complexType>
	</xs:element>
	<xs:element name="MessageSubject" type="xs:int">
		<xs:complexType>
	</xs:element>
	<xs:element name="DataInvio" type="xs:int">
		<xs:complexType>
	</xs:element>
	<xs:element name="EsitoInvio" type="xs:int">
		<xs:complexType>
	</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
```

Torna al sommario

6.4 Pacchetto di distribuzione (PdD)

Il pacchetto di distribuzione (PdD) può coincidere con un PdA, esserne un estratto, o essere la somma di più PdA. Per quanto concerne le specifiche tecniche del PdD, in conformità alle regole tecniche descritte nel DPCM del 3 Dicembre 2013, le stesse sono le medesime descritte nel precedente paragrafo 6.3.

Torna al sommario

7 IL PROCESSO DI CONSERVAZIONE

Il processo di conservazione realizzato ad eWitness, in conformità alle disposizioni dell'articolo 44, comma 1 del CAD, assicura la conservazione elettronica di lungo periodo a norma di legge, adottando regole, procedure e tecnologie in grado di garantire - relativamente ai documenti oggetto di conservazione - le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità.

Il sistema eWitness è in grado di assicurare il trattamento dell'intero ciclo dell'oggetto conservato all'interno del servizio di Conservazione, garantendo l'accesso - per il periodo previsto dalle norme secondo le diverse tipologie documentali - all'oggetto stesso fino al suo scarto.

Così come stabilito dall'articolo 4 del DPCM 3 dicembre 2013, gli oggetti della conservazione sono trattati all'interno del servizio di Conservazione in pacchetti informativi.

Articolo 4, DPCM 3 Dicembre 2013	
Oggetti della conservazione	[...] 1. Gli oggetti della conservazione sono trattati dal sistema di conservazione in pacchetti informativi che si distinguono in: a) pacchetti di versamento; b) pacchetti di archiviazione; c) pacchetti di distribuzione. 2. Ai fini dell'interoperabilità tra i sistemi di conservazione, i soggetti che svolgono attività' di conservazione dei documenti informatici adottano le specifiche della struttura dati contenute nell'allegato 4, almeno per la gestione dei pacchetti di archiviazione.

Dei pacchetti informativi sopra descritti:

- **pacchetti di versamento (PdV)**: hanno per oggetto i dati e i documenti oggetto di conservazione e di proprietà del Cliente, inviati al sistema di conservazione eWitness;
- **pacchetti di archiviazione (PdA)**: sono composti dall'IPdA e dall'insieme dei documenti oggetto di conservazione relativi allo stesso IPdA;
- **pacchetti di distribuzione (PdD)**: documenti conservati a norma, disponibili per la ricerca, consultazione ed esibizione, via portale web oppure da supporto auto consistente o altre modalità concordate con il Cliente e descritte nel presente documento.

In conformità con quanto stabilito dall'art. 9 del DPCM 3 Dicembre 2013, il processo di conservazione a norma eWitness prevede:

a) l'acquisizione da parte del sistema di conservazione del pacchetto di versamento per la

sua presa in carico;

b) la verifica che il pacchetto di versamento e gli oggetti contenuti siano coerenti con le modalità previste nel presente Manuale;
c) il rifiuto del pacchetto di versamento, nel caso in cui le verifiche di cui alla precedente lettera b) abbiano evidenziato delle anomalie;
d) la generazione, in modo automatico, 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 tutte le impronte calcolate sul contenuto del PdV, secondo le modalità descritte nel presente Manuale;
e) la preparazione, l'apposizione della firma digitale del Responsabile del servizio di Conservazione e la gestione del pacchetto di archiviazione sulla base delle specifiche della struttura dati contenute nell'allegato 4 del DPCM 3 Dicembre 2013 e secondo le modalità riportate nel presente Manuale;
f) la preparazione del pacchetto di distribuzione ai fini dell'esibizione richiesta dal Cliente;
g) ai fini della interoperabilità tra sistemi di conservazione, la produzione dei pacchetti di distribuzione coincidenti, in tutto in parte anche per estratto, con i pacchetti di archiviazione.

Di seguito, si riporta lo schema del processo di conservazione eWitness.

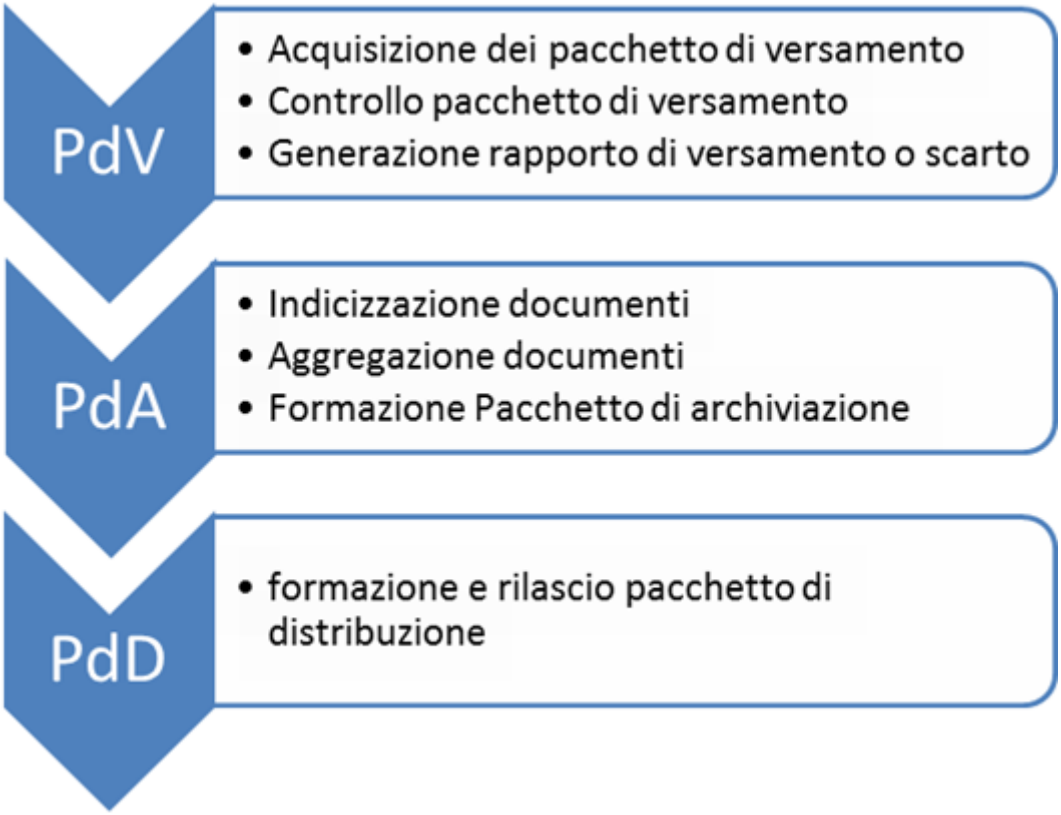


Figura 2 - Schema di processo conservazione eWitness Italia s.r.l.

Torna al sommario

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

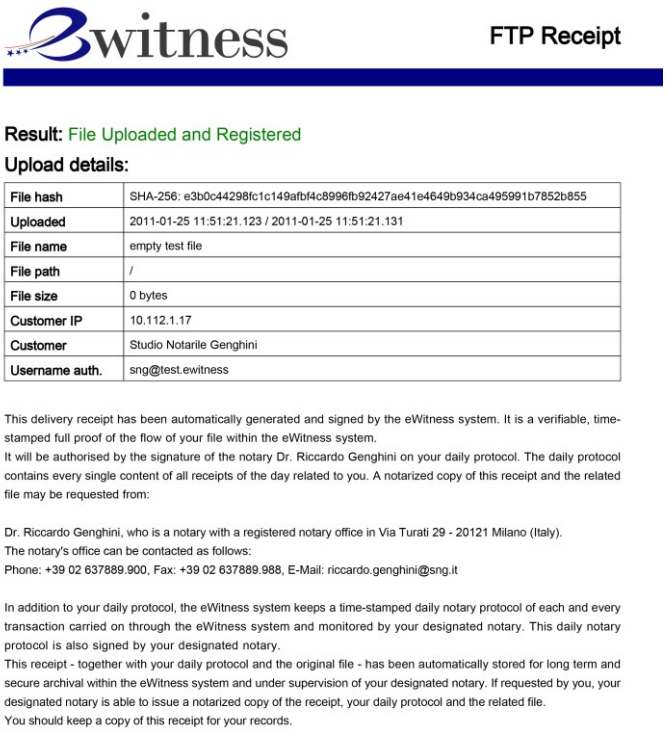
I PdV vengono inviati al sistema di conservazione tramite FTP o tramite web service, mediante il canale certificato descritto al successivo § 7.2.1.

Il Cliente, di fatto, è dotato della Not@reyes-box fornita in comodato d'uso da eWitness sul quale risiede il certificato X509 destinato alla creazione della VPN IPSec o SSL.

In caso di documenti nativi informatici generati su sistemi gestionali eWitness, quest'ultima invierà i documenti al Sistema di conservazione tramite la Not@reyes-box installata presso i suoi server.

Per ogni file trasferito verso il sistema di conservazione eWitness viene generata e trasferita al Cliente una ricevuta di presa in carico del file, munita di firma elettronica, attestante l'esito della trasmissione e riportante l'hash del file trasmesso.

Il Cliente ha l'onere di verificare il buon esito delle trasmissioni effettuate, anche riscontrando l'hash del file contenuto nella ricevuta di presa in carico eWitness, al fine di scongiurare la possibilità di corruzione o perdita dati in questa fase del processo di conservazione.



eWitness FTP Receipt

Result: File Uploaded and Registered

Upload details:

File hash	SHA-256: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
Uploaded	2011-01-25 11:51:21.123 / 2011-01-25 11:51:21.131
File name	empty test file
File path	/
File size	0 bytes
Customer IP	10.112.1.17
Customer	Studio Notarile Genghini
Username auth.	sng@test.ewitness

This delivery receipt has been automatically generated and signed by the eWitness system. It is a verifiable, time-stamped full proof of the flow of your file within the eWitness system.
It will be authorised by the signature of the notary Dr. Riccardo Genghini on your daily protocol. The daily protocol contains every single content of all receipts of the day related to you. A notarized copy of this receipt and the related file may be requested from:

Dr. Riccardo Genghini, who is a notary with a registered notary office in Via Turati 29 - 20121 Milano (Italy).
The notary's office can be contacted as follows:
Phone: +39 02 637889.900, Fax: +39 02 637889.988, E-Mail: riccardo.genghini@sng.it

In addition to your daily protocol, the eWitness system keeps a time-stamped daily notary protocol of each and every transaction carried on through the eWitness system and monitored by your designated notary. This daily notary protocol is also signed by your designated notary.
This receipt - together with your daily protocol and the original file - has been automatically stored for long term and secure archival within the eWitness system and under supervision of your designated notary. If requested by you, your designated notary is able to issue a notarized copy of the receipt, your daily protocol and the related file.
You should keep a copy of this receipt for your records.

Figura 2 - Ricevuta del sistema eWitness

La ricevuta rilasciata dal sistema eWitness riporta, per ogni documento ricevuto le seguenti informazioni:

- Timestamp: riferimento temporale corrispondente al momento in cui il file è stato

archiviato (secondo il formato yyyy-MM-dd HH:mm:ss.fff)

- Object ID
- Object name: Stringa identificativa univoca del documento (formato yyyy-MM-dd#12345)
- Customer ID: chiave univoca identificativa del cliente
- Customer name: Stringa descrittiva del cliente
- Customer IP: Indirizzo IP univoco e identificativo del cliente da cui provengono i trasferimenti (FTP o web service)
- Username auth.: Account/Username utilizzato per il trasferimento (FTP o web service)
- File name
- File full path: percorso completo della cartella in cui è stato caricato il file
- File size: dimensione in byte
- File hash (SHA-256): Impronta calcolata con algoritmo SHA-256 del file archiviato

Torna al sommario

7.1.1 Copie informatiche di documenti analogici originali anche unici

In caso di documenti analogici originali (anche unici) sottoposti a processo di dematerializzazione anche effettuata da service esterno al Cliente (interno o esterno a eWitness), eWitness provvederà a fornire e installare presso lo stesso service la Not@reyes-box eWitness.

La dotazione della Not@reyes-box eWitness presso il service esterno consente al RSC, che sovrintende il processo di conservazione, di certificare la produzione di copie informatiche (di uno o più documenti analogici) attribuendogli il maggior valore probatorio previsto dall'articolo 22, comma 2 del CAD, secondo cui

[...] *le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico hanno la stessa efficacia probatoria degli originali da cui sono estratte, se la loro conformità è attestata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata secondo le regole tecniche stabilite ai sensi dell'articolo 71.*

Occorre altresì tenere presente che l'attestazione di conformità rilasciata dal RSC, anche nella sua qualità di Notaio Pubblico Ufficiale, potrà essere rilasciata sulla base:

- del raffronto dei documenti;
- o attraverso la certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia.

In ogni caso il documento informatico, prodotto della dematerializzazione, verrà firmato digitalmente dal RSC anche nella sua qualità di Notaio Pubblico Ufficiale.

Torna al sommario

7.1.2 Aggiunta opzionale di una marca temporale detached

In modo opzionale, per i clienti che ne fanno richiesta o per servizi ritenuti particolarmente critici, è possibile produrre per ciascuna ricevuta del sistema eWitness un'ulteriore evidenza digitale dell'avvenuta conservazione costituita da una marca temporale qualificata, consentendo così una validazione temporale elettronica opponibile ai terzi (cfr. Art. 20, comma 3 Codice dell'Amministrazione Digitale Dlgs 82/2005).

eWitness utilizza un servizio di Validazione Temporale Elettronica Qualificata (Qualified Electronic Time-Stamp service) conforme alle norme di legge nazionali ed europee (Regolamento Europeo n.910/2014 "EIDAS"). La policy di riferimento del servizio sfruttato per l'apposizione delle marche è la BTSP (Best practice Time-Stamp Policy) definita nella norma ETSI TS 319 421.

Torna al sommario

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

Segue descrizione dei controlli effettuati dal sistema di conservazione sui PdV.

Verifica del soggetto che ha formato il documento: la paternità del soggetto che forma e/o invia il documento al sistema di conservazione è intrinsecamente garantita dal modello di sicurezza eWtiness, che prevede la cifratura del canale di trasmissione tra il Produttore e il sistema di conservazione mediante l'utilizzo di Router crittografico (di seguito anche solo "Not@reyes-box").

La tecnologia Not@reyes-box è in grado rendere sicuro e fidato il canale di comunicazione sui cui transano documenti, dati e/o flussi di dati destinati al sistema di conservazione eWitness.

Il Not@reyes-box è un router dotato di due interfacce di rete attive con un firewall pre-installato ("pfSense"), capace di instaurare un canale VPN (Virtual Private Network) di tipo IPSec o SSL, cifrato mediante certificato x509.

Il canale VPN gestisce la transazione dei documenti o dei dati (o flussi di dati), utilizzando un protocollo di invio standard FTP o web service.

La cifratura del canale VPN garantisce la confidenzialità e la riservatezza delle comunicazioni permettendo, al contempo la fruizione del sistema di conservazione eWitness da parte degli utenti (o dei processi) in modo assolutamente trasparente, senza che siano necessaria l'installazione di software o funzioni ad hoc.

L'utilizzo di un certificato x509, cablato all'interno della Not@reyes-box, garantisce:

- un livello di sicurezza superiore rispetto ad un sistema di autenticazione mediante user name e password;
- l'identificazione certa della provenienza di dati e/o documenti (o flusso di dati e/o documenti) – e quindi la riconducibilità del dispositivo al suo titolare – senza che sia possibile ripudiarne la titolarità;

- la certificazione da parte di una terza parte (Trusted Third Party) dell'avvenuta transazione dei dati sul canale VPN.

Verifica dei formati: Il sistema di conservazione provvede a eseguire la verifica del formato di ciascun file versato secondo le specifiche e i formati definiti e riconosciuti dallo IANA (Internet Assigned Numbers Authority) e comunque nei formati previsti dall'Allegato 2 del DPCM 3 Dicembre 2013.

Verifica di firma digitale: Se contrattualmente previsto, nel caso in cui il PdV sia costituito in tutto o in parte da uno o più documenti muniti di firma elettronica qualificata, il sistema di conservazione provvederà alla verifica delle sottoscrizioni apposte al documento o ai documenti alla data di generazione degli stessi, dando evidenza del protocollo di verifica.

Durante il processo di generazione del PdA verrà inoltre eseguito il seguente ordine di controlli.

Verifica tipo documento: Il sistema di conservazione provvede alla verifica delle tipologie di documenti ricevuti. Sulla base delle specificità previste contrattualmente con il Cliente, vengono predisposte adeguate procedure di controllo per verificare che i documenti ricevuti siano effettivamente coerenti alle tipologie attese. Tali controlli possono essere di diversa natura e basati su:

- controllo della naming convention dei file ricevuti;
- estrazione e riscontro di testo dal documento informatico, anche allo scopo di costituire i metadati necessari all'archiviazione;
- verifica della completezza dei metadati attesi per tipologia documentale.

7.2.1 Gestione dei virus

Nel Sistema eWitness si prevede una scansione full di tutto l'archivio da attuarsi in continuità ed a rotazione su porzioni di archivio al fine di andare a rilevare infezioni da eventuali nuovi virus scoperti ed inseriti nelle liste solo di recente, a seguito della prima scansione applicativa.

Oltre a quanto sopra riportato, per particolari tipologie documentali, attivabile in via opzionale, è implementato quanto segue:

- è installato un server antivirus che opera come servizio applicativo;
- a valle dell'acquisizione del pacchetto di versamento, ma prima del trasferimento a post-lavorazioni, viene effettuata una scansione antivirus dell'oggetto digitale ricevuto;
- se la scansione va a buon fine, l'oggetto digitale viene classificato come lavorabile;
- se la scansione non va a buon fine, l'oggetto digitale viene inserito in un'area di quarantena logica e viene inviata una segnalazione interna ad eWitness (interessati il Responsabile del Servizio di Conservazione, il Responsabile sicurezza dei sistemi per

la conservazione, il Responsabile della Funzione archivistica di conservazione, il Responsabile Sistemi informativi per la conservazione) e ci si attiverà per la gestione dell'anomalia. In particolare, sarà inviata una mail al cliente notificando l'accaduto per concordare le azioni da attuare;

- il documento infetto sicuramente non sarà sottoposto a post-lavorazioni (es. esposizione sul documentale o inclusione in pacchetto di archiviazione), per cui il pacchetto di versamento sarà scartato.
- da valutare con il cliente o internamente l'opportunità di conservare comunque il file infetto.

Torna al sommario

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

Il rapporto di versamento (RdV) coincide con l'indice di versamento sulla base dell'esito dei controlli enunciati al precedente §7.2.

La struttura e il formato del rapporto di versamento coincidono con l'indice del pacchetto di versamento e sono quindi descritti al precedente §6.2.

Il rapporto di versamento è munito di firma digitale dell'RSC e di marca temporale, che assolve all'indicazione contenuta nelle regole tecniche sul sistema di conservazione di cui al DPCM 3 Dicembre 2013 in relazione alla necessità di associare al rapporto di versamento un riferimento temporale UTC.

Nel PdA verranno riportati l'hash e gli identificativi univoci di uno o più RdV.

Per ogni pacchetto accettato il sistema di conservazione genera un rapporto di versamento che viene memorizzato nel database e associato logicamente al PdA cui si riferisce.

Torna al sommario

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

Di seguito si riporta l'elenco delle anomalie che possono portare al rifiuto di un PdV:

- problemi relativi al formato del file inviato;
- eventuali problemi riscontrati sulle firme digitali apposte ai documenti;
- problemi tecnici con il salvataggio del file in fase di presa in carico;
- problemi inerenti all'osservanza delle disposizioni contrattuali o la validità commerciale del contratto medesimo.

Il rifiuto del PdV viene notificato al Cliente a mezzo di PEC o eWitness mail (servizio di posta elettronica aderente allo standard REM ETSI TS 102 640-6-2), allegando il relativo IPdV.

Torna al sommario

7.5 Preparazione e gestione del pacchetto di archiviazione

Di seguito sono descritte le fasi di processo che portano alla formazione del pacchetto di archiviazione (PdA):

- elaborazione dei documenti contenuti nei PdV al fine di ottenere l'identificazione della tipologia documentale e il recupero dei metadati obbligatori identificativi di ogni tipologia;
- eventuale elaborazione dei documenti contenuti nei PdV per ottemperare alle eventuali specificità contrattuali;
- aggregazione dei documenti per la formazione del PdA con regole e logiche specifiche per ogni Contratto. Un PdA è formato da documenti provenienti da uno o più PdV. I documenti relativi ad un PdV non necessariamente saranno tutti contenuti nello stesso PdA;
- formazione dell'IPdA secondo lo standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010), standard riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione.

  L'IPdA contiene i seguenti dati:
  a. identificativo interno univoco;
  b. le evidenze (hash, file name, ecc.) già contenute all'interno del PdV;
  c. il relativo hash e indice univoco del PdV a cui fanno riferimento;
  d. i metadati obbligatori collegati alla relativa tipologia documentale;

- apposizione della firma digitale e della marca temporale sull'IPdA da parte del RSC;
- generazione - dal sistema di conservazione eWitness - di un log relativo a tutte le operazioni eseguite per generare il PdA.

Torna al sommario

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

La gestione dei PdD fa capo al Responsabile del servizio di Conservazione, al Responsabile della funzione archivistica e al Responsabile del trattamento esterno dei dati personali.

La produzione di Pacchetti di distribuzione avviene in seguito alla richiesta da parte del Cliente, così come indicato all'articolo 9, comma 1, lett. h) delle regole tecniche di cui al DPCM 3 Dicembre 2013. Tali Pacchetti, però, posso differire nei casi in cui il Cliente richieda l'esibizione tramite supporto ottico; in questo caso, il supporto dovrà necessariamente contenere elementi utili all'avvio del supporto e alla visualizzazione dei contenuti informativi.

La richiesta di generazione di uno o più pacchetti di distribuzione verso il sistema di conservazione eWitness, è permessa ai soli soggetti autorizzati. Devono ritenersi autorizzati il Cliente, in persona del legale rappresentante del soggetto titolare dei documenti inviati e presenti nel sistema di conservazione, o di un altro soggetto da esso delegato per iscritto.

A fronte di una richiesta di generazione del o dei PdD, il sistema di conservazione effettua delle verifiche di coerenza e correttezza del o dei PdD generati oltre che dei documenti contenuti.

A tal proposito, il sistema di conservazione verifica che le impronte dei documenti restituiti nel PdD corrispondano a quelle presenti nel relativo IPdA in modo da garantire che i documenti stessi non abbiano subito alterazioni o modifiche nei contenuti.

Qualora si renda necessaria la distribuzione dei PdD su supporti fisici rimovibili, questi non presenteranno esternamente alcun riferimento immediatamente identificativo del produttore o del loro contenuto; quest'ultimo sarà protetto con idonei sistemi crittografici e la relativa chiave di decriptazione sarà consegnata al destinatario attraverso canali differenti da quelli di consegna del supporto fisico.

Tali supporti saranno consegnati esclusivamente mediante personale selezionato, espressamente incaricato del loro trasporto.

Torna al sommario

7.7 Produzione di duplicati e copie informatiche

Viene fornita anche la descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti.

Torna al sommario

7.7.1 Duplicati informatici

Oltre alle modalità di conservazione standard descritte nel presente manuale, su richiesta del Cliente possono essere generati anche duplicati o copie su supporto ottico. Tali copie vengono inviate dal Responsabile del servizio di Conservazione al Cliente oppure mantenute da eWitness.

Dato che le copie e/o i duplicati vengono generati solo su richiesta del Cliente, quest'ultimo deve inoltrare apposita richiesta ai riferimenti concordati in fase di sottoscrizione del Contratto.

Data la particolarità del sistema di conservazione eWitness e del ruolo ricoperto dal Responsabile del servizio di Conservazione, quale Pubblico Ufficiale, la produzione del duplicato informatico del documento conservato può essere accompagnata dalla attestazione di conformità prevista dall'articolo 23, comma 2 del Codice dell'Amministrazione Digitale.

Torna al sommario

7.7.2 Copie informatiche

La produzione della copia informatica del documento conservato può rendersi necessaria oltre che per le normali esigenze di esibizione del documento verso terzi (ivi compresa la Pubblica Autorità), anche per ragioni conseguenti a processi di riversamento sostitutivo atti a sanare la parzialità o la totalità di archivi di conservazione gestiti da soggetti terzi, di cui il Cliente richiede l'acquisizione nel sistema di conservazione eWitness.

Tali copie, possono sempre essere accompagnate dall'attestazione prevista dall'articolo 23-bis

comma 2, del Codice dell'Amministrazione Digitale, rilasciata dal Responsabile del servizio di Conservazione.

Torna al sommario

7.8 Scarto dei pacchetti di archiviazione

Così come previsto dall'articolo 9 del DPCM 3 Dicembre 2013, il sistema di conservazione eWitness consente lo scarto dei documenti informatici conservati a norma e contenuti in uno o più PdA.

La possibilità di eseguire uno scarto dal sistema di conservazione non può prescindere dalla valutazione circa la natura giuridica del soggetto (Cliente) titolare dei documenti oggetto di conservazione.

A tal fine si distinguono:

- **soggetti privati**: con l'eccezione degli archivi "*dichiarati di notevole interesse storico*", il cui ambito di conservazione è oggetto di normativa speciale, per la documentazione ordinaria e, in particolar modo per la documentazione a rilevanza tributaria e/o fiscale, i termini prescrittivi sono dettati dalla norma codicistica (cfr. articolo 2220 c.c.) oltre che dalla norma fiscale di rango primario;

- **soggetti pubblici**: per quanto attiene ai documenti di carattere o valenza pubblica, fermi restando i principi cogenti della normativa codicistica, si rendono applicabili alcune disposizioni di carattere speciale tra cui quella concernente i beni culturali e ambientali di cui al D.lgs. 10 gennaio 2004, n. 42 (Codice dei beni culturali e ambientali).

Indipendentemente dalla natura giuridica del soggetto titolare dei documenti oggetto di conservazione, particolare attenzione viene prestata alla rilevanza di interesse storico-artistico che gli stessi possono ricoprire. In questi casi, lo scarto del PdA può essere realizzato solamente previa autorizzazione del Ministero per i beni e le attività culturali, richiesta a cura del Cliente, così come previsto dalla vigente normativa in materia.

Torna al sommario

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

Il sistema conservazione eWitness è predisposto per gestire i formati che possono maggiormente garantire i principi di interoperabilità tra i sistemi di conservazione, in base alla normativa vigente riguardante le specifiche tipologie documentali.

A tal fine il sistema di conservazione eWitness, in conformità a quanto previsto dall'allegato 2 del DPCM 3 Dicembre 2013, adotta i principali standard di formati e di gestione di tracciati di dati così come di seguito riportato:

- ai fini dell'accettazione degli oggetti conservati, l'aderenza ai formati previsti dal presente Manuale e dall'allegato 2 delle regole tecniche richiamate;
- ai fini della generazione dell'IPdA, l'aderenza allo standard UNI 11386 SInCRO dell'ottobre 2010;
- ai fini della generazione dei PdD, come specificato dall'articolo 9, comma 1, lett. h) delle regole tecniche, la corrispondenza univoca tra PdV preso in carico, PdA generato e PdD.

Torna al sommario

7.10 Procedura di distruzione dei PdV dal Sistema eWitness

La procedura per la rimozione dei documenti dal sistema di conservazione prevede in seguenti passaggi:

1) Il Cliente comunica un elenco di hash che devono essere cancellati. L'elenco deve pervenire in modo sicuro, per cui deve essere firmato digitalmente oppure deve essere trasferito tramite router Not@ryze-box (via FTP oppure via web service);
    - la modalità standard prevede di ricevere un file di testo con un elenco di hash, uno per ciascuna riga.
2) Sarà possibile definire convenzioni di formato differenti con il cliente.
3) Qualora l'elenco non arrivi tramite router, sia il mittente sia il titolare della firma digitale dovranno essere persone dotate di opportuni poteri, ovvero di opportuna delega da parte del Responsabile della Conservazione o del legale rappresentante del cliente. Qualora l'elenco arrivi via router, deve comunque essere accompagnato da una richiesta formale, sottoscritta digitalmente, e trasmessa a mezzo mail o PEC, con la quale si notifica l'attività di cancellazione. Tale richiesta sarà conservata digitalmente dal Responsabile del Servizio di Conservazione.
4) L'elenco di hash viene preso in carico dalla procedura di cancellazione del sistema eWitness che prepara il sistema per la cancellazione di determinati lotti di file.
5) Il riepilogo della preparazione viene sottoposto al Responsabile del Servizio di Conservazione per approvazione;
    - a seconda della tipologia di documenti, il Responsabile del Servizio di Conservazione potrebbe richiedere la presenza di un referente del cliente, in loco o anche in videoconferenza.
6) Ottenuta l'autorizzazione, il sistema eWitness fa partire la procedura di cancellazione.
7) Per grosse quantità di dati la lavorazione potrà avvenire anche per lotti, seppur in soluzione di continuità. Tutte le singole operazioni di cancellazione sono tracciate, comprensive di data e ora di cancellazione;
    - le operazioni sono riepilogate nel daily log del cliente.
8) Al termine dell'attività di cancellazione viene prodotto un verbale di riepilogo contente l'elenco degli hash che sono stati cancellati. Il verbale viene sottoscritto dal Responsabile della Conservazione ed è sottoposto esso stesso a conservazione a cura del Responsabile del Servizio di Conservazione.

9) Una copia del verbale è consegnata al cliente.

La cancellazione comporta l'eliminazione di un oggetto digitale corrispondente all'hash da tutti i sistemi eWitness: primario, secondario, copie di backup, altre copie sotto il controllo eWitness.

eWitness può offrire supporto al cliente per la definizione dell'elenco di hash da sottoporre a cancellazione (ad esempio effettuando dei filtri sulla base dei metadati disponibili e storicizzati in sistemi documentali di esibizione); tuttavia la responsabilità di approvazione dell'elenco di oggetti da distruggere spetta solo ed esclusivamente al Cliente.

L'operazione di completa cancellazione potrebbe richiedere anche diversi giorni.

Torna al sommario

8 IL SISTEMA DI CONSERVAZIONE

Nel presente paragrafo viene descritto il sistema di conservazione, analizzando le componenti logiche, tecnologiche e fisiche.

8.1 Componenti Logiche

Segue schema e descrizione delle entità funzionali relative al sistema di conservazione e al suo funzionamento.

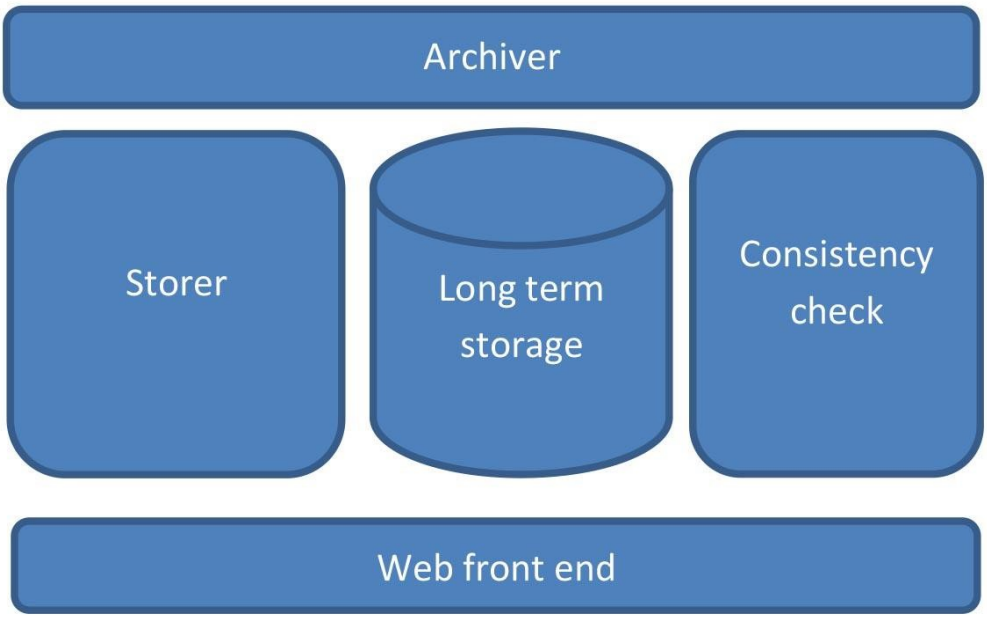


Figura 3 - Entità funzionali del sistema di conservazione eWitness

Archiver: si occupa della ricezione dei documenti da parte del Cliente. I documenti sono ricevuti con protocollo FTP o web service attraverso VPN IPSec o SSL, con autenticazione mediante certificati X509 rilasciati da eWitness (Not@reyes-box), al fine di garantire il non ripudio del dato trasmesso dal Cliente. Si occupa inoltre della formazione del PdV acquisendo le informazioni aggiuntive di base di ogni documento oggetto di conservazione.

Storer: si occupa della generazione dei PdA, dell'apposizione della firma digitale del RSC e della corretta archiviazione dei supporti e dei documenti a livello di *Long term sotrage*.

Web front end: rappresenta l'insieme delle procedure applicative destinate all'interazione con i diversi attori (Clienti, Utenti, Responsabile del servizio di Conservazione). L'elenco di tali funzioni è il seguente:

- sottoscrizione del PdV;
- ricerca e visualizzazione dei documenti conservati;
- richiesta di generazione del PdD.

Consistency check: agente che verifica la consistenza e la coerenza delle tre copie del PdA residenti nei data center principale e di backup. La consistenza è verificata calcolando e verificando gli hash dei documenti conservati in tutte e tre le istanze di storage.

Torna al sommario

8.2 Componenti Tecnologiche

Si elencano le componenti tecnologiche che implementano il sistema di conservazione eWitness così come schematizzato nel precedente paragrafo 8.1:

- **Archiver**: implementato da un servizio FTP e da un servizio web service con componenti realizzate con tecnologia Java su base dati MySQL;
- **Storer**: realizzato con tecnologia Java su base dati MySQL;
- **Web Front-end**: front-end applicativo sviluppato in tecnologia Microsoft Framework .NET e WebServices Java su database MySQL e Microsoft SQL Sever;
- **Consistency check**: il sottosistema deputato alla verifica della consistenza dei documenti in conservazione è realizzato utilizzando le seguenti tecnologie: Python per il calcolo massivo degli hash; MySQL come base dati per il confronto col database di conservazione; Java per l'esecuzione del controllo effettivo e l'invio dei report; infine bash come wrapper per semplificare l'esecuzione e l'integrazione di tutte le funzioni di controllo ed estrazione dei dati.

Torna al sommario

8.3 Componenti Fisiche

Segue schema e descrizione dei siti di conservazione e delle connessioni tra i diversi siti e tra i diversi componenti del sistema di conservazione eWitness.

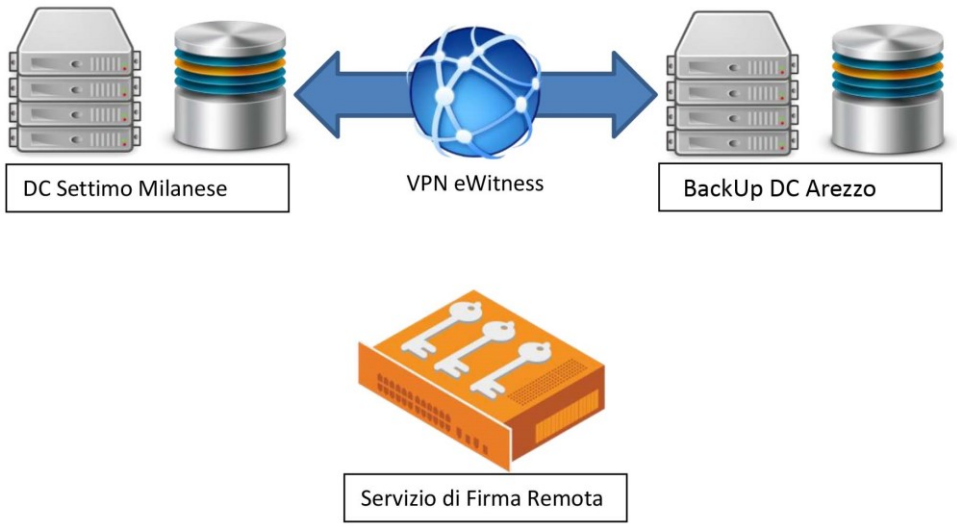


Figura 4 – Siti di conservazione e connessioni tra diversi componenti del sistema di conservazione eWitness

Il sistema di conservazione eWitness è ubicato in cage dedicato presso il datacenter di British Telecom a Settimo Milanese.

Le componenti applicative sono eseguite su server virtuali ospitati su cluster VMWare in configurazione attiva-attiva.

La persistenza dei documenti conservati è realizzata specularmente su due apparati storage dedicati e fisicamente distinti.

L'apposizione delle firme qualificate del RdC, o delegato alla firma, sui PdA avviene tramite l'utilizzo di apposito servizio di firma remota qualificata.

Applicazioni e dati (PdA) sono replicati su infrastruttura dedicata presso datacenter di backup sito in Arezzo. Le procedure di replica, basate su tecnologia VEEAM e rsync, sono eseguite attraverso tunnel VPN IPSEC tra i DC di Settimo Milanese e Arezzo.

Torna al sommario

8.4 Procedure di gestione

Il sistema di conservazione eWitness rispetta e rispecchia le procedure di gestione ed evoluzione previste nelle ottenute certificazioni ISO/IEC 27001:2013 ed ISO 9001:2015 relativamente a:

- **conduzione e manutenzione del sistema di conservazione**: le attività di manutenzione vengono sui processi, sulle strutture hardware e software, mediante verifiche quotidiane sulle infrastrutture. In parallelo a tali attività vengono pianificate le eventuali procedure straordinarie in caso di anomalie;
- **gestione e conservazione dei log**: tutti gli eventi relativi alla sicurezza sui sistemi critici o riservati sono registrati; i log di controllo sono protetti ed archiviati. I log di accesso di amministratori e operatori sono anche parte dei log degli eventi relativi alla sicurezza che vengono archiviati per tutte le macchine. Tutti i log di sistema sono archiviati e conservati per un periodo minimo coerente con il Regolamento UE 679/2016 (GDPR);
- **monitoraggio del sistema di conservazione**: adeguate ed efficaci procedure di monitoraggio del sistema di conservazione sono predisposte e dettagliate nel seguente §9;
- **verifica periodica di conformità a normativa e standard di riferimento**: è attuata la verifica periodica di conformità a normativa e standard di riferimento da parte del management anche mediante il coinvolgimento di personale esterno qualificato.

La gestione di tutti questi processi è effettuata dai responsabili di funzione che si sono succeduti nel tempo, riportati nel Registro delle Cariche.

Torna al sommario

8.5 Procedure di evoluzione e change management

I criteri di accettazione per i nuovi sistemi, aggiornamenti e nuove versioni sono preventivamente stabilite e vengono effettuate prove appropriate durante lo sviluppo e prima dell'approvazione.
Il processo operativo è certificato tramite procedura operativa ISO 27001 e descritto tramite un flussogramma per la "Progettazione e sviluppo di soluzioni e servizi per la gestione elettronica documentale e System Integration". Tale procedura indica le modalità operative e le responsabilità inerenti alle prestazioni/servizi che possono essere richieste dal Cliente, ove con Cliente si intende anche eWitness stessa, ovvero il cosiddetto Cliente interno.

Le prestazioni da erogare sulla base delle richieste del Cliente saranno svolte con modalità e livelli di approfondimento diversi a seconda del tipo di richiesta pervenuta.

Per quanto concerne la tracciatura delle informazioni, delle fasi, dei log, delle comunicazioni importanti, delle evidenze dei test, ecc. si è deciso di concentrare il tutto sullo strumento operativo tipo Agile Board – tool collaborativo.

Dal punto di vista dell'automazione di processo, gli strumenti in uso sono:

- un sistema per la gestione delle versioni;
- un sistema per la gestione automatizzate della integrazione continua;
- un sistema per l'automazione dei dispiegamenti tra i vari ambienti.

Tutti gli sviluppi interni sono testati anche su sistemi di test. L'accettazione del nuovo software è considerata dopo aver verificato se il suddetto software adempie ai criteri di accettazione.

Il Responsabile dello Sviluppo e della Manutenzione del Sistema di Conservazione unitamente al proprio staff è responsabile di tali controlli.

Torna al sommario

9 MONITORAGGIO E CONTROLLI

Data la natura articolata del sistema e del processo di conservazione adottato e descritto nel presente Manuale, eWitness ha definito un insieme di attività di analisi e verifica del funzionamento del sistema, finalizzate a misurare la performance globale del sistema di conservazione, monitorare il mantenimento dei livelli di sicurezza adottati e gestire in maniera proattiva le eventuali anomalie di sistema riscontrate.

Il sistema di monitoraggio e controllo delle funzionalità del sistema di conservazione eWitness è strutturato su tre livelli:

- attività di controllo e monitoraggio relativa agli host virtuali;
- attività di controllo e monitoraggio relativa ai servizi;
- attività di controllo e monitoraggio relativa ai dati archiviati.

A tutela del mantenimento di un elevato stato di efficienza operativa, infrastrutturale e tecnologica del sistema di conservazione, il sistema di monitoraggio implementato da eWitness prevede inoltre la regolare esecuzione di controlli sugli host fisici, indipendentemente dal sistema di conservazione.

Torna al sommario

9.1 Procedure di monitoraggio

L'intera struttura del sistema di conservazione eWitness è costantemente monitorata nelle sue componenti logiche e fisiche fondamentali. L'attività di monitoraggio è condotta da eWitness con una periodicità di dieci minuti.

I sistemi di controllo adottati sono strutturati su due diversi livelli di dettaglio:

- **Controlli di primo livello**: controlli di base effettuati sui server virtuali. Essi includono innanzitutto verifiche sulla raggiungibilità dei server e, in secondo luogo, controlli sull'utilizzo di tutte le risorse in uso: CPU, Memoria, Swap, Disco e Rete;

- **Controlli di secondo livello**: come secondo livello di controllo, viene costantemente verificata la raggiungibilità di tutti i servizi necessari all'infrastruttura del sistema di conservazione eWitness, mediante richieste apposite ad ognuno di essi. A titolo di esempio, per la verifica dei sistemi principali sono eseguite richieste FTP, richieste web service, interrogazioni SQL e richieste HTTP.

In caso di consumo eccessivo di risorse o di servizi non raggiungibili, il sistema di monitoraggio lancia immediatamente un'eccezione, che notifica inviando una e-mail a tutti i responsabili della manutenzione del sistema di conservazione.

Lo storico di tutti gli esiti delle attività di controllo e interrogazione è salvato su un apposito

database, da cui vengono periodicamente estratti dati al fine di verificare trend e migliorare il dimensionamento.

Un ulteriore livello di monitoraggio è infine incluso nel sistema modulare di conservazione stesso, in cui un processo interno verifica i log scritti dai vari moduli. Nel caso in cui il sistema rilevi errori o anche semplici warning, i responsabili della manutenzione del sistema vengono notificati in maniera automatica tramite e-mail. In caso di rilevamento di errori noti e non prevenibili, il sistema effettua giornalmente azioni automatiche di correzione e di ripristino degli stessi. Ognuna di queste azioni correttive viene tracciata all'interno di un apposito sistema di log. Al termine di queste operazioni, una e-mail notifica agli stessi manutentori le variazioni e le correzioni effettuate.

Torna al sommario

9.2 Verifica dell'integrità degli archivi

L'attività di verifica dell'integrità degli archivi consente al sistema di conservazione di controllare la conformità dei documenti conservati rispetto al momento del loro invio in conservazione.

Al fine di assicurare la costante integrità e leggibilità dei dati archiviati, il sistema di monitoraggio applicato al sistema di conservazione eWitness effettua periodicamente e in maniera automatica una articolata procedura per il controllo dell'integrità, a seguito descritta.

Tale procedura è effettuata direttamente a livello di file. Il sistema di conservazione eWitness è impostato in modo da inibire in maniera automatica eventuali operazioni di sovrascrittura o eliminazione di dati, limitando pertanto il numero di azioni eseguibili e compromettenti l'integrità dei dati archiviati. Tuttavia, per incrementare ulteriormente il grado di certezza dell'effettiva integrità di tutti i dati archiviati, il sistema esegue continuamente un *Consistency Check*, un controllo istituito ad hoc, che calcola l'hash SHA256 di ogni file presente in tutti gli archivi di conservazione a livello fisico (quindi i due host principali e l'host di backup) e lo confronta con il livello logico dei dati presenti nel database di conservazione. Qualora le verifiche effettuate segnalino file mancanti o difformità negli hash calcolati in uno qualsiasi degli archivi verificati, un sistema automatico di alert è segnalato via e-mail le anomalie riscontrate ai responsabili del sistema di manutenzione.

In aggiunta a tale procedura di controllo, il sistema utilizza dei particolari filesystem, che consentono il *Data Scrubbing,* che corregge in maniera automatica i (seppur rari) errori di scrittura/lettura del filesystem. A completamento delle suddette attività di controllo, il sistema genera un report inviato automaticamente ai gestori del sistema di manutenzione.

Torna al sommario

9.3 Soluzioni adottate in caso di anomalie

Nel caso in cui le verifiche sul sistema di conservazione sopra descritte rilevino delle anomalie, il sistema notifica in automatico tramite e-mail i responsabili del sistema precedentemente designati. Al momento della segnalazione di ogni eventuale problema, i responsabili del sistema ne analizzano e valutano la causa, in modo da poterne individuare la più efficace strategia di normalizzazione.

I responsabili applicano quindi le correzioni valutate necessarie per risolvere l'incongruenza, ad esempio ripristinando un file presente in uno degli archivi di backup (previa verifica dell'identicità dei metadati della copia ai metadati salvati nel database di conservazione).

Al termine dell'operazione di normalizzazione di ogni anomalia, i soggetti manutentori valutano ed eventualmente implementano delle correzioni al sistema atte a prevenire l'insorgere di ulteriori errori della stessa tipologia o quantomeno permetterne una più tempestiva rilevazione.

Torna al sommario