

Adozione autorizzata dal Ministero della Cultura –  
Soprintendenza Archivistica e Bibliografica della Puglia  
ai sensi dell'art. 21 comma 4 del D.lgs. 22 gennaio 2004  
n. 42, espressa con la nota prot. n. 3232-P del 16 dicembre  
2024



## Manuale di conservazione del Comune di Modugno

<b>Versione nr.</b>	<b>Data</b>	<b>Descrizioni delle modifiche</b>	<b>Note</b>
1.0	2025	versione allineata alle LG Agid sulla formazione, gestione e conservazione dei documenti informatici – 9 settembre 2020 s.m.i.	Delibera GC

# 1. Scopo e ambito del documento

## 1.1 Premesse e finalità

Il Comune di Modugno ha scelto per la conservazione dei documenti informatici prodotti un modello in outsourcing, esternalizzando il servizio di conservazione.

Lo scopo del presente Manuale è quello di illustrare l'organizzazione, i soggetti coinvolti e i rispettivi ruoli, il modello di funzionamento, la descrizione delle attività svolte dal Comune di Modugno relativamente alla creazione e al versamento dei pacchetti informativi (Submission information package o pacchetto di versamento) nel sistema di conservazione, nonché il controllo periodico dell'effettiva accessibilità e fruibilità del patrimonio informativo e documentario conservato su base digitale.

Per quanto riguarda la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione, delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento nel tempo del sistema di conservazione, la descrizione delle modalità di svolgimento del processo di esibizione e di esportazione delle unità conservate, la produzione dei duplicati e delle copie dei contenuti informativi conservati si rimanda ai Manuali di conservazione dei conservatori esterni.

## 1.2 Ambito di applicazione

Il presente Manuale è adottato ai sensi delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici paragrafo 4.6.

Esso descrive il sistema di conservazione dei documenti informatici e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture, fornendo le istruzioni per la corretta produzione dei pacchetti di versamento nonché per le fasi successive inerenti al processo di conservazione a lungo termine.

Si rinvia, per le parti di competenza, ai Manuali dei conservatori esterni, da considerarsi quale parte integrante e sostanziale anche se non materialmente allegati.

Si precisa che il Manuale illustra il solo procedimento di conservazione di documenti informatici, mentre non tratta alcun aspetto in merito alla gestione dei documenti analogici.

## 1.3 Modello di riferimento

Il sistema di conservazione, previsto dalla normativa nazionale, si basa sul modello internazionale OAIS - Open Archival Information System (ISO: 14721). Pertanto, la struttura e l'articolazione del sistema di conservazione nonché le modalità di gestione degli oggetti digitali si riferiscono al modello OAIS.

# 2. Terminologia e normativa

## 2.1 Glossario

<b>Accesso</b>	Operazione che consente di prendere visione dei documenti informatici
<b>Affidabilità</b>	Caratteristica che, con riferimento a un sistema di gestione documentale o conservazione, esprime il livello di fiducia che l'utente ripone nel sistema stesso mentre, con riferimento al documento informatico, esprime la credibilità e l'accuratezza della rappresentazione di atti e fatti in esso contenuta
<b>Agenzia per l'Italia digitale – AgID</b>	Ente preposto alla realizzazione degli obiettivi dell'Agenda digitale italiana, istituita con art. 19 del D.L. 22 giugno 2012, n.83, svolge funzioni di coordinamento, indirizzo e regolazione affidate prima a DigitPA

<b>Aggregazione documentale informatica</b>	Insieme di documenti informatici o insieme di fascicoli informatici riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente
<b>Archivio informatico</b>	Archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche
<b>Area Organizzativa Omogenea (AOO)</b>	Un insieme di funzioni e di uffici individuati dall'ente al fine di gestire i documenti in modo unitario e coordinato, secondo quanto disposto dall'art. 50 comma 4 del D.P.R. 28 dicembre 2000, n. 445. Essa rappresenta il canale ufficiale per l'invio di istanze e l'avvio di procedimenti amministrativi
<b>Autenticità</b>	Caratteristica in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto un oggetto è autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze
<b>Certification Authority (CA)</b>	Il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime
<b>Certificatore</b>	Soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto dall'AgID il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
<b>Certificazione</b>	Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi
<b>Conservatore</b>	Soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici
<b>Conservazione</b>	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governare la gestione in relazione al modello organizzativo adottato, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti
<b>Conservazione dei documenti informatici</b>	Processo finalizzato ad assicurare la permanenza nel tempo dell'integrità, della disponibilità, della leggibilità del documento nonché dei dati necessari per la sua rappresentazione ed individuazione
<b>Copia analogica di documento informatico</b>	Documento analogico avente contenuto identico a quello del documento informatico da cui è tratto, ai sensi dell'art. 23, del D. Lgs 7 marzo 2005, n.82
<b>Copia informatica di documento analogico</b>	Documento informatico avente contenuto identico a quello del documento analogico da cui è tratto (art 1 c. i-bis, D.Lgs 7 marzo 2005, n.82)
<b>Copia per immagine su supporto informatico di documento analogico</b>	Documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto (art. 1, c. i-ter, del D. Lgs. 7 marzo 2005, n. 82)
<b>Copia informatica di documento informatico</b>	Documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari (art. 1, c. i-quater, del D. Lgs. 7 marzo 2005, n. 82)
<b>Digitalizzazione</b>	Processo che, mediante opportuni strumenti tecnologici e un sistema documentale, consente la produzione nativa digitale dei documenti

<b>Documento elettronico</b>	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva
<b>Documento informatico</b>	Documento elettronico che contiene la rappresentazione informatica di atti, fatti giuridicamente rilevanti
<b>Documento amministrativo informatico</b>	Ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa
<b>Duplicato informatico</b>	Documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo, o su dispositivi diversi, della medesima sequenza di valori binari del documento originario
<b>Esibizione</b>	Operazione che consente di visualizzare un documento conservato
<b>Evidenza informatica</b>	Sequenza finita di bit che può essere elaborata da una procedura informatica
<b>Formato del documento informatico</b>	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
<b>Identificativo univoco</b>	Sequenza di numeri o caratteri alfanumerici associata in modo univoco e persistente ad un'entità all'interno di uno specifico ambito di applicazione
<b>Impronta crittografica</b>	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di hash crittografica ad un'evidenza informatica
<b>Manuale di conservazione</b>	Documento che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture
<b>Metadati</b>	Dati associati a un documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017
<b>Oggetto di conservazione</b>	Oggetto digitale versato in un sistema di conservazione
<b>Oggetto digitale</b>	Oggetto informativo digitale che può assumere varie forme tra le quali quelle di documento informatico, fascicolo informatico, aggregazione documentale informatica o archivio informatico
<b>Pacchetto di archiviazione - PdA</b>	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel manuale di conservazione
<b>Pacchetto di distribuzione - PdD</b>	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione
<b>Pacchetto di versamento - PdV</b>	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione
<b>Pacchetto informativo</b>	Contenitore logico che racchiude uno o più oggetti di conservazione con i relativi metadati, oppure anche i soli metadati riferiti agli oggetti di conservazione

<b>Piano della sicurezza del sistema di conservazione</b>	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi
<b>Presenza in carico</b>	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione e, in caso di affidamento del servizio all'esterno, dagli accordi stipulati tra il titolare dell'oggetto di conservazione e il responsabile del servizio di conservazione
<b>Processo di conservazione</b>	Insieme delle attività finalizzate alla conservazione dei documenti informatici
<b>Produttore dei PdV</b>	Persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel Sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con il Responsabile della gestione documentale
<b>Rapporto di versamento</b>	Documento informatico che attesta l'avvenuta presa in carico da parte del Sistema di conservazione dei pacchetti di versamento inviati dal Produttore
<b>Registro di protocollo</b>	Registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel Sistema di gestione informatica dei documenti
<b>Responsabile del servizio di conservazione</b>	Soggetto che coordina il processo di conservazione all'interno del conservatore, in possesso dei requisiti professionali individuati da AgID
<b>Responsabile della conservazione</b>	Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia
<b>Responsabile della sicurezza dei sistemi di conservazione</b>	Soggetto che assicura il rispetto dei requisiti di sicurezza all'interno del conservatore, in possesso dei requisiti professionali individuati da AgID
<b>Responsabile dello sviluppo e della manutenzione del sistema di conservazione</b>	Soggetto che assicura lo sviluppo e la manutenzione del sistema all'interno del conservatore, in possesso dei requisiti professionali individuati da AgID
<b>Responsabile del trattamento dei dati</b>	Persona fisica, o giuridica, o pubblica amministrazione o qualsiasi altro ente, associazione od organismo, preposti dal titolare al trattamento dei dati personali, di cui all'art. 28 del Regolamento UE 679/2016.
<b>Responsabile della protezione dei dati</b>	Persona con conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, in grado di assolvere i compiti di cui all'articolo 39 del Regolamento UE 679/2016
<b>Scarto</b>	Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico-culturale
<b>Sistema di conservazione - SdC</b>	Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, comma 1, del CAD
<b>Titolare dell'oggetto di conservazione</b>	Soggetto produttore degli oggetti di conservazione

<b>Utente abilitato</b>	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse
<b>Versamento di documento in conservazione</b>	Operazione mediante la quale il documento viene inviato al Sistema di conservazione

## 2.2 Acronimi

<b>AgID</b>	Agenzia per l'Italia digitale
<b>AIP</b>	Archival information package (Pacchetto di archiviazione - PdA)
<b>ASP</b>	Application Service Provider
<b>ASCII</b>	American Standard Code For Information Interchange
<b>CA</b>	Certification Authority
<b>CAD</b>	Codice dell'Amministrazione Digitale
<b>CAS</b>	Content Addressed Storage
<b>DIP</b>	Dissemination information package (Pacchetto di distribuzione - PdV)
<b>eIDAS</b>	Regolamento UE n.910 del 23 luglio 2014
<b>FTP</b>	File Transfer Protocol
<b>HSM</b>	Hardware Security Module
<b>IPA</b>	Indice delle Pubbliche Amministrazioni
<b>IPDA</b>	Cfr. Indice del pacchetto di archiviazione
<b>ISO</b>	International Organization for Standardization ovvero l'Organizzazione internazionale per la normazione (Organizzazione per la definizione di norme tecniche)
<b>OAIS</b>	Open Archival Information System
<b>PdA</b>	Pacchetto di Archiviazione
<b>PdD</b>	Pacchetto di Distribuzione
<b>PdV</b>	Pacchetto di Versamento
<b>PiC</b>	Presa in Carico
<b>RdV</b>	Rapporto di versamento
<b>SAN</b>	Storage Attached Network

<b>SinCro</b>	Supporto all'interoperabilità nella conservazione e nel recupero degli oggetti digitali
<b>SIP</b>	Submission Information Package (Pacchetto di versamento - PdD)
<b>TSA</b>	Time Stamping Authority
<b>URL</b>	Universal Resource Locator
<b>VdC</b>	Volume di Conservazione

## 2.3 Normativa di riferimento

Si richiama la normativa di riferimento citata in Glossario e normativa di riferimento, allegato 1 al Manuale di gestione documentale.

## 2.4 Standard di riferimento

Si elencano gli standard di riferimento previsti dalla normativa vigente.

- ISO 14721 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ISO/IEC 27001, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ETSI TS 101 533-1 V 1.3.1 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;
- UNI 11386 Standard SInCRO – Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali
- UNI ISO 15489-2 Informazione e documentazione - Gestione dei documenti di archivio – Linee Guida sul record management;
- ISO 15836 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core;
- ISO/TS 23081 Information and documentation - Records management processes –Metadata for records.

## 3. Modello operativo adottato

Il Comune di Modugno ha esternalizzato il servizio di conservazione come descritto nella tabella seguente:

Conservatore digitale	Durata del servizio/Atto di conferimento	Oggetto servizio
Unimatica	Avvio del servizio: 06/05/2024.	Servizio di conservazione dell'archivio digitale del Comune

Il presente Manuale integra, per le parti specifiche di competenza del Comune di Modugno e per quanto riguarda i rapporti con i conservatori, i Manuali di conservazione dei conservatori e gli Accordi di servizio sottoscritti tra i conservatori e il Comune di Modugno, in cui sono definite le specifiche operative e le modalità di descrizione e di versamento nel Sistema di conservazione digitale dei documenti informatici e delle aggregazioni documentali informatiche oggetto di conservazione.

## 4. Oggetti e responsabilità

Titolare dell'oggetto di conservazione, soggetto produttore degli oggetti di conservazione, è il Comune di Modugno. Al suo interno è stato individuato il produttore dei pacchetti di versamento (PdV) che provvede a monitorare la generazione automatica e la trasmissione al Sistema di conservazione dei pacchetti di versamento nelle modalità e con i formati concordati e descritti nel Manuale di conservazione del Sistema di conservazione.

L'Ente ha individuato il Responsabile della conservazione con Decreto Sindacale n. 24/2023 prot. n. 49323 del 09.10.2023, nella persona del Responsabile del Servizio Affari Generali Contratti Demografico che cura il rapporto con il Conservatore avvalendosi del supporto tecnico informatico del personale del Servizio Innovazione Tecnologica, che provvede a verificare il buon esito dell'operazione di trasferimento al Sistema di conservazione tramite la presa visione del rapporto di versamento prodotto dal Sistema di conservazione stesso.

Il Conservatore è soggetto esterno in grado di offrire idonee garanzie di sicurezza organizzative e tecnologiche certificate e validate, svolge materialmente il processo di conservazione ospitando l'infrastruttura hardware e software del sistema di conservazione; adotta le misure necessarie per la sicurezza fisica e logica del sistema preposto al processo di conservazione digitale e delle copie di sicurezza nei supporti di memorizzazione.

Il Conservatore è responsabile in merito alle procedure adottate nel processo di conservazione dalla presa in carico dei documenti e fino all'eventuale cancellazione, mentre la responsabilità del contenuto dei documenti versati nel sistema di conservazione è in capo al Comune di Modugno.

In sintesi, le responsabilità sono ripartite come segue.

#### Titolare dell'oggetto di conservazione:

- redazione dei documenti secondo la normativa vigente, comprese le attività di protocollazione, classificazione e fascicolazione;
- registrazione in appositi registri di alcune tipologie documentali;
- estrazione degli oggetti destinati alla conservazione dai propri sistemi (gestionali e specifici per la gestione documentale) e il versamento nei modi e nei tempi prestabiliti.

Inoltre, è responsabilità del Comune:

- inviare in conservazione i documenti in tempo utile affinché la conservazione possa avvenire nel rispetto delle tempistiche imposte dalla normativa;
- trasmettere i propri documenti al sistema di conservazione in forma stabile e non modificabile.

Nello specifico, ai sensi del paragrafo 4.5 delle Linee guida sulla formazione, gestione e conservazione dei documenti informatici, il Responsabile della conservazione:

- definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;
- gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
- genera e sottoscrive il rapporto di versamento, secondo le modalità previste dal Manuale di conservazione;
- genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal Manuale di conservazione;
- effettua il monitoraggio della corretta funzionalità del Sistema di conservazione;
- effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;
- 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; adotta analoghe misure con riguardo all'obsolescenza dei formati;
- provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal Manuale di conservazione;
- predispone le misure necessarie per la sicurezza fisica e logica del Sistema di conservazione come previsto dal par. 4.11;
- assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
- assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
- predispone il Manuale di conservazione di cui al par. 4.7 e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

#### Conservatore:

- definizione delle caratteristiche e dei requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare;
- gestione del processo di conservazione per garantire nel tempo la conformità alle normative vigenti;
- produzione del rapporto di versamento;
- generazione e sottoscrizione del pacchetto di distribuzione con firma digitale, nei casi previsti;
- monitoraggio della corretta funzionalità del Sistema di conservazione;
- verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
- al fine di garantire la conservazione e l'accesso ai documenti informatici, adozione di misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità;
- adozione analoghe misure con riguardo all'obsolescenza dei formati;

- duplicazione o copia dei documenti informatici in relazione all’evolversi del contesto tecnologico;
- adozione delle misure necessarie per la sicurezza fisica e logica del Sistema di conservazione;
- aggiornamento periodico del Manuale di conservazione in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti;
- attuazione di procedure di sicurezza e tracciabilità che consentano di risalire in ogni momento alle attività effettuate durante l’esecuzione operativa di conservazione;
- gestione delle procedure informatiche ed organizzative per la corretta tenuta dei supporti su cui vengono memorizzati i documenti informatici oggetto di conservazione;
- controllo funzionamento delle procedure informatiche atte ad esibire la documentazione conservata, in caso di richieste formulate da chi ne abbia titolo;
- adozione di un registro cronologico degli eventi (di gestione, accessi, attività, ecc.) del Sistema di conservazione;
- monitoraggio dei sistemi software e hardware coinvolti;
- analisi del log di sistema e di sicurezza;
- verifica della validità delle firme digitali e delle marche temporali utilizzate dal Sistema di conservazione ed emesse da *Certification Authority* italiane, accreditate e riconosciute.

Nel processo di conservazione intervengono diversi soggetti aventi profili, compiti e responsabilità differenziate. I ruoli e le responsabilità interne ai Conservatori sono elencate nel Manuale di conservazione degli stessi.

Si allega al presente documento il Manuale del Conservatore operante nel Comune: le eventuali modifiche nel tempo devono comportare un aggiornamento formale del presente documento.

I ruoli e le responsabilità interne nel Comune di Modugno sono i seguenti:

<b>Ruolo</b>	<b>Soggetto</b>	<b>Attività di competenza</b>
Legale rappresentante	Sindaco pro tempore	Definizione delle <i>policies</i> di formazione, gestione e conservazione dei documenti
Responsabile della conservazione	Responsabile del Servizio Affari Generali Contratti Demografico che cura il rapporto con il Conservatore avvalendosi del supporto tecnico informatico del personale del Servizio Innovazione Tecnologica.	Supervisione, controllo procedure e monitoraggio processo di conservazione digitale

<p>Responsabile del servizio di conservazione</p>	<p>Responsabile del servizio di conservazione presso il Conservatore</p>	<ul style="list-style-type: none"> <li>a) definire le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;</li> <li>b) gestire il processo di conservazione e garantirne nel tempo la conformità alla normativa vigente;</li> <li>c) generare e sottoscrivere il rapporto di versamento, secondo le modalità indicate specificatamente nel manuale di conservazione o con le modalità riportate dal contratto o dall'accordo di servizio;</li> <li>d) generare e sottoscrivere il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti specificatamente dal manuale di conservazione o con le modalità riportate dal contratto o dall'accordo di servizio;</li> <li>e) effettuare il monitoraggio della corretta funzionalità del sistema di conservazione;</li> <li>f) effettuare la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;</li> <li>g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adottare misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adottare analoghe misure con riguardo all'obsolescenza dei formati;</li> <li>h) provvedere alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;</li> <li>i) predisporre le misure necessarie per la sicurezza fisica e logica del sistema di conservazione come previsto dal par. 4.10 delle Linee guida dell'Agenzia per l'Italia digitale (AgID) sulla formazione, gestione e conservazione dei documenti informatici</li> </ul>
---	--	--

Responsabile della protezione dei dati	Responsabile incaricato dall'Amministrazione (DPO esterno)	Definizione delle policies per la gestione ed il trattamento dei dati personali
Responsabile della sicurezza informatica	Responsabile Servizio Informatica	Gestione dei sistemi informatici, gestione back up dei dati, profilazione delle utenze
Soggetto produttore PdV	Responsabile Servizio Affari Generali Contratti Demografico avvalendosi del supporto tecnico informatico del personale del Servizio Staff Sindaco e Giunta - Innovazione Tecnologica.	Produzione del pacchetto di versamento con responsabilità del trasferimento del suo contenuto nel Sistema di conservazione
Delegati all'operatività dal Responsabile della conservazione	Incaricati per la gestione operativa	Gestione operativa dell'attività di conservazione

Le Linee guida sulla formazione, gestione e conservazione dei documenti informatici prevedono al Par. 4.5 che nel caso in cui il servizio di conservazione venga affidato ad un conservatore, le attività suddette o alcune di esse ricadenti sul Responsabile della conservazione, ad esclusione della stesura del Manuale di conservazione, potranno essere affidate al responsabile del servizio di conservazione, rimanendo in ogni caso inteso che la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile, rimane in capo al responsabile della conservazione, chiamato altresì a svolgere le necessarie attività di verifica e controllo in ossequio alle norme vigenti sui servizi affidati in outsourcing dalle PA.

Il Comune, avvalendosi di tale possibilità normativa, ha delegato il Responsabile del servizio di conservazione del Conservatore, con specifico atto (n. prot. 15765 del 26-03-2024).

Le Linee guida sulla formazione, gestione e conservazione dei documenti informatici prevedono inoltre il ruolo dell'Utente abilitato, inteso come una persona, ente o sistema che interagisce con i servizi del Sistema di conservazione al fine di fruire delle informazioni di interesse.

Il Responsabile della conservazione abilita nel ruolo di Utente gli operatori che possono accedere ai documenti versati secondo le regole di visibilità e di accesso concordate con il Conservatore e riportate negli Accordi di servizio sottoscritti tra le parti.

Gli operatori abilitati nel ruolo di Utente per il Servizio di conservazione dell'archivio digitale del Comune sono:

- Responsabile della conservazione;
- I delegati del Servizio Innovazione Tecnologica in qualità di referenti tecnici;
- I delegati del Servizio Innovazione Tecnologica in qualità di referenti tecnici per il controllo periodico sui report;

Gli operatori abilitati nel ruolo di Utente per gli altri Servizi e solo per l'accesso agli strumenti del relativo conservatore, sono autorizzati previa verifica e comunicazione da parte del Responsabile della conservazione.

Le Autorità incaricate di effettuare i controlli hanno diritto di accedere in qualsiasi momento al Sistema di conservazione.

L'Utente abilitato richiede al Sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge.

Il Sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, ai documenti informatici conservati e consente la produzione di un Pacchetto di distribuzione direttamente acquisibile dai soggetti autorizzati con le modalità e orari indicati negli Accordi di servizio sottoscritti dalle parti.

## 5. Oggetti sottoposti a conservazione

Ai sensi del paragrafo 4.6 delle Linee guida sulla formazione, gestione e conservazione dei documenti informatici vi è obbligo in carico alla Pubblica Amministrazione di individuare e pubblicare i tempi di versamento, le tipologie documentali trattate, i metadati, le modalità di trasmissione dei PdV e le tempistiche di selezione e scarto dei propri documenti informatici. Nel presente paragrafo e nei successivi verranno esplicitati i suddetti aspetti.

Gli oggetti sottoposti a conservazione sono:

- documenti informatici con i metadati ad essi associati;
- aggregazioni documentali informatiche (fascicoli e serie) con i metadati ad esse associati contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che costituiscono le aggregazioni medesime.

Gli oggetti digitali sono trattati dal Sistema di conservazione come pacchetti informativi, intesi come contenitori che racchiudono uno o più oggetti da trattare (documenti informatici, fascicoli informatici, aggregazioni informatiche oppure anche i soli metadati riferiti agli oggetti da conservare o conservati) e comprendono anche le informazioni per la loro interpretazione e rappresentazione.

I pacchetti informativi quindi contengono non solo il documento e/o l'aggregazione (ciò che deve essere conservato) ma anche i metadati necessari a garantirne la conservazione e l'accesso nel lungo periodo.

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.

Il pacchetto informativo, a seconda che sia utilizzato per versare, conservare o distribuire gli oggetti digitali sottoposti a conservazione, assume la forma, rispettivamente di:

- PdV - pacchetti di versamento;
- PdA - pacchetti di archiviazione;
- PdD - pacchetti di distribuzione.

Il trasferimento nel Sistema di conservazione avviene sotto forma di pacchetti di versamento (PdV), che contengono gli oggetti da conservare. In base alle esigenze possono contenere una o più unità archivistiche, una o più unità documentarie, eventuali aggiornamenti all'unità documentaria già versata o solo informazioni da associare a un'unità documentaria già conservata.

La presa in carico dei pacchetti di versamento da parte del Conservatore dà origine ai pacchetti di archiviazione (PdA) contenenti tutte le informazioni già contenute nel pacchetto informativo con associate le informazioni generate dal Sistema di conservazione durante il processo di versamento e presa in carico. Le informazioni sono rappresentate in un file .xml.

Gli oggetti sottoposti a conservazione sono resi disponibili dal Conservatore, su richiesta da parte del Soggetto produttore, mediante pacchetti di distribuzione (PdD).

I documenti informatici sono suddivisi in tipologie documentarie, che identificano gruppi documentali omogenei per natura e funzione giuridica, modalità di registrazione o di produzione. Tale suddivisione è funzionale all'individuazione, per ogni singola tipologia documentaria, di un set di metadati standard e di articolazioni o strutture di composizione omogenee.

## 5.1 Metadati

Così come previsto nell'allegato n. 5 alle Linee guida sulla formazione, gestione e conservazione dei documenti informatici, ad ogni oggetto digitale versato è associato un set di metadati, rappresentati in un file .xml e ritenuti essenziali per la corretta conservazione dei documenti. Le tipologie documentarie individuate ed i relativi metadati concordate con il Conservatore, sono elencate nella documentazione tecnica descrittiva del servizio di conservazione.

## 5.2 Formati

I documenti informatici sottoposti a conservazione devono essere rappresentati in formati idonei alla conservazione a lungo termine. In conformità alle indicazioni fornite dall'allegato n. 2 delle Linee guida di Agid sulla formazione, gestione e conservazione dei documenti informatici il Comune di Modugno ammette per l'invio in conservazione documenti informatici nei seguenti formati standard: \*.avi, \*.bmp, \*.csv, \*.docx, \*.dwg, \*.eml, \*.gif, \*.htm, \*.html, \*.jpg, \*.log, \*.m7d, \*.m7m, \*.mp3, \*.mp4, \*.mpeg, \*.png, \*.pptx, \*.psp, \*.rtf, \*.tif, \*.tiff, \*.tsd, \*.txt, \*.wav, \*.xlsx, \*.xml, \*.ods, \*.odt, \*.p7c, \*.p7m, \*.p7s, \*.pdf, \*.pdf/A.

Si elencano di seguito i formati delle classi documentali che vengono mandate attualmente in conservazione:

Tipologie documentarie	Formati
Registro giornaliero di protocollo	.pdf; .pdf/A
Registro annuale pubblicazioni albo pretorio	.pdf/A; .p7m

Deliberazioni di Consiglio comunale comprensive degli allegati parte integrante e non parte integrante	.pdf; .pdf/A; .p7m;
Verbali delle sedute del Consiglio comunale	.pdf; .pdf/A; .p7m
Deliberazioni di Giunta comunale comprensive degli allegati parte integrante e non parte integrante	.pdf; .pdf/A; .p7m
Determinazioni dei Responsabili dei Servizi comprensive degli allegati parte integrante e non parte integrante	.pdf; .pdf/A; .p7m
Contratti e scritture private formalizzati dal Servizio Contratti e contratti attuativi degli accordi quadro dei Servizi Lavori Pubblici e Servizio Assetto del Territorio	.pdf; .pdf/A; .p7m
Scritture private formalizzate dagli altri Servizi (protocolli d'intesa, patti di collaborazione, accordi di collaborazione)	.pdf; .pdf/A; .p7m
Ordinativi informatici di incasso	.pdf; .pdf/A; .tiff; .jpeg; office open xml; .odf; .xml
Avvisi di accertamento ICI-IMU-TASI	.pdf; .pdf/A; .tiff; .jpeg; office open xml; .odf; .xml
Fatture elettroniche	.xml
Fatture attive	.xml
Ordinativi informatici di pagamento	.pdf; .pdf/A; .tiff; .jpeg; office open xml; .odf; .xml
Appalti di servizi e forniture: documenti aggiudicatario prodotti per la partecipazione alla procedura; verbali: verbale di individuazione elenco operatori o operatore singolo, verbali sedute di gara, verbale proposta aggiudicazione; verbale congruità offerta; verbale di efficacia	.pdf; .pdf/A; .p7m
Pratiche edilizie	.pdf; .pdf/A; .p7m
Elaborati progettuali di lavori/opere pubbliche	.pdf; .pdf/A; .p7m
Appalti di lavori/opere pubbliche: documenti aggiudicatario prodotti per la partecipazione alla procedura; verbali: verbale di individuazione elenco operatori o operatore singolo, verbali sedute di gara, verbale proposta aggiudicazione; verbale congruità offerta, verbale di efficacia	.pdf; .pdf/A; .p7m;
Verbali di contravvenzione al Codice della strada	.pdf; .pdf/A; .tiff; .jpeg; office open xml; .odf; .xml
Relazioni di servizio del Settore Polizia Locale	.pdf; .pdf/A; .tiff; .jpeg; office open xml; .odf; .xml
Verbali degli accertamenti nei diversi settori (edilizio, sanitario, commerciale, anagrafico, sociale, etc.)	.pdf; .pdf/A; .tiff; .jpeg; office open xml; .odf; .xml

### 5.3 Gestione del fascicolo informatico

Il Conservatore, mediante il proprio sistema di conservazione, deve essere in grado di accettare e gestire, come richiesto ai sensi dell'art. 44, comma 1-bis, del CAD:

- a) i fascicoli informatici chiusi e le serie informatiche chiuse;
- b) i fascicoli informatici e le serie non ancora chiusi accettando i documenti in essi contenuti sulla base di specifiche esigenze del soggetto produttore. In particolare, in questo caso, il Titolare e il Conservatore garantiscono specifico monitoraggio al fine di evitare rischi di obsolescenza tecnologica che possono sopravvenire prima della chiusura.

Il sistema di conservazione deve essere predisposto per accettare aggregazioni documentali e tutte le tipologie di documenti informatici relativi a diversi ambiti applicativi. L'indicazione delle tipologie documentali, compresa la gestione di queste, è indicata nella scheda cliente allegata al contratto stipulato con il soggetto produttore. Il conservatore accetta e conserva solo documenti informatici. Il sistema di conservazione permette l'acquisizione sia di documenti firmati digitalmente, sia di documenti non firmati. Con l'ausilio del Responsabile del servizio di conservazione, è il Soggetto produttore a definire nella scheda cliente le modalità di trattamento dei documenti firmati o non firmati.

## 6. Il processo di conservazione

### 6.1 Creazione e versamento dei pacchetti di versamento (PdV)

La creazione dei pacchetti informatici di versamento sulla base dei modelli e delle regole concordati con i conservatori e definiti nei rispettivi Accordi di servizio, avviene come di seguito descritto:

Tipologie documentarie	Modalità di versamento	Canale privilegiato di trasmissione del PdV
Registro giornaliero di protocollo	Automatica schedulata	conferimento tramite Webservices (SOAP XML) con comunicazione tra sistemi tramite canale di invio S-FTP)
Registro annuale pubblicazioni albo pretorio	no	Attraverso piattaforma informatica messa a disposizione dal conservatore
Deliberazioni di Consiglio comunale comprensive degli allegati parte integrante e non parte integrante	Automatica schedulata	conferimento tramite Webservices (SOAP XML) con comunicazione tra sistemi tramite canale di invio S-FTP)
Verbali delle sedute del Consiglio comunale	no	conferimento tramite Webservices (SOAP XML) con comunicazione tra sistemi tramite canale di invio S-FTP)
Deliberazioni di Giunta comunale comprensive degli allegati parte integrante e non parte integrante	Automatica schedulata	conferimento tramite Webservices (SOAP XML) con comunicazione tra sistemi tramite canale di invio S-FTP)
Determinazioni dirigenziali comprensive degli allegati parte integrante e non parte integrante	Automatica schedulata	conferimento tramite Webservices (SOAP XML) con comunicazione tra sistemi tramite canale di invio S-FTP)
Contratti e scritture private formalizzati dal Servizio Contratti e contratti attuativi degli accordi quadro dei Servizi Lavori Pubblici e Servizio Assetto del Territorio	no	Attraverso piattaforma informatica messa a disposizione dal conservatore
	no	

Scritture private formalizzate dagli altri Servizi (protocolli d'intesa, patti di collaborazione, accordi di collaborazione)	no	Attraverso piattaforma informatica messa a disposizione dal conservatore
--	----	--

d'intesa, patti di collaborazione, accordi di collaborazione)		
Ordinativi informatici di incasso	Come specificato nella convenzione relativa al Servizio di tesoreria	Come specificato nella convenzione relativa al Servizio di tesoreria
Avvisi di accertamento ICI-IMU-TASI	Automatica schedulata	conferimento tramite Webservices (SOAP XML) con comunicazione tra sistemi tramite canale di invio S-FTP)
Fatture elettroniche	Automatica schedulata	conferimento tramite Webservices (SOAP XML) con comunicazione tra sistemi tramite canale di invio S-FTP)
Fatture attive	Manuale	Attraverso piattaforma informatica messa a disposizione dal conservatore
Ordinativi informatici di pagamento	Come specificato nella convenzione relativa al Servizio di tesoreria	Come specificato nella convenzione relativa al Servizio di tesoreria
Appalti di servizi e forniture: documenti aggiudicatario prodotti per la partecipazione alla procedura; verbali: verbale di individuazione elenco operatori o operatore singolo, verbali sedute di gara, verbale proposta aggiudicazione; verbale congruità offerta, verbale di efficacia	Automatica schedulata	conferimento tramite Webservices (SOAP XML) con comunicazione tra sistemi tramite canale di invio S-FTP)
Pratiche edilizie	Automatica schedulata	conferimento tramite Webservices (SOAP XML) con comunicazione tra sistemi tramite canale di invio S-FTP)
Elaborati progettuali di lavori/opere pubbliche	Automatica schedulata	conferimento tramite Webservices (SOAP XML) con comunicazione tra sistemi tramite canale di invio S-FTP)
Appalti di lavori/opere pubbliche: documenti aggiudicatario prodotti per la partecipazione alla procedura; verbali: verbale di individuazione elenco operatori o operatore singolo, verbali sedute di gara, verbale proposta aggiudicazione; verbale congruità offerta, verbale di efficacia	Automatica schedulata	conferimento tramite Webservices (SOAP XML) con comunicazione tra sistemi tramite canale di invio S-FTP)

Verbali di contravvenzione al Codice della strada	Automatica schedulata	Conferimento tramite web services con comunicazione tra sistemi mediante canale di invio HTTPS o SFTP
Relazioni di servizio del Servizio Polizia Locale	Automatica	Conferimento tramite web services con comunicazione tra sistemi mediante canale di invio HTTPS o SFTP
Verbali degli accertamenti nei diversi settori (edilizio, sanitario, commerciale, anagrafico, sociale, etc.)	Automatica schedulata	Conferimento tramite web services con comunicazione tra sistemi mediante canale di invio HTTPS o SFTP

Le tempistiche di generazione e invio dei pacchetti di conservazione sono a cadenza programmata, concordata con il Conservatore sulla base delle esigenze del Produttore, della natura dei documenti trasferiti e delle normative di settore. Le tempistiche stabilite, specificate nella documentazione tecnica descrittiva del Servizio di conservazione, sono:

<b>Tipologie documentarie</b>	<b>Periodicità di conferimento pacchetto di versamento</b>	<b>Periodicità creazione pacchetto di archiviazione</b>
Registro giornaliero di protocollo	Giornaliero	Giornaliero
Registro annuale di protocollo	Annuale	Annuale
Registro pubblicazione albo pretorio	Annuale	Annuale
Deliberazioni di Consiglio comunale comprensive degli allegati parte integrante e non parte integrante	Giornaliero	Al raggiungimento di una dimensione di pacchetto concordata
Verbali della seduta del Consiglio comunale	9 mesi dopo la seduta	9 mesi dopo la seduta
Deliberazioni di Giunta comunale comprensive degli allegati parte integrante e non parte integrante	Giornaliero	Al raggiungimento di una dimensione di pacchetto concordata
Determinazioni dei Responsabili di Servizio comprensive degli allegati parte integrante e non parte integrante	Giornaliero	Al raggiungimento di una dimensione di pacchetto concordata
Contratti e scritture private formalizzati dal Servizio Contratti e contratti attuativi degli accordi quadro dei Settori Edilizia scolastica, Edilizia civile e sociale	Mensile	Mensile

Copie autentiche digitali di atti notarili (in cui il Comune è parte) a partire dall'anno 2021	Mensile	Mensile
Scritture private formalizzate dagli altri Settori (protocolli d'intesa, patti di collaborazione, accordi di collaborazione)	Giornaliero	Al raggiungimento di una dimensione di pacchetto concordata
Ordinativi informatici di incasso	Annuale	Annuale
Avvisi di accertamento ICI-IMU-TASI	Mensile	Al raggiungimento di una dimensione di pacchetto concordata
Fatture elettroniche	Giornaliero	Al raggiungimento di una dimensione di pacchetto concordata
Fatture attive	Annuale	Annuale
Ordinativi informatici di pagamento	Annuale	Annuale
Appalti di servizi e forniture: documenti aggiudicatario prodotti per la partecipazione alla procedura; verbali: verbale di individuazione elenco operatori o operatore singolo, verbali sedute di gara, verbale proposta aggiudicazione; verbale congruità offerta, verbale di efficacia	Giornaliero	Al raggiungimento di una dimensione di pacchetto concordata
Pratiche edilizie	Giornaliero	Al raggiungimento di una dimensione di pacchetto concordata
Elaborati progettuali di lavori/opere pubbliche	Giornaliero	Al raggiungimento di una dimensione di pacchetto concordata
Appalti di lavori/opere pubbliche: documenti aggiudicatario prodotti per la partecipazione alla procedura; verbali: verbale di individuazione elenco operatori o operatore singolo, verbali sedute di gara, verbale proposta aggiudicazione; verbale congruità offerta, verbale di efficacia	Giornaliero	Al raggiungimento di una dimensione di pacchetto concordata
Verbali di contravvenzione al Codice della strada	Giornaliero	Giornaliero
Relazioni di servizio del Servizio Polizia Locale	Giornaliero	Giornaliero
Verbali degli accertamenti nei diversi settori (edilizio,	Giornaliero	Giornaliero

sanitario, commerciale, anagrafico, sociale, etc.)		
---	--	--

## 6.2 Modalità di acquisizione pacchetti versamento

I pacchetti di versamento (PdV) acquisiti dal Sistema di conservazione sono sottoposti ai controlli stabiliti negli Accordi di servizio.

A titolo esemplificativo i controlli riguardano integrità del documento, completezza delle informazioni di conservazione, uso di formati compatibili con il processo di conservazione, leggibilità e verificabilità delle firme associate agli oggetti digitali, dimensioni dei file e dei pacchetti di versamento, ecc.

Se le verifiche si concludono positivamente viene generato il rapporto di versamento che determina la presa in carico del contenuto informativo e l'assunzione di responsabilità da parte del Conservatore.

I rapporti di versamento sono trasmessi tramite automatismo informatico, al termine del processo di invio in conservazione al Responsabile della conservazione del Comune di Modugno, al Responsabile del Servizio Staff Sindaco e Giunta - Innovazione Tecnologica in qualità di referente tecnico e infine al Soggetto produttore del PdV.

Il rapporto di versamento attesta la corretta esecuzione del processo di immissione dei pacchetti, ha la funzione di raccogliere evidenze dei documenti del pacchetto e garantisce due principali funzioni:

- provare l'integrità dei dati di ogni file contenuto nel pacchetto,
- 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 viene conservato all'interno del Sistema di conservazione, garantendone l'ininterrotta custodia e la non modificabilità.

Le verifiche sopra indicate possono dare anche esito negativo e in tal caso il sistema segnala la presenza di un'anomalia. Si hanno documenti anomali quando è avvenuta una corruzione o perdita di dati, ad esempio i dati sono memorizzati su formati non compatibili, sono presenti metadati mancanti, documenti con firma scaduta, ecc.

In questi casi il pacchetto di versamento non viene accettato nel Sistema di conservazione e viene inviata opportuna comunicazione al Responsabile della conservazione e al Produttore dei PdV affinché si proceda alla verifica e risoluzione dell'anomalia, rielaborando e reinviando successivamente un nuovo PdV.

## 6.3 Pacchetto di archiviazione (PdA)

Il pacchetto di archiviazione (PdA) è il pacchetto di informazioni destinato alla conservazione a lungo termine.

Il PdA si ottiene dalla trasformazione di uno o più pacchetti di versamento (PdV). Le specifiche tecniche e le modalità operative per la creazione dei pacchetti di archiviazione da parte dei Conservatori sono descritte nei Manuali di conservazione dei conservatori coinvolti.

Tutti i PdA sono firmati digitalmente dal Responsabile del servizio di conservazione e su di essi viene apposta una marca temporale.

Il lotto di documenti sottoposti a conservazione viene riepilogato in un file di chiusura, detto Indice del pacchetto di archiviazione (IPdA) o Indice di conservazione, il quale costituisce l'evidenza informatica associata ad ogni PdA. L'indice viene sottoscritto digitalmente e marcato temporalmente.

Nel caso di difformità rispetto a quanto concordato tra il Comune e il Conservatore, che riguardano la generazione dei pacchetti di archiviazione, sarà necessario redigere un verbale di non conformità da allegare al pacchetto di archiviazione.

Le notifiche ricevute relative alla certificazione del pacchetto di archiviazione sono conservate tramite interfaccia web sul Sistema di conservazione.

## 6.4 Pacchetto di distribuzione (PdD)

Il documento conservato deve essere leggibile in qualunque momento presso il Sistema di conservazione e disponibile su richiesta anche su supporto ottico e/o analogico.

Al fine di rendere disponibile l'informazione (*dissemination*) e rispettare così l'obbligo di esibizione dei documenti conservati, il sistema deve restituire in qualsiasi momento la documentazione richiesta dal produttore o altro "utente" assicurandone l'autenticità rispetto all'originale. In base agli ID univoci dei documenti il sistema localizza i documenti conservati nei diversi PdA ed effettua un duplicato. I duplicati dei documenti informatici richiesti sono inseriti all'interno di un pacchetto di distribuzione (PdD) che viene firmato digitalmente dal responsabile del servizio di conservazione.

La modalità di richiesta di un pacchetto di distribuzione e l'esibizione dello stesso avvengono come di seguito specificato:

<b>Formato dei documenti esibiti</b>	<b>Modalità di richiesta di esibizione degli oggetti</b>	<b>Modalità di esibizione degli oggetti digitali</b>
File ZIP	Tramite interfaccia web sul sistema di conservazione	Tramite interfaccia web sul sistema di conservazione

Gli utenti abilitati dal Comune all'accesso al sistema sono elencati al precedente capitolo 4 e sono riportati negli Accordi di Servizio sottoscritti con il Conservatore.

In merito alla produzione delle copie si rimanda al Manuale di conservazione del Conservatore.

## 7. Sistema di conservazione

L'architettura generale del Sistema di conservazione, gli applicativi software utilizzati, le componenti logiche e tecnologiche del sistema installato presso il Conservatore sono descritti nel Manuale di conservazione del conservatore, allegato al presente documento.

## 8. Monitoraggio e controlli

Conservare un contenuto informativo digitale significa mantenere nel tempo la capacità di riprodurlo con il contenuto e la forma originaria. In altre parole, significa mantenere, attraverso il Sistema di conservazione, la capacità di leggere la relativa sequenza binaria nella sua interezza, di interpretarla con le regole del formato elettronico, di visualizzare, a video, a stampa o su un altro dispositivo di output, il documento risultante.

Per mantenere nel lungo periodo l'autenticità, l'integrità e la leggibilità di tutti i documenti conservati nel sistema, il Conservatore ha predisposto e attua un piano della sicurezza volto ad individuare e correggere tempestivamente eventuali processi di corruzione dei documenti e dei supporti.

E' compito del Conservatore pianificare le tempistiche e le attività inerenti i controlli per la verifica dei documenti conservati e assicurare la leggibilità nel tempo.

Rimane di competenza del Responsabile della conservazione del Comune di Modugno effettuare controlli sull'attività dei Conservatori e verificare la disponibilità del patrimonio documentale versato.

Le modalità di verifica avvengono attraverso degli accessi mensili al Sistema di conservazione nonché in caso di notifica relativa al mancato versamento del/dei pacchetto/i.

## 9. Scarto

Il processo di selezione e scarto include gli interventi finalizzati da una parte alla selezione e conservazione della documentazione avente valore giuridicamente e storicamente rilevante e dall'altra alla distruzione di parte della documentazione giudicata irrilevante.

Tale eliminazione è necessaria per ottenere una ordinata tenuta dell'archivio e per evitare l'accumulo di masse ingenti di documentazione che ha esaurito la propria validità giuridica e/o amministrativa e che può essere scartata.

Il processo di cancellazione/inibizione avviene per tutte le repliche dei documenti presenti sul sistema di conservazione, oltre che nell'archivio di deposito digitale e, nelle more di adozione dello stesso, nel sistema di gestione documentale.

Il Comune di Modugno si è dotato del Piano di conservazione come disposto dall'art. 68 del DPR 28 dicembre 2000 n. 445, allegato al Manuale di gestione documentale.

I tempi di conservazione dei documenti inviati in conservazione sono i seguenti:

<b>Tipologie documentarie</b>	<b>Tempi di conservazione</b>
Registro giornaliero di protocollo	Illimitato
Registro pubblicazioni albo pretorio	20 anni
Deliberazioni di Consiglio comunale comprensive degli allegati parte integrante e non parte integrante	Illimitato
Verbali delle sedute del Consiglio comunale	Illimitato
Deliberazioni di Giunta comunale comprensive degli allegati parte integrante e non parte integrante	Illimitato
Determinazioni dirigenziali comprensive degli allegati parte integrante e non parte integrante	Illimitato
Contratti e scritture private formalizzati dal Servizio Contratti e contratti attuativi degli accordi quadro dei Settori Edilizia scolastica, Edilizia civile e sociale	Illimitato
Copie autentiche digitali di atti notarili (in cui il Comune è parte) a partire dall'anno 2021	Illimitato
Scritture private formalizzate dagli altri Settori (protocolli d'intesa, patti di collaborazione, accordi di collaborazione)	Illimitato
Ordinativi informatici di incasso	10 anni
Avvisi di accertamento ICI-IMU-TASI	10 anni salvo contenziosi
Fatture elettroniche	10 anni
Fatture attive	10 anni
Ordinativi informatici di pagamento	10 anni
Appalti di servizi e forniture: documenti aggiudicatario prodotti per la partecipazione alla procedura; verbali: verbale di individuazione elenco operatori o operatore singolo, verbali sedute di gara, verbale proposta aggiudicazione; verbale congruità offerta, verbale di efficacia	Illimitato
Pratiche edilizie	Illimitato
Elaborati progettuali di lavori/opere pubbliche	Illimitato
Appalti di lavori/opere pubbliche: documenti aggiudicatario prodotti per la partecipazione alla procedura; verbali: verbale di individuazione elenco operatori o operatore singolo, verbali sedute di gara, verbale proposta aggiudicazione; verbale congruità offerta, verbale di efficacia	Illimitato
Verbali di contravvenzione al Codice della strada	10 anni salvo contenziosi
Relazioni di servizio del Settore Polizia Locale	20 anni salvo contenziosi
Verbali degli accertamenti nei diversi settori (edilizio, sanitario, commerciale, anagrafico, sociale, etc.)	Illimitato

Per ciascuna operazione di scarto viene generato un rapporto di scarto che dovrà essere conservato ed inviato alla Soprintendenza archivistica e bibliografica della Puglia per certificare l'avvenuta distruzione della documentazione. Le modalità pratiche di attivazione e gestione della procedura di scarto sono descritte nel Manuale di conservazione dei conservatori.

## 10. Misure di sicurezza

Ai sensi delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici paragrafo

**4.10 Misure di sicurezza** “le Pubbliche Amministrazioni sono tenute ad ottemperare alle misure minime di sicurezza ICT emanate dall’AgID con circolare del 18 aprile 2017, n. 2/2017. In tale ottica, il responsabile della conservazione, di concerto con il responsabile per la transizione digitale, con il responsabile della gestione documentale e acquisito il parere del responsabile della protezione dei dati personali, predisponde il piano della sicurezza del sistema di gestione informatica dei documenti, prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali, ai sensi dell’art. 32 del Regolamento UE 679/2016, anche in funzione delle tipologie di dati trattati, quali quelli riferibili alle categorie particolari di cui agli artt. 9-10 del Regolamento stesso”.

Nel caso di affidamento esterno del Servizio di conservazione le misure di sicurezza tecniche e organizzative sono le seguenti:

- Gestione delle utenze: le utenze devono essere rilasciate da un ente (o persona) differente dall’ente o persona che le utilizzerà. Nell’ambito del servizio di conservazione, le utenze applicative e di sistema sono gestite secondo criteri idonei a garantire il rispetto dell’applicazione di misure di sicurezza tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio ai sensi dell’art. 32 del GDPR. Si riportano di seguito alcune delle misure di sicurezza da adottarsi: utilizzo di password complesse (la password non deve essere visibile in fase di inserimento nelle sessioni di login e sia criptata all’interno del Data Base; la password deve avere una lunghezza compresa fra 8 e 25 caratteri e 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 scadenza della password è configurabile attraverso un parametro; il sistema deve forzare l’utente a cambiare la password al primo utilizzo; 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);
- Gestione sistemi di protezione: la realizzazione logica della rete deve essere fatta secondo i seguenti criteri: controllo degli accessi e dei flussi realizzato tramite firewall in cross-mode (doppio Cisco Pix-535) ed utilizzo di software IP Tables per il port e IP filtering; filtro sui flussi di traffico da/per Internet costituito da sistemi McAfee Sidewinder ridonati, che effettuano deep packet inspection e forniscono funzionalità di firewall applicativo (livello 7 OSI); segregazione della rete e suddivisione della medesima in differenti porzioni dedicate alla rete di Back End dati per i server contenenti i data base, alla rete di Front End per la parte di presentazione, alla rete di gestione per l’amministrazione (funzione di supporto tecnico) della piattaforma; gli accessi alla rete sono segregati a livello di porte ed indirizzi IP. Gli accessi agli apparati di rete devono essere sottoposti a misure rigide di controllo e sono consentiti solamente agli amministratori della medesima. Allo scopo di evitare che eventuali malintenzionati possano forzare le protezioni presenti per accedere in maniera illecita a dati riservati, la barriera di firewall applicativi deve fornire anche un costante monitoraggio contro accessi non autorizzati tramite funzionalità IPS (Intrusion Prevention System). La gestione degli incidenti di sicurezza deve essere regolamentata da specifiche procedure dettagliatamente descritte secondo requisiti conformi allo standard ISO 27001:2013. La segnalazione di anomalie può scaturire: dalle attività di monitoraggio; da specifica segnalazione da parte di un utente o di personale interno. In entrambi i casi, qualora la segnalazione implichi un problema di sicurezza, inficiando quindi l’integrità, riservatezza o disponibilità del dato, la prassi per la gestione degli incidenti può prevedere l’apertura di un ticket. Il Service Owner (ovvero il responsabile del Settore), designa operatori per la gestione operativa degli incidenti; una volta preso in carico il ticket da un operatore egli diventa Incident Owner, cui sono delegate le azioni di: Contenimento, Eliminazione delle cause, Ripristino.
- Gestione dei back-up e disaster recovery: l’architettura del sistema backup deve essere composta da un master server per ogni sito e da differenti media server che hanno il compito di archiviare i dati ed inserirli in una rete dedicata, parallela a quella di erogazione dei singoli servizi, per non impattare sulle prestazioni e sulla disponibilità di questi ultimi, durante la normale esecuzione delle attività di backup. I singoli agent installati sull’infrastruttura di virtualizzazione e sui server non virtualizzati comunicano con il backup server che esegue il salvataggio dei dati su un appliance Data Domain. Il salvataggio dei dati su un appliance Data Domain viene replicato sul sito secondario. Questo sistema deve consentire: semplicità di integrazione anche con future evoluzioni del software di backup; de-duplicazione del dato ad alta velocità; replica efficiente in rete; scalabilità dell’infrastruttura. L’architettura di backup deve utilizzare le seguenti tecnologie: data domain DD4200; data

domain DD4100; data domain DD2500; software di backup NetBackup di Symantec; software di backup vRanger di DELL; software di backup con modulo di cifratura dei dati; rete di backup con throughput a 10 Gbit/s; replica dei dati di backup tramite link a 400 Mbit/s fra sito primario e secondario. I servizi di conservazione devono essere erogati tramite Data Center Primari e Data Center Secondari che svolgono il compito di Backup Remoto e di Disaster Recovery (D/R), al fine di garantire gli opportuni livelli di continuità del servizio. I Data Center devono avere una distanza fra loro superiore 200 e 300 Km e la disponibilità di servizio è H24 per tutti e 4. I Data Center secondari permettono di usufruire dei servizi in Produzione anche in caso di indisponibilità dei Data Center Primari.

## **11. Tutela dei dati personali**

### **11.1. Responsabile del trattamento dei dati personali**

A norma del Regolamento generale sulla protezione dei dati personali 679/2016 dell'Unione Europea (Regolamento 679/2016/UE) art. 28 e del D. Lgs. 196/2003 come novellato dal D. Lgs. 101/2018, il Conservatore effettua trattamenti per conto del Titolare del trattamento dei dati personali, intesi come “(...) qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale”. In qualità di Responsabile del trattamento dei dati il Conservatore mette in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti previsti dalla normativa e garantisca la tutela dei diritti dell'interessato.

## **12. Disposizioni finali**

### **12.1 Revisione**

Il Responsabile della conservazione cura l'aggiornamento periodico del Manuale di conservazione in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Atteso il rapido evolversi della legislazione in materia di gestione e conservazione documentale e di digitalizzazione della Pubblica Amministrazione, si evidenzia che le disposizioni normative citate, in vigore al momento dell'approvazione, potrebbero subire variazioni prima dell'aggiornamento del presente Manuale.

# **Unimatica** by Namirial

## MANUALE DEL SISTEMA DI CONSERVAZIONE



## Sommario

<b>Registro delle versioni .....</b>	<b>4</b>
<b>1. Scopo e ambito del documento.....</b>	<b>6</b>
1.1. Trattamento dei dati personali .....	6
1.2. Trasparenza .....	8
<b>2. Terminologia .....</b>	<b>10</b>
<b>3. Normativa e standard di riferimento .....</b>	<b>15</b>
3.1. Normativa di Riferimento.....	15
3.2. Standard di Riferimento.....	16
<b>4. Ruoli e responsabilità .....</b>	<b>18</b>
4.1. Ruoli di ausilio al processo di conservazione .....	21
4.2. Precedenti responsabili.....	22
<b>5. Struttura organizzativa per il servizio di conservazione .....</b>	<b>23</b>
5.1. Organigramma.....	23
5.2. Strutture organizzative .....	24
<b>6. Oggetti sottoposti a conservazione .....</b>	<b>27</b>
6.1. Metadati.....	27
6.1.1 Metadati del documento informatico .....	28
6.1.2 Metadati del documento amministrativo informatico .....	30
6.1.3 Metadati delle aggregazioni documentali informatiche .....	32
6.1.4 Metadati del documento informatico di natura fiscale e contabile .....	35
6.2 Formati .....	35
6.2.1 Riversamento.....	35
6.3 Struttura dati del Pacchetto di versamento .....	36
6.4 Struttura dati del Pacchetto di archiviazione.....	36
6.5 Struttura dati del Pacchetto di distribuzione .....	36
<b>7. Il processo di erogazione del servizio di conservazione .....</b>	<b>38</b>
7.1. Il processo di conservazione .....	38
7.2. Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico.....	39
7.3. Verifiche effettuate sui Pacchetti di versamento e sugli oggetti in esso contenuti .....	40
7.4. Accettazione dei Pacchetti di versamento e generazione del Rapporto di versamento di presa in carico.....	41
7.5. Rifiuto dei Pacchetti di versamento e modalità di comunicazione delle anomalie .....	42
7.6. Preparazione e gestione dei Pacchetti di archiviazione .....	42
7.7. Preparazione e gestione dei Pacchetti di distribuzione ai fini dell'esibizione .....	43
7.8. Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento di un pubblico ufficiale.....	44
7.9. Scarto dei Pacchetti di archiviazione .....	44
7.10. Predisposizione di misure per l'interoperabilità e la trasferibilità ad altri conservatori .....	45
7.11. Chiusura del contratto .....	46
<b>8. Procedure di gestione e di evoluzione .....</b>	<b>47</b>
8.1. Misure di sicurezza logica .....	47
8.1.1 Gestione utenze.....	47
8.1.2 Gestione sistemi di protezione .....	48
8.1.3 Gestione degli incidenti di sicurezza.....	48
8.1.4 Gestione dei backup e Disaster Recovery .....	49
8.1.4.1 Siti Settimo e Firenze .....	49
8.1.4.2 Siti di Bologna e Acilia (Roma) .....	50
8.1.4.3 Disaster Recovery .....	51
8.1.5 Gestione dei supporti di memorizzazione.....	51
8.2. Procedure di evoluzione e Change management.....	52
8.3. Cessazione del Servizio di conservazione.....	52
<b>9. Monitoraggio e controlli .....</b>	<b>53</b>
9.1 Audit interni e Verifica dell'integrità degli archivi .....	53

---

9.2 Reportistica di servizio .....	54
<b>10. La server farm di Unimatica .....</b>	<b>55</b>
10.1 UniStorage - Il sistema per la conservazione .....	58
<b>Appendice A .....</b>	<b>59</b>

## Indice delle figure

Figura 1 - Struttura volumi .....	<b>Errore. Il segnalibro non è definito.</b>
Figura 2 - Modello OAIS .....	38
Figura 3 - Architettura di conservazione .....	57

## Registro delle versioni

Revisione	Data	Motivo Revisione	Redatto da	Approvato da
1.0	03/10/2009	Emissione	AA	SG
2.0	12/02/2010	Aggiornamento funzionalità	AA	SG
3.0	20/06/2010	Aggiornamento funzionalità	AA	SG
4.0	28/09/2010	Aggiornamento funzionalità	AA	SG
5.0	15/10/2010	Aggiornamento funzionalità	AA	SG
6.0	10/02/2011	Modifica gestione anomalie – Ampliamento funzionalità Unistorage	AA	SG
7.0	20/05/2011	Aggiornamento composizione societaria Unimatica	AA	SG
8.0	30/11/2012	Aggiornamento Data Center	AA	SG
8.1	11/12/2012	Personalizzazioni	AA	SG
8.2	20/06/2013	Aggiornamento compiti e responsabilità della conservazione	SF	AA
8.3	04/07/2013	Aggiornamento normative	SF	AA
8.4	05/02/2014	Aggiornamento normative	SF	AA
8.5	11/02/2014	Aggiornamento Data Center	SF	AA
8.6	05/03/2014	Adeguamento normative	SF	AA
8.7	17/02/2015	Adeguamento DPCM 03/12/2013	RR	SG
8.8	15/10/2015	Passaggio alla ISO 27001:2013	RR	SG
8.9	20/01/2016	Adeguamento Schema Manuale della conservazione AgID	RR	SG
9.0	11/04/2017	Modifica ruolo Responsabile della Funzione Archivistica	RR	SG
9.1	14/06/2017	Aggiornamento definizioni per termine "Produttore"	RR	SG
9.2	05/10/2017	<ul style="list-style-type: none"> <li>· Aggiornamento Server farm</li> <li>· Visualizzazione di 200 risultati da portale</li> </ul>	RR	SG
9.3	20/10/2017	<ul style="list-style-type: none"> <li>· Capitolo Trasparenza</li> <li>· Aggiornamento elenco formati</li> <li>· Aggiunto testo alternativo mancante su alcune immagini</li> <li>· Sostituita immagine 7 precedentemente con parti nascoste</li> </ul>	RR	SG
9.4	25/10/2018	<ul style="list-style-type: none"> <li>· Aggiornamento par. 1.1 adeguamento GDPR</li> <li>· Modifica ruolo Privacy Manager cap. 4</li> <li>· Aggiornamento tabella normativa par. 3.1</li> <li>· Aggiunto ruolo DPO al par.4.1</li> </ul>	RR	SG
9.5	29/01/2019	<ul style="list-style-type: none"> <li>· Recepimento N.C. AgID Recepimento Oss. Audit interno</li> <li>· Aggiornamento Nomina ad Interim Responsabile della funzione archivistica</li> <li>· Aggiornamento proc. Gestione Incident par. 8.1.3</li> </ul>	RR	SG
9.6	19/04/2019	<ul style="list-style-type: none"> <li>· Revoca nomina ad Interim per la Responsabilità della funzione archivistica</li> <li>· Aggiornamento nomina ad interim DPO</li> </ul>	RR	SG
9.7	27/09/2019	<ul style="list-style-type: none"> <li>· Aggiornamento Ruoli (Delegato Responsabile del servizio di conservazione – Responsabile dello sviluppo e della manutenzione – Responsabile dei sistemi informative – DPO)</li> <li>· Aggiornamento proc. Gestione Incident par. 8.1.3</li> <li>· Aggiornamento estensioni ISO 27017 – 27018</li> <li>· Aggiornamento descrizione par. 7.5 Rifiuto PDV</li> </ul>	RR PV	SG
9.8	20/12/2019	<ul style="list-style-type: none"> <li>· Aggiornamento capp. 4 e 5 a seguito della sostituzione del Delegato alla Responsabilità del servizio di conservazione, della Responsabile della funzione archivistica e della Responsabile dello sviluppo e manutenzione</li> </ul>	RR PV	SG

		· A seguito delle NC ricevute in fase di audit è stato eliminato il par. 9.2 ed aggiornato il par. 8.1.3 sulla Gestione degli incidenti di sicurezza.		
9.9	13/01/2021	· Aggiornamento cap. 4 a seguito di Oss da Audit interno. Aggiunto nominativo Resp. dello sviluppo in carica. · Aggiornamento tabella formati par. 6.2	RR	SG
10	13/09/2021	· Aggiornamenti a seguito del cambio ragione sociale · Aggiornamento par. 1.1 sulla privacy · Aggiornamento par. 1.2 per certificazione ISO 14001 · Aggiornamento modifica sito d/r secondario Acilia (RM)	RR	SG
11	30/12/2021	· Aggiornamento a seguito dell'adeguamento alle Linee guida per la formazione, gestione e conservazione del documento informatico (revisionati cap. 1-2-3-4-6-7)	EL	PV
12	21/06/2022	· Capitolo 4.1.: riportato nuovo responsabile del servizio; rimossa evidenza della delega assegnata a PV dal precedente responsabile del servizio; · Aggiunto capitolo '4.2. Precedenti responsabili' · Rivisto capitolo '5.1. Organigramma' in funzione della nuova nomina	EL	PV
13	01/09/2022	· Indicazione socio unico a piede pagina	EL	PV
14	30/01/2023	· Aggiornamento logo RINA alla ISO 37001	EL	PV
15	22/08/2023	· Aggiornamento nominativi organigramma; · Aggiornamento paragrafo 4.2 "Precedenti responsabili"	EL	PV
16	22/12/2023	· Aggiornamento logo Unimatica – a Namirial Company · Aggiornamento cap. 1.1 Trattamento dei dati personali	EL	PV
17	12/06/2024	· Aggiornamento Ruolo Responsabile del Servizio di Conservazione; · Aggiornamento logo Unimatica	EL	CC
18	04/07/2024	· Revisione dei processi di scarto, di produzione PdD e di fine contratto	CC EL	CC
19	02/12/2024	· Specifica sulle modalità di accesso al portale di conservazione	CC	CC

## 1. Scopo e ambito del documento

Il presente documento costituisce il Manuale del servizio di conservazione erogato da Unimatica 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.

Il Manuale del servizio unitamente alla Scheda cliente predisposta da Unimatica, al fine di personalizzare il rapporto contrattuale con il Cliente Soggetto produttore (da ora in poi Soggetto produttore), costituiscono parte integrante del contratto di fornitura del servizio e mira a garantire e illustrare formalmente ai propri clienti il sistema di conservazione e le sue caratteristiche di disponibilità nel tempo di documenti integri, autentici, legalmente validi e facilmente consultabili.

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

[Torna al sommario](#)

### 1.1. Trattamento dei dati personali

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 (d'ora innanzi anche "GDPR" o "Regolamento") 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, il Soggetto produttore, nella sua qualità di Titolare del trattamento, affida a Unimatica, che diventa Responsabile del trattamento dei dati personali trattati in esecuzione del contratto, i seguenti compiti e impartisce le seguenti istruzioni per il trattamento dei dati cui Unimatica deve attenersi:

1. Unimatica per espletare le attività pattuite per conto del Soggetto produttore potrebbe trattare direttamente o anche solo indirettamente una o più delle seguenti categorie di dati:
  - dati personali,
  - dati rientranti nelle categorie "particolari" di dati personali,
  - dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, di cui è Titolare il Soggetto produttore. Per i dettagli, occorre fare riferimento a quanto pattuito nel contratto/ordine/accordo.
2. I dati trattati da Unimatica si riferiscono potenzialmente, a titolo esemplificativo, ma non esaustivo, alle seguenti categorie di interessati: clienti, dipendenti, utenti, fornitori, richiedenti impiego, soci, etc.
3. Il trattamento dei dati in questione è effettuato da Unimatica esclusivamente per lo svolgimento del servizio di Conservazione a norma, in modo lecito e secondo correttezza, attenendosi alle prescrizioni della normativa sulla protezione dei dati personali nonché alle previsioni della specifica delega a Responsabile del Servizio di Conservazione o successivamente concordate tra le parti; è fatto esplicito divieto di diffondere o comunicare i dati in questione a soggetti che siano estranei all'esecuzione del trattamento.
4. Unimatica, nella sua qualità di Responsabile del trattamento, in particolare è tenuta a:
  - a) trattare direttamente, o per il tramite dei propri dipendenti, collaboratori, consulenti - designati incaricati del trattamento - i dati personali del Titolare, per le sole finalità connesse allo svolgimento delle attività previste dal contratto/ordine/accordo, in modo lecito e secondo correttezza, nonché nel pieno rispetto delle disposizioni impartite dal GDPR e delle presenti istruzioni;

- b) non diffondere o divulgare o rendere noti a terzi -per alcuna ragione ed in alcun momento, presente o futuro ed anche una volta cessati i trattamenti oggetto del contratto/ordine/accordo- i dati personali ricevuti dal Titolare o pervenuti a sua conoscenza in relazione all'esecuzione del servizio prestato, se non previamente autorizzato per iscritto dal Titolare, fatti salvi eventuali obblighi di legge o ordini dell'Autorità Giudiziaria e/o di competenti Autorità amministrative;
  - c) collaborare con il Titolare per garantire la puntuale osservanza e conformità alla normativa in materia di protezione dei dati personali;
  - d) non creare banche dati nuove senza espressa autorizzazione del Titolare, fatto salvo quando ciò risulti strettamente indispensabile ai fini dell'esecuzione degli obblighi assunti;
  - e) in caso di ricezione di richieste specifiche avanzate dall'Autorità Nazionale per la protezione dei dati personali o altre Autorità, coadiuvare il Titolare per quanto di propria competenza;
  - f) segnalare eventuali criticità al Titolare che possono mettere a repentaglio la sicurezza dei dati, al fine di consentire idonei interventi da parte dello stesso;
  - g) vigilare affinché i dati personali degli interessati vengano comunicati solo a quei soggetti preventivamente autorizzati dal Titolare che presentino garanzie sufficienti secondo le procedure di autorizzazione disposte e comunicate dal Titolare. Sono altresì consentite le comunicazioni richieste per legge nei confronti di soggetti pubblici.
5. Istruzioni specifiche per il trattamento dati particolari e/o relativi a condanne penali e reati. Il Titolare indica al Responsabile la presenza nei propri documenti di tali categorie di dati nel contratto/ordine/accordo e nella scheda cliente/scheda tecnica/scheda di attivazione. Nel caso di trattamento di tali dati, il Responsabile, oltre a quanto già sopra garantito, si impegna a:
- a) prestare particolare attenzione al trattamento di tali dati conosciuti in esecuzione dell'incarico affidato, procedendo al loro trattamento solo ove ciò si renda necessario per lo svolgimento delle attività di competenza e istruendo in tal senso le persone autorizzate che operano all'interno della propria struttura;
  - b) gestire la documentazione contenente tali dati adottando, implementando e aggiornando misure di sicurezza adeguate e idonee, concordate con il Titolare, al fine di evitare accessi non autorizzati, distruzione, perdita e/o qualunque violazione dei dati.
6. Il trattamento dei dati deve intendersi effettuato sotto la vigilanza del Soggetto produttore il quale, in ogni momento e con congruo preavviso, potrà operare controlli e impartire eventuali ulteriori specifiche istruzioni per il suo svolgimento, nonché chiederne la cessazione se imposta dalla necessità di adempiere a divieti od obblighi di legge, ovvero a provvedimenti dell'Autorità Garante e/o Giudiziaria.
7. Sicurezza dei dati personali. Il Responsabile, ai sensi dell'art. 32 del GDPR, deve mettere in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio (di distruzione, di perdita, di modifica, di divulgazione non autorizzata o dell'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati) di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.
- Il Titolare concorda sulle misure di sicurezza adottate dal Responsabile e le ritiene adeguate. Il Responsabile, su richiesta, fornirà al Titolare l'elenco aggiornato delle misure di sicurezza adottate, in particolare, in merito alle Politiche di crittografia si rimanda al documento di dettaglio presente al seguente link: <https://www.unimaticaspa.it/it/trasparenza-dei-servizi>.
8. Unimatica si impegna a notificare al Titolare, senza ingiustificato ritardo e, ove possibile, entro 24 ore dal momento in cui è venuto a conoscenza, con comunicazione da inviarsi all'indirizzo PEC del Titolare ogni violazione dei dati personali (data breach) che riguardi il trattamento di cui in argomento. Ulteriori informazioni possono essere fornite dal Responsabile, su richiesta, anche successivamente e appena disponibili senza giustificato ritardo. Il Responsabile si

impegna a prestare assistenza al Titolare al fine di consentirgli di assolvere agli obblighi di cui agli artt. 32 - 34 del GDPR.

9. In esecuzione degli accordi in essere, il Titolare del trattamento concede al Responsabile l'autorizzazione generale ad affidare l'attività -parziale o totale- a soggetti terzi, dei quali garantisce il possesso dei requisiti di esperienza, capacità ed affidabilità, ivi compreso il profilo relativo alla sicurezza. Ove ricorra tale ipotesi, il Responsabile provvede personalmente a designare Responsabili del trattamento ai sensi dell'art. 28 del GDPR i suddetti soggetti terzi (nel seguito anche "Sub-Responsabile del trattamento") con idoneo atto giuridico e ne dà notizia al Titolare tramite la pubblicazione dell'elenco sul proprio sito web al seguente link: <https://www.unimaticaspa.it/it/gdpr-elenco-sub-responsabili>. Il Titolare può opporsi entro e non oltre 14 giorni dalla pubblicazione.
10. Unimatica assicura che nessun dato personale potrà essere trasferito all'esterno dell'Area Economica Europea (EEA).
11. Premesso che l'accesso ai dati personali da parte degli interessati esercitato ai sensi degli artt. 15 e seguenti del GDPR sarà gestito direttamente dal Soggetto produttore, Unimatica si rende disponibile a collaborare con il Soggetto produttore stesso fornendogli tutte le informazioni necessarie a soddisfare le eventuali richieste ricevute in tal senso.
12. Unimatica – ove tale obbligo si applichi anche alla stessa, nella sua qualità di Responsabile del trattamento e in base alle disposizioni del comma 5 dell'art. 30 del GDPR - mantiene un registro di tutte le categorie di attività relative al trattamento svolte per conto del Soggetto produttore.
13. Unimatica si impegna a mettere a disposizione del Soggetto produttore tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di sicurezza descritti nel presente documento e, in generale, il rispetto delle obbligazioni assunte in forza del GDPR, consentendo e, su richiesta, contribuendo alle attività di audit, comprese le ispezioni, realizzate dal Soggetto produttore o da altro soggetto da esso incaricato.
14. L'autorizzazione al trattamento dei dati personali avrà la medesima validità ed efficacia della durata della conservazione legale dei documenti, stabilita dalla normativa.

[Torna al sommario](#)

## 1.2. Trasparenza

La conservazione a norma di Unimatica è rivolta a Pubbliche amministrazioni, banche, assicurazioni, strutture sanitarie ed ai privati in genere.

Al fine di rendere tali servizi agevoli ed accessibili ad un pubblico variegato e disomogeneo, Unimatica rende disponibili una serie di strumenti ed informazioni utili a garantire una totale trasparenza delle proprie attività mediante canali diretti ed indiretti.

In generale, nel sito internet aziendale [www.unimaticaspa.it](http://www.unimaticaspa.it) sono disponibili:

- i contatti principali quali telefono, fax, email ed indirizzo.
- La certificazione per la Qualità ISO 9001:2015 (Unimatica è certificata dal 2006)
- La certificazione per il Sistema di Gestione Ambientale ISO 14001:2015
- La certificazione per la Sicurezza delle Informazioni ISO 27001:2013 (Unimatica è certificata dal 2014) con estensioni alle Linee guida ISO 27017:2015, ISO 27018:2019 ed ISO 27701:2019
- Il Codice Etico aziendale
- Il Modello di Organizzazione, Gestione e Controllo (MOG), ai sensi della L. 231/01 (consultabile a richiesta)

- La Politica Aziendale (consultabile a richiesta)
- L'elenco delle Associazioni di cui l'azienda fa parte e delle Partnership tecnico/commerciali
- La descrizione dei servizi e prodotti offerti dall'azienda e le modalità attraverso cui ottenere informazioni dettagliate su di essi e su come richiederli
- Le informazioni sulle principali attività svolte o in corso

Oltre alle certificazioni sopra elencate, Unimatica ha implementato un sistema di gestione anticorruzione ISO 37001:2016.

Tale certificazione, obbligatoria ai fini dell'adeguamento alle Linee guida per la formazione, gestione e conservazione dei documenti informatici in vigore dal 1° gennaio 2022, è stata aggiunta alle altre presenti nella sezione Trasparenza.

Negli anni, il settore Conservazione di Unimatica ha ottemperato a tutti gli obblighi normativi applicabili. Nello specifico, infatti, da marzo del 2015 ha mantenuto l'accreditamento presso l'Agenzia per l'Italia Digitale (AgID) con la pubblicazione del Manuale della conservazione nell'apposita area a ciò dedicata sul sito web di AgID.

Dall'ottobre del 2017 fino ad abrogazione, in continuità con le disposizioni normative, ha ottenuto e mantenuto la certificazione in conformità all'art. 24 del Regolamento eIDAS e alla check list "*Lista di riscontro per la visita ispettiva AgID e la certificazione di conformità*".

Tali strumenti, oltre ad essere sinonimo di eccellenza, sono risultati negli anni passi indispensabili per la crescita dell'azienda, del team e per migliorare continuamente il prodotto Unistorage e il servizio offerto ai clienti.

Unimatica considera altrettanto importante il concetto di trasparenza rivolto ai propri dipendenti. Sull'intranet aziendale, infatti, ogni dipendente ha a disposizione strumenti e materiali informativi relativi al sistema di gestione integrato della Qualità, della Sicurezza, dell'Ambiente, della Privacy e dell'Anticorruzione (ISO/IEC 27001, ISO 9001, ISO 14001, ISO 37001) e a tutte le Procedure di conservazione. L'impegno, l'attenzione, la formazione e le competenze di tutta l'azienda sulla tematica specifica ed i risultati raggiunti nel corso degli anni di attività hanno permesso ad Unimatica di ottenere l'iscrizione quale socio sostenitore presso l'associazione ANORC (Associazione Nazionale per Operatori e Responsabili della Conservazione Digitale).

Per dimostrare trasparenza ed affidabilità, inoltre, Unimatica garantisce da sempre la propria disponibilità ad ospitare audit finanziari e/o di seconda parte, rispettando così le disposizioni delle autorità di controllo e, previo accordo, anche gli accordi stabiliti con clienti per i quali presta servizi.

[Torna al sommario](#)

## 2. Terminologia

TERMINE	DEFINIZIONE
<b>Accesso</b>	Operazione che consente di prendere visione dei documenti informatici.
<b>Affidabilità</b>	Caratteristica che, con riferimento a un sistema di gestione documentale o conservazione, esprime il livello di fiducia che l'utente ripone nel sistema stesso, mentre con riferimento al documento informatico esprime la credibilità e l'accuratezza della rappresentazione di atti e fatti in esso contenuta.
<b>Aggregazione documentale informatica</b>	Insieme di documenti informatici o insieme di fascicoli informatici riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente.
<b>Archivio</b>	Complesso dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività.
<b>Archivio informatico</b>	Archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche
<b>Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico</b>	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.
<b>Autenticità</b>	Caratteristica in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto un oggetto è autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze.
<b>Certificazione</b>	Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi.
<b>Classificazione</b>	Attività di organizzazione di tutti i documenti secondo uno schema costituito da un insieme di voci articolate in modo gerarchico e che individuano, in astratto, le funzioni, competenze, attività e/o materie del soggetto produttore.
<b>Cloud della PA</b>	Ambiente virtuale che consente alle Pubbliche Amministrazioni di erogare servizi digitali ai cittadini e alle imprese nel rispetto di requisiti minimi di sicurezza e affidabilità.
<b>Conservatore</b>	Soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici.
<b>Conservazione</b>	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.
<b>Convenzioni di denominazione del file</b>	Anche detta <i>Naming convention</i> , è l'insieme di regole sintattiche che definisce il nome dei file all'interno di un filesystem o pacchetto.
<b>Coordinatore della Gestione Documentale</b>	Soggetto responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 nei casi di amministrazioni che abbiano istituito più AOO.
<b>Destinatario</b>	Soggetto o sistema al quale il documento informatico è indirizzato.
<b>Documento amministrativo informatico</b>	Ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa
<b>Documento elettronico</b>	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva

<b>Documento informatico</b>	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
<b>Duplicato informatico</b>	Vedi art. 1, comma 1, lett) i quinquies del CAD.
<b>Esibizione</b>	Operazione che consente di visualizzare un documento conservato.
<b>Estratto di documento informatico</b>	Parte del documento tratto dal documento originale
<b>Estratto per riassunto di documento informatico</b>	Documento nel quale si attestano in maniera sintetica fatti, stati o qualità desunti da documenti informatici.
<b>Estrazione statica dei dati</b>	Estrazione di informazioni utili da grandi quantità di dati (es. database, datawarehouse ecc...), attraverso metodi automatici o semi-automatici
<b>Evidenza informatica</b>	Sequenza finita di <i>bit</i> che può essere elaborata da una procedura informatica.
<b>Fascicolo informatico</b>	Aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento.
<b>File</b>	Insieme di informazioni, dati o comandi logicamente correlati, raccolti sotto un unico nome e registrati, per mezzo di un programma di elaborazione o di scrittura, nella memoria di un computer.
<b>Firma elettronica</b>	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare; (art.3 del Regolamento eIDAS).
<b>Firma elettronica avanzata</b>	Per essere definite tale una FEA deve soddisfare I seguenti requisiti: essere connessa unicamente al firmatario; essere idonea a identificare il firmatario; essere creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; essere collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati; (artt. 3 e 26 del Regolamento eIDAS).
<b>Firma elettronica qualificata</b>	Una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche; (art. 3 del Regolamento eIDAS).
<b>Formato del documento informatico</b>	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
<b>Formato "deprecato"</b>	Formato in passato considerato ufficiale il cui uso è attualmente sconsigliato a favore di una versione più recente.
<b>Funzione di hash crittografica</b>	Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o <i>digest</i> (vedi) in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
<b>Gestione Documentale</b>	Processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta, uso, selezione e conservazione dei documenti.
<b>Hash</b>	Termine inglese usato, impropriamente, come sinonimo d'uso di "impronta crittografica" o " <i>digest</i> " (vedi).
<b>Identificativo univoco</b>	Sequenza di numeri o caratteri alfanumerici associata in modo univoco e persistente ad un'entità all'interno di uno specifico ambito di applicazione.
<b>Impronta crittografica</b>	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di <i>hash</i> crittografica a un'evidenza informatica.
<b>Integrità</b>	Caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità.

<b>Interoperabilità</b>	Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi.
<b>Leggibilità</b>	Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica.
<b>Manuale di conservazione</b>	Documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture. Con l'entrata in vigore delle LLGG AgID sulla formazione, gestione e conservazione dei documenti informatici (1 gennaio 2022) vengono sancite due forme distinte di manuale di conservazione: uno proprio del soggetto conservatore e uno proprio del Titolare dell'oggetto di conservazione.
<b>Manuale di gestione</b>	Documento informatico che descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.
<b>Metadati</b>	Dati associati a un o documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017.
<b>Oggetto di conservazione</b>	Oggetto digitale versato in un sistema di conservazione.
<b>Oggetto digitale</b>	Oggetto informativo digitale, che può assumere varie forme tra le quali quelle di documento informatico, fascicolo informatico, aggregazione documentale informatica o archivio informatico.
<b>Pacchetto di archiviazione (PdA)</b>	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel manuale di conservazione.
<b>Pacchetto di distribuzione (PdD)</b>	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione.
<b>Pacchetto di file (<i>file package</i>)</b>	Insieme finito di più file (possibilmente organizzati in una struttura di sottoalbero all'interno di un filesystem) che costituiscono, collettivamente oltre che individualmente, un contenuto informativo unitario e auto-consistente.
<b>Pacchetto di versamento (PdV)</b>	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione.
<b>Pacchetto informativo</b>	Contenitore logico che racchiude uno o più oggetti di conservazione con i relativi metadati, oppure anche i soli metadati riferiti agli oggetti di conservazione.
<b>Pathname</b>	Concatenazione ordinata del percorso di un file e del suo nome.
<b>Percorso</b>	Informazioni relative alla localizzazione virtuale del file all'interno del filesystem espressa come concatenazione ordinata del nome dei nodi del percorso. Detto anche <i>path</i> .
<b>Periodo di conservazione dei documenti</b>	La durata temporale per ciascuna tipologia documentale, espressa in anni, per la quale il Soggetto produttore richiede il servizio di conservazione. Tale durata temporale sarà riportata all'interno del piano di conservazione, qualora redatto dal Soggetto produttore,
<b>Piano della sicurezza del sistema di conservazione</b>	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi.
<b>Piano di classificazione (Titolario)</b>	Struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata.
<b>Piano di conservazione</b>	Documento, allegato al manuale di gestione e integrato con il sistema di classificazione, in cui sono definiti i criteri di organizzazione dell'archivio,

	di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445.
<b>Piano di organizzazione delle aggregazioni documentali</b>	Strumento integrato con il sistema di classificazione a partire dai livelli gerarchici inferiori di quest'ultimo e finalizzato a individuare le tipologie di aggregazioni documentali (tipologie di serie e tipologie di fascicoli) che devono essere prodotte e gestite in rapporto ai procedimenti e attività in cui si declinano le funzioni svolte dall'ente
<b>Piano generale della sicurezza</b>	Documento che pianifica le attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza.
<b>Presa in carico</b>	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione e, in caso di affidamento del servizio all'esterno, dagli accordi stipulati tra il titolare dell'oggetto di conservazione e il responsabile del servizio di conservazione.
<b>Processo</b>	Insieme di attività correlate o interagenti che trasformano elementi in ingresso in elementi in uscita.
<b>Produttore dei PdV</b>	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. Nelle pubbliche amministrazioni, tale figura si identifica con il responsabile della gestione documentale.
<b>Rapporto di versamento</b>	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore
<b>Registro di protocollo</b>	Registro informatico ove sono memorizzate le informazioni prescritte dalla normativa per tutti i documenti ricevuti e spediti da un ente e per tutti i documenti informatici dell'ente stesso.
<b>Registro particolare</b>	Registro informatico individuato da una pubblica amministrazione per la memorizzazione delle informazioni relative a documenti soggetti a registrazione particolare.
<b>Regolamento eIDAS</b>	electronic IDentification Authentication and Signature, Regolamento (UE) № 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
<b>Repertorio</b>	Registro su cui vengono annotati con un numero progressivo i fascicoli secondo l'ordine cronologico in cui si costituiscono all'interno delle suddivisioni del piano di classificazione
<b>Responsabile dei sistemi informativi per la conservazione</b>	Soggetto che coordina i sistemi informativi all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID.
<b>Responsabile del servizio di conservazione</b>	soggetto che coordina il processo di conservazione all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
<b>Responsabile della conservazione</b>	Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia. Nella PA il ruolo deve essere rivestito da un soggetto interno all'organigramma; negli enti privati può essere rivestito da un soggetto interno all'organigramma o da un soggetto esterno, purchè diverso dal Conservatore a cui si è affidato il servizio di conservazione dei documenti informatici.
<b>Responsabile della funzione archivistica di conservazione</b>	Soggetto che coordina il processo di conservazione dal punto di vista archivistico all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
<b>Responsabile della gestione documentale</b>	Soggetto responsabile della gestione del sistema documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445.

<b>Responsabile della protezione dei dati</b>	Persona con conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, in grado di assolvere i compiti di cui all'articolo 39 del Regolamento (UE) 2016/679.
<b>Responsabile della sicurezza dei sistemi di conservazione</b>	sogetto che assicura il rispetto dei requisiti di sicurezza all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
<b>Responsabile dello sviluppo e della manutenzione del sistema di conservazione</b>	sogetto che assicura lo sviluppo e la manutenzione del sistema all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
<b>Riferimento temporale</b>	Insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC).
<b>Riversamento</b>	Procedura mediante la quale uno o più documenti informatici sono convertiti da un formato di file (ovvero di busta, ovvero di pacchetto di file) ad un altro, lasciandone invariato il contenuto per quanto possibilmente permesso dalle caratteristiche tecniche del formato (ovvero dei formati) dei file e delle codifiche di destinazione.
<b>Scarto</b>	Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico-culturale.
<b>Serie</b>	Raggruppamento di documenti con caratteristiche omogenee (vedi anche aggregazione documentale informatica).
<b>Sigillo elettronico</b>	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi.
<b>Sistema di conservazione</b>	Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, comma 1, del CAD.
<b>Sistema di gestione informatica dei documenti</b>	Insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle organizzazioni per la gestione dei documenti. Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445
<b>Termine del contratto del servizio di conservazione</b>	Termine contrattualmente previsto per il servizio di conservazione occorso il quale il Titolare dell'oggetto di conservazione può decidere se estendere il contratto o optare per la restituzione dei documenti conservati..
<b>Timeline</b>	Linea temporale virtuale su cui sono disposti degli eventi relativi ad un sistema informativo o a un documento informatico. Costituiscono esempi molto diversi di <i>timeline</i> un file di log di sistema, un flusso multimediale contenente essenze audio\video sincronizzate.
<b>Titolare dell'oggetto di conservazione</b>	Soggetto produttore degli oggetti di conservazione e per estensione eventuali soggetti terzi delegati.
<b>Trasferimento</b>	Passaggio di custodia dei documenti da una persona o un ente ad un'altra persona o un altro ente.
<b>Utente abilitato</b>	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.
<b>Versamento</b>	Passaggio di custodia, di proprietà e/o di responsabilità dei documenti. Nel caso di un organo giudiziario e amministrativo dello Stato operazione con la quale il responsabile della conservazione trasferisce agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali.

[Torna al sommario](#)

### 3. Normativa e standard di riferimento

Il sistema di conservazione sviluppato da Unimatica è conforme alla normativa e agli standard elencati nei successivi paragrafi.

Periodicamente vengono effettuate verifiche per l'aggiornamento dei requisiti normativi al fine di assicurare una puntuale conformità alle disposizioni legislative. Eventuali ulteriori riferimenti normativi non direttamente riconducibili alla conservazione, ma comunque applicabili per via di servizi correlati ad essa, sono elencati in uno specifico documento facente parte del sistema di gestione integrato, denominato SIC040 – Monitoraggio.

[Torna al sommario](#)

#### 3.1. Normativa di Riferimento

Notazione abbreviata	Riferimento
<b>Codice Civile</b>	[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.
<b>RD 1163/1911</b>	Regolamento per gli archivi di Stato
<b>DPR 1409/1963</b>	Norme relative all'ordinamento ed al personale degli archivi di Stato
<b>Legge 241/1990</b>	Nuove norme sul procedimento amministrativo
<b>DPR 445/2000</b>	Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
<b>DPR 37/2001</b>	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
<b>D.lgs 196/2003</b>	Recante il Codice in materia di protezione dei dati personali
<b>D.lgs 42/2004</b>	Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n.137
<b>Legge 9 gennaio 2004, n. 4 aggiornata dal decreto legislativo 10 agosto 2018, n. 106</b>	Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici
<b>D.lgs 82/2005 e ss.mm.ii.</b>	Codice dell'amministrazione digitale
<b>D.lgs 33/2013</b>	Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni
<b>DPCM 22 febbraio 2013</b>	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
<b>DPCM 21 marzo 2013</b>	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;
<b>Reg. UE 910/2014</b>	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;
<b>Circolare 40 e 41 del 14 dicembre 2015 della</b>	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;

<b>Direzione generale degli archivi</b>	
<b>Reg. UE 679/2016 (GDPR)</b>	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;
<b>Circolare 18 aprile 2017 n. 2/2017 dell’Agenzia per l’Italia Digitale</b>	Recante le misure minime di sicurezza ICT per le pubbliche amministrazioni;
<b>Circolare n. 2 del 9 aprile 2018</b>	Recante i criteri per la qualificazione dei Cloud Service Provider per la PA;
<b>Circolare n. 3 del 9 aprile 2018</b>	Recante i criteri per la qualificazione di servizi SaaS per il Cloud della PA;
<b>Reg. UE 2018/1807</b>	Relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea;
<b>DPCM 19 giugno 2019 n. 76</b>	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.
<b>Linee guida AgID ed Allegati</b>	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
<b>Regolamento AgID ed Allegati</b>	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

[Torna al sommario](#)

### 3.2. Standard di Riferimento

<b>Sigla</b>	<b>Titolo standard</b>
<b>UNI 11386</b>	Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.
<b>ISO 14721</b>	OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione.
<b>ISO 15836</b>	Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core
<b>ISO/TR 18492</b>	Long-term preservation of electronic document-based information.
<b>ISO 20652</b>	Space data and information transfer systems - Producer-Archive interface - Methodology abstract standard.
<b>ISO 20104</b>	Space data and information transfer systems — Producer-Archive Interface Specification (PAIS).
<b>ISO/CD TR 26102</b>	Requirements for long-term preservation of electronic records.
<b>SIARD</b>	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 données pour l'archivage. Transfert – Communication – Élimination – Restitution - Modification, ver. 2.1, 2018
<b>METS</b>	Metadata Encoding and Transmission Standard
<b>PREMIS</b>	PREservation Metadata: Implementation Strategies.
<b>EAD 3</b>	Encoded Archival Description
<b>ISAD (G)</b>	General International Standard Archival Description

<b>EAC-CPF 2.0</b>	Encoded Archival Context-Corporate Bodies, Persons and Families
<b>ISAAR (CPF)</b>	International Standard Archival Authority Records for Corporate Bodies, Persons and Families
<b>ISDIAH</b>	International Standard for Describing Institutions with Archival Holdings
<b>NIERA (EPF)</b>	Norme italiane per l'elaborazione dei record di autorità archivistici di enti, persone, famiglie

[Torna al sommario](#)

## 4. 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:

- **Titolare dell'oggetto di conservazione** (citato nel manuale come soggetto produttore), identificato come il soggetto produttore degli oggetti di conservazione.
- **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
- **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
- **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.
- **Conservatore**, è quella figura che si occupa dell'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.

Il processo di conservazione vede direttamente coinvolti tutti i soggetti sopra elencati.

Unimatica ha individuato le seguenti figure di responsabilità per l'erogazione del servizio di conservazione, a garanzia di elevati standard di qualità e sicurezza:

**Il Responsabile del servizio di conservazione** espleta, a seguito di delega formale e in ogni caso rimanendo inteso che la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile, rimane in capo al responsabile della conservazione, le seguenti attività:

1. definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato
2. gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
3. genera e sottoscrive il Rapporto di Versamento, secondo le modalità previste dal manuale di conservazione;
4. genera il pacchetto di archiviazione conforme allo Standard SInCRO UNI 11386 - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali e lo sottoscrive con firma digitale;
5. genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione, ai fini dell'esibizione richiesta dall'utente;

6. effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
7. effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;
8. 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. Adotta analoghe misure con riguardo all'obsolescenza dei formati;
9. provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
10. adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione;
11. assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
12. assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
13. provvede per le amministrazioni statali centrali e periferiche a versare i documenti informatici, le aggregazioni informatiche e gli archivi informatici, nonché gli strumenti che ne garantiscono la consultazione, rispettivamente all'Archivio centrale dello Stato e agli archivi di Stato territorialmente competenti, secondo le tempistiche fissate dall'art. 41, comma 1, del Codice dei beni culturali

garantendo un particolare riguardo alla:

- 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.

**Il Responsabile del servizio di conservazione** nominato da Unimatica è **Cecilia Canova**.

In assenza del Responsabile del servizio di conservazione, le sue funzioni operative vengono delegate a **Valentina Vetri**.

**Il Responsabile della funzione archivistica di conservazione**, in accordo con il Responsabile del servizio di conservazione, si occupa di

- definire e gestire il processo di conservazione, incluse le modalità di trasferimento da parte del produttore dei PDV, 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

- monitorare set di metadati di conservazione dei documenti, dei fascicoli informatici e delle aggregazioni documentali informatiche
- monitorare il processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema
- collaborare con il Produttore dei PDV 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.

La **Responsabile della funzione archivistica di conservazione** nominata da Unimatica è **Eleonora Luzi**.

**Responsabile sicurezza dei sistemi per la conservazione** il quale si occupa di:

- monitorare e rispettare i requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza. In caso di eventuali difformità si occupa di segnalarle al Responsabile del servizio di conservazione e, quindi, individua e pianifica le necessarie azioni correttive.

Il **Responsabile sicurezza dei sistemi per la conservazione** nominato da Unimatica è **Massimo Ortensi**.

**Responsabile dei sistemi informativi per la conservazione** il quale si occupa di:

- gestire l'esercizio delle componenti hardware e software del sistema di conservazione e monitorare il mantenimento dei livelli di servizio (SLA) concordati con il Titolare e il Produttore
- segnalare le eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuare e pianificare le necessarie azioni correttive
- pianificare lo sviluppo delle infrastrutture tecnologiche del sistema di conservazione e verifica i livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.

Il **Responsabile dei sistemi informativi per la conservazione** nominato da Unimatica è **Massimo Ortensi**.

**Responsabile sviluppo e manutenzione del sistema di conservazione** il quale si occupa di:

- coordinare lo sviluppo e la manutenzione delle componenti hardware e software del sistema di conservazione
- pianificare e monitorare i progetti di sviluppo del sistema di conservazione
- monitora gli SLA relativi alla manutenzione del sistema di conservazione
- interfacciarsi con il Produttore dei PDV relativamente alle modalità di trasferimento dei documenti, fascicoli informatici e aggregazioni documentali informatiche in merito ai formati

elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche

- gestire lo sviluppo di siti web e portali connessi al servizio di conservazione.

Il **Responsabile dello sviluppo e manutenzione del sistema di conservazione** nominato da Unimatica è **Matteo Rossi**.

Nell'attribuire ruoli e responsabilità Unimatica presta importante attenzione alle competenze delle risorse valutate, vanta infatti personale altamente specializzato e formato sulle tematiche legate alla conservazione e all'archiviazione digitale.

Tale personale è costantemente aggiornato sull'evoluzione della normativa e sugli aspetti tecnologici, grazie alla documentazione interna messa a disposizione dall'azienda e garantisce, inoltre, l'opportunità ai dipendenti di partecipare ad appositi corsi qualificanti di approfondimento, interni ed esterni.

[Torna al sommario](#)

## 4.1. Ruoli di ausilio al processo di conservazione

In ottemperanza a quanto previsto dal Regolamento (UE) 2016/679 Unimatica, al fine di garantire una maggior tutela dei dati propri e di quelli dei clienti, ha nominato un **Data Protection Officer** il quale si occupa di

- offrire idonea consulenza per progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali, interagendo coi sistemi di gestione aziendali, compreso il sistema di conservazione, per curare l'adozione di misure di sicurezza finalizzate alla tutela dei dati trattati dall'azienda, che soddisfino i requisiti di legge e per evitare i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

La **DPO** nominato da Unimatica è **Anna Veltri**.

[Torna al sommario](#)

## 4.2. Precedenti responsabili

Ruolo	Nominativo	Periodo
Responsabile servizio di conservazione	SG	01/2004 – 06/2022
	PV	06/2022 – 06/2024
Delegato Responsabile del Servizio di Conservazione	AA	01/2009 – 09/2019
	PV	09/2019 – 06/2022
	RN	01/2010 – 12/2019
	CC	12/2019 – 06/2024
Responsabile Funzione Archivistica	SF	01/2012 – 06/2017
	RN	06/2017 – 12/2019
	RR ( <i>ad interim</i> )	06/2018 – 04/2019
Responsabile Trattamento Dati Personali	SG	01/2004 – 09/2021
	AM	10/2021 – 05/2023
Responsabile Sistemi Informativi per la conservazione	AA	01/2008 – 09/2019
Responsabile Sviluppo e Manutenzione	SG	01/2008 – 09/2019
	PV	09/2019 – 12/2019
	AC	12/2019 – 03/2023
DPO	RR ( <i>ad interim</i> )	04/2019 – 09/2019

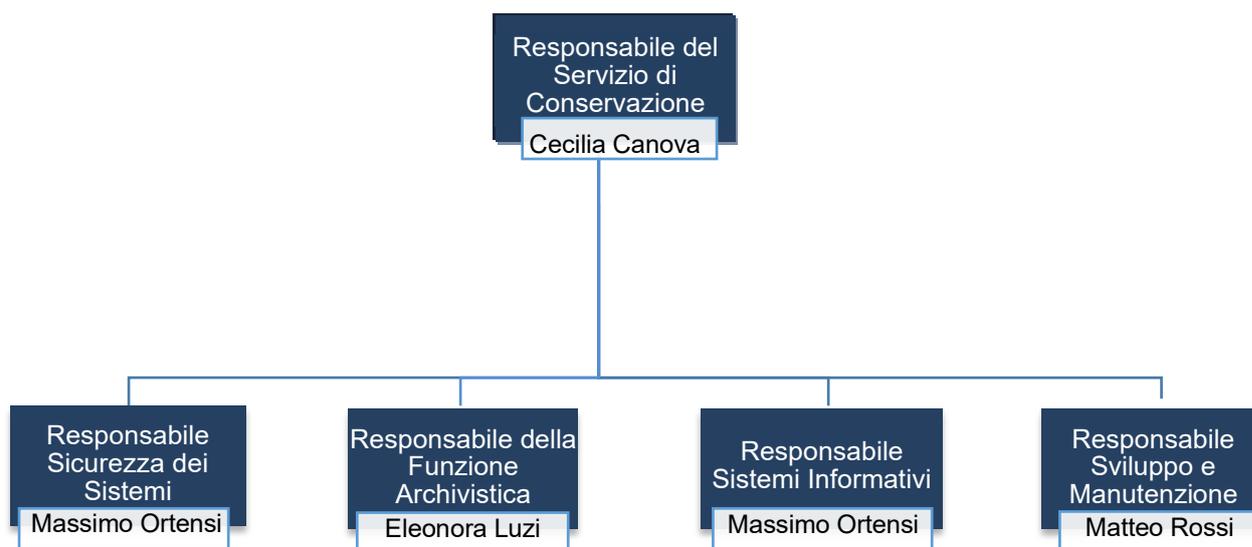
[Torna al sommario](#)

## 5. Struttura organizzativa per il servizio di conservazione

Il presente capitolo ha lo scopo di illustrare la struttura organizzativa del settore conservazione di Unimatica. L'espletamento di un processo di conservazione prevede una serie di complesse attività, pertanto la società si avvale di personale altamente qualificato e con esperienza decennale. Si riporta di seguito l'organigramma della struttura organizzativa e una sintetica descrizione<sup>1</sup> delle funzioni e delle responsabilità che intervengono nel processo di conservazione.

[Torna al sommario](#)

### 5.1. Organigramma



[Torna al sommario](#)

<sup>1</sup> La descrizione dettagliata del processo di conservazione è riportata nel capitolo 7 "Il processo di erogazione del servizio di conservazione".

## 5.2. Strutture organizzative

Nel presente paragrafo vengono descritte sinteticamente le fasi principali del processo di conservazione e le attività di gestione dei sistemi informativi, individuando per ciascuna di queste le figure che ne assumono le responsabilità.

Attività proprie di ciascun contratto di servizio			
Fase	Attività	Descrizione	Responsabilità
1	Attivazione del servizio di conservazione (a seguito della sottoscrizione del contratto).	Il Soggetto produttore invia una richiesta di attivazione del servizio che avviene in seguito alla compilazione del modulo "Scheda cliente" dove vengono dichiarati dettagli degli oggetti da conservare, come: dimensioni, frequenza invio, ecc.	RSC PM RFA RSM
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 produttore, la firma digitale, formati e metadati sulla base di quanto concordato nella Fase 1. In caso di verifiche andate a buon fine viene generato il RdV, altrimenti viene generata la Comunicazione delle anomalie.	RSC RFA
3	Preparazione e gestione dei Pacchetti di archiviazione <sup>2</sup> .	Gli oggetti versati vengono trasformati in PdA contenenti, oltre agli oggetti da conservare, l'IdPA <sup>3</sup> formato secondo le regole dello standard SInCRO. L'IdPA viene sottoscritto con firma digitale dal RSC e viene marcato temporalmente.	RSC RFA
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 dell'Utente. Possono essere visualizzati mediante interfaccia web, WS o, se richiesto, tramite memorizzazione su supporto.	RSC RFA PM
5	Scarto dei pacchetti di archiviazione	Entro tre mesi prima della scadenza del Periodo di conservazione per i documenti conservati da Unimatica, il Titolare dell'oggetto di conservazione dovrà prendere contatto con Unimatica ed indicare la volontà di continuare la conservazione digitale a norma, con opportuna estensione contrattuale ove necessario, oppure di procedere con l'attività dello scarto.	RSC RFA PM

<sup>2</sup> Traduzione di Archival Information Package dal Modello OAIS Open Archival Information Standard che individua nel sistema di archiviazione tre diversi tipi di Pacchetti: Submission Information Package (SIP), Archival Information Package (AIP) e Dissemination Information Package (DIP).

<sup>3</sup> Indice del pacchetto di archiviazione.

		Qualora ciò avvenga Unimatica attiverà la procedura di scarto e provvederà all'eliminazione delle UD selezionate. Per le UD provenienti da enti pubblici o da archivi privati per i quali è stato dichiarato l'interesse culturale si terrà conto dei piani di conservazione di questi e della decisione ultima della Soprintendenza archivistica. <i>(Per maggiori dettagli si rimanda al par. 7.9 del presente manuale).</i>	
6	Chiusura del servizio di conservazione (al termine di un contratto)	Il Titolare dell'oggetto della conservazione, in qualsivoglia momento, ha il diritto di rescindere dal contratto. Qualora ciò avvenga prima del termine previsto per il servizio di conservazione, il Soggetto Produttore potrà richiedere la restituzione dei documenti inviati in conservazione secondo le modalità operative concordate con il RSC. <i>(Per maggiori dettagli si rimanda al par. 7.11 del presente manuale).</i>	RSC PM

### Attività proprie di gestione dei sistemi informativi

Fase	Attività	Descrizione	Responsabilità
1	Conduzione e manutenzione del sistema di conservazione	Le attività di manutenzione vengono svolte sia sui processi che sulle strutture hardware e software e viene condotta una quotidiana verifica delle attività sulle infrastrutture parallelamente ad una pianificazione delle eventuali procedure straordinarie da condurre in caso di anomalie.	RSM RSSI
2	Monitoraggio del sistema di conservazione	Viene effettuato il monitoraggio del sistema di Log che consente la registrazione degli accessi e degli eventi (operazioni). Tra le attività di monitoraggio rientrano anche la verifica dell'integrità degli archivi e la gestione delle anomalie.	RSC RFA RSSI
3	Change management	Vengono definite politiche, priorità e tempistiche dell'adeguamento all'evoluzione tecnologica affinché il sistema di conservazione possa garantire nel tempo integrità, disponibilità e sicurezza.	RFA RSI

4	Verifica periodica di conformità a normativa e standard di riferimento	La conformità a normativa e standard è costantemente monitorata ed eventualmente aggiornata.	RSC RSSI
---	--	--	-------------

Legenda	
RSC	Responsabile del Servizio di Conservazione
RSSI	Responsabile Sicurezza dei Sistemi Informativi per la Conservazione
PM	Privacy Manager
RFA	Responsabile Funzione Archivistica per la Conservazione
RSI	Responsabile Sistemi Informativi per la Conservazione
RSM	Responsabile Sviluppo e Manutenzione del Sistema di Conservazione

[Torna al sommario](#)

---

## 6. Oggetti sottoposti a conservazione

---

Unimatica mediante il proprio sistema di conservazione Unistorage, sviluppato integralmente dalla società, è in grado di accettare e gestire, come richiesto ai sensi dell'art. 44, comma 1-bis, del CAD<sup>4</sup>,

- a) I fascicoli informatici chiusi e le serie informatiche chiuse,
- b) i fascicoli informatici e le serie non ancora chiusi accettando i documenti in essi contenuti sulla base di specifiche esigenze del soggetto produttore. In particolare, in questo caso, il Titolare e il Conservatore garantiscono specifico monitoraggio al fine di evitare rischi di obsolescenza tecnologica che possono sopravvenire prima della chiusura.

Unistorage è predisposto per accettare aggregazioni documentali e tutte le tipologie di documenti informatici relativi a diversi ambiti applicativi.

In accordo con il soggetto produttore, Unimatica si riserva infatti la facoltà di accettare qualsiasi tipologia documentale. L'indicazione delle tipologie documentali, compresa la gestione di queste, verrà indicata nella scheda cliente allegata al contratto stipulato con il soggetto produttore.

Unimatica accetta e conserva solo documenti informatici. Il sistema di conservazione permette l'acquisizione sia di documenti firmati digitalmente, sia di documenti non firmati. Entrambe le tipologie entrano nel medesimo processo di Ingestion. Con l'ausilio del Responsabile del servizio di conservazione, è il Soggetto produttore a definire nella scheda cliente le modalità di trattamento dei documenti firmati o non firmati.

[Torna al sommario](#)

---

### 6.1. Metadati

---

Come previsto dal par. 4.1 delle Linee guida, il sistema di conservazione assicura dalla presa in carico fino all'eventuale scarto, la conservazione di oggetti digitali tramite l'adozione di regole, procedure e tecnologie, necessarie al mantenimento delle caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità.

Al fine di rendere agevole ed efficiente la ricerca di un documento, di un fascicolo, o di un'aggregazione documentale informatica conservati, è necessario corredare tali oggetti da un set di metadati che ne descrivono il contenuto e lo identificano all'interno del sistema. Unimatica, in piena conformità alle Linee guida e all'Allegato 5, garantisce l'acquisizione, la gestione e la conservazione di:

- Metadati del documento informatico
- Metadati del documento amministrativo informatico
- Metadati delle aggregazioni documentali informatiche
- Metadati del documento informatico di natura fiscale e contabile

Nei paragrafi successivi si elencano per ogni tipologia, a titolo esemplificativo e non esaustivo, i metadati obbligatori individuati dalle Linee guida. Per tutti i dettagli specifici sul lessico, campi e schemi si rimanda alle schede di dettaglio presenti all'interno dell'*Allegato 5* alle Linee guida e

---

<sup>4</sup> L'art. 44, comma 1-bis, del CAD prevede che: "[...] Almeno una volta all'anno il responsabile della gestione dei documenti informatici provvede a trasmettere al sistema di conservazione i fascicoli e le serie documentarie anche relative a procedimenti non conclusi"

all'Elenco AgID "L'utilizzo dei metadati del documento informatico - I metadati del documento informatico di natura fiscale e contabile"

[Torna al sommario](#)

## 6.1.1 Metadati del documento informatico

Di seguito vengono elencati i metadati, ed i principali campi e sottocampi *obbligatori* del documento informatico:

**IdDoc:** Identificativo univoco e persistente associato in modo univoco e permanente al documento informatico in modo da consentirne l'identificazione

Il metadato è costituito dai seguenti:

- Impronta: sottocampo in cui viene memorizzato l'hash del documento
- Algoritmo: sottocampo nel quale deve essere indicata la tipologia dell'algoritmo applicato riportati nell'Allegato 6 delle Linee Guida nella tabella 1 del paragrafo 2.2 "Regole di processamento"
- Identificativo: come da sistema di identificazione formalmente definito

**Modalità di formazione:** modalità di generazione del documento informatico

Sono previste le seguenti modalità:

- creazione tramite l'utilizzo di strumenti software che assicurino la produzione di documenti nei formati previsti nell'Allegato 2 delle Linee Guida;
- acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;
- memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;
- generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica

**Tipologia documentale:** metadato funzionale che indica la tipologia del documento tra quelle trattate per lo svolgimento delle attività

Metadato testuale libero per indicare le tipologie documentali trattate (ad esempio, fatture, delibere, determine, etc)

**Dati di registrazione:** Metadato che comprende i dati di registrazione del documento sia nel caso di documento protocollato che non protocollato. Si intende per registrazione l'operazione che, in senso lato, associa ad un documento una data e un numero. In tale ottica, quindi potrebbe non essere identificabile uno specifico registro, ma sono sempre identificabili una data di registrazione e un numero di registrazione del documento.

Sono previsti i seguenti campi:

- Tipologia di flusso: indica se si tratta di un documento in uscita, in entrata o interno.
- Tipo registro: indica il sistema di registrazione adottato: protocollo ordinario/protocollo emergenza, o Repertorio/Registro.
- Data: è la data associata al documento all'atto della registrazione
- Numero documento: Numero identificativo del documento nel caso di documento non protocollato (ad esempio, numero fattura), numero di protocollo nel caso di documento protocollato.
- Codice Registro: Identificativo del registro nel caso in cui il tipo registro sia protocollo ordinario/protocollo emergenza, o Repertorio/Registro.

**Soggetti:** indica il metadato che consente di individuare le informazioni relative a tutti i soggetti coinvolti e competenti sul documento a vario titolo e definiti dal campo Ruolo.

Sono definiti i seguenti attributi:

- Ruolo: consente di indicare, a seconda delle necessità, l'autore del documento, il mittente, il destinatario, l'assegnatario. Al fine di rendere i dati di registrazione univoci deve essere sempre indicato il Soggetto che effettua la registrazione del documento (tipicamente l'Organizzazione che protocolla). Obbligatorio inoltre indicare almeno l'autore o il mittente. Nel caso di documento protocollato deve essere obbligatoriamente indicato il mittente.
- Tipo soggetto: consente di tipizzare i soggetti come persone fisiche, giuridiche, amministrazioni pubbliche (italiane ed estere). Il Tipo Soggetto = SW è indicabile solo se si è indicato il ruolo = "Produttore". Per ogni Tipo Soggetto sono indicati i metadati di riferimento

**Chiave descrittiva:** metadato funzionale volto a riassumere il contenuto del documento o comunque a chiarirne la natura.

È costituito da seguenti campi:

- Oggetto: testo libero

**Allegati:** Indica il numero di allegati al documento e, nell'eventualità che il numero di allegati indicati sia maggiore di zero, devono essere compilati, in modalità ricorsiva, i dati:

- IdDoc: Identificativo del documento relativo all'allegato
- Descrizione: Titolo dell'Allegato

**Classificazione:** classificazione del documento secondo il Piano di classificazione utilizzato da indicare sia nel caso di documento protocollato che nel caso di documento non protocollato (*facoltativo*, per le specifiche si rimanda all'Allegato 5)

**Riservato:** rappresenta il livello di sicurezza di accesso al documento:

- vero: se il documento è considerato riservato
- falso: se il documento non è considerato riservato

Consente di gestire gli accessi al documento al solo personale autorizzato.

**Identificativo del formato:** indica il formato del documento e la versione del software utilizzato per la creazione del documento stesso.

È costituito da:

- formato: secondo quanto previsto dall'Allegato 2 delle Linee Guida.
- prodotto software: prodotto software utilizzato per la creazione del documento e relativa versione, suddiviso a sua volta in tre sottocampi:
  - nome prodotto
  - versione prodotto
  - produttore

**Verifica:** check di controllo presenza Firma elettronica, Sigillo, Marcatura temporale e Conformità copie immagine nelle modalità di formazione del documento informatico previste nelle Linee Guida.

**Identificativo dell'Aggregazione documentale:** identificativo univoco dell'Aggregazione come definito nel paragrafo dei Metadati delle aggregazioni documentali informatiche. Metadato ricorsivo (*facoltativo*, per le specifiche si rimanda all'Allegato 5).

**Identificativo del Documento Primario:** identificativo univoco e persistente del Documento primario (*obbligatorio nel caso in cui sia presente un documento primario*).

**Nome del documento\file:** nome del documento\file così come riconosciuto all'esterno.

**Versione del documento:** versione del documento.

**Tracciatore modifiche documento:** metadato volto a tracciare la presenza di operazioni di modifica effettuate sul documento e la data in cui esse sono state effettuate. L'autore delle modifiche è tracciato nel metadato "Soggetti" con il ruolo "Operatore" (*obbligatorio nel caso di versione > 1 o in caso di annullamento*).

**Tempo di conservazione:** tempo di conservazione del documento desunto dal Piano di conservazione integrato con il Piano di classificazione (ove presenti) o prescritto dalla normativa salvo contenzioso. In generale il tempo di conservazione a livello di singolo documento deve essere indicato solo qualora esso presenti un tempo di conservazione distinto da quello assegnato all'aggregazione documentale informatica a cui il documento stesso appartiene. Espresso in numero di anni, il valore 9999 indica un tempo di conservazione "Permanente" (*facoltativo*).

**Note:** eventuali indicazioni aggiuntive utili ad indicare situazioni particolari (*facoltativo*).

Nella scheda cliente è possibile personalizzare ed indicare i set di metadati in base alle esigenze del soggetto produttore e alle diverse tipologie documentali conservate. In un'apposita tabella il cliente specificherà i metadati di proprio interesse.

[Torna al sommario](#)

## 6.1.2 Metadati del documento amministrativo informatico

Di seguito vengono elencati i metadati, ed i principali campi e sottocampi obbligatori del documento informatico:

**IdDoc:** Identificativo univoco e persistente associato in modo univoco e permanente al documento informatico in modo da consentirne l'identificazione

Il metadato è costituito dai seguenti:

- Impronta crittografica del documento: a sua volta suddiviso in:
  - Impronta: sottocampo in cui viene memorizzato l'hash del documento
  - Algoritmo: sottocampo nel quale deve essere indicata la tipologia dell'algoritmo applicato riportati nell'Allegato 6 delle Linee Guida nella tabella 1 del paragrafo 2.2 "Regole di processamento"
- Identificativo: come da sistema di identificazione formalmente definito
- Segnatura: segnatura di protocollo, da indicare obbligatoriamente nel caso di documento amministrativo protocollato, a sua volta strutturato come da Allegato 6 delle Linee Guida.

**Modalità di formazione:** modalità di generazione del documento informatico

Sono previste le seguenti modalità:

- creazione tramite l'utilizzo di strumenti software che assicurino la produzione di documenti nei formati previsti nell'Allegato 2 delle Linee Guida;
- acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;
- memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;
- generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica

**Soggetti:** indica il metadato che consente di individuare le informazioni relative a tutti i soggetti coinvolti e competenti sul documento a vario titolo e definiti dal campo Ruolo.

Sono definiti i seguenti attributi:

- Ruolo: consente di indicare, a seconda delle necessità, l'autore del documento, il mittente, il destinatario, l'assegnatario. Al fine di rendere i dati di registrazione univoci deve essere sempre indicato il Soggetto che effettua la registrazione del documento (tipicamente l'Organizzazione che protocolla). Obbligatorio inoltre indicare almeno l'autore o il mittente. Nel caso di documento protocollato deve essere obbligatoriamente indicato il mittente.
- Tipo soggetto: consente di tipizzare i soggetti come persone fisiche, giuridiche, amministrazioni pubbliche (italiane ed estere). Il Tipo Soggetto = SW è indicabile solo se si è indicato il ruolo = "Produttore". Per ogni Tipo Soggetto sono indicati i metadati di riferimento

**Chiave descrittiva:** metadato funzionale volto a riassumere il contenuto del documento o comunque a chiarirne la natura.

È costituito da seguenti campi:

- Oggetto: testo libero

**Allegati:** Indica il numero di allegati al documento e, nell'eventualità che il numero di allegati indicati sia maggiore di zero, devono essere compilati, in modalità ricorsiva, i dati:

- IdDoc: Identificativo del documento relativo all'allegato
- Descrizione: Titolo dell'Allegato

**Classificazione:** classificazione del documento secondo il Piano di classificazione utilizzato da indicare sia nel caso di documento protocollato che nel caso di documento non protocollato

- Indice di classificazione: codifica del documento secondo il Piano di classificazione utilizzato
- Descrizione: descrizione per esteso dell'Indice di classificazione indicato.

**Riservato:** rappresenta il livello di sicurezza di accesso al documento:

- vero: se il documento è considerato riservato
- falso: se il documento non è considerato riservato

Consente di gestire gli accessi al documento al solo personale autorizzato.

**Identificativo del formato:** indica il formato del documento e la versione del software utilizzato per la creazione del documento stesso.

È costituito da:

- formato: secondo quanto previsto dall'Allegato 2 delle Linee Guida.
- prodotto software: prodotto software utilizzato per la creazione del documento e relativa versione, suddiviso a sua volta in tre sottocampi:
  - nome prodotto

- versione prodotto
- produttore

**Verifica:** check di controllo presenza Firma elettronica, Sigillo, Marcatura temporale e Conformità copie immagine nelle modalità di formazione del documento informatico previste nelle Linee Guida.

**Identificativo dell'Aggregazione documentale:** identificativo univoco dell'Aggregazione come definito nel paragrafo dei Metadati delle aggregazioni documentali informatiche. Metadato ricorsivo.

**Identificativo del Documento Primario:** identificativo univoco e persistente del Documento primario (*obbligatorio nel caso in cui sia presente un documento primario*).

**Nome del documento\file:** nome del documento\file così come riconosciuto all'esterno.

**Versione del documento:** versione del documento.

**Tracciatore modifiche documento:** metadato volto a tracciare la presenza di operazioni di modifica effettuate sul documento e la data in cui esse sono state effettuate. L'autore delle modifiche è tracciato nel metadato "Soggetti" con il ruolo "Operatore" (*obbligatorio nel caso di versione > 1 o in caso di annullamento*).

**Tempo di conservazione:** tempo di conservazione del documento desunto dal Piano di conservazione integrato con il Piano di classificazione (ove presenti) o prescritto dalla normativa salvo contenzioso. In generale il tempo di conservazione a livello di singolo documento deve essere indicato solo qualora esso presenti un tempo di conservazione distinto da quello assegnato all'aggregazione documentale informatica a cui il documento stesso appartiene. Espresso in numero di anni, il valore 9999 indica un tempo di conservazione "Permanente" (*facoltativo*).

**Note:** eventuali indicazioni aggiuntive utili ad indicare situazioni particolari (*facoltativo*).

Nella Scheda Cliente predisposta da Unimatica, è possibile personalizzare ed indicare i set di metadati in base alle esigenze del soggetto produttore e alle diverse tipologie documentali conservate. In un'apposita tabella il cliente specificherà i metadati di proprio interesse.

### **6.1.3 Metadati delle aggregazioni documentali informatiche**

Di seguito vengono elencati i metadati, ed i principali campi e sottocampi obbligatori delle aggregazioni documentali informatiche:

**Identificativo dell'Aggregazione documentale:** si tratta di una sequenza di caratteri alfanumerici associata in modo univoco all'aggregazione documentale informatica in modo da consentirne l'identificazione, indica se si tratta di un Fascicolo o di una Serie Documentale o di una Serie di Fascicoli.

Il fascicolo è una aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento.

Le serie documentarie sono costituite da documenti singoli accorpati per ragioni funzionali in base alla tipologia di riferimento.

Le serie di fascicoli sono costituite da fascicoli accorpati per ragioni funzionali in base alla classe di riferimento o alla tipologia di fascicoli.

Sono definiti i seguenti attributi:

- TipoAggregazione
  - Fascicolo
  - Serie Documentale
  - Serie Di Fascicoli
- IdAggregazione: come da sistema di identificazione formalmente definito

**Tipologia fascicolo:** I fascicoli sono organizzati per:

- **affare:** conserva i documenti relativi a una competenza non proceduralizzata, ma che nella consuetudine amministrativa la PA deve concretamente portare a buon fine. Il fascicolo per affare ha una data di apertura e una durata circoscritta.
- **attività:** comprende i documenti prodotti nello svolgimento di un'attività amministrativa semplice che implica risposte obbligate o meri adempimenti, per la quale quindi non è prevista l'adozione di un provvedimento finale. Ha in genere durata annuale.
- **persona fisica:** comprende tutti i documenti, anche con classifiche diverse, che si riferiscono a una persona fisica. Quasi sempre i fascicoli intestati alle persone restano correnti per molti anni, costituendo serie aperte.
- **persona giuridica:** comprende tutti i documenti, anche con classifiche diverse, che si riferiscono a una persona giuridica. Quasi sempre i fascicoli intestati alle persone restano correnti per molti anni, costituendo serie aperte
- **procedimento amministrativo:** conserva una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un provvedimento amministrativo.

**Soggetti:** indica il metadato che consente di individuare le informazioni relative a tutti i Soggetti che, a vario titolo, sono coinvolti nella costituzione dell'aggregazione.

Sono definiti quindi i seguenti attributi:

- **Ruolo:**
  - Amministrazione titolare
  - Amministrazioni partecipanti
  - Assegnatario
  - Soggetto intestatario persona fisica
  - Soggetto intestatario persona giuridica
  - RUP: da indicare solo in caso di TipoAggregazione = 'Fascicolo'
- **Tipo soggetto:** consente di tipizzare i soggetti come persone fisiche, giuridiche, amministrazioni pubbliche (italiane ed estere) in funzione del Ruolo. Per ogni tipo soggetto sono indicati i metadati di riferimento. Nel caso in cui sia stato definito un Ruolo=RUP è obbligatorio indicare anche l'UOR corrispondente.

**Assegnazione:** indica il metadato che consente di individuare le informazioni relative all'assegnazione per conoscenza o per competenza. I Soggetti indicati in questo metadato devono essere stati dichiarati nel metadato Soggetti. Sono definiti quindi i seguenti attributi:

- Tipo assegnazione (obbligatorio in caso di fascicolo)
- Soggetto assegnatario (obbligatorio in caso di fascicolo)
- Data inizio assegnazione (obbligatorio in caso di fascicolo)
- Data fine assegnazione (facoltativo)

Il metadato ha una struttura ricorsiva.

**Data Apertura:** data di apertura dell'aggregazione documentale.

**Classificazione:** classificazione dell'aggregazione:

- Indice di classificazione: Codifica del documento secondo il Piano di classificazione utilizzato
- Descrizione: Descrizione per esteso dell'Indice di classificazione indicato.
- Piano di classificazione: se presente, riportare eventualmente l'URI di pubblicazione del Piano di classificazione (facoltativo)

**Progressivo:** progressivo numerico calcolato nell'ambito della chiave della classificazione o in ordine cronologico nell'ambito dell'anno.

**Chiave descrittiva:** metadato funzionale volto a chiarire la natura del fascicolo o della serie.

È costituito da seguenti campi:

- Oggetto: testo libero

**Data Chiusura:** data di chiusura dell'aggregazione documentale.

**Procedimento Amministrativo:** metadato funzionale volto ad indicare il procedimento a cui il fascicolo afferisce, nonché lo stato di avanzamento e le relative fasi.

È costituito da seguenti campi:

- Materia\ Argomento\ Struttura: indicare la materia o l'argomento o la struttura per la quale sono stati catalogati i procedimenti amministrativi
- Procedimento: denominazione del Procedimento
- Catalogo procedimenti: URI di pubblicazione del catalogo
- Fasi: a sua volta suddiviso, in una struttura ricorsiva:
  - Tipo Fase
    - Preparatoria
    - Istruttoria
    - Consultiva
    - decisoria o deliberativa
    - integrazione dell'efficacia
  - Data inizio fase
  - Data fine fase (facoltativo)

da "Data inizio fase" e "Data fine fase" deve considerarsi dinamico, destinato ad essere aggiornato con lo stato di avanzamento dell'iter del procedimento\processo.

**Indice documenti:** elenco degli identificativi dei documenti contenuti nell'aggregazione, definiti secondo le regole indicate per i documenti informatici o i documenti amministrativi informatici. Metadato ricorsivo.

È costituito da seguenti campi:

- Tipo documento
  - documento amministrativo informatico
  - documento informatico
- IdDoc
  - se documento amministrativo informatico  
IdDoc come definito nel precedente paragrafo dei Metadati del documento amministrativo informatico
  - se documento informatico

IdDoc come definito nel precedente paragrafo dei Metadati del documento informatico

**Posizione fisica Aggregazione Documentale:** posizione fisica dell'aggregazione. Nel caso di fascicoli ibridi indica la posizione della componente cartacea del fascicolo.

## 6.1.4 Metadati del documento informatico di natura fiscale e contabile

In relazione alla valorizzazione dei metadati specifici del documento informatico di natura fiscale e contabile si rimanda alle specifiche descritte nelle istruzioni dal titolo *I metadati del documento informatico di natura fiscale e contabile* pubblicato nella sezione Linee guida del sito di AgID.

[Torna al sommario](#)

## 6.2 Formati

Unistorage, in conformità all'*Allegato 2 "Formati di file e riversamento"* alle Linee guida AgID, accetta e gestisce formati aperti, non proprietari, standard de iure, estendibili, parlanti, completamente robusti, indipendenti dal dispositivo e che garantiscano i principi dell'interoperabilità.

Tuttavia, in accordo con il soggetto produttore, Unimatica permette anche l'accettazione di formati non esplicitati nell'*Allegato 2*. Infatti qualora l'ordinamento giuridico preveda degli obblighi relativamente all'uso di formati specifici per alcuni Titolari, questi assolvendo tali obblighi, sono chiamati ad effettuare una valutazione di interoperabilità utile anche per garantire la conservazione e la fruibilità degli stessi nel tempo. L'indicazione di tali formati, compresa la gestione di questi, verrà indicata nella scheda cliente.

[Torna al sommario](#)

### 6.2.1 Riversamento

Unistorage, in relazione all'obsolescenza dei formati, tiene un censimento dei formati di file ricevuti in conservazione a seguito di un'attività di ingestione (compreso il recupero da precedente conservatore). Il responsabile del servizio di conservazione, assieme al responsabile della funzione archivistica, al responsabile sviluppo e manutenzione del sistema di conservazione e al responsabile sicurezza dei sistemi per la conservazione, con cadenza non superiore ai 5 anni, fatta una fotografia dei formati di file censiti al momento sul sistema, ne valuta il grado di obsolescenza.

In fase di analisi dei formati, come da procedura stabilita, per ogni formato si attribuisce un grado di obsolescenza, basandosi sulle caratteristiche di apertura, sicurezza, portabilità, funzionalità, supporto allo sviluppo e diffusione. Al termine della verbalizzazione di questo processo di verifica, a fronte di evidenze di formati di file per cui è impossibile individuare soluzioni in grado di rappresentare fedelmente il contenuto di questi file, il responsabile del servizio di conservazione attiva il processo di riversamento dei file appartenenti ai formati risultati a rischio di obsolescenza, previa certificazione di processo.

Per tutti i dettagli inerenti all'intero processo di gestione del riversamento si rimanda al documento di sistema "PRO\_CONS01 - Procedure di Conservazione".

[Torna al sommario](#)

## 6.3 Struttura dati del Pacchetto di versamento

Unimatica mediante il prodotto applicativo UniStorage, con la supervisione del Responsabile del servizio di conservazione permette un duplice iter per la ricezione dei Pacchetti di Versamento: ricezione dei file tramite canale SSH File Transfert Protocol e ricezione tramite sistema Web service.

- La ricezione mediante SSH File Transfert Protocol prevede l'upload del Pacchetto di versamento composto da un file indice e da un insieme di file, in formato .zip. Per maggiori dettagli circa la struttura dei Pacchetti di versamento, fare riferimento al documento Flusso per la conservazione dei Documenti in Unistorage.
- La ricezione tramite Sistema Web Service è possibile da qualsiasi piattaforma che permetta di eseguire e ricevere chiamate Web Service conformi allo standard WS-I Basic Profile 1.0. Con questo servizio il sistema di conservazione riceve singoli documenti ed eventuali allegati, ne verifica la firma digitale se presente e ne gestisce la conservazione autentica. Per maggiori dettagli circa la ricezione degli oggetti digitali tramite Sistema Web Service si rimanda al documento "Specifiche del servizio web per la consegna anticipata di documenti nel Sistema di conservazione".

[Torna al sommario](#)

## 6.4 Struttura dati del Pacchetto di archiviazione

Terminato il processo di acquisizione dei Pacchetti di versamento, il prodotto applicativo UniStorage sotto la supervisione del Responsabile del servizio di conservazione e del Responsabile della funzione archivistica provvede alla creazione dei Pacchetti di archiviazione e dell'Indice del pacchetto di archiviazione previsto dallo standard UNI 11386 SInCRO – Supporto all'interoperabilità nella conservazione e nel recupero degli oggetti digitali.

I Pacchetti di archiviazione contengono<sup>5</sup>:

- l'oggetto o gli oggetti da conservare;
- l'Indice del Pacchetto di archiviazione, formato secondo le regole dettate dallo Standard UNI 11386 SInCRO – Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.

Tutti i pacchetti di archiviazione prodotti fino al 31 dicembre 2021 implementano lo standard UNI 11386:2010 SInCRO. A partire dal 1° gennaio 2022 viene applicata la versione 2020 dello standard.

[Torna al sommario](#)

## 6.5 Struttura dati del Pacchetto di distribuzione

La produzione di Pacchetti di distribuzione avviene in seguito alla richiesta da parte dell'Utente.

<sup>5</sup> Sono elencate le caratteristiche indicate nell'allegato 4 al DPCM 3 dicembre 2013 Regole tecniche in materia di sistema di conservazione.

L'esibizione del materiale di interesse avviene via interfaccia web o, su esplicita richiesta al team di delivery conservazione, mediante deposito su canale sicuro SFTP o memorizzazione su supporto rimovibile fornito dal titolare dell'oggetto di conservazione. La descrizione dettagliata delle procedure è indicata nel capitolo 7 "Il processo di erogazione del servizio di conservazione", Fase 6.

I Pacchetti di distribuzione generati contengono sia gli oggetti che l'insieme delle evidenze di conservazione.

[Torna al sommario](#)

## 7. Il processo di erogazione del servizio di conservazione

Il processo di conservazione eseguito da Unimatica adotta il modello standard OAIS - Open Archival Information System<sup>6</sup> che definisce concetti e funzionalità degli archivi digitali. Lo schema seguente illustra brevemente gli aspetti principali di un generico processo di conservazione: il Soggetto produttore invia il Pacchetto di versamento, di cui ha piena responsabilità, al Soggetto conservatore il quale provvede a trasformarlo in Pacchetto di archiviazione. Ai fini dell'esibizione e della distribuzione richiesti dalla comunità di riferimento<sup>7</sup>, il Soggetto conservatore provvederà a creare i Pacchetti di distribuzione in una forma tale che venga garantita la corretta visualizzazione di questi.

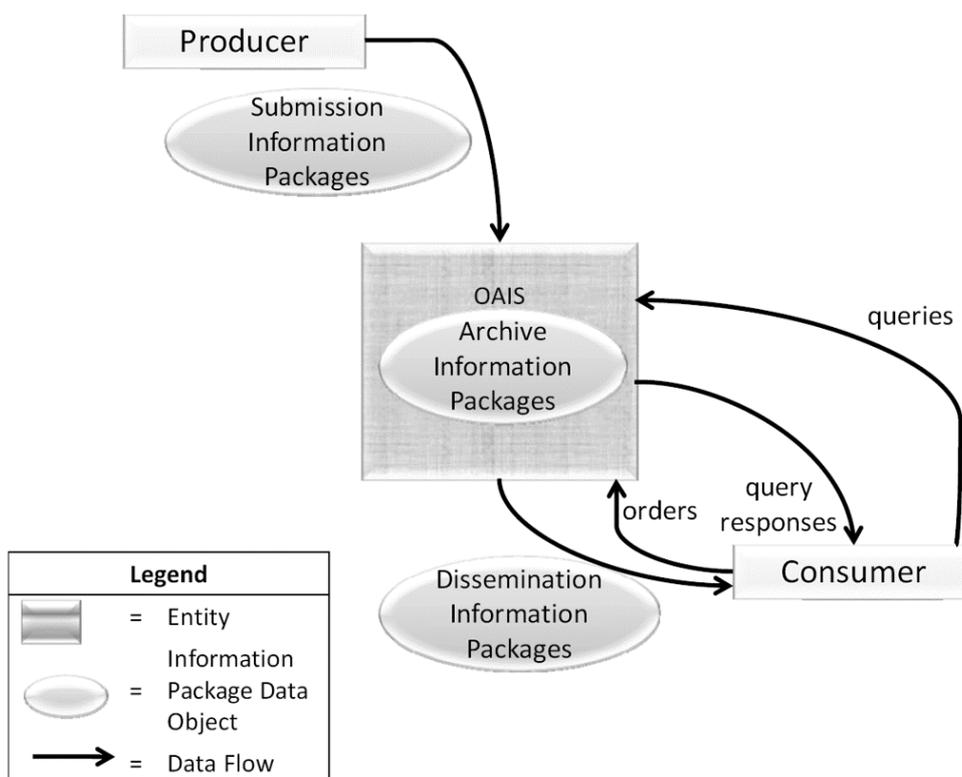


Figura 2 - Modello OAIS

[Torna al sommario](#)

### 7.1. Il processo di conservazione

Il servizio offerto da Unimatica ad ogni Soggetto produttore viene avviato al termine di un processo di attivazione che segue queste fasi fondamentali:

<sup>6</sup> L'Open Archival Information System è lo standard ISO per la conservazione a lungo termine di archivi digitali.

<sup>7</sup> Comunità di riferimento: il sottoinsieme degli utenti in grado di comprendere autonomamente l'informazione archiviata nella forma in cui è conservata e resa disponibile dall'OAIS

- 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.

Di seguito vengono dettagliate le fasi del processo.

[Torna al sommario](#)

## **7.2. Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico**

In questa fase il Soggetto produttore veicola al Responsabile del servizio di conservazione, al Privacy Manager e al Responsabile della funzione archivistica la richiesta di attivazione del servizio per l'invio di Pacchetti di versamento. Le tre figure responsabili sopracitate, con l'ausilio del Responsabile dello sviluppo e della manutenzione, incaricato di curare l'interfaccia con il Soggetto produttore relativamente alle modalità di trasferimento dei documenti, valuteranno la domanda di acquisizione del servizio affinché venga accertato che i requisiti del Soggetto produttore siano compatibili con le policy di Unimatica

L'attivazione del servizio avviene attraverso la compilazione del Modulo 'Scheda cliente'. In particolare, tale modulo deve essere compilato con le seguenti informazioni:

- ragione sociale;
- indirizzo;
- partita iva;
- e-mail
- oggetti documentali gestiti
- tipo di protocollo da utilizzare per lo scambio dei Pacchetti.
- metadati specifici di tipologia
- utenze da abilitare per l'accesso al portale di distribuzione.

Per ogni Pacchetto di versamento dichiarato dal Soggetto produttore, è possibile definire:

- i volumi in termini di numero documenti annui previsti da gestire e spazio di occupazione previsto per i dati da Conservare (GB);
- la dimensione massima del Pacchetto di versamento;
- la frequenza di invio dei Pacchetti;

Il Responsabile del servizio di conservazione, valuterà in accordo con il Privacy manager, con il Responsabile della funzione archivistica e con il Responsabile dello sviluppo e della manutenzione

la domanda di acquisizione del servizio collaborando con il Soggetto produttore guidandolo nella compilazione della domanda per l'attivazione del servizio.

Il Responsabile del servizio di conservazione e il Responsabile della funzione archivistica una volta ricevuta la richiesta, si impegnano a valutarne l'impatto stimando la data di evasione e fornendo al Soggetto produttore una pianificazione delle fasi successive. Se la richiesta di configurazione implica un aggravio di costi, verrà fornita parallelamente al Soggetto produttore la quotazione economica dell'attività redatta dal Referente Commerciale di Unimatica

L'acquisizione dei Pacchetti di versamento avviene mediante due canali: tramite SSH File Transfert Protocol e tramite canale Web service descritti dettagliatamente nel capitolo "Oggetti sottoposti in conservazione", paragrafo 6.3.

Ad ogni attivazione verranno consegnate le credenziali per accedere all'applicativo web reso disponibile da Unimatica, in base ai dati presenti nella Scheda cliente. Tale accesso garantirà la piena esibizione dei Pacchetti di distribuzione.

[Torna al sommario](#)

### **7.3. Verifiche effettuate sui Pacchetti di versamento e sugli oggetti in esso contenuti**

I parametri gestionali del Pacchetto di versamento vengono verificati e messi a punto dal Responsabile del servizio di conservazione e dal Responsabile della funzione archivistica in accordo con il Soggetto produttore. Le verifiche effettuate sui Pacchetti di versamento sono le seguenti:

- **identificazione certa del Soggetto produttore;**
- verifica delle **firme digitali** se presenti mediante un controllo crittografico dell'integrità del documento e della validità formale delle firme stesse. In un secondo momento viene verificata l'identità del sottoscrittore. Se una chiave privata sia stata usata in una firma è verificabile, mediante processo crittografico, con la corrispondente chiave "pubblica". Le chiavi pubbliche sono riportate nei "certificati di firma digitale", documenti informatici anch'essi, che definiscono anche i dati d'identità del sottoscrittore. I certificati sono a loro volta firmati da una autorità di certificazione emittente (C.A. - Certification Authority). In generale si risalirà la catena di certificazione fino a raggiungere un "certificato fidato", ovvero pubblicamente noto. Tra le evidenze informatiche che Unimatica conserva ci sono, per ogni Pacchetto, tutti i certificati a vario modo coinvolti nelle catene di certificazione necessarie alle verifiche di firma digitale. Questo consente di costituire un insieme "auto-contenuto" di evidenze che possono essere verificate anche a posteriori. Si può anche verificare il caso che l'autorità emittente non sia direttamente un'autorità pubblicamente nota, ma che esista una "catena di certificazione" (trust chain) per cui l'autorità di un certificato vada a sua volta identificata risalendo ad un'autorità terza.
- verifica che i **formati** degli oggetti da conservare siano conformi con quanto dichiarato nella scheda cliente e nell'Allegato 2 alle Linee guida per la Formazione, gestione e conservazione dei documenti informatici. Alla ricezione del documento il sistema, attraverso l'uso di una libreria WAZFORMAT, la cui procedura utilizzerà un metodo di indagine diretta con tecniche euristiche, riconosce il formato controllando il valore descritto nel magic number. Questo passaggio permette di associare il formato al documento per garantirne la corretta visualizzazione e quindi leggibilità utilizzando gli opportuni i visualizzatori.

- relativamente alle verifiche dei **metadati** sono previste tre livelli di controllo:
  - o *strict*: l'assenza di anche solo un metadato obbligatorio (Allegato 5 alle Linee guida) comporta la restituzione di un errore alla richiesta di versamento ed il documento non viene conservato
  - o *permissive*: l'assenza di metadati obbligatori (Allegato 5 alle Linee guida) viene segnalata con un warning, ma il processo di conservazione prosegue generando i metadati assenti con un valore nullo.
  - o *skip*: applicato a tutti i soggetti produttori non vincolati alla normativa italiana (Allegato 5 alle Linee guida). In questo caso i metadati obbligatori sono concordati con il soggetto produttore in base alle buone prassi o ai vincoli normativi del paese di origine.

[Torna al sommario](#)

## 7.4. Accettazione dei Pacchetti di versamento e generazione del Rapporto di versamento di presa in carico

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 (Tcons).

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.

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).

La modalità di conservazione mediante Rapporto di versamento permette di verificare l'integrità di ogni singolo file, a prescindere da tutti gli altri file conservati nello stesso pacchetto. Infatti sarà sufficiente essere in possesso di un file "candidato" e conoscere il suo URN identificativo per poter eseguire la funzione di hash e confrontare l'impronta ricalcolata con la stringa riportata nel Rapporto. In questa fase vengono associate all'indice tutte le evidenze di autenticità delle firme digitali che verranno verificate all'istante del riferimento temporale:

- i certificati di firma di tutte le firme presenti nel Pacchetto di versamento,
- tutti i certificati appartenenti alle catene di certificazione (trusting chain),
- le liste di revoca dei singoli certificati (CRL).

Il Rapporto di versamento viene conservato all'interno del sistema garantendone l'ininterrotta custodia e la non modificabilità.

[Torna al sommario](#)

## 7.5. Rifiuto dei Pacchetti di versamento e modalità di comunicazione delle anomalie

Le verifiche effettuate sui Pacchetti di versamento possono risultare negative. Nei casi in cui anche solo su uno dei controlli indicati nella fase 2 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.

Le anomalie, in relazione a quanto descritto nella fase 2, possono essere identificate nell'assenza dei metadati obbligatori ovvero nella mancata corrispondenza di ciò che viene versato a quanto dichiarato dal soggetto produttore nella scheda cliente in termini di firma digitale, formati e metadati. Qualora l'anomalia venisse riscontrata soltanto su una parte di documenti inclusi nel Pacchetto di versamento, è facoltà del soggetto produttore decidere se bloccare l'intero pacchetto o soltanto i documenti segnalati. In questo ultimo caso i file conformi vengono inviati in conservazione e gli altri spediti successivamente mediante nuovo Pacchetto di versamento.

[Torna al sommario](#)

## 7.6. Preparazione e gestione dei Pacchetti di archiviazione

I Pacchetti versati in UniStorage, con la supervisione del Responsabile del servizio di conservazione e del Responsabile della funzione archivistica vengono raggruppati in Pacchetti di archiviazione. Questi pacchetti vengono assemblati dal sistema nei tempi e con i criteri di raggruppamento scelti e concordati con il Soggetto produttore, indicati nella Scheda Cliente (ad es. Pacchetti di archiviazione per tipologie documentali o in base alla cadenza temporale di consegna).

Il processo di costruzione dei Pacchetti di archiviazione, così come previsto dallo standard SInCRO UNI 11386– Supporto all'interoperabilità nella conservazione e nel recupero degli oggetti digitali, avviene con le seguenti modalità:

- individuazione dei documenti destinati a far parte del pacchetto di archiviazione sulla base dei criteri scelti. Tali criteri vengono concordati con il cliente e sono definiti nella scheda cliente e si possono basare sia su caratteristiche legate allo stato del documento, sia sui metadati.
- i Pacchetti di archiviazione vengono chiusi in seguito a due tipi di regole:
  - automatiche: collocano nel pacchetto i documenti per i quali ci sia almeno un certificato di firma prossimo alla scadenza. Questa tipologia di regole ha la precedenza su quelle descritte nel punto successivo, le quali riguardano la dimensione massima del Pacchetto di archiviazione e il tempo limite oltre il quale un Pacchetto di archiviazione deve essere forzatamente chiuso,
  - attuate dal Responsabile del servizio di conservazione in accordo con il soggetto produttore: definite nella scheda cliente.

Nei casi in cui i Pacchetti di archiviazione contengano referti sanitari, questi vengono crittografati mediante funzione crittografica della suite standard del linguaggio Java. In particolare è definita nel package crypto di JCE e impiega l'algoritmo AES a 128 bit ECB.

I Pacchetti di archiviazione vengono sottoscritti con firma digitale dal Responsabile del servizio di conservazione e marcati temporalmente.

La sottoscrizione dei Pacchetti di archiviazione effettuata da Unimatica attesta esclusivamente la corretta esecuzione del processo di conservazione secondo la normativa vigente in materia di conservazione. Unimatica non è responsabile dell'errato contenuto informativo degli oggetti versati.

[Torna al sommario](#)

## 7.7. Preparazione e gestione dei Pacchetti di distribuzione ai fini dell'esibizione

La gestione dei Pacchetti di distribuzione fa capo al Responsabile del Servizio di Conservazione, al Responsabile della Funzione archivistica e al Privacy manager.

La produzione di Pacchetti di distribuzione avviene in seguito alla richiesta da parte dell'utente.

UniStorage, prevedendo la conservazione dei Pacchetti di archiviazione firmati, implementa un formato di composizione delle marche tale da permettere l'esibizione probatoria di un singolo documento. Quindi, ogni singolo file può essere esibito insieme ai suoi metadati, registrati nel data base, e alle sue prove di conservazione in maniera assolutamente INDIPENDENTE dagli altri documenti.

Unimatica permette l'accesso ai Pacchetti di distribuzione esclusivamente agli utenti autorizzati. I livelli di accesso vengono definiti in base alle esigenze delle richieste effettuate, rendendo disponibile soltanto il materiale richiesto grazie all'utilizzo di filtri predefiniti che selezionano i canali previsti per la visualizzazione di un determinato pacchetto.

È possibile visualizzare i documenti tramite triplice canale:

- via web: i Soggetti produttori titolari dei documenti potranno ricercare e visualizzare tutti i documenti conservati direttamente sul portale di Unimatica attraverso l'apposita funzionalità. L'accesso avviene tramite il portale al quale è demandata la sicurezza e la gestione della sessione. I documenti saranno disponibili per l'esibizione on-line per tutto il periodo di conservazione. Per la ricerca dei documenti è possibile utilizzare dei filtri valorizzando gli appositi campi delle maschere di ricerca con i metadati dichiarati in fase di versamento. La descrizione di dettaglio dell'interfaccia web per le richieste di esibizione dei documenti è contenuta nell'allegato 'Funzionalità\_portale'. L'accesso al portale può avvenire tramite credenziali nominali fornite al momento dell'attivazione delle utenze o tramite SPID. Vengono inoltre resi disponibili servizi web (Web Services) per le eventuali integrazioni con i portali dei Soggetti produttori.
- copia del documento su supporto removibile. La descrizione dettagliata circa la visualizzazione dei Pacchetti di distribuzione mediante supporto removibile è presente nel capitolo 6 Oggetti sottoposti a conservazione, paragrafo 6.5.
- restituzione via canale SFTP. In questo caso viene richiesto al soggetto produttore di generare una coppia di chiavi (pubblica e privata) in formato OpenSSH RSA, di lunghezza minima 2048 bit e di fornirci la chiave pubblica della coppia per l'apertura del canale.

La struttura architettuale di UniStorage consente di definire diversi livelli operativi e garantisce che ciascuna Azienda/Ente, Area Organizzativa, Agenzia, Ufficio, Dipartimento, ecc. possa accedere

solo ed esclusivamente ai propri documenti, in base alle credenziali e alle politiche di accesso attivate.

[Torna al sommario](#)

## **7.8. Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento di un pubblico ufficiale**

Con la richiesta da parte dell'utente di esibizione dei Pacchetti di distribuzione mediante supporto removibile, viene generata una copia autentica del documento, conforme all'originale. Per i dettagli sulla modalità di richiesta di esibizione dei Pacchetti di distribuzione, fare riferimento al capitolo 6 "Oggetti sottoposti a conservazione" paragrafo 6.5 e al capitolo 7 "Il processo di erogazione del servizio di conservazione", fase 6.

Nei casi in cui, come previsto dall'art. 23-bis, c. 2 del Codice dell'Amministrazione Digitale<sup>8</sup> il Soggetto produttore richiede la presenza di un pubblico ufficiale, Unimatica garantirà tale presenza mettendo a disposizione tutte le necessarie risorse che serviranno all'espletamento delle attività, rimandando in ogni caso la scelta al Soggetto produttore al quale saranno addebitate le spese.

Inoltre, in caso di adeguamento del formato dovuto all'evoluzione tecnologica verranno rispettate tutte le procedure elencate nell'Allegato 'Infrastrutture' al presente Manuale. Anche in questo caso, l'eventuale presenza del pubblico ufficiale per l'attestazione di conformità, sarà garantita in seguito alla richiesta del Soggetto produttore a cui vengono attribuiti i costi di gestione.

[Torna al sommario](#)

## **7.9. Scarto dei Pacchetti di archiviazione**

Il Periodo di conservazione dei documenti è, per ciascuna tipologia documentale, la durata temporale, espressa in anni, per la quale il Soggetto produttore prevede il servizio di conservazione. Tale durata temporale sarà riportata all'interno del piano di conservazione, qualora redatto dal Soggetto produttore, e sarà condivisa dal Soggetto produttore con Unimatica per mezzo di una comunicazione certa, relativamente a tutte le tipologie documentali per le quali Unimatica eroga servizi di conservazione al Soggetto produttore. Il Soggetto produttore si impegna altresì a comunicare tempestivamente ad Unimatica eventuali modifiche apportate ai Periodi di conservazione per le tipologie documentali conservate da Unimatica.

Entro tre mesi prima della scadenza del Periodo di conservazione per i documenti conservati da Unimatica, il Titolare dell'oggetto di conservazione dovrà prendere contatto con Unimatica ed indicare la volontà di continuare la conservazione digitale a norma, con opportuna estensione contrattuale ove necessario, oppure di procedere con l'attività dello scarto.

Qualora il Titolare non prenda contatti si intenderà prorogato, a parità di condizioni contrattuali, il periodo di conservazione per un ulteriore anno rispetto all'avvenuta scadenza.

Qualora il Titolare prenda contatto con Unimatica e decida di avviare la procedura di scarto, saranno concordate con il Responsabile del servizio di conservazione di Unimatica le modalità operative per procedere allo scarto.

<sup>8</sup> "Le copie e gli estratti informatici del documento informatico, se prodotti in conformità alle vigenti regole tecniche di cui all'articolo 71, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale, in tutti le sue componenti, è attestata da un pubblico ufficiale a ciò autorizzato o se la conformità non è espressamente disconosciuta. Resta fermo, ove previsto, l'obbligo di conservazione dell'originale informatico."

Su indicazione del Titolare, il responsabile del servizio di Unimatica genera l'elenco delle Unità Documentarie da destinare allo scarto e lo invia al Titolare dell'oggetto di conservazione che a sua volta, verificato il rispetto dei termini temporali stabiliti dal piano di conservazione, lo comunica al responsabile della gestione documentale o al coordinatore della gestione documentale, ove previsto.

In caso di archivi pubblici o privati dichiarati di interesse storico particolarmente importante l'autorizzazione finale è rilasciata ai sensi della normativa vigente in materia di beni culturali<sup>9</sup>.

Il Titolare, una volta effettuate le verifiche e/o ricevuta l'autorizzazione da eventuali parti coinvolte, provvede a firmare digitalmente ed a trasmettere i seguenti documenti:

- a) Provvedimento di autorizzazione allo scarto, del Titolare, che indichi gli allegati di cui ai due punti seguenti;
- b) Elenco definitivo dei documenti per i quali si autorizza lo scarto;
- c) Nulla osta da parte dell'autorità competente in materia di beni culturali, ove previsto dalla normativa vigente;

Il Responsabile del servizio di conservazione di Unimatica analizza la richiesta ricevuta ed in caso di congruità avvia la procedura di scarto con conseguente cancellazione dei documenti e successiva conservazione della documentazione formale di scarto.

Al termine della procedura di scarto viene generato un verbale di scarto sottoscritto digitalmente dal Responsabile del servizio di conservazione e marcato temporalmente, che verrà conservato insieme ai documenti di cui ai precedenti punti a), b), c) , e di cui verrà data opportuna comunicazione al Titolare.

[Torna al sommario](#)

## **7.10. Predisposizione di misure per l'interoperabilità e la trasferibilità ad altri conservatori**

Unimatica, come descritto al par. 6.4 Struttura dati del Pacchetto di archiviazione, genera i PDA applicando le specifiche tecniche dalla norma UNI 11386 - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali. Accoglie, inoltre, formati conformi all'Allegato 2 delle Linee guida o concordati a seguito di opportuna valutazione di interoperabilità, pertanto Unistorage supporta sia l'acquisizione di PDD provenienti da altri conservatori, sia il riversamento verso altro sistema di conservazione.

[Torna al sommario](#)

---

<sup>9</sup> L'intervento della Soprintendenza archivistica è previsto anche nel caso di archivi privati per i quali è stato dichiarato l'interesse culturale, secondo quanto disposto dall'art. 21, comma 1, lettera d del Codice dei beni culturali (D. Lgs. 22 gennaio 2004, n. 42).

## 7.11. Chiusura del contratto

Il Titolare dell'oggetto di conservazione, in qualsivoglia momento, ha il diritto di rescindere dal contratto. La procedura prevede la compilazione di un apposito modulo, debitamente firmato e timbrato, da inviare ad Unimatica utilizzando una delle modalità di seguito indicate:

1. invio dell'originale cartaceo con firma autografa tramite posta all'indirizzo corrispondente alla sede legale di Unimatica S.p.A.;
2. invio dell'originale firmato digitalmente dal rappresentante legale, all'indirizzo di posta elettronica certificata (PEC): pec@pec.unimaticaspa.it

Qualora il Titolare intenda disdire il servizio di conservazione a norma dei documenti informatici affidato alla società Unimatica prima del termine contrattualmente previsto per il servizio di conservazione, potrà richiedere la restituzione degli stessi secondo modalità operative che saranno concordate con il Responsabile del servizio di conservazione di Unimatica. A seguito della restituzione le credenziali di accesso al sistema saranno disattivate.

Qualora, per un sottoinsieme di documenti informatici versati in conservazione, si raggiunga il termine contrattualmente previsto per il servizio di conservazione ma non sia stata raggiunta la scadenza del Periodo di conservazione, il Titolare potrà decidere di:

- a) mantenere il servizio di conservazione a norma per una durata che sarà concordata tra il Titolare ed Unimatica, che terrà conto del periodo di conservazione previsto per le tipologie documentali trattate e che sarà formalizzata con un apposito contratto;
- b) non mantenere la conservazione a norma dei documenti informatici presso Unimatica e procedere alla restituzione degli stessi secondo modalità operative che saranno concordate con il Responsabile del servizio di conservazione di Unimatica. A seguito della restituzione le credenziali di accesso al sistema saranno disattivate.

Qualora, per un sottoinsieme di documenti informatici versati in conservazione, si raggiunga il termine contrattualmente previsto per il servizio di conservazione e questo coincida con la scadenza del Periodo di conservazione, varrà quanto previsto al paragrafo Scarto dei Pacchetti di archiviazione

I documenti informatici che sono stati oggetto di conservazione a norma possono essere restituiti, a richiesta, all'utente nel formato standard previsto dalla normativa in vigore (SInCRO – standard UNI 11386 – Supporto all'Interoperabilità nella Conservazione e nel recupero degli Oggetti digitali).

[Torna al sommario](#)

---

## 8. Procedure di gestione e di evoluzione

---

A coordinare la gestione del sistema, l'aggiornamento di questo e le procedure di adeguamento all'evoluzione tecnologica è la figura del Responsabile sviluppo e manutenzione che esegue una costante attività di controllo dell'attività di conservazione in conformità agli standard di qualità e sicurezza ISO 9001 e ISO 27001.

Affinché venga garantito un controllo totale sul sistema e un buon funzionamento di questo, le attività di manutenzione vengono svolte sia sui processi che sulle strutture hardware e software e viene condotta una quotidiana verifica delle attività sulle infrastrutture parallelamente ad una pianificazione delle eventuali procedure straordinarie da condurre in caso di anomalie.

[Torna al sommario](#)

---

### 8.1. Misure di sicurezza logica

---

Il presente paragrafo ha l'obiettivo di descrivere le misure di sicurezza adottate per l'erogazione del Servizio e per la protezione dei dati che fanno riferimento al Piano per la sicurezza del sistema di conservazione di Unimatica. In particolare, verranno descritte, a titolo esemplificativo ma non esaustivo, le misure di sicurezza tecniche e organizzative adeguate adottate da Unimatica per garantire un livello di sicurezza adeguato al rischio ai sensi dell'art. 32 del GDPR:

- la gestione utenze,
- la gestione sistemi di protezione,
- la gestione degli incidenti di sicurezza,
- la gestione dei backup,
- la gestione dei supporti di memorizzazione.

[Torna al sommario](#)

---

#### 8.1.1 Gestione utenze

---

La policy di riferimento per la gestione delle utenze applicative e di sistema adottata da Unimatica prevede che le utenze siano rilasciate da un ente (o persona) differente dall'ente o persona che le utilizzerà.

Nell'ambito del servizio di conservazione, le utenze applicative e di sistema sono gestite secondo criteri idonei a garantire il rispetto dell'applicazione di misure di sicurezza tecniche e organizzative adeguate a 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 e sia criptata 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 scadenza della password è configurabile attraverso un parametro;
- il sistema deve forzare l'utente a cambiare la password al primo utilizzo;
- 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.

[Torna al sommario](#)

## 8.1.2 Gestione sistemi di protezione

### Net Security

La realizzazione logica della rete è fatta secondo i seguenti criteri:

- controllo degli accessi e dei flussi realizzato tramite firewall in cross-mode (doppio Cisco Pix-535) ed utilizzo di software IP Tables per il port e IP filtering;
- filtro sui flussi di traffico da/per Internet costituito da sistemi McAfee Sidewinder ridondati, che effettuano deep packet inspection e forniscono funzionalità di firewall applicativo (livello 7 OSI);
- segregazione della rete e suddivisione della medesima in differenti porzioni dedicate alla rete di Back End dati per i server contenenti i data base, alla rete di Front End per la parte di presentazione, alla rete di gestione per l'amministrazione (funzione di supporto tecnico) della piattaforma;

Gli accessi alla rete sono segregati a livello di porte ed indirizzi IP. Gli accessi agli apparati di rete sono sottoposti a misure rigide di controllo e sono consentiti solamente agli amministratori della medesima.

### IDS e IPS

Allo scopo di evitare che eventuali malintenzionati possano forzare le protezioni presenti per accedere in maniera illecita a dati riservati, la barriera di firewall applicativi fornisce anche un costante monitoraggio contro accessi non autorizzati tramite funzionalità IPS (Intrusion Prevention System).

[Torna al sommario](#)

## 8.1.3 Gestione degli incidenti di sicurezza

Si definisce incident un stato, in un sistema, un servizio od una rete, che implichi il mancato funzionamento, il possibile mancato rispetto di uno SLA o il mancato funzionamento di contromisure.

Se l'incident coinvolge le proprietà di sicurezza dell'informazione (RID), si configura come incident di sicurezza.

La segnalazione di anomalie può scaturire

- dalle attività di monitoraggio
- da specifica segnalazione da parte di un utente o di personale interno

In entrambi i casi, qualora la segnalazione implichi un problema di sicurezza inficiando quindi l'integrità, riservatezza o disponibilità del dato, la prassi per la gestione degli incident può prevedere l'apertura di un ticket sulla specifica coda OTRS (strumento elettronico di ticketing Open-source Ticket Request System) del servizio di conservazione oppure dell'area sistemi.

Una volta preso in carico il ticket dal Responsabile del settore Conservazione o da un operatore designato egli diventa Incident Owner, cui sono delegate le azioni di: Contenimento<sup>10</sup>, Eliminazione delle cause<sup>11</sup>, Ripristino<sup>12</sup>.

La gestione degli incidenti di sicurezza è regolamentata da specifiche procedure dettagliatamente descritte secondo requisiti conformi allo standard ISO 27001:2013. Maggiori dettagli sono descritti nel capitolo 3 del Piano della Sicurezza.

[Torna al sommario](#)

## 8.1.4 Gestione dei backup e Disaster Recovery

### 8.1.4.1 Siti Settimo e Firenze

L'architettura del sistema backup è composta da un master server per ogni sito e da differenti media server che hanno il compito di archiviare i dati ed inserirli in una rete dedicata, parallela a quella di erogazione dei singoli servizi, per non impattare sulle prestazioni e sulla disponibilità di questi ultimi, durante la normale esecuzione delle attività di backup.

I singoli agent installati sull'infrastruttura di virtualizzazione e sui server non virtualizzati comunicano con il backup server che esegue il salvataggio dei dati su un appliance Data Domain. Il salvataggio dei dati su un appliance Data Domain viene replicato sul sito secondario. Questo sistema consente:

- Semplicità di integrazione anche con future evoluzioni del software di backup
- De-duplicazione del dato ad alta velocità
- Replica efficiente in rete
- Scalabilità dell'infrastruttura

L'architettura di backup utilizza le seguenti tecnologie:

<sup>10</sup> **Contenimento:** processo che rappresenta la fase di esecuzione delle attività di contrasto, atte a mitigare le compromissioni della sicurezza derivanti da un incidente. Una delle attività principali del processo di contenimento è quella di determinare il patrimonio informativo che viene messo a rischio a seguito di un incidente.

<sup>11</sup> **Eliminazione delle cause:** processo che elenca le azioni indirizzate alla rimozione delle cause che scatenano un incidente informatico. E' opportuno sottolineare l'importanza che rappresenta la comprensione del problema che è all'origine dell'incidente; a tale scopo appare determinante descrivere con il maggior dettaglio possibile il modo con cui l'evento di sicurezza si è verificato.

<sup>12</sup> **Ripristino:** processo tramite il quale viene attuato il ritorno alle normali condizioni di operatività aziendale e di chiusura formale dell'incidente. Un obiettivo determinante che emerge dalla corretta applicazione delle misure qui contemplate, è garantire che per i dati e per i sistemi/applicazioni siano ristabilite le funzionalità e performance in essere prima dell'incidente.

- Data Domain DD4200
- Data Domain DD4100
- Data Domain DD2500
- Software di backup NetBackup di Symantec
- Software di backup vRanger di DELL
- Software di backup con modulo di cifratura dei dati
- Rete di backup con throughput a 10 Gbit/s
- Replica dei dati di backup tramite link a 400 Mbit/s fra sito primario e secondario

La funzionalità di backup sulla base dati è implementata utilizzando Oracle RMAN o BARMAN, con cadenza giornaliera e settimanale a seconda delle necessità.

[Torna al sommario](#)

#### 8.1.4.2 Siti di Bologna e Acilia (Roma)

L'architettura di backup si basa sul software open-source bacula, costituito da un modulo director che sovrintende le operazioni di backup, su due unità dischi SATA (una con dischi fissi e una con dischi rimovibili) collegate a server di backup su cui gira il modulo storage di bacula, e su una serie di moduli client (agenti) di bacula disposti sulle macchine contenenti i dati di cui effettuare il backup.

Le categorie di dati oggetto del backup sono:

- Directory di sistema dei sistemi Unimatica
- DB Postgres[nella modalità export DB]

Nell'ambito del backup dei dati appartenenti alla categoria Directory di sistema, è eseguito anche il backup delle cartelle di rete utilizzate dal personale Unimatica.

Il backup avviene in due modalità:

- diretto: i dati vengono backuppati direttamente sul server che li contiene tramite un agente bacula
- indiretto: i dati vengono backuppati su NAS da uno script di backup che gira sul server da backuppare, e dal NAS vengono poi prelevati da un agente bacula che li inserisce nel flusso dei backup diretti

Le modalità di backup sono riassumibili in estrema sintesi nei seguenti punti:

- i dati di backup sono conservati per 7 giorni su Dischi, i backup full eseguiti ogni fine settimana sono conservati per 1 mese su dischi;
- vengono eseguiti backup mensili su dischi rimovibili, in singola copia, conservati in cassaforte ignifuga, con retention di un anno;
- l'ultimo backup mensile su disco di ogni anno viene conservato con ritenzione infinita;
- backup su disco di dati con esigenze di retention specifiche (superiori all'anno), sono eseguiti in doppia copia, in base a specifiche degli "owner" dei dati;
- il salvataggio dei documenti su CD-ROM con consegna al Soggetto produttore, può essere eseguito su richiesta;
- il salvataggio dell'applicazione sia server che client è realizzato su supporto fisico esterno (Data tape o CD-ROM) per eseguire una rapida reinstallazione in caso di necessità;
- i supporti di backup hanno rotazione con frequenza settimanale.

Per le attività di salvataggio si eseguono i seguenti controlli:

- monitoraggio e controllo dei log-files dei risultati dei salvataggi (con frequenza quotidiana);
- ripristino periodico a campione dei dati;
- controllo della validità e della funzionalità (leggibilità) dei supporti.

[Torna al sommario](#)

### 8.1.4.3 Disaster Recovery

I servizi di conservazione di Unimatica sono erogati tramite due Data Center Primari due Data Center Secondari che svolgono il compito di Backup Remoto e di Disaster Recovery (D/R), al fine di garantire gli opportuni livelli di continuità del servizio.

I Data Center hanno una distanza fra loro superiore 200 e 300 Km e la disponibilità di servizio è H24 per tutti e 4.

I Data Center secondari permettono di usufruire dei servizi in Produzione anche in caso di indisponibilità dei Data Center Primari.

Per questo servizio Unimatica definisce con il Cliente il livello dei parametri che caratterizzano il servizio di D/R e di continuità operativa.

- Recovery Point Objective (RPO)

Rappresenta il massimo tempo che intercorre tra la produzione di un dato sui siti primari e la sua messa in sicurezza (ad esempio attraverso backup) e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di disastro e che devono essere successivamente ripresi.

- Recovery Time Objective (RTO)

È il tempo necessario per il pieno recupero dell'operatività di un sistema e del relativo processo organizzativo.

[Torna al sommario](#)

## 8.1.5 Gestione dei supporti di memorizzazione

La gestione dei supporti di memorizzazione, ove richiesti, segue i seguenti criteri:

- i media di memorizzazione elettronica sono correttamente etichettati in modo da fornire le seguenti informazioni: tipologia del media, tecnica della scrittura, data della scrittura, contenuto. Per tecnica della scrittura si intende il formato in cui il media è stato preparato, nel nostro caso formato ISO, dipendentemente dal tipo supporto (CD o DVD);
- in caso di media che vengano riutilizzati per altri dati, essi vengono preventivamente riformattati tramite le tecniche di formattazione a basso livello, allo scopo di evitare che le informazioni ed i dati in essi contenuti possano essere presi e divulgati a soggetti non autorizzati;
- nel caso in cui i dati registrati sui media non più utilizzati non possano essere definitivamente cancellati si procede alla distruzione del media stesso, impedendone quindi il riutilizzo;
- i media sui quali sono eseguiti i salvataggi aziendali sono conservati in una sede differente rispetto a quella dove sono le strumentazioni cui i salvataggi si riferiscono ed in un luogo non accessibile se non al personale autorizzato,
- periodicamente è eseguita una verifica dei media e della disponibilità degli strumenti di accesso ai medesimi. In caso che per qualche media sia verificata la non disponibilità (anche prevista nel breve futuro) degli strumenti di accesso, si procede allo svecchiamento dei media tramite riversamento del loro contenuto in altro media.

[Torna al sommario](#)

## 8.2. Procedure di evoluzione e Change management

I cambiamenti che vengono apportati al sistema di conservazione di Unimatica risultano essere il prodotto di un'adeguata 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.

La descrizione delle procedure di evoluzione e gestione dei cambiamenti è riportata nel paragrafo 3.2.2 del documento "Piano della sicurezza del sistema di conservazione".

[Torna al sommario](#)

## 8.3. Cessazione del Servizio di conservazione

Il servizio di Conservazione digitale a norma è, dal 2005, uno dei principali asset di Unimatica e gli obiettivi della Direzione per gli anni futuri sono di continuare ad evolvere il sistema ed il servizio di conservazione per mantenerlo adeguato alla tecnologia ed alla normativa e di espandere sempre più nel mercato target, non solo italiano, la penetrazione dell'azienda.

A fronte dei suddetti obiettivi, è stata comunque stabilita una procedura per definire le modalità secondo le quali dovrà essere gestito l'evento, ad oggi non prevedibile, di cessazione del servizio di Conservazione da parte di Unimatica

La gestione della cessazione del Servizio di Conservazione, in fase iniziale, è in carico alla Direzione la quale stabilisce un tempo di almeno 10 mesi prima della data di attuazione prevista.

Dal momento della comunicazione, la Direzione, supportata in questo dal Responsabile del servizio di conservazione, provvede a far sì che non vengano stipulati nuovi contratti, in vista della cessazione del servizio.

Alla ricezione della comunicazione suddetta il Responsabile del servizio di conservazione coinvolge i Responsabili delle diverse aree inerenti alla Conservazione (Sicurezza, Servizio, Archivistica, Sviluppo) con i quali deve collaborare strettamente per la gestione della cessazione e la relativa pianificazione delle attività.

La procedura e le attività che verranno eventualmente eseguite sono descritte nel dettaglio all'interno del documento PRO\_CONS - Piano di Cessazione, qualora venga richiesto, tale procedura viene resa disponibile fornendola al soggetto produttore interessato.

[Torna al sommario](#)

## 9. Monitoraggio e controlli

L'attività di monitoraggio e controllo viene portata avanti dal Responsabile della sicurezza dei sistemi e dal Responsabile della funzione archivistica, in accordo con il Responsabile del sistema di conservazione. Tale attività è finalizzata alla rilevazione di eventi di sicurezza, identificabili come stati che indicano il mancato rispetto delle politiche di sicurezza, che possano costituire una possibile fonte di rischio per il sistema di conservazione. Nello specifico gli obiettivi delle attività di monitoraggio sono la valutazione del livello del rischio associato agli eventi di sicurezza e la gestione di tali eventi, mediante strumenti come i Report dei controlli, agendo per il contenimento e/o eliminazione delle cause.

Gli eventi di sicurezza sono monitorati tramite il sistema di Log che consente la registrazione degli accessi e degli eventi (operazioni). Il sistema di Log è organizzato per registrare eventi ai vari livelli di astrazione della piattaforma:

- log del sistema operativo (incluso file system) atto ad identificare ingressi, anomalie ed errori;
- log del Data Base atti ad identificare ingressi, anomalie ed errori;
- log dei sistemi di rete (firewall e router) atti ad identificare ingressi, anomalie ed errori;
- log delle applicazioni software utilizzate (realizzati con vista a livello di singolo utente) atti ad identificare ingressi, principali attività svolte dagli utenti, sequenze del processo, accessi ai dati.

I log file degli applicativi contengono almeno le seguenti informazioni:

- utente che ha eseguito l'operazione;
- data e ora dell'operazione;
- operazione eseguita.

I file di log non sono modificabili o eliminabili da parte degli Utenti che usano il sistema (che non dispongono dei diritti di accesso).

I log di sistema sono analizzati da parte dei sistemisti qualora si rendesse necessaria un'indagine a seguito di un malfunzionamento del sistema.

La dettagliata descrizione dei processi relativi alle attività di monitoraggio e controlli è riportata nel documento "Piano della sicurezza del sistema di conservazione", capitolo 3 e nella PRO\_CONS - Procedure di conservazione.

I log vengono successivamente inviati in conservazione per mantenere traccia delle comunicazioni tra Soggetto produttore e sistema di conservazione.

[Torna al sommario](#)

### 9.1 Audit interni e Verifica dell'integrità degli archivi

Le verifiche ispettive interne vengono pianificate dal Responsabile del sistema di gestione per la sicurezza delle informazioni e dal Responsabile della qualità in accordo con il Responsabile sviluppo e manutenzione del sistema di conservazione, dal Responsabile sicurezza dei sistemi per la conservazione e dal Responsabile del servizio di conservazione tenendo conto dello stato e dell'importanza dei processi e delle aree oggetto di verifica, nonché dei risultati delle precedenti verifiche. La frequenza con la quale vengono disposte le verifiche ispettive interne è almeno annuale. Unimatica si rende disponibile qualora un soggetto produttore volesse richiedere audit di terza parte. La scelta del personale verificatore viene fatta in modo da garantire obiettività ed imparzialità nel processo di verifica.

Unimatica prevede in allegato al Manuale “Elenco delle modifiche apportate al Manuale della conservazione e dei documenti obsoleti” tenente traccia delle seguenti informazioni:

- registro delle modifiche al Manuale del sistema di conservazione
- registro dei documenti distrutti

[Torna al sommario](#)

## 9.2 Reportistica di servizio

Il sistema di conservazione UniStorage gestisce un sistema di tracciatura nel quale vengono registrati tutti i singoli eventi che riguardano sia la gestione dei Pacchetti, dalla fase di versamento a quella di distribuzione, sia i singoli documenti. Questa tracciatura, costruita per implementare un “forensic log”, è in un formato rigido e non disabilitabile. La tracciatura è prerequisito indispensabile per l’esecuzione delle operazioni.

Nel dettaglio, il sistema di log prevede la registrazione di informazioni relative alle diverse funzioni del processo di conservazione per tutte le fasi descritte nel capitolo 7 “Il processo di erogazione del servizio di conservazione”.

La reportistica di servizio che Unimatica gestisce è di due Tipologie:

1. Reportistica relativa al processo di Conservazione,
2. Reportistica del servizio di Supporto Utente (Service Desk e AM Settore conservazione e Settore sistemi).

### Tipologia 1:

vengono prodotti periodicamente i seguenti report:

- Report Consuntivo Pacchetti di archiviazione,
- Report Excel che fornisce la lista dei Pacchetti di archiviazione e che comprende questo set Minimo di informazioni:
  1. Ragione Sociale Cliente;
  2. Numero documenti conservati e spazio occupato nel periodo totali e per tipologia di documento;
  3. Numero documenti conservati e spazio occupato totali e per tipologia di documento.

### Tipologia 2:

viene prodotto un report di Servizio che fornirà le seguenti evidenze:

- Numero Incident Segnalati
- Media Tempo di presa in carico Incident
- Media Tempo di chiusura Incident
- Numero Service Request
- Media Tempo di presa in Carico Service Request
- Media Tempo di Chiusura Service Request

[Torna al sommario](#)

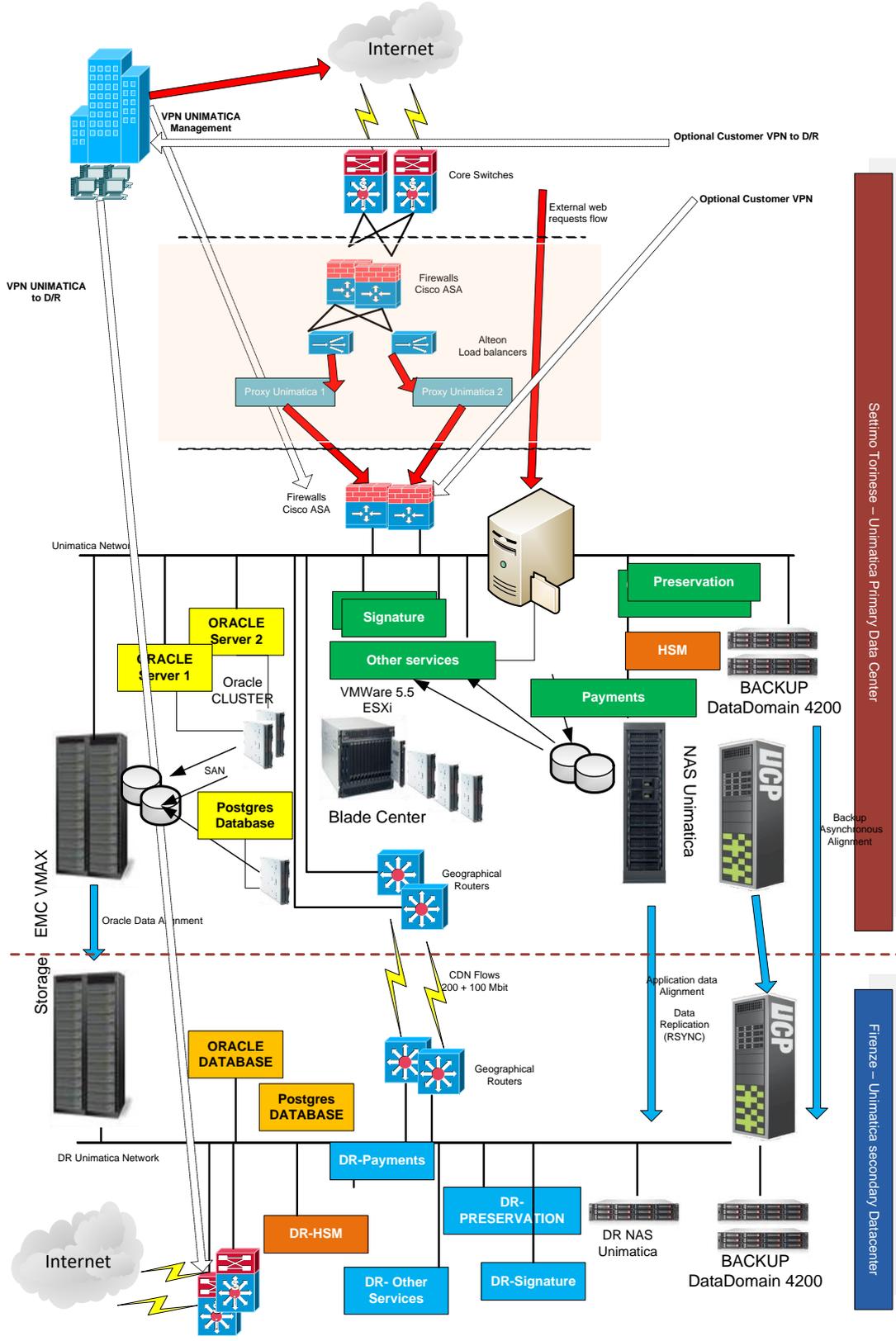
---

## 10. La server farm di Unimatica

---

Dal punto di vista infrastrutturale, i data center dai quali Unimatica eroga i propri servizi consentono di offrire un servizio di alta qualità in termini di continuità e affidabilità. Tale qualità deriva dalle caratteristiche progettuali che hanno contraddistinto la realizzazione dei Data Center, con criteri focalizzati sempre sull'obiettivo di fornire le massime garanzie di sicurezza, disponibilità e continuità, sia per quanto riguarda l'erogazione di energia elettrica, sia attraverso un opportuno condizionamento climatico, sia attraverso un adeguato meccanismo di sicurezza fisica (impianto antincendio e sorveglianza con allarmi 24x7), sia attraverso la ridondanza architetturale dei sistemi, delle infrastrutture di rete e delle connessioni verso l'esterno.

Lo schema seguente rappresenta l'implementazione hardware/software dell'architettura di conservazione presso i siti di Settimo Torinese e Bologna (siti primari), Firenze, e Acilia (Roma) (siti secondari) nei quali sono allocati i data center:



Settimo Torinese – Unimatica Primary Data Center

Firenze – Unimatica secondary Datacenter

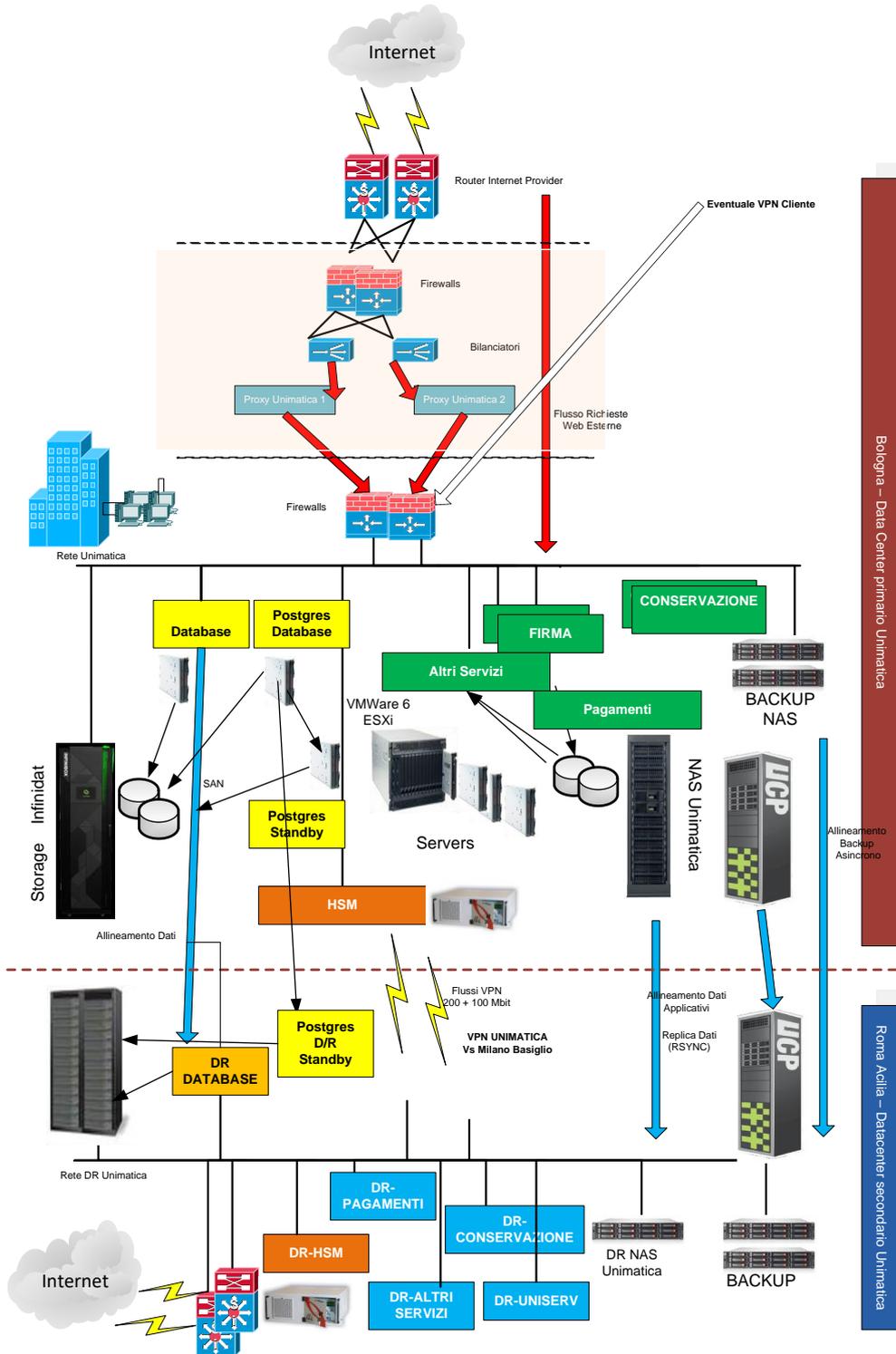


Figura 3 - Architettura di conservazione

[Torna al sommario](#)

## 10.1 UniStorage - Il sistema per la conservazione

Il sistema software utilizzato per la gestione del processo di conservazione dei documenti informatici è costituito dal prodotto applicativo UniStorage.

UniStorage, sviluppato internamente e totalmente da Unimatica, è un sistema integrato e completo per la conservazione dei documenti informatici che viene fornito in modalità Outsourcing/ASP/SaaS congiuntamente a tutti i servizi di gestione e supporto correlati, oppure in modalità pacchetto applicativo, installando le applicazioni presso il Data Center del Soggetto produttore.

I servizi offerti, oltre che di tipo applicativo e tecnologico, comprendono tutto il necessario supporto normativo, organizzativo e contrattuale (deleghe, privacy, ecc.).

UniStorage esegue la conservazione nel tempo dei documenti sottoscritti con firma digitale e le seguenti caratteristiche generali:

- completezza - presenza di qualsiasi documento emesso
- robustezza - garanzia di consistenza dei dati inseriti
- sicurezza - protezione dalla manipolazione non autorizzata dei dati
- affidabilità - indipendenza dai guasti dell'hardware
- chiarezza - facilità di consultazione secondo diversi criteri di ricerca

garantendo:

- la completezza e l'inalterabilità delle registrazioni dei Pacchetti documenti inviati in conservazione
- la possibilità di verifica dell'integrità delle registrazioni
- i riferimenti temporali certi.

Il sistema è progettato per partizionare in maniera opportuna i dati gestiti al fine di garantire la separazione per contesto organizzativo e la consistenza dei dati. Il partizionamento opera tra i dati di Aziende diverse o di diversi dipartimenti o uffici afferenti ad una stessa Azienda (Aree Organizzative Omogenee). I Pacchetti versati provenienti anche da flussi diversi di conservazione, vengono mantenuti separati tramite una chiave primaria che li identifica, fin dal loro ingresso in conservazione, come appartenenti ad una data AOO e non ad un'altra. Il sistema di partizionamento è direttamente collegato al sistema di controllo degli accessi e tracciatura, viene quindi garantita la riservatezza dei dati presenti in archivio.

UniStorage è una applicazione Web a tre livelli (desktop, application e database) e utilizzabile da posti di lavoro dotati di sistema operativo Windows o Linux, per mezzo dei principali browser di riferimento sul mercato. Per le postazioni che dovranno operare sulle funzionalità di firma è necessario che localmente siano attivi i driver del dispositivo di firma (lettore, smart card o token USB di firma, tablet per la firma grafometrica, ecc.), oppure che sia utilizzato un dispositivo HSM (Hardware Security Module) raggiungibile via rete.

Il servizio in outsourcing ASP del servizio di conservazione dei documenti informatici prodotti ed inviati dal Soggetto produttore prevede lo svolgimento da parte di Unimatica, dietro apposita nomina e delega da parte del Soggetto produttore, delle funzioni e responsabilità di conservazione dei documenti.

La descrizione dettagliata delle componenti logiche, tecnologiche e fisiche è riportata nel documento "Infrastruttura" allegato al Manuale del sistema di conservazione.

[Torna al sommario](#)

---

## Appendice A

---

Allegati al Manuale del sistema di conservazione:

- Allegato 'Infrastrutture'.
- PRO\_CONS - Piano di Cessazione

Specificità del contratto e documenti di riferimento:

- Scheda Cliente.
- Flusso per la conservazione dei Documenti in Unistorage
- Specifiche del servizio web per la consegna anticipata di documenti nel Sistema di conservazione.
- 'Funzionalità\_portale'.
- Elenco delle modifiche apportate al Manuale della conservazione e dei documenti obsoleti.

[Torna al sommario](#)