TRENITALIA
GRUPPO FERROVIE DELLO STATO ITALIANE

MANUALE DI CONSERVAZIONE

Revisione: 0 **Nuova ☒ Parziale ☐ Totale ☐**	**Data:** 21/03/2025
Approvato da: Responsabile della conservazione	

Tavola della Revisione N° REV.	**DATA**	**DESCRIZIONE**
0	21/03/2025	Prima emissione

Sommario

1 Generalità

1.1 Scopo del documento

Il presente documento costituisce il Manuale del servizio di conservazione di TRENITALIA ed ha lo scopo di illustrare la struttura del sistema di conservazione descrivendone analiticamente gli oggetti sottoposti a conservazione, il processo di conservazione e le componenti logiche, tecnologiche e fisiche relative al suo funzionamento.

Delinea, inoltre, i soggetti che sono coinvolti nelle attività e nei processi di conservazione, i quali hanno la responsabilità del sistema.

Questo documento è reso disponibile a tutte le parti interessate a seguito di apposita richiesta.

torna al sommario

1.2 Terminologia

La terminologia e gli acronimi utilizzati in questo manuale richiamano quelli elencati nell' Allegato 1 al documento "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici" (linee Guida AGID), al quale si rimanda.

1.3 Normativa e prassi di riferimento

Notazione abbreviata	Riferimento
Codice Civile	[Libro Quinto del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle Scritture contabili], art. 2215 bis – Documentazione informatica.
RD 1163/1911	Regolamento per gli archivi di Stato
DPR 1409/1963	Norme relative all'ordinamento ed al personale degli archivi di Stato
Legge 241/1990	Nuove norme sul procedimento amministrativo
DPR 445/2000	Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
DPR 37/2001	Regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli uffici dello Stato
D.lgs 196/2003	Recante il Codice in materia di protezione dei dati personali

Notazione abbreviata	Riferimento
D.lgs 42/2004	Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n.137
Legge 9 gennaio 2004, n. 4 aggiornata dal decreto legislativo 10 agosto 2018, n. 106	Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici
D.lgs 82/2005 e ss.mm.ii.	Codice dell'amministrazione digitale
D.lgs 33/2013	Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni
DPCM 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, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71
DPCM 21 marzo 2013	Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni;
Reg. UE 910/2014	In materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE - Regolamento eIDAS;
Circolare 40 e 41 del 14 dicembre 2015 della Direzione generale degli archivi	Autorizzazione alla distruzione di originali analogici riprodotti secondo le regole tecniche di cui al DPCM 13.11.2014 e conservati secondo le regole tecniche di cui al DPCM 13.12.2013;
Reg. UE 679/2016 (GDPR)	Relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
Circolare 18 aprile 2017 n. 2/2017 dell'Agenzia per l'Italia Digitale	Recante le misure minime di sicurezza ICT per le pubbliche amministrazioni;

Notazione abbreviata	Riferimento
Circolare n. 2 del 9 aprile 2018	Recante i criteri per la qualificazione dei Cloud Service Provider per la PA;
Circolare n. 3 del 9 aprile 2018	Recante i criteri per la qualificazione di servizi SaaS per il Cloud della PA;
Reg. UE 2018/1807	Relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea;
DPCM 19 giugno 2019 n. 76	Regolamento di organizzazione del Ministero per i beni e le attività culturali, degli uffici di diretta collaborazione del Ministro e dell'Organismo indipendente di valutazione della performance.
Linee guida AgID ed Allegati	Linee guida sulla Formazione, Gestione, Conservazione dei documenti informatici Allegato 1 Glossario dei termini e degli acronimi Allegato 2 Formati di File e Riversamento Allegato 3 Certificazione di processo Allegato 4 Standard e specifiche tecniche Allegato 5 Metadati
Regolamento AgID ed Allegati	Regolamento sui criteri di conservazione Allegato A Requisiti per l'erogazione del servizio di conservazione per conto delle pubbliche amministrazioni Allegato B Piano di cessazione del servizio di conservazione dei documenti informatici
UNI 11386	Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.
ISO 14721	OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione.
ISO 15836	Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core
ISO/TR 18492	Long-term preservation of electronic document-based information.
ISO 20652	Space data and information transfer systems - Producer-Archive interface - Methodology abstract standard.
ISO 20104	Space data and information transfer systems — Producer-Archive Interface Specification (PAIS).

Notazione abbreviata	Riferimento
ISO/CD TR 26102	Requirements for long-term preservation of electronic records.
SIARD	Software Independent Archiving of Relational Databases 2.0 Ministère de la culture et de la communication, Service interministériel des Archives de France, Standard d'échange de donnéès pour l'archivage. Transfert – Communication – Élimination – Restitution - Modification, ver. 2.1, 2018
METS	Metadata Encoding and Transmission Standard
PREMIS	PREservation Metadata: Implementation Strategies.

torna al sommario

1.4 Riferimenti Tecnici

Riferimenti Tecnici	
Linee guida sulla formazione, gestione e conservazione dei documenti informatici	Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici, entrate in vigore il 1° gennaio 2022 come previsto nella proroga inserita nella determinazione n. 371/2021 del 17 maggio 2021.
Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici	Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici (testo con annessi Allegato A R*equisiti per l'erogazione del servizio di conservazione per conto delle pubbliche amministrazioni* e Allegato B *Piano di cessazione del servizio di conservazione dei documenti digitali*) che dal 1° gennaio 2022 abroga la Circolare AgID 10 aprile 2014, n. 65

torna al sommario

1.5 Ruoli e Responsabilità

Conformemente al par. 4.4 delle Linee guida sulla Formazione, gestione e conservazione dei documenti informatici, si individuano i seguenti ruoli coinvolti nel processo di conservazione:

a) **Titolare dell'oggetto della conservazione** (citato nel manuale come soggetto produttore), identificato come il soggetto produttore degli oggetti di conservazione.

   Trenitalia S.p.A.

   Sede Sociale: Piazza della Croce Rossa, 1 - 00161 Roma

   PI 05403151003

b) **Produttore dei PdV,** ovvero la persona fisica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione, identificato con il responsabile della gestione documentale nelle pubbliche amministrazioni

   Per Trenitalia il ruolo di Produttore dei PdV viene ricoperto dal responsabile della conservazione

c) **Utente abilitato,** ossia la persona, l'ente o il sistema che interagisce con i servizi di un sistema per la conservazione dei documenti informatici al fine di fruire delle informazioni di interesse.
   Trenitalia ha individuato degli utenti abilitati all'accesso, alla ricerca, alla visualizzazione e al download dei documenti posti in conservazione in funzione della Unità Locale a cui sono associati.

d) **Responsabile della conservazione**, ovvero il soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.

e) **Conservatore,** identificato come l'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, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti.

Trenitalia, con lettera di affidamento (vedi all. 4), ha affidato a Ferservizi la gestione del servizio di conservazione a norma in relazione agli obblighi di legge della documentazione del modulo MyRifiuto. Ferservizi a sua volta ha incaricato Unimatica – quale conservatore qualificato presso l'AgID - per l'esecuzione dell'attività. In merito ai ruoli e alle responsabilità del conservatore si rimanda a quanto esplicitato al par.4 del Manuale del Servizio di Conservazione di UNIMATICA, parte integrante del presente documento così come previsto dalla normativa attualmente vigente in materia.

torna al sommario

2 Processo di conservazione digitale a norma

2.1 Classi documentali

Le classi documentali oggetto della conservazione sono:

- ✓ Registro cronologico carico e scarico rifiuti

Tipo documento	formati	Metadati
Registro cronologico carico e scarico rifiuti	xml;	IDDOC__IMPRONTA IDDOC__ALGORITMO IDDOC__ID FORMAZIONE TIPO_DOCUMENTO TIPO_FLUSSO TIPO_REGISTRO NOREG__DATADOC NOREG__NUMDOC SOGGETTO__RUOLO#1 SOGGETTO__PG__ORGANIZZAZIONE#1 SOGGETTO__PG__CFPIVA#1 SOGGETTO__RUOLO#2 SOGGETTO__PG__ORGANIZZAZIONE#2 SOGGETTO__PG__CFPIVA#2 OGGETTO RISERVATO FORMATO FIRMATODIGITALMENTE SIGILLATOELETTRONICAMENTE MARCATURATEMPORALE CONFORMITACOPIEIMMAGINESUSUPPORTOINFORMATICO NOME_FILE VERSIONE TEMPO_CONSERVAZIONE

2.2 Processo di conservazione digitale del documento informatico

La conservazione dei documenti e dei fascicoli informatici è l'attività volta a proteggere e mantenere, cioè custodire, nel tempo gli archivi di documenti e dati informatici.

Il tempo di conservazione, come ricordato dall'art. 43 del CAD può essere “permanente”, cioè illimitato nel tempo oppure può avere una durata che sulla base del titolare di riferimento può equivalere a 1, 2, 5, 10 o 20 anni.

L’obiettivo primario di un sistema di conservazione a norma (fondato sullo standard ISO 14721:2012 altrimenti conosciuto come standard OAIS - Open Archival Information System) è quello di impedire la perdita o la distruzione non autorizzata dei documenti e di mantenere nel tempo le loro caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità. Per fare ciò è necessario offrire effettive garanzie di mantenimento delle caratteristiche dei documenti che assicurano il valore di fonte attendibile e di prova giuridicamente rilevante, avendo la capacità di dimostrare in sede giuridica che il processo conservativo è stato correttamente eseguito e il risultato è stato realmente conseguito. La sfida è garantire che in un futuro anche lontano i documenti informatici prodotti oggi possono continuare ad essere letti e utilizzati assicurando il loro valore giuridico e la loro corretta collocazione nell'ambito dell'archivio dei soggetti produttori.

Le caratteristiche sopra riportate sono definite nel glossario contenuto nell’Allegato 1 alle LLGG AgID.

Per riassumere in breve si può dire che:

- Autenticità: è la caratteristica di un documento informatico che fornisce la garanzia che il documento sia ciò che dichiara di essere, senza avere subito alterazioni o modifiche. Insieme di identità (identificazione e provenienza) e integrità;
- Integrità: è la qualità di un documento di essere completo e inalterato, cioè non avere subito modifiche non autorizzate;
- Affidabilità: esprime il livello di fiducia che l'utente, cioè colui che legge il documento ripone, o può riporre nel documento informatico, in particolare nella sua visualizzazione leggibile allo stesso;

- Leggibilità: è la caratteristica che definisce il mantenimento della fruibilità delle informazioni contenute nel documento durante l'intero ciclo di gestione dei documenti, cioè al momento della sua formazione o produzione, nelle sue forme di diffusione, nella sua memorizzazione e archiviazione e nella sua conservazione; in certi casi si può distinguere tra leggibilità da parte di sistemi informatici o leggibilità da parte di un essere umano;
- Reperibilità: esprime la capacità di reperire ed esibire il documento con le caratteristiche sopra riportate.

Quindi un documento correttamente conservato deve essere reperibile ed avere le caratteristiche di autenticità, integrità, affidabilità e leggibilità.

Tuttavia il tema della integrità, intesa come mantenimento della immodificabilità della sequenza di bit originari, fidando soprattutto su tecniche quali la firma digitale e sul mantenimento di supporti non riscrivibili, non è sufficiente per garantire una corretta conservazione permanente o nel lungo termine poiché non assicura il mantenimento della reperibilità, affidabilità e leggibilità degli oggetti conservati, rendendo in certi casi difficile anche verificarne l'autenticità soprattutto in rapporto al contesto di provenienza.

Tale consapevolezza ha trovato la sua prima definizione nell'art. 44 del CAD che ha introdotto il concetto di “sistema di conservazione”, definendolo come sistema che deve assicurare:

- l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione o dell'area organizzativa omogenea di riferimento, quindi identificazione della provenienza per valutarne le caratteristiche di autenticità;
- l'integrità del documento;
- la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi i dati di registrazione e di classificazione originari, quindi dei metadati associati ai documenti e la definizione delle aggregazioni documentali e delle articolazioni d'archivio di riferimento;
- il rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del D. Lgs. 30 giugno 2013, n. 196, e dal disciplinare tecnico pubblicato in allegato B a tale decreto.

Un sistema di conservazione è quindi un insieme di persone, apparecchiature, applicazioni e procedure dedicate in questo caso ad assicurare la conservazione, anche nel lungo termine, dei

documenti e delle aggregazioni documentali informatiche, con i rispettivi metadati garantendo il mantenimento delle caratteristiche sopra citate.

Nello specifico grande rilevanza hanno le regole e le procedure che si applicano, la professionalità delle persone addette e la qualità, in particolare in termini di robustezza, sicurezza ed affidabilità, delle tecnologie applicate.

Questo concetto è stato sviluppato nelle Linee guida AgID che hanno esplicitamente definito che gli oggetti della conservazione, per i quali il sistema di conservazione deve garantire le caratteristiche sopracitate dalla presa in carico dal Titolare dell'oggetto della conservazione, sono:

a) i documenti informatici e i documenti amministrativi informatici con i metadati ad essi associati;

b) i fascicoli informatici ovvero le aggregazioni documentali informatiche con i metadati ad essi associati.

Tali oggetti, conformemente allo standard OAIS sono trattati dal sistema in pacchetti informativi distinti in: pacchetti di versamento (Submission Information Package, SIP), pacchetti di archiviazione (Archival Information Package, AIP), pacchetti di distribuzione (Dissemination Information Package, DIP).

Tali pacchetti secondo il modello OAIS sono entità composte di quattro elementi:

- il contenuto informativo, cioè l'oggetto da conservare, il quale comprende: l'oggetto dati (data object) e l'insieme delle informazioni che ne permettono la rappresentazione e la comprensione (representation information);
- le informazioni sulla conservazione (preservation description information);
- le informazioni sull'impacchettamento;
- le informazioni descrittive sul pacchetto utilizzate per ricercare il pacchetto.

In sintesi, si può dire che la conservazione di un contenuto informativo presuppone la formazione e il mantenimento di un pacchetto informativo che, oltre al contenuto, contiene i metadati che lo identificano, lo qualificano sotto il profilo dell'integrità e lo collocano nel contesto di provenienza.

2.3 Sottoscrizione elettronica

Il file xml del Registro contiene la vidimazione virtuale rilasciata dal portale ministeriale RENTRI.

2.4 Marca temporale

non prevista

2.5 Estensione della validità del documento informatico

La marca temporale ha una validità limitata nel tempo pari a 20 anni e pertanto è sufficiente a coprire gli attuali periodi di conservazione delle tipologie di documenti con rilevanza fiscale, fissata al massimo in 10 anni.

Qualora un documento possa risultare utile anche oltre il periodo di validità della marca temporale associata, è possibile estenderne la validità, così come dichiarato all'art.53 comma 1 del DPCM 22 febbraio 2013 apponendo un'ulteriore marca prima della scadenza della precedente e così via nel tempo.

Il valore temporale di tale marca è determinato dal periodo in cui il certificatore avrà cura di conservarla. Conformemente al DPCM sopra citato le marche temporali sono valide per tutta la durata del periodo di conservazione.

Unimatica utilizza per il processo di conservazione marche temporali emesse da Certification Authority (CA) che garantiscono la loro conservazione su supporto non riscrivibile per la durata di venti anni. Ne consegue che il documento elettronico, sottoscritto con firma digitale e dotato di marca temporale è valido fino ad un massimo di 20 anni. Una nuova marca temporale può essere apposta per estenderne ulteriormente la validità nel caso gli effetti si debbano protrarre nel tempo oltre tale limite.

2.6 Memorizzazione del documento informatico

La memorizzazione di un documento informatico in un sistema di conservazione più in particolare deve rispettare quanto previsto dall'art. 44 del CAD, garantendo tra l'altro che, tramite l'adozione

di regole, procedure e tecnologie, il documento sia sempre leggibile e facilmente reperibile nell'archivio.

Nelle Linee guida AgID vengono anche definite le regole tecniche per la copia, duplicazione, riproduzione dei documenti informatici in modo tale che sia sempre possibile rispettare i dettami previsti per il sistema di conservazione al manifestarsi della eventuale obsolescenza delle tecnologie di memorizzazione adottate dal sistema stesso.

3 L'organizzazione del Servizio di Conservazione

Per l'organizzazione del lavoro del responsabile del servizio di conservazione si rimanda la lettura al paragrafo 5 Struttura organizzativa per il servizio di conservazione del Manuale del servizio di conservazione di Unimatica, parte integrante del presente manuale.

3.1 La manutenzione

Il Responsabile del servizio di conservazione, al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; si occupa, inoltre, di adottare analoghe misure con riguardo all'obsolescenza dei formati.

Ai fini della realizzazione, rafforzamento e mantenimento della sicurezza delle applicazioni, Unimatica ha definito regole e procedure che consentono di gestire in maniera controllata tutte le fasi costituenti il ciclo di vita delle applicazioni che si articolano in:

- sviluppo, ovvero definizione dei requisiti, disegno e implementazione e unit test;
- collaudo, ovvero test funzionali e di certificazione;
- manutenzione e modifica, ovvero gestione dei cambiamenti di natura adeguativa, correttiva ed evolutiva.

I cambiamenti che vengono apportati al sistema di conservazione risultano essere il prodotto di una proporzionata corrispondenza alle procedure di evoluzione tecnologica sia sulle strutture hardware sia su quelle software. Il Responsabile della funzione archivistica e il Responsabile dei sistemi informativi definiscono politiche, priorità e tempistiche affinché vengano garantite nel tempo integrità, disponibilità e sicurezza.

In caso di disservizi causati da problematiche riscontrate durante il processo di aggiornamento è possibile effettuare il ripristino delle versioni precedenti così da assicurare il corretto e continuo svolgimento delle attività.

Il Responsabile del servizio di conservazione e il Responsabile della sicurezza dei sistemi informativi periodicamente si occuperanno di aggiornare la normativa e gli standard di riferimento in base all'evoluzione di questi ultimi.

Per la manutenzione hardware e software del sistema di conservazione Unimatica si rimanda la lettura al paragrafo 8 Procedure di gestione ed evoluzione del Manuale del servizio di conservazione di Unimatica, parte integrante del presente manuale

3.2 Controllo degli accessi fisici e logici

In riferimento al controllo degli accessi, Unimatica ha predisposto una specifica procedura nella quale vengono dettagliatamente elencate le responsabilità ed i criteri per la gestione delle identità e degli accessi. Gli aspetti considerati dal responsabile della sicurezza oltre ai requisiti di sicurezza sono:

- identificazione: che rappresenta l'atto con cui un soggetto dichiara la propria identità; è il primo passo dell'autenticazione;
- autenticazione: consiste nel processo di verifica dell'identità dichiarata dal soggetto ed è correlata all'identificazione;
- autorizzazione: è la concessione dei diritti di accesso al soggetto dopo che questo sia stato identificato ed autenticato;
- tracciabilità: è l'azione continua di registrazione delle azioni svolte dal soggetto precedentemente identificato in modo univoco.

L'accessibilità al servizio di conservazione per l'attività di consultazione tramite apposito portale è consentita al solo personale autorizzato dal responsabile della conservazione o suo delegato, attraverso log-in con credenziali personali (userID e password) rilasciate dal conservatore.

Le credenziali affidate al personale autorizzato sono personali, devono essere custodite con cura e non devono essere rese note ad altri. Nel caso l'utente abbia il dubbio che le proprie credenziali non siano più sicure è indispensabile che modifichi quanto prima la propria password. Nel caso in cui non sia in grado di cambiarla dovrà esplicitamente fare richiesta ad Unimatica di reset della password.

Per il controllo degli accessi logici e fisici al sistema di conservazione Unimatica si rimanda la lettura al paragrafo 8.1 Misure di sicurezza logica del manuale del servizio di conservazione di Unimatica, parte integrante del presente manuale.

3.3 Registrazione e de-registrazione degli utenti

Unimatica prevede e attua una procedura formale per la registrazione e disattivazione degli utenti, per garantire e revocare l'accesso a tutte le informazioni ed i servizi del sistema di conservazione sulla base di quanto richiesto esplicitamente dal Responsabile della conservazione o suo delegato.

La creazione o la rimozione di una utenza viene richiesta dal titolare dell'oggetto della conservazione a Unimatica attraverso l'invio di una email da recapitare alla casella del servizio di assistenza a ciò dedicato. L'email deve riportare gli estremi per l'individuazione certa dell'operatore da abilitare e le autorizzazioni da attribuire. Verificata l'autorevolezza del richiedente e la validità delle informazioni (nominativi utenti da abilitare, ruoli e ragione sociale azienda), il personale di Unimatica a ciò autorizzato genera le utenze sul portale. La creazione dell'utenza comporta l'invio automatico alla casella email dell'utente di una password temporanea da modificare al primo accesso al portale.

3.4 Caratteristiche e gestione delle password

Le utenze applicative sono gestite secondo criteri idonei a garantire il rispetto dell'applicazione di misure di sicurezza tecniche e organizzative tali da garantire un livello di sicurezza adeguato al rischio ai sensi dell'art. 32 del GDPR. Si riportano di seguito alcune delle misure di sicurezza adottate:

- ✓ Utilizzo di password complesse definite secondo i seguenti criteri:
  - la password non deve essere visibile in fase di inserimento nelle sessioni di login ed è cifrata all'interno del Data Base;
  - la password:
    - deve avere una lunghezza compresa fra 8 e 25 caratteri;
    - deve contenere almeno un carattere speciale, un carattere maiuscolo, un carattere minuscolo ed un numero;
    - non può contenere il nome dell'utente;
    - non può contenere il cognome dell'utente;
    - non può contenere l'username dell'utente;
    - non può essere una delle ultime 4 utilizzate;
  - la password ha una scadenza oltre la quale deve essere rinnovata;

- al primo utilizzo si deve creare la password, il sistema invia una mail all'utente con l'indicazione del link a cui accedere per creare la sua password che rimane crittografata;
- il sistema deve avvertire l'utente della necessità di rinnovare la password;

✓ Applicazione del principio 'segregation of duty' nel rilascio delle credenziali (utente, password e profilo), vale a dire separazione tra chi rilascia e chi utilizza le credenziali di accesso ai dati;

✓ Applicazione del principio 'need to know' nel rilascio dei profili, vale a dire rilascio dei soli diritti per eseguire le attività di competenza;

✓ Assegnazione ad ogni utente di credenziali (user e password) personali, uniche e non assegnabili ad altri utenti;

✓ Revisione periodica degli utenti e dei relativi profili.

Per le caratteristiche e la gestione delle password sul sistema di conservazione Unimatica si rimanda la lettura al paragrafo 8.1.1 Gestione Utenze del Manuale del servizio di conservazione di Unimatica, parte integrante del presente manuale.

4 Processo di Conservazione

4.1 Struttura Pacchetto di Versamento (PdV)

I documenti prodotti da MyRifiuto verranno inviati tramite il servizio GoToDoc al servizio di conservazione di Unimatica con chiamate REST.

4.2 Interfaccia di alimentazione

Il conservatore lavora a lotti di documenti.

L'unità minima di caricamento è quindi un lotto che corrisponde al pacchetto di versamento (PdV).

Un lotto è composto dal documento principale e dal rispettivo indice di versamento.

4.3 Struttura e logiche di generazione del PdV

MyRifiuto in qualità di Produttore genera il documento da conservare in formato xml che contiene:

- Le informazioni del registro generate da RENTRI
- i movimenti elaborati dai dati presenti su MyRifiuto secondo le regole espresse da RENTRI ed in osservanza di AGID

Invia con una frequenza mensile il PdV a FileNet tramite Go2Doc chiedendone la conservazione. È dunque Go2Doc che genera formalmente il Pacchetto di Versamento che verrà inviato in conservazione.

4.4 Trasferimento del Pacchetto di Versamento

La trasmissione del PdV verso il servizio di conservazione prevede l'uso del servizio REST.

4.5 Controlli effettuati sui PdV e sugli oggetti in esso contenuti

All'atto della ricezione dei documenti contenuti all'interno del PdV, il sistema di conservazione esegue le seguenti operazioni:

- ✓ Verifica della presenza dei metadati obbligatori e di quelli concordati;

- ✓ Verifica della correttezza dell'impronta hash del documento ricevuto;
- ✓ Verifica del formato del documento con quanto concordato col Titolare dell'oggetto della conservazione;
- ✓ Verifica della firma digitale su ogni documento.

Il sistema verifica le firme presenti su tutti i documenti inviati ed acquisisce le informazioni sulla validità e scadenza dei certificati.

L'esito positivo delle verifiche effettuate sui Pacchetti di versamento viene registrato in un Rapporto di versamento di presa in carico. Il Rapporto conterrà un'impronta del file originale comprensivo di algoritmo con la quale tale impronta viene calcolata (hash) e un riferimento temporale certificato che costituisce evidenza dell'esistenza e dell'esatta composizione del Rapporto collegato all'istante indicato.

Le verifiche effettuate sui Pacchetti di versamento possono risultare negative. Nei casi in cui anche solo su uno dei controlli indicati si dovesse riscontrare una mancanza o non corrispondenza di informazioni viene generato un file di Comunicazione delle anomalie che verrà comunicato mediante un file di esito al Soggetto produttore. Tale Comunicazione comprenderà i dettagli delle verifiche eseguite sui Pacchetti di versamento comprensive delle precisazioni sulle anomalie.

Per il dettaglio del processo si rimanda ai paragrafi 7.4 Accettazione dei Pacchetti di versamento e generazione del Rapporto di versamento di presa in carico e 7.5 Rifiuto dei Pacchetti di versamento e modalità di comunicazione delle anomalie del Manuale del sistema di conservazione di Unimatica, parte integrante del presente manuale.

4.6 Portale Unimatica

Per l'erogazione del servizio di conservazione, Unimatica mette a disposizione un Portale Web di produzione attraverso il quale gli utenti, autorizzati e opportunamente profilati, possono ricercare e visualizzare tutti i documenti conservati.

I documenti sono disponibili per l'esibizione on-line per tutto il periodo di conservazione, cioè nella finestra temporale di almeno 10 anni antecedenti dalla data di conservazione dell'ultimo documento conservato.

4.7 Rapporto di versamento

Il Rapporto di versamento attesta la corretta esecuzione del processo di immissione dei Pacchetti, ha la funzione di raccogliere evidenze indirette di tutti i documenti del Pacchetto e garantisce due principali funzioni:

- ✓ la possibilità di provare l'integrità dei dati di ogni file contenuto nel pacchetto,
- ✓ di permettere il controllo dell'integrità per ogni file in modo separato, senza creare un'interdipendenza tra i file ai fini dell'esibizione e del controllo.

Il Rapporto di versamento è un file in formato XML che riporta, per ognuno dei file inclusi nel Pacchetto, alcune informazioni tra cui un "URN" (unified resource name) e un "hash". L'URN è una stringa univoca che identifica l'oggetto digitale, mentre l'hash è un'impronta del documento ovvero una sequenza di bit che può essere ricavata dal file in modo ripetibile e standardizzato e che garantisce una corrispondenza esatta col contenuto originale (in modo pratico possiamo dire di avere la garanzia che a due file differenti corrispondono sempre due impronte distinte).

Apponendo un timestamp al Rapporto di versamento lo si "sigilla" e contemporaneamente si fissa il riferimento temporale. Tale procedimento costituisce un riferimento temporale certificato per il Rapporto di versamento.

Per il dettaglio del processo si rimanda al paragrafo 7.4 Accettazione dei Pacchetti di versamento e generazione del Rapporto di versamento di presa in carico del Manuale del sistema di conservazione di Unimatica, parte integrante del presente manuale.

4.8 Pacchetti di Distribuzione (PdD)

Il Pacchetto di Distribuzione (PdD), disponibile per ogni documento posto in conservazione digitale a norma e fruibile tramite l'interfaccia web del sistema di conservazione a cui gli utenti autenticati possono accedere, è composto da:

- Attestazione – Contiene le prove di conservazione del documento conservato e, in particolare, il Rapporto di Versamento (RdV) e il Pacchetto di Archiviazione (PdA). In quest'ultimo folder possono essere presenti sia la Marca di Conservazione prodotta da

Unimatica che l'attestazione del precedente conservatore (Marca di Conservazione Esterna) nel caso di documento migrato e riconservato.

- Documenti – Contiene il documento conservato nel suo formato originale e un subfolder "Allegati" contenente la quota parte di metadati relativi al documento conservato estratti dal PdV.
- Regole di Attestazione - In questa cartella verranno posizionati tutti i file xsd di validazione presenti nel documento SiNCro per rendere auto-consistente il pacchetto in fase di esibizione anche in modalità offline.

4.9 Verifica Impronta Hash

Il calcolo dell'impronta hash di un documento conservato viene effettuata tramite apposito software utilizzando l'algoritmo SHA 256 con trasformazione su base 64.

Per convertire l'impronta sha 256 Hex to Base64 può essere utilizzato un qualunque convertitore presente in rete.

4.10 Processo di Conservazione a norma

Il servizio offerto dal conservatore viene avviato al termine di un processo di attivazione che segue queste fasi fondamentali:

- condivisione di informazioni tecniche di richiesta configurazione e invio dei Pacchetti di versamento;
- verifiche sui Pacchetti di versamento e sugli oggetti in esso contenuti;
- accettazione dei Pacchetti di versamento e generazione del Rapporto di versamento di presa in carico;
- rifiuto dei Pacchetti di versamento e modalità di comunicazione delle anomalie;
- preparazione e gestione del Pacchetto di archiviazione;
- preparazione e gestione del Pacchetto di distribuzione ai fini dell'esibizione;

Ognuno degli step sopra indicati viene eseguito per ogni tipologia di configurazione richiesta.

Per il dettaglio del processo si rimanda all'intero capitolo 7 Il processo di erogazione del servizio di conservazione del Manuale del sistema di conservazione di Unimatica, parte integrante del presente manuale.

4.11 Procedura di gestione delle copie di sicurezza

Le procedure informatiche adottate consentono la gestione globale del processo di conservazione: dall'importazione del flusso informatico (file immagini e file dati) alla costituzione automatica dell'archivio digitale su supporti magnetici di tipo Storage in modalità DR presso i Data Center Unimatica.

Sono disponibili due modalità di esibizione dei documenti, comprendente il documento stesso e le relative prove di conservazione (il cosiddetto PdD):

- mediante interazione con il Portale di Conservazione "on the fly", estraendo il singolo PdD;
- mediante estrazione massiva dei documenti conservati su richiesta esplicita da parte del Titolare dell'oggetto della conservazione.

Il risultato di tale estrazione viene reso disponibile su media cumulativi, contenenti i documenti, le prove di conservazione e un sottosistema applicativo autonomo che consente la ricerca dei documenti, la visualizzazione dei metadati ad essi associati e lo scaricamento del PdD.

Tali media possono essere resi disponibili mediante canale telematico (SFTP, S3 o altro da concordare) oppure su supporto fisico (HDU o solid state device).

Per garantire la continuità dei servizi Unimatica ha predisposto non solo le componenti tecnologiche necessarie allo scopo, ma anche un adeguato piano di "Disaster-Recovery" (di seguito più semplicemente indicato anche come "DR") e di "Back-Up e Restore" che coinvolgono tutte le risorse aziendali necessarie e quindi: il personale, gli impianti ed i processi organizzativi interni necessari per l'attuazione di quanto previsto nei suddetti piani operativi.

Il sistema di monitoraggio e di auditing consente di effettuare una costante supervisione dell'intera operatività del sistema e del rispetto delle indicazioni previste dai diversi piani operativi. Compito

della Direzione Aziendale è quindi la costante verifica dell'attuazione dei piani operativi necessari per garantire la continuità di servizio e di porre rimedio ad eventuali difformità dovessero essere segnalate dal personale preposto alla gestione operativa dei sistemi o dovessero pervenire da clienti ed utenti dei servizi informatici erogati dalla Server Farm di Unimatica S.p.A

La società Unimatica nel suo complesso (e quindi per tutti i reparti dell'azienda) ha adottato i criteri di gestione della qualità previsti dalla normativa ISO 9001:2015 ed è in possesso della relativa certificazione per i settori EA 33 ed EA 35.

Unimatica è certificata ISO/IEC 27001:2013 per la sicurezza dei sistemi informativi e dei servizi erogati dall'azienda tramite le proprie server farm e data center. Relativamente ai servizi di Conservazione a norma, inoltre, Unimatica è qualificata presso il Marketplace di AgID ed è certificata in conformità ai requisiti individuati nell'art. 24 del Regolamento (UE) 910/2014 eIDAS ed opera quindi in piena conformità agli standard normativi, procedurali e di sicurezza richiesti da AgID.

Per il dettaglio del processo si rimanda all'intero capitolo 7 il processo di erogazione del servizio di conservazione e al paragrafo 8.1.4 Gestione dei backup e Disaster Recovery del Manuale del sistema di conservazione di Unimatica, parte integrante del presente manuale.

4.12 Procedure di gestione della Privacy

Ai sensi e per gli effetti dell'articolo 28 del Regolamento (UE) n. 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e del D.lgs. 30 giugno 2003 n. 196, relativamente e limitatamente ai trattamenti riguardanti la conservazione degli oggetti digitali affidati a Unimatica, a partire dalla data di sottoscrizione del contratto, Trenitalia, nella sua qualità di Titolare del trattamento ed in virtù del contratto con protocollo "Ferservizi-AD\PRT\P\2024\0004843" del 21/02/2024 stipulato con Ferservizi, affida a quest'ultima (vedi All.4), che si avvarrà a sua volta di Unimatica, il trattamento dei dati personali previsto dal contratto in essere tra le Parti. A tale proposito si evidenzia che, come da contratto "Accordo Quadro Rubrica n. 86/2023/FSTECH dell'11/10/2023", in essere tra Ferservizi S.p.A ed Unimatica S.p.A., l'Allegato A include un accordo di Data Protection Titolare-Responsabile tra Ferservizi S.p.A. ed Unimatica.

4.13 Analisi dei rischi e contromisure

Il servizio di conservazione erogato da Unimatica SpA è certificato ISO 27001 ed ha inoltre il certificato di conformità all'art 24 del Regolamento eIDAS basato sui controlli della check list disposta da AgID. Nell'ambito di queste certificazioni Unimatica ha definito le modalità con cui sono valutati i rischi potenziali sugli asset del servizio, trattati durante l'intero processo di conservazione.

Per il dettaglio del processo si rimanda la lettura ai paragrafi 8.1.3 8.1.3 Gestione degli incidenti di sicurezza e 8.1.4 Gestione dei backup e Disaster Recovery del Manuale del sistema di conservazione di Unimatica, parte integrante del presente manuale.

4.14 Verifica ispettiva presso Unimatica (esibizione, ricerca e consultazione documenti

Nei casi in cui, come previsto dall'art. 23-bis, c. 2 del Codice dell'Amministrazione Digitale il Titolare dell'oggetto della conservazione richieda la presenza di un pubblico ufficiale, Unimatica garantirà tale presenza mettendo a disposizione tutte le necessarie risorse che serviranno all'espletamento delle attività

Le attività di esibizione, ricerca e consultazione seguono il consueto iter previsto per la distribuzione dei pacchetti, pertanto si garantisce l'adeguata fornitura di documenti e relative prove di conservazione.

Con la richiesta da parte dell'utente di esibizione dei Pacchetti di distribuzione viene generata una copia autentica del documento, conforme all'originale.

Inoltre, in caso di adeguamento del formato dovuto all'evoluzione tecnologica verranno rispettate tutte le procedure messe in atto da Unimatica. Anche in questo caso, sarà garantita l'eventuale presenza del pubblico ufficiale per l'attestazione di conformità.

5 Allegati

5.1 Allegato 1: Manuale del servizio di conservazione UNIMATICA SPA

5.2 Allegato 2: Allegato A Servizio di Conservazione a norma e provider SDI - Accordo di Data Protection

5.3 Allegato 3: Incarico e Delega a Unimatica Spa al ruolo di Responsabile del servizio di Conservazione Digitale a Norma

5.4 Allegato 4: Richiesta Affidamento a Ferservizi del Servizio di Conservazione Digitale a Norma

5.5 Allegato 5: Affidamento a Ferservizi del Servizio di Conservazione Digitale a Norma