Comune di Romano di Lombardia

Provincia di Bergamo

Manuale di Conservazione

1 Introduzione al documento

1.1 Scopo e campo di applicazione del documento

Il presente documento è il Manuale di Conservazione come previsto dalle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici di Agid Determinazioni 407/2020 e 371/2021, in vigore dal 10 settembre 2020 (di seguito indicate come Linee Guida di Agid) e dal Codice dell'Amministrazione Digitale di cui al D.Lgs 82/2005.

Come richiesto dalle Linee Guida di Agid, il presente documento "deve illustrare dettagliatamente l'Amministrazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione 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".
In caso di ispezione da parte delle autorità di vigilanza preposte, il Manuale di Conservazione permette un agevole svolgimento di tutte le attività di controllo.
L'Amministrazione si avvale del servizio di conservazione erogato dai conservatori Unimatica-RGI, Maggioli e InfoCert.
Il Manuale di Conservazione integra e dettaglia i manuali dei conservatori sopra elencati.

Si rimanda ai manuali Unimatica-RGI, Maggioli e InfoCert per indicazioni dettagliate circa:

- struttura organizzativa e ruoli di responsabilità del Conservatore
- formati e metadati associati agli oggetti conservati
- processo di conservazione e trattazione dei pacchetti di versamento, archiviazione e distribuzione
- dettaglio tecnico del sistema di conservazione
- monitoraggio e controlli effettuati dal Conservatore
- disposizioni in vigore nei luoghi dove sono conservati i documenti

1.2 Principi del Manuale

Il Manuale di Conservazione mira a:

- fornire una chiara presentazione del sistema di conservazione e dei processi erogati
- descrivere l'insieme delle fasi del processo
- includere le informazioni rilevanti, con un livello di dettaglio sufficiente ad agevolare le ispezioni, evitando informazioni tecniche articolate e non necessarie

Il Manuale di Conservazione è adottato dall'Amministrazione con provvedimento formale ed è pubblicato sul sito istituzionale, nella sezione Amministrazione Trasparente.

1.3 Normativa e standard di riferimento, terminologia

I principali riferimenti normativi relativi alla conservazione sono:

- Codice dell'Amministrazione Digitale D.Lgs 82/2005
- Linee Guida sulla formazione, gestione e conservazione dei documenti informatici di Agid, adottate con determinazioni 407/2020 e 371/2021, in vigore dal 10 settembre 2020 e da applicare dal 1° gennaio 2022

Per ulteriori indicazioni e per quanto riguarda la terminologia (glossario e acronimi) e gli standard in uso si rimanda ai Manuali dei Conservatori.

2 Modello organizzativo, ruoli e responsabilità

2.1 Modello organizzativo

Il modello organizzativo adottato è in outsourcing: l'Amministrazione affida il servizio di conservazione a conservatore esterno, ai sensi dall'articolo 34, comma 1-bis del Codice dell'Amministrazione Digitale di cui al D.Lgs 82/2005, fatte salve le competenze del Ministero della cultura, ai sensi del Codice dei beni culturali e del paesaggio D.Lgs 42/2004.

2.2 Amministrazione, Titolare dell'oggetto della conservazione

L'Amministrazione, Comune di Romano di Lombardia, è il Titolare dei documenti e dei fascicoli informatici posti in conservazione e, in relazione al modello organizzativo adottato, affida ai Conservatori: Unimatica-RGI, Maggioli e InfoCert, la gestione del servizio di conservazione secondo quanto previsto dalla normativa in materia e specificato nei contratti di servizio.

Amministrazione: Comune di Romano di Lombardia
Sede: Piazza Giuseppe Longhi 5, 24058 Romano di Lombardia (BG)
Sito web: https://www.comune.romano.bg.it/
Codice fiscale: 00622580165

2.3 Responsabile della conservazione

Il Responsabile della conservazione opera secondo quanto previsto dall'articolo 44, comma 1-quater, del Codice dell'Amministrazione Digitale di cui D.Lgs 82/2005.
Il Responsabile della conservazione:

- è un ruolo previsto dall'organigramma del Titolare dell'oggetto di conservazione
- è un dirigente o un funzionario interno formalmente designato e in possesso di idonee competenze giuridiche, informatiche e archivistiche
- può essere svolto dal responsabile della gestione documentale

Il Responsabile della conservazione dell'Amministrazione definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità e autonomia, in relazione al modello organizzativo adottato.
Il Responsabile della conservazione è persona fisica inserita stabilmente nell'organico dell'Amministrazione titolare dell'oggetto della conservazione; la normativa gli attribuisce compiti riguardanti le funzioni, gli adempimenti, le attività e le responsabilità del processo di conservazione. L'obiettivo principale del Responsabile della conservazione è definire e impostare le modalità di trattamento della documentazione soggetta a conservazione.
Le Linee guida di Agid enfatizzano il ruolo del Responsabile della conservazione che diviene fondamentale all'interno del processo di conservazione, insieme ai suoi delegati o ai terzi affidatari.
Le attività in capo al Responsabile della conservazione sono demandate ai Responsabili del servizio di conservazione dei Conservatori, rimanendo in ogni caso inteso che la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile, rimane in capo al Responsabile della conservazione dell'Amministrazione.
Il Responsabile della conservazione provvede a predisporre il manuale di conservazione e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Le attività attribuite dalle Linee guida di Agid al Responsabile della conservazione (gestite direttamente o tramite i Responsabili del servizio di conservazione dei Conservatori, secondo le specifiche definite nei manuali di conservazione dei relativi Conservatori) sono:

- definire le politiche di conservazione ed 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 e aggregazioni informatiche), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato
- gestire il processo di conservazione e garantire nel tempo la conformità alla normativa vigente
- generare il rapporto di versamento
- generare e sottoscrivere il pacchetto di distribuzione con firma digitale o firma elettronica qualificata (Responsabile del servizio di conservazione del Conservatore)
- effettuare il monitoraggio della corretta funzionalità del sistema di conservazione
- 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
- 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
- provvedere alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico
- predisporre le misure necessarie per la sicurezza fisica e logica del sistema di conservazione
- assicurare 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
- assicurare agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza.

Responsabile della conservazione: Alcaini Sonia
Amministrazione: Comune di Romano di Lombardia
Atto di nomina: deliberazione della Giunta Comunale n. 78 del 9 giugno 2022, esecutiva ai sensi di legge
Data inizio incarico: 9 giugno 2022

Il Responsabile della conservazione, sotto la propria responsabilità, può delegare lo svolgimento delle proprie attività o parte di esse a uno o più soggetti, che all'interno dell'Amministrazione, abbiano specifiche competenze ed esperienze.

Con il presente atto, vengono delegati:
- *Raffaele Cotugno*

Amministrazione: Comune di Romano di Lombardia
Riferimento Tecnico: supporta nelle attività legate al versamento in conservazione e si interfaccia con il conservatore Maggioli relativamente agli aspetti tecnici

- *Elena Vezzoli*

Amministrazione: Comune di Romano di Lombardia
Riferimento Tecnico: supporta nelle attività legate al versamento in conservazione e si interfaccia con il conservatore Unimatica relativamente agli aspetti tecnici

- *Roberto Casiraghi*

Amministrazione: Comune di Romano di Lombardia
Riferimento Tecnico: supporta nelle attività legate al versamento in conservazione e si interfaccia con il conservatore Infocert relativamente agli aspetti tecnici

2.4 Conservatore
Il Comune di Romano di Lombardia, avvalendosi di quanto previsto dal Codice dell'Amministrazione Digitale di cui al D.Lgs 82/2005 e dalle Linee guida di Agid, ha affidato lo svolgimento delle attività di conservazione a:

Unimatica-RGI
Denominazione sociale UNIMATICA-RGI spa
Sede legale e operativa Via Cristoforo Colombo 21, 40131 Bologna
Sito web https://www.unimaticaspa.it/
Pec posta.certificata.unimatica@actaliscertymail.it
Codice Fiscale 02098391200
Numero REA 413696

Maggioli
Denominazione sociale Maggioli SpA
Sede legale via del Carpino 8, 47822 Santarcangelo di Romagna (RN)
Sito web https://www.maggioli.com/it-it
Pec segreteria@maggioli.legalmail.it
Codice Fiscale 06188330150
Numero REA 219107

InfoCert
Denominazione sociale InfoCert SpA, Società soggetta alla direzione e coordinamento di Tinexta SpA
Sede legale piazza Sallustio 9, 00187 Roma
Sito web https://infocert.digital/it/
Pec infocert@legalmail.it
Codice Fiscale 07945211006
Numero REA 1064345

Gli obiettivi dei conservatori tramite il servizio di conservazione sono:

- garantire conservazione, archiviazione e gestione dei documenti informatici e dei fascicoli informatici
- erogare servizio di accesso basato sui contenuti digitali conservati
- fornire supporto, formazione e consulenza al Titolare dell'oggetto di conservazione per i processi di dematerializzazione

Unimatica-RGI, Maggioli e InfoCert assumono l'incarico di svolgere le attività affidate dal Responsabile della conservazione dell'Amministrazione, in accordo con quanto previsto dal contratto, dagli allegati tecnici contrattuali e dalle disposizioni delle Linee guida di Agid.
I Conservatori esterni provvedono ad attribuire lo svolgimento delle attività al relativo Responsabile del servizio della conservazione e questo, eventualmente in funzione della propria organizzazione, a più persone che, per competenza ed esperienza, garantiscano la corretta esecuzione dei processi di conservazione definiti dalle norme, dal contratto e dal proprio manuale. Per il dettaglio delle figure di responsabilità interne ai Conservatori si rimanda ai relativi manuali dei sistemi di conservazione.
Gli estremi identificativi dei responsabili del servizio di conservazione dei Conservatori esterni sono riportati anche nelle informazioni associate ai documenti conservati.
L'affidamento dello svolgimento delle attività del Responsabile della conservazione è stato conferito da Comune di Romano di Lombardia a Unimatica-RGI, Maggioli e InfoCert alla sottoscrizione del contratto di adesione al servizio di conservazione.

2.5 Produttore dei pacchetti di versamento

Il Responsabile della gestione documentale svolge il ruolo di Produttore dei pacchetti di versamento e provvede a trasmettere i pacchetti al sistema di conservazione dei Conservatori Unimatica-RGI, Maggioli e InfoCert. Per pacchetto di versamento si intende: 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 e che viene inviato dal Produttore al sistema di conservazione.
Il Comune di Romano di Lombardia, per il tramite delle applicazioni informatiche in uso (Halley, Concilia, Winedil ed Impresainungiorno), provvede a:

- generare e trasmettere al sistema di conservazione i pacchetti di versamento nelle modalità e con i formati concordati con i Conservatori e descritti nei manuali dei Conservatori
- verificare il buon esito della operazione di trasferimento al sistema di conservazione tramite la presa visione del rapporto di versamento prodotto dal sistema di conservazione stesso.

2.6 Utente

L'utente è il soggetto che può richiedere al sistema di conservazione l'accesso per acquisire le informazioni di interesse nei limiti previsti dalla legge. Tali informazioni vengono fornite dal sistema di conservazione secondo le modalità definite nei manuali dei Conservatori.
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.
Per pacchetto di distribuzione si intende: 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 e che è inviato dal sistema di conservazione all'utente in risposta a una sua richiesta di accesso a oggetti di conservazione.
Il Responsabile della conservazione è identificato come Utente del sistema di conservazione. L'Amministrazione ha attribuito il ruolo di Utente agli ulteriori operatori a tal fine abilitati (operatori indicati al precedente paragrafo 2.3 quali delegati).
L'abilitazione e l'autenticazione degli utenti avviene in base alle procedure di gestione utenze indicate nel Piano della sicurezza del sistema di conservazione e nel rispetto delle misure di sicurezza previste dal Codice in materia di protezione dei dati personali D.Lgs 196/2003 e successive modificazioni ed integrazioni.

3 Formazione e gestione dei documenti e dei fascicoli informatici

3.1 Formazione e gestione dei documenti e dei fascicoli informatici da conservare

Il Comune di Romano di Lombardia forma e gestisce i documenti e i fascicoli informatici seguendo le disposizioni del Codice dell'Amministrazione Digitale di cui al D.Lgs 82/2005 e delle Linee guida di Agid, utilizzando gli strumenti informatici a disposizione.

3.2 Controlli

Il Comune di Romano di Lombardia assicura che i documenti inviati in conservazione siano statici e non modificabili, in modo tale che il contenuto non possa essere alterabile durante le fasi di conservazione e accesso e siano quindi immutabili nel tempo.

3.3 Gestione delle anomalie

I sistemi di conservazione dei Conservatori esterni sono configurati per accettare documenti in formati prestabiliti e con metadati definiti. Al venir meno di una di queste condizioni, sopraggiungendo l'impossibilità di accettare il documento, i sistemi lasciano in attesa il documento in entrata senza immetterlo nel sistema di conservazione.
Il trattamento delle anomalie avviene mediante l'utilizzo di un'interfaccia disponibile e accessibile alle risorse preposte al monitoraggio degli invii in conservazione.

3.4 Formato dei documenti informatici

Il Comune di Romano di Lombardia utilizza per formare i documenti destinati alla conservazione i formati idonei per la conservazione a lungo termine (DPCM 3/12/2013 Regole tecniche per il protocollo informatico, Allegato 2 Formati sino al 1° gennaio 2022 e successivamente Linee guida di Agid, Allegato 2 Formati di file e riversamento) e definiti nei manuali dei Conservatori.

3.5 Metadati dei documenti informatici

Il Comune di Romano di Lombardia associa ai documenti i metadati previsti per il Documento amministrativo informatico (DPCM 3/12/2013 Regole tecniche per il protocollo informatico, Allegato 5 Metadati sino al 1° gennaio 2022 e successivamente Linee guida di Agid, Allegato 5 I metadati) e descritti nei manuali dei Conservatori.
Eventuali ulteriori metadati aggiuntivi, sono individuati e specificati nei documenti contrattuali di Unimatica-RGI, Maggioli e InfoCert, allegati tecnici parte integrante e sostanziale del contratto per l'affidamento del servizio di conservazione digitale di documenti informatici, che dettagliano le caratteristiche delle tipologie di documenti conservati dall'Amministrazione.

3.6 Metadati dei fascicoli informatici

Il Comune di Romano di Lombardia associa ai fascicoli i metadati previsti per le Aggregazioni documentali informatiche (DPCM 3/12/2013 Regole tecniche per il protocollo informatico, Allegato 5 Metadati sino al 1° gennaio 2022 e successivamente Linee guida di Agid, Allegato 5 I metadati) e descritti nei manuali dei Conservatori.

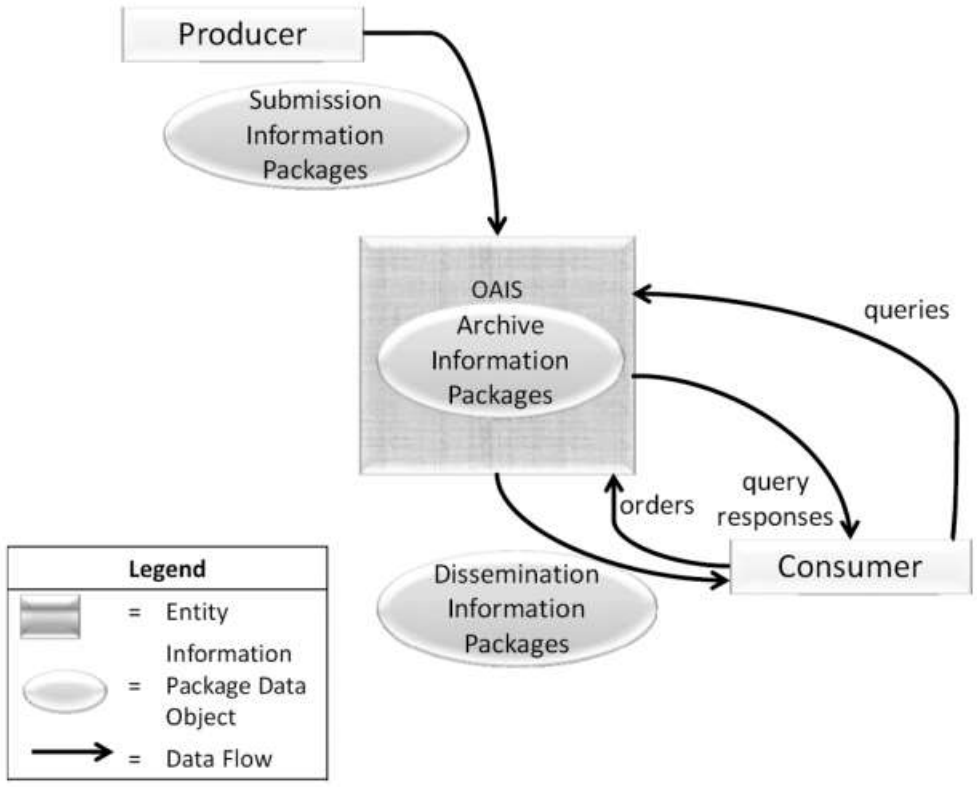
4 Sistema di conservazione in uso

4.1 Sistema di conservazione di Unimatica-RGI

Il sistema software utilizzato per la gestione del processo di conservazione dei documenti informatici è costituito dal prodotto applicativo UniStorage. UniStorage 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.
Il sistema esegue la conservazione nel tempo dei documenti sottoscritti con firma digitale e possiede 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 di documenti inviati in conservazione
  - la possibilità di verifica dell'integrità delle registrazioni
  - i riferimenti temporali certi.

Il processo di conservazione adotta il modello standard OAIS – Open Archival Information System 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, il Soggetto conservatore provvederà a creare i pacchetti di distribuzione in una forma tale che venga garantita la corretta visualizzazione



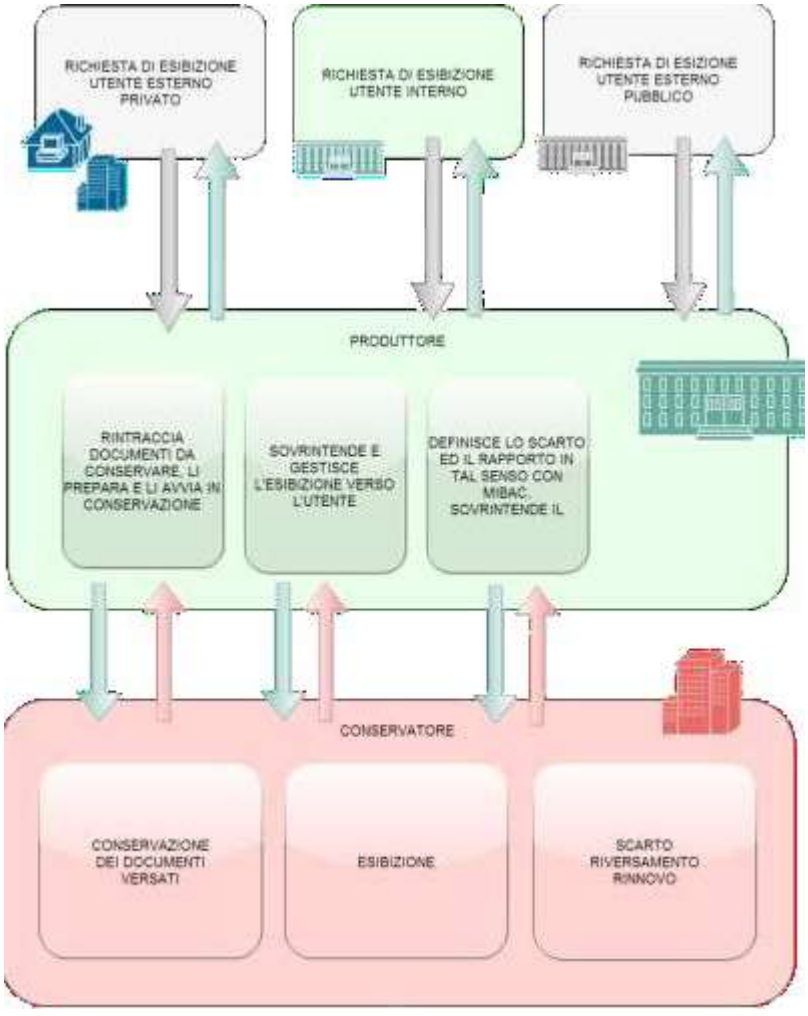
Per quanto concerne audit interni e la verificabilità degli archivi, le verifiche ispettive interne vengono pianificate tenendo conto dello stato e dell'importanza dei processi e delle aree oggetto di verifica, nonché dei risultati delle precedenti verifiche. La frequenza con la quale vengono disposte le verifiche ispettive interne è almeno annuale. La scelta del personale verificatore viene fatta in modo da garantire obiettività e imparzialità nel processo di verifica.
Per informazioni dettagliate e specifiche tecniche si rimanda al manuale di Unimatica-RGI.

4.2 Sistema di conservazione di Maggioli

Il servizio di conservazione di Maggioli permette di mantenere e garantire nel tempo le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità e la validità legale dei documenti informatici, nel rispetto della normativa vigente.
Il sistema di conservazione integra i sistemi e gli strumenti di produzione e gestione documentale in uso presso l'Amministrazione, intervenendo solamente nella fase di conservazione per i documenti che l'Amministrazione sceglie di conservare.
Gli applicativi Concilia di Maggioli per la riscossione delle contravvenzioni al codice della strada e delle sanzioni amministrative sono interfacciati con il sistema di conservazione.
Il versamento in conservazione dei documenti informatici è effettuato unicamente dagli operatori abilitati dall'Amministrazione, utilizzando la modalità messe a disposizioni da Maggioli.

Il processo di conservazione realizzato da Maggioli si articola nei passaggi elencati di seguito:

1. Acquisizione dei pacchetti di versamento per la loro presa in carico
2. Verifiche sui pacchetti di versamento
3. Accettazione dei pacchetti di versamento e generazione del rapporto di versamento
4. Rifiuto dei pacchetti di versamento in caso di anomalie
5. Preparazione e gestione del pacchetto di archiviazione
6. Preparazione e gestione dei pacchetti di distribuzione ai fini dell'esibizione
7. Produzione di duplicati e copie informatiche su richiesta
8. Scarto dei pacchetti di archiviazione relativi a documenti che hanno esaurito la validità giuridica e amministrativa



Tutte le comunicazioni, intese come il trasferimento dei dati da e per il sistema di conservazione, avvengono tramite canale criptato (HTTPS o SFTP).

La funzionalità di verifica di integrità degli archivi permette di verificare l'integrità del documento informatico dal momento della sua conservazione, confrontando l'impronta attuale con quella contenuta nell'Indice di Conservazione. Tale funzionalità viene applicata durante il processo di conservazione subito dopo la fase di memorizzazione nel file system, e risulta poi utile, nell'assolvimento dei requisiti di verifica periodica della leggibilità dei documenti.
La funzionalità è schedulata con cadenza periodica, almeno ogni 5 anni, o più di frequente, in relazione al volume di dati versato dall'Amministrazione. Ogni verifica effettuata genera un report in formato xml che può essere consultato da parte del responsabile del servizio di conservazione per attestare la corretta esecuzione della verifica o per diagnosticare eventuali anomalie.
In aggiunta o congiuntamente a questa verifica sono previste procedure operative "umane" atte a verificare l'effettiva fruibilità dei dati conservati; in concreto il Conservatore può definire un campione di dati da ricercare e di cui simulare un'esibizione, scaricando il relativo pacchetto di distribuzione e procedendo alla verifica del file conservato tramite il viewer a esso associato.
Per informazioni dettagliate e specifiche tecniche si rimanda al manuale di Maggioli.

4.3 Sistema di conservazione di InfoCert

Il sistema di conservazione è implementato da un'applicazione software appositamente sviluppata a tale scopo (applicazione Java in architettura distribuita, ossia costituita da molteplici componenti) e da una serie di servizi di interesse generalizzato condivisi con altre applicazioni (marca temporale, HSM, supporti di conservazione, PEC).
Il sistema è reso in modalità SaaS (Softwareas a Service) e consente al Soggetto Produttore di accedere ai sistemi di conservazione dei documenti informatici su un elaboratore elettronico, gestito da InfoCert e fisicamente posto nei locali di quest'ultima. Il sistema è accessibile dalla apposita URL di rete e il Soggetto Produttore richiama il sistema di conservazione secondo le modalità concordate.
Dal punto di vista architetturale LegalDoc è realizzato utilizzando la tecnologia dei Web Services.
I Web Services di LegalDoc sono implementati secondo architettura REST su protocollo HTTPS.
LegalDoc è dotato anche di un'interfaccia (LegalDoc WEB) utilizzata sia per il versamento manuale di alcune tipologie documentali, sia per la ricerca e l'esibizione a norma di documenti conservati.
L'esibitore è un'applicazione in tecnologia web, che permette a un utente, precedentemente definito e in possesso delle debite autorizzazioni e credenziali, di accedere al sistema di conservazione LegalDoc da un qualsiasi computer, purché collegata in rete.
Per quanto riguarda la verifica degli archivi, il sistema di memorizzazione utilizzato, grazie alle caratteristiche intrinseche dei supporti, alla configurazione architetturale e alle procedure di memorizzazione permanente dei dati, garantisce l'immodificabilità, l'integrità, la leggibilità e la reperibilità nel sistema di quanto conservato, ai fini della corretta esibizione. Il sistema mantiene traccia di tutte le operazioni effettuate sui documenti in appositi file di log.
Per informazioni dettagliate e specifiche tecniche si rimanda al manuale di InfoCert.

5 Documenti conservati

5.1 Tipologie di documenti conservati nel sistema di conservazione di Unimatica-RGI

Il Comune di Romano di Lombardia concorda con Unimatica-RGI le tipologie di documenti da conservare attinenti alle seguenti procedure:

- Atti amministrativi
- Messi notificatori
- Protocollo informatico (sono inclusi gli allegati ai fascicoli informatici; è in fase di attivazione la conservazione anche dei fascicoli informatici)
- Contabilità finanziaria
- Territorio

Le tipologie di documenti gestite dal sistema di conservazione sono elencate nella documentazione tecnica di seguito allegata, distinte per singole procedure.
In allegato vengono altresì elencati i possibili formati dei documenti conservati; per la descrizione e le caratteristiche delle tipologie di documenti conservati si rimanda al Manuale del sistema di conservazione di Unimatica-RGI.
La generazione dei pacchetti di conservazione è automatica

5.2 Tipologie di documenti conservati nel sistema di conservazione di Maggioli

Il Comune di Romano di Lombardia concorda con Maggioli le tipologie di documenti da conservare.
Le tipologie di documenti gestite dal sistema di conservazione sono descritte nel Modulo di affidamento del Servizio di conservazione digitale degli Archivi informatici della Pubblica Amministrazione.

Le tipologie di documenti sono:

- Verbali al Codice della strada notificati a mezzo posta elettronica certificata (Verbale, ricevuta di consegna e relata di notifica);
- Verbali di polizia amministrativa diversi da quelli del Codice della strada (Verbale, ricevuta di consegna e relata di notifica).

I formati ammessi sono: PDF, XML, JPG, JPEG, EML, P7S.

Per la descrizione e le caratteristiche delle tipologie di documenti conservati nel sistema di conservazione di Maggioli si rimanda al Manuale di conservazione.

La generazione dei pacchetti di conservazione è automatica.

5.3 Tipologie di documenti conservati nel sistema di conservazione di InfoCert

Il Comune di Romano di Lombardia concorda con InfoCert le tipologie di documenti da conservare.
Le tipologie di documenti gestite dal sistema di conservazione sono descritte nella documentazione tecnica parte integrante e sostanziale del contratto per l'affidamento del servizio di conservazione.
L'allegato tecnico per ciascuna tipologia di documento conservato definisce formati, metadati, sottoscrizione digitale, frequenza di versamento e software/altre informazioni per la visualizzazione dei documenti.

Le tipologie di documenti sono relative alle pratiche SUE Sportello Unico Edilizia.
Le categorie di archiviazione sono:

- presentazione pratica (sottocategoria Presentazione pratica)
- istruttoria (sottocategorie (sottocategorie Comunicazione R.P., Richieste integrazione, Richieste modifiche progettuali, Pareri, Conferenza servizi, Volture, Comunicazioni)
- provvedimento (sottocategorie Rilascio, Contradditorio, Diniego)

I formati ammessi sono PDF o PDF/A, firme digitali pades e cades.
Per la descrizione e le caratteristiche delle tipologie di documenti conservati nel sistema di conservazione di InfoCert si rimanda al Manuale di conservazione.

La generazione dei pacchetti di conservazione è manuale.

6 Misure di sicurezza

6.1 Misure di sicurezza dell'Amministrazione

Il Comune di Romano di Lombardia provvede alle misure di sicurezza nelle fasi di trattamento, formazione e gestione dei documenti e dei fascicoli informatici definiti come da conservare.
All'interfaccia per la gestione dei documenti inviati in conservazione (dedicata alle operazioni di verifica stato dei documenti, esibizione, ecc.) accedono solo gli utenti individuati dall'Amministrazione e che possiedono i privilegi di accesso.
L'Amministrazione si assicura preventivamente all'invio in conservazione che i documenti siano privi di qualsiasi agente di alterazione, pertanto i documenti da conservare non devono contenere virus, macroistruzioni corrispondenti in comandi interni che, al verificarsi di determinati eventi, possono generare automaticamente modifiche o variazione dei dati contenuti nel documento, né codici eseguibili corrispondenti in istruzioni, non sempre visibili all'operatore, che consentono all'elaboratore di modificare il contenuto del documento informatico.
Il Conservatore declina ogni responsabilità nel caso non sia rispettata la reciproca salvaguardia.

6.2 Misure di sicurezza del sistema di conservazione

I sistemi di conservazione di Unimatica-RGI, Maggioli e InfoCert sono conformi ai requisiti di sicurezza prescritti dalla normativa.
Come previsto dalle norme vigenti in materia, i Conservatori esterni adottano idonee e preventive misure di sicurezza al fine di ridurre al minimo i rischi di:

- distruzione o perdita, anche accidentale, dei documenti informatici
- danneggiamento delle risorse hardware su cui i documenti informatici sono registrati e dei locali ove i medesimi vengono custoditi
- accesso non autorizzato
- trattamenti non consentiti dalla legge o dai regolamenti aziendali

Le misure di sicurezza adottate assicurano:

- l'integrità dei documenti informatici, da intendersi come salvaguardia dell'esattezza dei dati, difesa da manomissioni o modifiche da parte di soggetti non autorizzati
- la disponibilità dei dati e dei documenti informatici da intendersi come la certezza che l'accesso sia sempre possibile quando necessario; indica quindi la garanzia di fruibilità dei documenti informatici, evitando la perdita o la riduzione dei dati anche accidentale utilizzando un sistema di backup
- la riservatezza dei documenti informatici da intendersi come garanzia che le informazioni siano accessibili solo da persone autorizzate e come protezione delle trasmissioni e controllo degli accessi stessi.

Per la descrizione delle misure di sicurezza e delle infrastrutture si rimanda ai manuali dei sistemi di conservazione di Unimatica-RGI, Maggioli e InfoCert.

7 Trattamento dei dati personali

7.1 Misure per la protezione e il trattamento dei dati *Unimatica-RGI*

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-RGI, a partire dalla data di sottoscrizione del contratto, il Soggetto produttore, nella sua qualità di Titolare del trattamento, affida a Unimatica-RGI, 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-RGI deve attenersi:

1. Unimatica-RGI 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

2. I dati trattati da Unimatica-RGI 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-RGI 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-RGI, nella sua qualità di Responsabile del trattamento, in particolare è tenuta a:
   - effettuare tutte le operazioni in termini di mansioni, definendo regole e modelli di comportamento che assicurino la riservatezza e il rispetto del divieto di comunicazione e diffusione dei dati ai quali si ha accesso
   - trattare direttamente, o per il tramite dei propri dipendenti, collaboratori esterni, consulenti, etc. - designati autorizzati al trattamento - i dati personali del Soggetto produttore, Titolare del trattamento, 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, nonché, infine, dalle presenti istruzioni
   - non 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
   - collaborare con il Titolare per garantire la puntuale osservanza e conformità alla normativa in materia di protezione dei dati personali
   - incaricare per iscritto i soggetti che abbiano le caratteristiche di Responsabili di Sistema e di Amministratori di Sistema, tenerne l'elenco aggiornato a disposizione del Soggetto produttore e fornirne eventualmente copia a semplice richiesta dello stesso
   - adottare, se del caso, adeguate misure di sicurezza, in modo da ridurre al minimo i rischi di distruzione e perdita, anche accidentale dei dati/documenti stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta
   - informare immediatamente il Soggetto produttore di qualsiasi richiesta o comunicazione da parte dell'Autorità Garante e/o Giudiziaria, per concordare congiuntamente l'evasione delle stesse
   - collaborare con il Soggetto produttore per l'attuazione delle prescrizioni eventualmente impartite dall'Autorità Garante
   - comunicare al Soggetto produttore qualsiasi accadimento che possa compromettere il corretto trattamento dei dati personali
   - segnalare eventuali criticità al Soggetto produttore che possono mettere a repentaglio la sicurezza dei dati, al fine di consentire idonei interventi da parte dello stesso
   - prestare particolare attenzione all'eventuale trattamento di dati personali rientranti nelle categorie particolari e/o relative a condanne penali o reati degli interessati conosciuti, anche incidentalmente, in esecuzione dell'incarico affidato, procedendo alla loro raccolta e archiviazione 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.

5. 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.

6. Unimatica-RGI, nella sua qualità di Responsabile esterno del trattamento, si impegna a notificare al Soggetto produttore, Titolare del trattamento, senza ingiustificato ritardo dall'avvenuta conoscenza, e comunque entro 24 ore dalla scoperta con comunicazione da inviarsi all'indirizzo PEC del Soggetto produttore, (salvo diversa email indicata) ogni violazione dei dati personali (data breach). Unimatica-RGI si impegna a prestare ogni più ampia assistenza al Soggetto produttore al fine di consentirgli di assolvere agli obblighi di cui agli artt. 32 - 34 del GDPR. Una volta definite le ragioni della violazione, Unimatica-RGI di concerto con il Soggetto produttore e/o altro soggetto da quest'ultimo indicato, si attiverà per implementare nel minor tempo possibile tutte le misure di sicurezza fisiche e/o logiche e/o organizzative atte ad arginare il verificarsi di una nuova violazione della stessa specie di quella verificatasi.

7. In esecuzione degli accordi in essere con il Soggetto produttore, Unimatica-RGI potrà affidare l'esecuzione - parziale o totale - delle relative attività 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, Unimatica-RGI , nella sua qualità di Responsabile esterno del trattamento, provvede personalmente a designare Responsabile 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 Soggetto produttore tramite il seguente link:
https://www.unimaticaspa.it/it/gdpr-elenco-sub-responsabili

8. Unimatica-RGI assicura che nessun dato personale potrà essere trasferito all'esterno dell'Area Economica Europea (EEA).

9. 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-RGI si rende disponibile a collaborare con il Soggetto produttore stesso fornendogli tutte le informazioni necessarie a soddisfare le eventuali richieste ricevute in tal senso.

10. Unimatica-RGI – 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.

11. Unimatica-RGI 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.

12. L'autorizzazione al trattamento dei dati personali avrà la medesima validità ed efficacia della durata della conservazione legale dei documenti, stabilita dalla normativa.

Per i dettagli, occorre fare riferimento a quanto pattuito nel contratto/ordine/accordo.

7.2 Misure per la protezione e il trattamento dei dati personali Maggioli

I dati personali gestiti nell'esecuzione del servizio sono sempre:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato
- raccolti per le sole finalità previste per l'erogazione del Servizio e successivamente eliminati in modo da non entrare in contrasto non con tali finalità (nessun un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici)
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati")
- esatti e, se necessario, tempestivamente aggiornati ("esattezza")
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal GDPR a tutela dei diritti e delle libertà dell'interessato ("limitazione della conservazione")
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali ("integrità e riservatezza"). Rispetto ai diritti dell'interessato dal trattamento dei dati personali, diverso dal Titolare degli elementi (e dei dati) trattati nell'erogazione del Servizio, si ricorda che le pubbliche autorità e gli altri enti che conservano

archivi nel pubblico interesse sono servizi che hanno "l'obbligo legale" di trattare archivi selezionati per la conservazione e la cancellazione di dati personali contenuti in documenti archivistici renderebbe impossibile, per questi organismi, assolvere alla missione istituzionale assegnatagli dalla legge

- il diritto alla cancellazione delineato dall'art. 17 del GDPR non si applica ai documenti selezionati per la conservazione permanente
- il diritto di oblio, così come affermato dalla Corte di giustizia della Unione Europea (cioè non cancellazione, ma deindicizzazione dei dati personali) può essere messo in pratica, senza pregiudicare i reciproci compiti istituzionali, deindicizzando o prevenendo in altro modo la ricerca di nomi all'interno dei documenti da parte dei motori di ricerca, senza mettere a rischio la loro integrità e conservazione
- l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento dei dati personali che lo riguardano, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico (art. 21, c. 6 del GDPR)
- gli Archivi possono impedire la ricerca dei nomi contenuti in un documento pubblicato, mantenendo la possibilità di rintracciarlo utilizzando chiavi di ricerca diverse dai dati personali.

L'informativa privacy completa è resa disponibile sul sito istituzionale di Maggioli spa, all'indirizzo:
https://privacy.maggiolicloud.it/privacy/wwwmaggioli.it

7.3 Misure per la protezione e il trattamento dei dati personali InfoCert

InfoCert S.p.A., in qualità di Titolare del trattamento dei dati forniti dal Produttore/Cliente e di cui quest'ultimo è l'"interessato" ai sensi dell'art. 4, n. 1), del Regolamento UE n. 679/2016 ("Regolamento"), informa lo stesso, ai sensi e per gli effetti di cui all'art. 13 del Regolamento, che i predetti dati personali saranno trattati, con l'ausilio di archivi cartacei e di strumenti informatici idonei a garantire la massima sicurezza e riservatezza, per le finalità e nelle modalità illustrate nell'Informativa "Privacy Policy – Attivazione Servizi InfoCert", nella pagina "Documentazione" presente sul sito: www.infocert.it.

InfoCert, quale soggetto esterno cui il Cliente/Produttore affida il servizio di conservazione, assume il ruolo di responsabile del trattamento dei dati personali di cui il Cliente/Produttore è "titolare del trattamento" ai sensi dell'art. 4, n. 7), del Regolamento. In particolare, il Cliente/Produttore affida ad InfoCert l'esecuzione delle seguenti operazioni di trattamento, da effettuarsi con l'ausilio di strumenti elettronici e negli specifici limiti previsti dalle Linee Guida e dal Contratto: raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, selezione, estrazione, interconnessione, comunicazione, cancellazione e (eventuale) distruzione di dati.

Il Cliente/Produttore, pertanto, garantisce di fondare il trattamento dei suddetti dati personali (e la relativa delega in favore di InfoCert) su idonea base giuridica, ai sensi dell'art. 6 del Regolamento (UE) 679/2016, presentandosi quali autonomo titolare del trattamento (il "Titolare del trattamento"). Il Titolare del trattamento, pertanto, nomina InfoCert quale responsabile del trattamento dei dati (il "Responsabile"), assumendo tutti gli obblighi e le responsabilità connesse e manlevando InfoCert da ogni pretesa eventualmente proveniente da terzi in riferimento alle operazioni di trattamento messe in atto da InfoCert in virtù dell'incarico conferitole.

La natura stessa del Servizio implica che le uniche istruzioni che il Responsabile riceverà saranno quelle previste dal Contratto, dai suoi Allegati e dalla normativa in materia di conservazione dei documenti informatici.

Alla luce di quanto sopra, InfoCert si impegna a:

- adottare le misure di sicurezza previste dalla normativa applicabile, ivi comprese quelle di cui all'art. 32 del Regolamento (UE) 679/2016
- rispettare gli obblighi posti in capo al responsabile del trattamento dall'art. 28 del Regolamento (UE) 679/2016
- assistere il Titolare del trattamento nell'adempimento degli obblighi derivanti dal Regolamento (UE) 679/2016, nei limiti degli impegni assunti ai sensi del Contratto, al fine di garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del Regolamento (UE) 2016/679, tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile
- con particolare riferimento agli obblighi in materia di notificazione dei dati personali ex artt. 33 e 34 del Regolamento, informare il Titolare del trattamento della eventuale violazione di dati personali senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione stessa
- delegare singole operazioni di trattamento a eventuali società terze, debitamente designate per iscritto quali sub-responsabili del trattamento e istruite in modo da assumere i medesimi obblighi assunti da InfoCert in virtù della presente nomina rispetto alla tutela dei dati personali
- incaricare per iscritto le persone che tratteranno dati personali per conto del Cliente/Produttore, autorizzando le stesse allo svolgimento delle sole operazioni di trattamento strettamente necessarie

alla corretta erogazione del Servizio, con impegno alla riservatezza e indicazione di ogni istruzione necessaria all'esecuzione di un trattamento conforme al D.L.vo 196/2003 e al Regolamento (EU) 679/2016

- dar seguito a richieste o provvedimenti del Garante per la protezione dei dati personali o altra autorità competete in relazione al trattamento dei dati cui InfoCert è preposta
- effettuare le operazioni di cancellazione dei dati, quando richieste dal Cliente/Produttore nel corso dell'efficacia del Contratto e nei termini stabiliti nel Contratto
- cancellare e/o restituire - a scelta del Titolare del trattamento - i dati oggetto di trattamento alla cessazione del Contratto, salvi gli obblighi di conservazione dei dati personali eventualmente derivanti dal diritto dell'Unione o degli Stati membri
- non comunicare a terzi i dati personali oggetto di trattamento.

Nel caso in cui il Cliente manifesti per iscritto necessità tali da richiedere un trattamento diverso rispetto a quello di cui al Contratto, previa valutazione relativa alla compliance normativa della richiesta del Cliente, InfoCert informerà per iscritto il Cliente circa la percorribilità della soluzione richiesta e i relativi costi, mediante specifica offerta, eventualmente rivalutando altresì l'inquadramento da conferire al rapporto, anche ai sensi del Regolamento (UE) 2016/679.

Il Cliente/Produttore, in qualità di Titolare del trattamento, prende atto e accetta che il Responsabile InfoCert è autorizzato ad avvalersi di Amazon Web Services, Inc. quale Sub-Responsabile del trattamento per l'espletamento dei Servizi di storage dei dati in cloud. Il Responsabile informa il Titolare che lo storage dei dati in cloud presso Amazon Web Services, Inc. si svolge su server localizzati in Italia.

MANUALE DEL
SERVIZIO DI CONSERVAZIONE DIGITALE
DI MAGGIOLI SPA

Maggioli spa è qualificata AgID per l'erogazione del Servizio di conservazione digitale
a tutte le Organizzazioni pubbliche e private di cui all'art. 2.2 del *CAD* [1]

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

"Pochi sono grandi abbastanza da poter cambiare il corso della storia. Ma ciascuno di noi può cambiare una piccola parte delle cose, e con la somma di tutte quelle azioni verrà scritta la storia di questa generazione." (Robert Francis Kennedy)

Versione: 05	04-03-06-01	Data approvazione: 15/12/2021
Redazione	Fabio Tiralongo	Responsabile Sviluppo e Manutenzione del Servizio
Revisione	Andrea Furiosi	Product Manager
Approvazione	Robert Ridolfi	Direttore, Responsabile

[1] **Gli obblighi di conservazione e di esibizione di documenti** previsti dalla legislazione vigente si intendono soddisfatti a tutti gli effetti di legge a mezzo di documenti informatici, se le procedure utilizzate sono conformi alle regole tecniche dettate ai sensi dell'articolo 71 del C.A.D (Codice per l'Amministrazione Digitale) – "Linee Guida AgID"

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.215.200
interamente versato

Allegati:

- Formati di conservazione v3
- Indici di conservazione (ex-metadati) v5
- Specifiche tecniche v5
- Modulo di Richiesta di Attivazione o Variazione del Servizio di conservazione digitale v6
- Manuale utente per il Servizio di conservazione digitale v3
- Piano di Cessazione del Servizio di conservazione digitale v1
- Privacy policy di Maggioli spa

Registro delle variazioni al Manuale:

Versione	Data emissione	Modifiche apportate	Osservazioni
1.0	01/06/2015	Prima stesura	
1.1	05/06/2015	Verifica della struttura del documento e stralcio delle ridondanze	
1.2	10/07/2015	Integrazioni al Manuale di conservazione	
1.3	14/07/2015	Reintroduzione delle tabelle e degli schemi XSD omessi in prima stesura	Capitolo 6
2	23/06/2016	Rettifica rispetto il regolamento EIDAS e best practice ETSI: §1, 2, 3, 4. §6 limitatamente all'elenco delle tipologie documentali, dei metadati e dei formati ammessi. §7 Eliminate ridondanze sui capitoli precedenti	Porta in evidenza aspetti già previsti dal servizio (in vigore a partire dal 1° agosto 2016)
2.5	06/02/2017	Revisione generale	Si applica a: - Condizioni di fornitura del servizio di conservazione v.2.5 - Specifiche tecniche di erogazione del servizio di conservazione v.2.5
3.1	5/12/2017	Revisione generale (forma); assorbimento del documento recante le specificità del contratto (condizioni di fornitura); maggior dettaglio alle attività preliminari in carico al Cliente §4 e §5 aggiornamento ruoli/figure interne	Si applica a: - Specifiche tecniche di erogazione del servizio di conservazione v.2.5
3.2	16/01/2018	§1 – Mission (maggior dettaglio); §2 – Glossario (aggiornamento); §3 – Normativa (riordino); §4.1.1 – Affidamento (maggior dettaglio); §4.1.5 – Segregazione ruoli (maggior dettaglio); §5.2 – Strutture interne (maggior dettaglio); §5.3 – Gestione fornitori (maggior dettaglio); §8.3.1 – SLA (inserimento della gestione eventi)	Si applica: - Modulo di affidamento del servizio v.5.1
3.3	13/09/2018	§5 – revisione membri operativi coinvolti	
4	16/10/2019	Revisione generale – vedere capitolo 1.1	Incorpora "schemi di referenziazione metadati", le "specificità di contratto" ad integrazione del "modulo di affidamento del servizio" dalla versione 5 in poi e parte delle specifiche tecniche
4.1	07/11/2019	§4.2 gestione file virati	
4.2	02/11/2020	§5.1 aggiornato organigramma (solo definizioni)	Non necessita trasmissione AgID
5	15/12/2021	Adeguamento al nuovo Regolamento AgID e alle LLGG AgID di cui all'art.71 del CAD; espunto ogni riferimento sovrapponibile a quanto reso in altra documentazione o al sito istituzionale di Maggioli spa; revisione degli allegati al manuale	Revisione dell'intera struttura del Manuale, ma senza sostanziali variazioni applicative o procedurali

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.215.200
interamente versato

SOMMARIO P.TE 1 (CARATTERISTICHE GENERALI)

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.215.200
interamente versato

SOMMARIO P.TE 2 (SPECIFICITÀ DEL SERVIZIO)

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405
Capitale sociale:
Euro 2.215.200
interamente versato

1 SCOPO E AMBITO

Questo Manuale (**Accordo di servizio tra Maggioli spa e il Cliente**), approvato, sottoscritto ed adottato dal Cliente (**Soggetto Produttore e Titolare dei dati oggetto del servizio**) all'atto dell'incarico, completo delle specifiche tecniche di versamento e del modulo di attivazione o variazione del servizio, **fa da disciplinare all'esecuzione del Servizio** e **descrive il Sistema di conservazione nelle misure tecnologiche, procedurali ed organizzative disposte da Maggioli spa per l'erogazione delle attività previste dal Servizio** di conservazione digitale a norma AgID[2]. Per ragioni di sicurezza alcune tematiche sono espunte dal presente Manuale e rimandate a Piani o allegati specifici resi disponibili in sede di audit.

Il presente Manuale si applica esclusivamente al Servizio di conservazione digitale a Norma erogato da Maggioli spa: a tal proposito si rimanda all'attenta analisi delle Linee Guida AgID di riferimento che vogliono in **Servizio di conservazione digitale a Norma come Sistema**[3] **e Archivio digitale di deposito**

- **separato** rispetto all'Archivio di gestione corrente (Pratiche in corso di trattazione)
- **diverso** e "anticipato" rispetto all'Archiviazione storica, in quanto "restano esclusi (dal Regolamento AgID) i servizi di conservazione a lungo termine disciplinati dal Codice dei Beni Culturali e le conseguenti attività di vigilanza e sanzionamento

Ciò premesso:

il Soggetto Conservatore (SC, Maggioli spa), attraverso l'applicazione delle Norme e il conseguimento delle certificazioni richieste dal Regolamento AgID di riferimento, assicura il più alto livello possibile di qualità e sicurezza, affinché il Sistema di conservazione (SdC) possa **garantire per quanto conservato il mantenimento delle caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità proprie di ogni Unità Documentale** (UD, Fasciolo o Documento) prodotta dal Cliente;

il Sistema Versante (Cliente) alimenta il Sistema di conservazione secondo quanto definito dal Cliente **nel Suo Manuale di gestione e conservazione documentale**, che descrive tra l'altro le procedure, gli strumenti e le regole che il Cliente applica alla formazione, gestione, raccolta (selezione) e conservazione delle Sue evidenze informatiche, fino alla loro destinazione finale prevista (Scarto o Versamento agli Archivi storici dello Stato);

in questo senso, il Sistema di conservazione digitale opera ed agisce in virtù di un preciso incarico, secondo quanto riportato in questo manuale e **limitatamente nei tempi e per le sole tipologie documentarie oggetto dell'incarico specifico**.

SCOPO: Gli esiti della conservazione digitale a norma sono resi in forma di IdC, PdA e PdD ovvero quanto necessario a dimostrare l'avvenuta e tempestiva conservazione digitale e procedere all'esibizione a norma (es. in sede di contenzioso legale) dei documenti informatici oggetto del Servizio. La conservazione opera per scopi e ambito differenti rispetto ai sistemi di backup o di gestione documentale del Cliente.

L'ambito di applicabilità del Servizio può essere esteso a ogni evidenza informatica che il cliente intende versare nella propria istanza di conservazione (archivio digitale di deposito) attivato nel Sistema di Conservazione di Maggioli spa, purché formata e trasmessa in conservazione come concordato tra Produttore e Conservatore nell'atto di incarico.

torna al sommario

[2] Det. AGID 455/2021 – Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici

[3] Nel testo si differenza "sistema" da "Sistema" (con la maiuscola) come pure "archivio" da "Archivio" per distinguere la "soluzione IT" dalla Soluzione Organizzativa ovvero l'insieme delle disposizioni organizzative (regole, risorse e strumenti) tese ad un obbiettivo specifico e condiviso (v. Manuale di gestione e conservazione documentale del Cliente/Produttore)

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.215.200
interamente versato

1.1 Norme e standard di riferimento

Le norme di primario riferimento per il Servizio sono il CAD e il GDPR, il TUDA (per la PA), il Regolamento eIDAS, le Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici ed il relativo Regolamento per l'erogazione del servizio di conservazione che riporta i requisisti organizzativi, di qualità e sicurezza previsti dall'Agenzia.

Il Conservatore rimanda a queste norme per ogni miglior dettaglio o riferimento non riportato in questo Manuale o nei suoi allegati.

Nota Bene: Ai flussi documentali oggetto di conservazione si applicano anche altre norme, generali e specifiche, esterne al perimetro e al contesto del Servizio di conservazione digitale e che perciò, anche se necessariamente previste e giustamente applicate da Cliente e Produttore, ad esempio in fase di formazione e gestione dei documenti, non trovano spazio in questo Manuale.

Si riportano qui in dettaglio tutte le norme e gli standard tenuti in considerazione (assessment) da Maggioli spa nella definizione e costante adeguamento del Servizio descritto in questo manuale.

torna al sommario

1.1.1 Norme Comunitarie

Titolo	Descrizione
Reg. UE 2014_910	Regolamento eIDAS - electronic IDentification Authentication and Signature
Reg. UE 2016_679	GDPR - General data protection regulation (Regolamento Generale per la protezione dei dati personali)
Reg. UE 2019_424	progettazione dei server e altri sistemi di archiviazione dei dati
LLGG EAG 2018_10	Guida alla protezione dei dati personali per gli archivi. Linee guida del Gruppo Europeo degli Archivi per l'applicazione nel settore archivistico del Regolamento europeo sulla protezione dei dati personali
Reg. UE 2018_1807	Regolamento relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea

torna al sommario

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405
Capitale sociale:
Euro 2.215.200
interamente versato

1.1.2 Norme Nazionali

Rif.	Descrizione
Codice Civile	artt. 2214, 2215, 2220
DL 2004_42	Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137. (GU n.45 del 24-2-2004 - Suppl. Ordinario n. 28)
DPR 2005_68	Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3.
DPCM 3 dicembre 2013	Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del CAD. (14A02098) (GU Serie Generale n.59 del 12-03-2014 - Suppl. Ordinario n. 20)
DPCM 13 novembre 2014	Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del CAD. (15A00107) (GU Serie Generale n.8 del 12-01-2015)
Circ. AgID 2014_65	Regolamento sulle modalità per l'accreditamento e la vigilanza sui soggetti che svolgono attività di conservazione dei documenti informatici
DM-MEF_GU 2014_146	DECRETO Ministeriale (MEF) del 17 giugno 2014: Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005. (14A04778) (GU n.146 del 26-6-2014)
Circ. AgID 2017_02	Misure minime di sicurezza ICT per le pubbliche amministrazioni
Decreto Min. Interni 18 dicembre 2017	Disciplina delle procedure per la notificazione dei verbali di accertamento delle violazioni del codice della strada, tramite posta elettronica certificata. (18A00263) (GU Serie Generale n.12 del 16-01-2018) www.gazzettaufficiale.it/eli/id/2018/01/16/18A00263/sg
Circ. AgID 2018_03	Criteri per la qualificazione di servizi SaaS per il Cloud della PA
Piano_triennale AgID 2019-2021	Il Piano Triennale per l'informatica della Pubblica Amministrazione
LLGG AgID 20_06_2019	Linee Guida per la sottoscrizione elettronica di documenti ai sensi dell'art.20 del CAD
DL 2020_76	Decreto Semplificazioni
DL 2005_82 (v. 2020)	CAD - Codice dell'Amministrazione Digitale
DPCM 17 luglio 2020	Approvazione Piano Triennale per l'informatica nella PA 2020-2022
Piano_triennale AgID 2020-2022	Il Piano Triennale per l'informatica nella Pubblica Amministrazione
DPR 2000_445 (2020)	TUDA - Testo Unico sulla Documentazione Amministrativa
LLGG AgID 06_05_2020	Linee guida per lo sviluppo del software sicuro
LLGG AgID 23_07_2020	Linee Guida sull'Accessibilità degli strumenti informatici
LLGG AgID 18_05_2021	Linee Guida sulla formazione, gestione e conservazione dei documenti informatici
Det. AGID 2021_74	Regolamento recante le modalità per la vigilanza ai sensi dell'art. 14-bis comma 2, lett. i) e per l'esercizio del potere sanzionatorio ai sensi dell'art. 32-bis del CAD
Det. AGID 2021_455	Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici

torna al sommario

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405
Capitale sociale:
Euro 2.215.200
interamente versato

1.1.3 Standard di riferimento

Rif.	Descrizione
ACCREDIA: check list AgID	Conservatore di documenti informatici ai sensi dell'art. 29, comma 1, del D.lgs. 7 marzo 2005, n. 82
ENISA - WP2017 O-2-2-5	Guidelines for SMEs on the security of personal data processing
ETSI EN 319 401	General Policy Requirements for Trust Service Providers (paragrafo 7.12)
ETSI TS 101 533-1	Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni
ETSI TS 119 511	Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques
ETSI TS 119 512	Protocols for trust service providers providing long-term data preservation service
ISAD (G):2000	General International Standard Archival Description, Second Edition, Adopted by the Committee on Descriptive Standards
ISO 14721	OAIS - Reference Model for an Open Archivial Information System
ISO 16363	Space data and information transfer systems - Audit and certification of trustworthy digital repositories
ISO 20000	service management system requirement
ISO 27001:2013	Sistemi di gestione della sicurezza delle informazioni
ISO 9001	sistemi di gestione per la qualità
ISO_IEC 27017:2015	Code of practice for information security controls based on ISO/IEC 27002 for cloud services
ISO_IEC 27018:2014	Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
ISO_TR 18492	Long-term preservation of electronic document-based information
MIBACT - NIERA(EPF) 2014	Norme italiane per l'elaborazione dei record di autorità archivistici di enti, persone, famiglie
OWASP Testing Giude : 2020	La Guida alla verifica di sicurezza di OWASP
UNI 11386	Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (SinCRO)
UNI 37001	Sistema di Gestione per la Prevenzione della Corruzione
UNI EN ISO 22301:2019	Sistemi di gestione per la continuità operativa - Requisiti
UNI EN ISO 22313:2020	Guida all'utilizzo della ISO 22301
UNI ISO 15489-1:2006	Gestione dei documenti di archivio (record) - Principi generali
UNI ISO 31000:2018	Gestione del rischio - Linee guida

torna al sommario

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405
Capitale sociale:
Euro 2.215.200
interamente versato

1.1.4 Certificazioni

Le certificazioni di **Maggioli spa** applicate al Servizio sono:

ISO/IEC:27001 (posseduta), ISO:9001 (posseduta), ISO/IEC:20000-1 (posseduta), ISO:37001 (in via di definizione) e la certificazione di conformità all'art.24 eIDAS per la conservazione dei documenti informatici;

inoltre Maggioli spa adotta il Modello 231/2001, un Piano per la Sicurezza delle informazioni (SGSI), un Piano di cessazione del Servizio, lo standard OAIS ISO:14721 e tutti gli standard indicati nel capitolo corrispondente.

Maggioli spa, già Conservatore accreditato AgID, è iscritta nell'elenco dei Cloud Service Provider per la pubblica amministrazione, CSP da cui è erogato il Servizio di conservazione, già inserito nell'elenco dei Servizi SaaS per la PA del marketplace AgID.

torna al sommario

1.2 Terminologia (glossario e acronimi)

In questo Manuale e nell'erogazione del servizio si utilizzano termini obbligatoriamente noti ai Ruoli coinvolti nelle funzioni interessate dalle attività previste; rimandandone l'elenco completo all'allegato 1 delle LLGG AgID di riferimento, questo capitolo si limita a riportare i termini più ricorrenti in questo testo e le abbreviazioni utilizzate nel proseguo con l'unico fine di agevolarne lettura e comprensione.

Termine	Descrizione
AgID	Agenzia per l'Italia Digitale
autenticazione	un processo elettronico che consente di confermare l'identificazione elettronica di una persona fisica o giuridica, oppure l'origine e l'integrità di dati in forma elettronica
CAD	Codice dell'Amministrazione Digitale di cui al d.Lgs. 7 marzo 2005, n. 82 e s.m.i;
Codice	Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137. (GU n.45 del 24-2-2004 - Suppl. Ordinario n. 28)
documento elettronico	qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva;
documento informatico	un documento elettronico riportante atti o fatti giuridicamente rilevanti
GDPR	Reg. UE 2016_679
IdC	indice di conservazione redatto secondo lo standard UNI 11386 (UNISinCRO)
il Servizio	il Servizio di conservazione digitale erogato da Maggioli spa
Linee Guida	le linee guida applicabili ai sensi dell'articolo 71 del CAD
LLGG	Linee Guida sulla formazione, gestione e conservazione dei documenti informatici
Originalità, Duplicato o copia	copia informatica, bit-a-bit, identica all'originale informatico
PdA	Pacchetto di Archiviazione (contiene elementi conservati e indici di conservazione; per dettaglio vedere specifiche tecniche)
PdD	Pacchetto di Distribuzione - è prodotto su richiesta dal sistema di conservazione: contiene gli elementi conservati selezionati per l'esibizione a norma e i relativi indici di conservazione
PdV	Pacchetto di Versamento - predisposto e trasmesso dal Produttore, contiene gli oggetti da conservate e i metadati/indici di conservazione
Persona	Un qualsiasi soggetto giuridico o persona fisica
Persona Fisica	La persona fisica per l'ordinamento giuridico è qualsiasi essere umano (dalla nascita alla morte), soggetto di diritto: è dotato di capacità giuridica, è titolare di diritti e doveri. Per le finalità del Servizio ogni persona fisica corrisponde ad un Ruolo all'interno di una Organizzazione, AOO, Ufficio o Funzione.

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405
Capitale sociale:
Euro 2.215.200
interamente versato

Termine	Descrizione
Persona Giuridica	ai sensi del TFUE si intendono tutte le entità costituite conformemente al diritto di uno Stato membro o da esso disciplinate, a prescindere dalla loro forma giuridica
Regolamento	Det. AGID 2021_455 - Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici
Regolamento eIDAS	REGOLAMENTO (UE) N. 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
Ruolo	insieme di conoscenze, competenze, responsabilità e possibilità di azione nel conseguimento di un obbiettivo o nell'erogazione di un servizio
Servizio	Erogazione di uno i più Sistemi ad uno o più clienti (istanze o tenant)
SGD	Sistema di gestione documentale (SGD) o Trasmittente che registra, raccoglie e gestisce le Unità Documentali, le trasmette in conservazione e ne cura accesso, scarto e riversamento.
Sistema (IT)	Insieme di regole, infrastrutture IT, risorse e strumenti operanti sinergicamente, nel medesimo ambito e con uno scopo comune
Sistema di conservazione (SdC)	Il sistema che eroga la componente principale del servizio di conservazione digitale
Sistema versante (SdV)	Sistema di gestione documentale (SGD) o Trasmittente che registra, raccoglie e gestisce le Unità Documentali, le trasmette in conservazione e ne cura accesso, scarto e riversamento.
SLOT	Porzione logica di storage, riservata ad un Tenant specifico, la cui dimensione (quantità di dati binari che può contenere) è espressa in GB (Giga-byte) o MB (Mega-byte), dove 1 GB corrisponde a 1000MB
Soggetto	Persona fisica o giuridica
Soggetto Conservatore (SC)	Il Responsabile del Servizio e del sistema di conservazione erogato o gestito per conto del Soggetto Produttore
Soggetto Produttore (SP)	il Titolare Responsabile delle Unità Documentali trasmesse in conservazione
Tenant	o istanza. Rappresenta una porzione logia del Sistema, riservata ad una singola Organizzazione o ad un Titolare/Responsabile. Per il Servizio di conservazione un tenant rappresenta un'unica combinazione di Rapporto (v. incarico o contratto), Organizzazione Titolare (v. cliente) e Sistema Versante (SGD).
Trasferimento	è l'azione di copia bit-a-bit da un sistema all'altro che può o meno comportare la cancellazione della copia originale dal sistema sorgente
Unità Documentale (UD)	o Elemento Documentale. Una qualsiasi evidenza elettronica, opportunamente registrata o classificata, contenete la registrazione o la raccolta atti o fatti giuridicamente rilevanti (Documenti, Fascicoli, Registri, Repertori, Libri, flussi/stream informativi, database, ecc.)
validazione temporale elettronica qualificata	o marcatura temporale. una validazione temporale elettronica che soddisfa i requisiti di cui all'articolo 42 del CAD
Versamento	in conservazione digitale l'azione di versamento consiste nel trasferimento dei dati al sistema di conservazione, senza trasferimento della titolarità dei dati stessi come avviene invece ad esempio con il versamento agli archivi storici

torna al sommario

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.215.200
interamente versato

1.3 Oggetto del servizio (Mission)

Lo scopo del Servizio è, limitatamente ai termini di servizio riportati nell'incarico (quantità, tipologia flussi e tempi) quello di preservare l'efficacia giuridico-probatoria di evidenze informatiche prodotte dal Cliente[4] a dimostrazione di un rapporto/fatto giuridicamente rilevante tra il cliente e una sua controparte ovvero a dimostrazione dell'operato dell'Organizzazione Cliente, proteggendone le informazioni ivi contenute, sia da eventi interni che esterni all'Organizzazione Titolare delle Unità Documentali oggetto del Servizio.

Le **3 fattispecie documentarie**, specificatamente normate da AgID nelle citate Linee Guida sono:

1) **Raccolte di elementi documentali** differenti, aggregati dal Cliente perché afferenti al medesimo obiettivo, procedimento o per finalità giuridica (es. fascicoli, pratiche o altri pacchetti informativi)
2) **Documenti amministrativi informatici,** esito dell'azione amministrativa del Cliente, evidenza di un diritto o di un obbligo giuridico, eventualmente fascicolati, sempre classificati e normalmente iscritti in una specifica serie o registro d'archivio
3) **Documenti informatici** o stream/flussi informativi elettronici, aventi valore giuridico e probatorio per il Cliente, sempre opportunamente classificati, ma non necessariamente fascicolati, numerati o iscritti in un Registro (es. PEC, flussi SIOPE+, FEL, Registri o altre aggregazioni)

torna al sommario

1.4 Destinatari del Servizio

Il Servizio di conservazione è rivolto a tutti i soggetti pubblici e privati ed in particolare:

- Per quanto all'art. 1 del Codice dei beni culturali (**Stato, le regioni, le città metropolitane, le province e i comuni e gli altri soggetti pubblici**, nello svolgimento della loro attività; **i privati** proprietari, possessori o detentori di beni appartenenti al patrimonio culturale)
- **Chiunque**, rispetto all'art. 20 del DL 82/2005 (CAD) sulla validità ed efficacia probatoria dei documenti informatici;
- Agli artt. 2214 e 2220 del Codice Civile (**imprenditori e professionisti**), in merito all'obbligo di conservare ordinatamente e per ciascun affare ogni evidenza documentale giuridicamente rilevante (es. comunicazioni, fatture, ecc.);

e **tutti i Soggetti di cui all'art. 2 comm. 2 e 3 del DL 82/2005 (CAD)**[5] per gli adempimenti previsti dagli articoli

- 53 e 67 del DPR 445/2000 (TUDA), sulla tenuta del Protocollo informatico;
- 43 e 44 del DL 82/2005 (CAD) in merito alla corretta formazione, gestione e conservazione dei documenti informatici, la tenuta delle registrazioni, nonché come elemento imprescindibile al rispetto dei requisiti di tutela e sicurezza delle informazioni, del patrimonio informativo pubblico, delle evidenze circa l'attività amministrativa eseguita e in applicazione ai diritti/doveri di trasparenza, accessibilità e partecipazione di cui allo stesso CAD.

torna al sommario

[4] Per la corretta formazione, registrazione e gestione dei documenti informatici fare riferimento alle LLGG AgID 18_05_2021 e alla normazione specifica di ogni flusso (es. fatturazione elettronica, ordinativi informatici, ecc.)

[5] (comma 2) "**le pubbliche amministrazioni** di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, nel rispetto del riparto di competenza di cui all'articolo 117 della Costituzione, ivi comprese le autorità di sistema portuale, nonché alle autorità amministrative indipendenti di garanzia, vigilanza e regolazione;
i gestori di servizi pubblici, ivi comprese le società quotate, in relazione ai servizi di pubblico interesse;
le società a controllo pubblico, come definite nel decreto legislativo 19 agosto 2016, n. 175, escluse le società quotate di cui all'articolo 2, comma 1, lettera p), del medesimo decreto che non rientrino nella categoria di cui alla lettera b)".
(comma 3) "[…] **le disposizioni del Codice e le relative Linee guida** […] **si applicano anche ai privati**, ove non diversamente previsto".

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405
Capitale sociale:
Euro 2.215.200
interamente versato

1.5 Soggetti coinvolti

Rinviando al capitolo specifico le funzioni, i ruoli e le responsabilità iscritte ad ogni Soggetto, si riportano qui in elenco i diversi Attori coinvolti nel processo di conservazione:

Committente o Stazione appaltante – Può coincidere con il Cliente o essere un intermediario commerciale che definisce per conto del Cliente alcuni dettagli della fornitura (costo e durata) ed eventuali personalizzazioni del Servizio (SLA, limiti alle fattispecie documentarie coinvolte dalla fornitura, modalità di versamento e recupero delle informazioni conservate, ecc.) al fine di normalizzare il servizio stesso rispetto ad un bacino di utenza specifico e predeterminato (es. tipologia di Organizzazione; competenza territoriale o di funzione; Sistemi di gestione integrata, ecc.).

Cliente – è il Titolare delle Unità Documentali oggetto del Servizio e, eccezion fatta per l'Autorità Giudiziaria, **è l'unico Soggetto che, per tramite dei suoi incaricati, è autorizzato ad accedere ai dati conservati**.

Soggetto Produttore (SP) – coincide con il **Tenant** di conservazione. Ogni Tenant corrisponde all'insieme di regole e di flussi documentali che hanno medesima origine (Sistema Versante) e medesimo Titolare (Cliente).

Sistema Versante (SV) – nella PA (Pubblica Amministrazione) è **il Sistema di gestione documentale** (**SGD**)del Cliente, che opera secondo quanto definito dal cliente stesso nel Suo Manuale di gestione e conservazione documentale; nelle Organizzazioni private può essere un Sistema diverso, anche totalmente esternalizzato, che forma i pacchetti di versamento destinati alla conservazione digitale e ne verifica la messa in conservazione. Ogni sistema versante deve comunque poter dimostrare la reale gestione dell'intero iter di conservazione dei flussi (o serie) documentali oggetto dell'incarico, tracciandone l'esito (Rapporti di Versamento prodotti dal Sistema di conservazione) e gestendo eventuali anomalie, rifiuti o altre non conformità rilevate in fase di selezione ed invio in conservazione o come esito del processo di conservazione stesso. Sono escluse dalle funzionalità (minime) specifiche del Sistema Versante, le attività di Riversamento e di verifica periodica dei "lotti conservati", descritte nei capitoli dedicato e di competenza condivisa del Produttore e del Conservatore.

Produttore – è la Persona responsabile (giuridicamente) della formazione e dell'effettivo invio in conservazione delle Unità Documentali destinate alla Conservazione digitale a Norma. Nella PA, questa figura coincide con **il Responsabile della Gestione Documentale** dell'Ente "Soggetto Produttore", Titolare dei dati oggetto del servizio e non può essere mai delegata.

Maggioli spa – è il Conservatore (SC, Soggetto Conservatore) abilitato da AgID ad erogare questo Servizio a tutte le Pubbliche Amministrazioni italiane e naturalmente anche alle Organizzazioni private. Il Servizio di conservazione digitale di Maggioli spa è iscritto tra i Servizi SaaS del Marketplace AgID ed è erogato esclusivamente dai datacenter di Proprietà di Maggioli spa o di sue controllate, collocati su territorio italiano e già iscritti come CSP (cloud service provider) allo stesso marketplace.

AgID – L'Agenzia per l'Italia Digitale è l'agenzia tecnica della Presidenza del Consiglio che ha il compito di garantire la realizzazione degli obiettivi dell'Agenda digitale italiana; l'Agenzia definisce le modalità operative per realizzare l'attività di conservazione; le pubbliche amministrazioni sono tenute a conservare tutti i documenti formati nell'ambito della loro azione amministrativa.

MiBACT –in quanto "Coerentemente con quanto stabilito dal Codice dei beni culturali, il trasferimento a un sistema di conservazione di documenti e aggregazioni documentali informatiche, appartenenti ad archivi pubblici e privati dichiarati di interesse storico particolarmente importante, è assoggettato all'obbligo di cui all'art. 21 del Codice dei Beni Culturali. I documenti informatici e le aggregazioni documentali informatiche possono essere oggetto di selezione e scarto nel sistema di gestione informatica dei documenti nel rispetto della normativa sui beni culturali."

torna al sommario

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.215.200
interamente versato

1.6 Descrizione del Servizio

Il Soggetto Produttore forma, classifica ed eventualmente registra nel proprio Sistema di gestione documentale ogni Unità Documentale destinata alla conservazione digitale a norma, applicando oltre alle norme di riferimento per il procedimento, flusso, documento o atto specifico, anche le disposizioni del CAD e le Linee Guida AgID in materia di formazione, gestione e conservazione dei documenti informatici.

Secondo la relativa classificazione e in base al Piano di conservazione del Cliente, **le Unità Documentali così formate sono raccolte dal Produttore e trasmesse in conservazione** il più tempestivamente possibile e comunque entro un anno dalla loro registrazione o ultima modifica, inclusi i documenti relativi a fascicoli aperti o a procedimenti ancora in corso. Per le PPAA, i registri informatici prodotti (di Protocollo Generale, ma anche dei registri particolari istituiti presso l'Ente, Cliente) sono atti pubblici di fede privilegiata che richiedono, oltre ai già previsti registri annuali, la produzione dell'elenco quotidiano delle registrazioni eseguite da inviare in conservazione digitale entro il giorno lavorativo successivo.

Le Unità Documentali sono tramesse in conservazione **in Pacchetti di Versamento (PdV), accompagnate dagli indici di conservazione previsti per la relativa fattispecie**.

I PdV ammessi in conservazione cono convertiti in PdA (Pacchetti di Archiviazione) e conservati, mentre quelli "non conformi" sono rifiutati e contestualmente eliminati dal Sistema di conservazione.

L'elenco dei formati file (mime-type) ammessi in conservazione digitale è costantemente aggiornato in base alle indicazioni di AgID e secondo le valutazioni del Cliente e del Conservatore. Al fine di evitarne l'obsolescenza tecnologica, i formati previsti per il Servizio sono nel tempo verificati dal Conservatore che provvede ad informare per tempo il Produttore in caso si renda necessario procedere con un riversamento dei dati già conservati in formato non più idoneo. Se il Cliente vuole utilizzare formati diversi da quelli raccomandati, il Produttore trasmette al Conservatore un file di "informazioni di rappresentazione" da associare ad ogni documento da conservare e una manleva rispetto al controllo sull'obsolescenza dei formati e sull'effettiva leggibilità ed intellegibilità dei dati conservati "non accessibili", ad esempio se cifrati.

La mancanza di uno degli indici (metadati) di conservazione previsti o la presenza di file non ritenuti idonei alla conservazione digitale comporta il rifiuto del PdV da parte del conservatore.

L'attività di versamento in conservazione a carico del Produttore si conclude con la gestione degli esiti del processo di conservazione, necessaria ad associare alle UD del Sistema di Gestione Documentale il relativo stato di archiviazione, l'UID e la URI all'elemento documentale conservato ovvero procedere alla gestione e alla bonifica di eventuali anomalie rilevate in fase di versamento, in modo da raggiungere la completa e corretta conservazione degli Elementi Documentali previsti dal Cliente.

Le UD conservate devono essere mantenute in un idoneo sistema di conservazione digitale secondo i termini di legge previsti, in base alla loro classificazione nel Massimario di scarto del Cliente:

Il Conservatore garantisce il ricorso agli standard di interoperabilità definiti da AgID, alla diligente esecuzione delle attività descritte in questo manuale e alla verifica periodica dei dati conservati e dell'intero sistema (vedere il capitolo sulle verifiche periodiche)

il Cliente predispone gli altri strumenti, le risorse, le procedure e gli incarichi necessari a garantire il mantenimento e il transito delle Unità Documentali conservate nei Sistemi di conservazione, Suoi Archivi digitali di deposito, per tutto il tempo necessario e **finché le Unità Documentali in questione giungono alla loro destinazione finale** (procedura di selezione e scarto di archivio del cliente) ovvero all'eliminazione o al loro versamento agli Archivi Storici dello Stato.

torna al sommario

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405
Capitale sociale:
Euro 2.215.200
interamente versato

1.7 Attività accessorie

Fuori dal perimento di erogazione del Servizio e con incarico specifico, il Cliente può rivolgersi a Maggioli spa per avere supporto specialistico, manageriale o IT per:

- MIGRAZIONE PdA per trasferire i dati da un Sistema di conservazione ad un altro;
- VERSAMENTO AUTOMATICO - alimentare in modo parallelo Sistemi di conservazione diversi oppure averne alcuni dedicati al solo mantenimento dei dati in essi conservati;
- VERSAMENTO MASSIVO O ESPORTAZIONE MASSIVA - unire, migrare o separare interi archivi;
- attività di RIVERSAMENTO (es. conversione formato file per obsolescenza tecnologica)
- attività di DIGITALIZZAZIONE (da documento analogico a documento informatico)
- attività di FORMAZIONE del personale e dei dirigenti in materia di digitalizzazione (CAD)
- REDAZIONE, aggiornamento, revisione o definizione del Suo Manuale di gestione e conservazione documentale

Queste “attività accessorie” e qualsiasi altra azione che non sia descritta in questo manuale, sono da ritenersi escluse dal perimento di applicabilità del presente Accordo di Servizio.

torna al sommario

1.8 Cambio di mission (cessazione del Servizio)

Per quanto sia una situazione non prevista, su indicazione di AgID Maggioli spa ha disposto un Piano di cessazione del Servizio, depositato presso l’Agenzia per l’Italia Digitale, aggiornandolo entro 20 giorni da ogni variazione disposta e reso disponibile a richiesta ai clienti in sere di audit.

Il Piano di cessazione si attiva solo nel caso in cui Maggioli spa ritenga di interrompere l’erogazione del servizio alla totalità dei suoi clienti o limitatamente a particolari categorie di fondi o archivi: descrive le attività e le comunicazioni previste e prevede i tempi e le modalità di restituzione dei documenti conservati ai clienti ovvero il passaggio dei PdA conservati ad altro soggetto conservatore preventivamente individuato.

L’attivazione del Piano di cessazione prevede un preavviso ai clienti coinvolti di almeno 180 giorni, salvo diversa disposizione di AgID o dell’autorità di riferimento che ne dovesse richiedere l’attivazione.

Ogni altra interruzione o cessazione nell’erogazione del servizio rientra nell’accordo contrattuale tra Cliente e Fornitore, come riportato in questo Manuale.

torna al sommario

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.215.200
interamente versato

2 *PERIMETRO DI EROGAZIONE DEL SERVIZIO*

Il presente manuale si applica alle Unità Documentali (Fascicoli, Raccolte e Documenti) prodotte dal Cliente secondo le vigenti Linee Guida AgID, eventualmente integrate da ulteriori evidenze informatiche (e flussi) di cui all'incarico specifico.

L'incarico è composto da

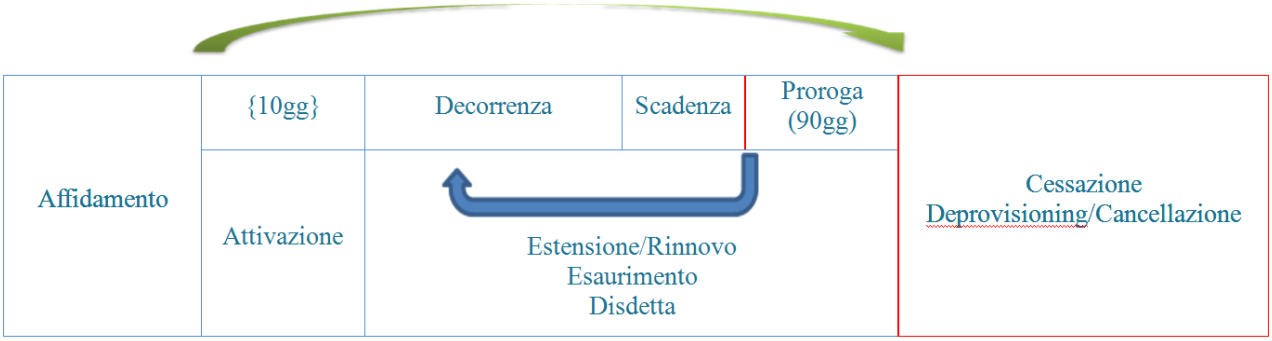
- un **ordine** (o atto equivalente) che dettaglia tempi, importi economici e quantità di dati concordati;
- un atto, o modulo di **richiesta di attivazione** che dettaglia i flussi documentali e i Soggetti coinvolti;
- la sottoscrizione per accettazione integrale di **questo Manuale e** dei **suoi allegati** da parte del Cliente;
- la **nomina** a Maggioli spa come Responsabile esterno al trattamento dati.

L'atto di incarico determina i tempi, le quantità e le tipologie (o i flussi) documentali oggetto dall'incarico, a cui **Maggioli spa applica i trattamenti a suo carico previsti da questo Manuale, nel capitolo "Dettaglio attività previste"**.

torna al sommario

2.1 Durata del rapporto (attivazione istanza)

Il periodo temporale di erogazione del servizio



1-Periodo di erogazione del servizio

- parte dall'accettazione della richiesta di attivazione (Modulo) con l'invio a mezzo PEC delle credenziali di utilizzo del Servizio al cliente
- può prevedere la trattazione di dati anche pregressi (formati prima dell'avvio del Servizio)
- può essere estesa con proroghe o nuovi incarichi di conservazione (o di solo mantenimento dati)
- termina con
  - la scadenza del periodo previsto dall'incarico o dalle proroghe attivate
  - una disdetta da parte del Cliente
  - la cessazione del servizio da parte del cliente (es. chiusura della ragione sociale)
  - cessazione del servizio da parte di Maggioli spa (con preavviso di 6 mesi – per i dettagli vedere il Piano di cessazione del servizio di conservazione digitale)

torna al sommario

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405
Capitale sociale:
Euro 2.215.200
interamente versato

2.2 Limiti all'erogazione del Servizio

Il Servizio prevede esclusivamente le attività e le modalità di fruizione previste in questo Manuale (ambito, descrizione, dettaglio);

sono escluse e descritte in documenti specifici le attività accessorie eventualmente richieste dal Cliente e qualsiasi altra azione non descritta in questo Manuale;

il presente Manuale si applica esclusivamente all'erogazione del Servizio di conservazione digitale a norma erogato da Maggioli spa, come richiesto dal Cliente con specifico incarico, atto a dettagliare i flussi documentali coinvolti e i tempi e le quantità previste dal Cliente per il Servizio; saturato lo spazio (GB) richiesto il servizio rimane disponibile per solo mantenimento e richiesta dati, fino a scadenza dell'incarico.

I dati conservati sono resi disponibili esclusivamente e senza ulteriori limitazioni al Cliente (utenti abilitati) e, in caso di specifica richiesta, al soggetto istituzionale abilitato (es. Autorità Giudiziaria).

torna al sommario

2.3 Sospensione, prosecuzione e cessazione del rapporto

Le utenze di accesso al portale web del Servizio sono sospese (bloccate) in caso di:

- 5 tentativi di accesso con password errata
- Trascorsi 3 mesi di inutilizzo
- Rilevazione o sospetto di rischi per la sicurezza correlati all'utilizzo delle credenziali

Un'istanza di conservazione può essere sospesa (SP Bloccato dal conservatore e PdV rifiutati) in caso di

- esaurimento dello (spazio) SLOT-GB ordinato
- superamento del periodo previsto dall'incarico
- rilevazione o sospetto di un utilizzo improprio o anomalo del Servizio (es. eccessivo frazionamento dei lotti/PdV)

Il Servizio può essere temporaneamente sospeso per tutti i tenant coinvolti da un intervento o da un evento che comporti un fermo prolungato del sistema di erogazione

- previa notifica – in caso di intervento di manutenzione programmata
- senza notifica – in caso di intervento di manutenzione urgente
- con notifica successiva – in caso di incident

Al fine di dare continuità all'erogazione del servizio, **durante la definizione del successivo reincarico**, il periodo di erogazione può essere prorogato, d'ufficio o su richiesta del cliente, senza impegno e per massimo 3 mesi e 3 volte per ogni incarico

- in caso di nuovo incarico (conservazione, solo mantenimento o esportazione massiva dei dati), il relativo ordine dovrà coprire anche il periodo di erogazione di cui si è usufruito durante la proroga;
- nulla è dovuto da parte del cliente, in caso di semplice cessazione (disdetta o mancato reincarico), dove il Cliente ha 3 mesi di tempo dalla cessazione dell'incarico o della proroga per scaricare autonomamente i dati conservati, utilizzando il portale web del servizio.

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405
Capitale sociale:
Euro 2.215.200
interamente versato

Il servizio di conservazione digitale termina sempre con la distruzione degli Elementi Documentali conservati per conto del Cliente: il Conservatore è autorizzato al trattamento dei dati (e dei documenti) oggetto del servizio, limitatamente per l'esecuzione delle attività previste da questo Manuale e rientranti nel periodo di validità dell'incarico specifico. Come indicato al capitolo "Descrizione del Servizio", il Cliente può disporre uno o più incarichi, anche avvalendosi di diversi Conservatori che si avvicenderanno, fino al momento in cui le Unità Documentali conservate giungeranno alla loro "Destinazione Finale", determinata dal Cliente in base alla loro Classificazione nella Sua "procedura di Selezione e Scarto" ovvero con l'effettiva eliminazione della UD dagli Archivi del Cliente e la loro eventuale trasmissione ad altro Organo competente.

Compiuta la cessazione del rapporto, i dati sono rimossi dal sistema di conservazione digitale e rimangono disponibili per 6 mesi, in forma di "immagini di backup", valide per la sola esportazione massiva e successivo inoltro ad altro sistema di conservazione qualificato; successivamente, secondo le politiche di sicurezza e backup in uso presso Maggioli spa, sono definitivamente rimosse dal Sistema di conservazione tutte le copie (file) e le occorrenze (record/DB) riferite ai dati conservati per l'istanza (tenant di conservazione) cessata.

Per tutto quanto non qui riportato si rimanda al Piano di cessazione del servizio di conservazione digitale di Maggioli spa.

torna al sommario

2.4 Alert previsti

L'erogazione del servizio prevede 4 ordini di notifiche:

1. Trasmissione semestrale e a mezzo PEC di un report periodico che riporta
   a. gli estremi del servizio (attivazione, scadenza, saturazione SLOT, ecc.);
   b. le utenze attivate, il loro stato e i ruoli registrati per il tenant;
   c. le quantità di dati conservati per ogni flusso (tipologia) e anno (esercizio)
2. In presenza di eventuali alert (es. prossima scadenza o saturazione SLOT o altro) lo stesso report è trasmesso, aggiornato, con cadenza trimestrale
3. Al 90% di saturazione SLOT o all'approssimarsi della scadenza dell'incarico il sistema trasmette delle notifiche email, via posta elettronica ordinaria
4. Le notifiche automatiche di processo inviate via email al riferimento tecnico del cliente nei casi di
   - errore di elaborazione (SP Bloccato o errore di validazione del file IdV)
   - elaborazione eseguita con successo
   - blocco utente (dopo 5 tentativi di accesso con password errata)
   - accesso da parte dell'utente a record che potrebbero contenere dati personali

Le email di notifica sono trasmesse ai riferimenti indicati nell'atto di incarico o nella richiesta di attivazione, mentre le PEC, salvo diversa indicazione del Cliente, sono trasmesse ai domicili digitali indicati nei pubblici registri di riferimento.

torna al sommario

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405
Capitale sociale:
Euro 2.215.200
interamente versato

3 CARATTERISTICHE TECNICHE E TECNOLOGICHE

Il Servizio di conservazione digitale di Maggioli spa è erogato esclusivamente in modalità cloud.

Le regole generali descritte in questo manuale sono applicate ad ogni istanza di conservazione erogata dal Sistema di conservazione. Eventuali personalizzazioni o modifiche sono registrate nel sistema di conservazione e nella modulistica dedicata, archiviata tra la documentazione relativa al rapporto in questione presso il Conservatore.

I manuali, le guide d'uso e altro materiale di supporto, ivi compresa la documentazione tecnica delle API e delle interfacce SOAP/REST in lingua italiana sono disponibili online sul sito primario di erogazione del Servizio.

Cambiamenti e migliorie introdotti in seguito ad aggiornamenti delle modalità di funzionamento e fruizione dei servizi sono comunicati entro 30 giorni tramite aggiornamento del presente manuale e, se necessario, sono notificati via PEC alla casella istituzionale di ogni Cliente coinvolto.

torna al sommario

3.1 Datacenter

Trattando principalmente documenti delle Pubbliche Amministrazioni, che la norma identifica come Beni Culturali e Patrimonio dello Stato, contenenti anche dati personali o sensibili, **Maggioli spa conserva tutti i all'interno del territorio nazionale, in datacenter** (**CSP qualificati AgID**) di proprietà della stessa Maggioli spa o di sue controllate, limitandone l'eventuale diffusione.

LA NOSTRA INFRASTRUTTURA CLOUD:

sito primario – [Milano Campus Data4, eLogic srl] – Via Monzoro, 101-105, 20007 Cornaredo MI

sito secondario – [DC Mantova, Gruppo Maggioli] – Via Pietro Verri, 27, 46100 Mantova MN

torna al sommario

3.2 Segregazione dei sistemi

Solo gli Utenti e le risorse assegnate al Servizio accedono ai dati conservati.

Il Sistema di conservazione digitale è fisicamente e logicamente distinto dal Sistema di gestione documentale del Cliente; anche all'interno delle infrastrutture IT di Maggioli spa, le risorse (IT e VM) dedicate alla conservazione digitale sono riservate al Sistema stesso e non sono accessibili ad altri che agli Amministratori di sistema indicati al capitolo "Il Conservatore".

torna al sommario

3.3 Firme digitali, PEC e Marcatura temporale

Il sistema di conservazione di Maggioli spa utilizza servizi fiduciari eIDAS quali PEC, Firma digitale e Marcatura temporale erogati da soggetti terzi, TSP italiani, qualificati come previsto da AgID e dal citato Regolamento eIDAS. Il ricorso a questi fornitori e tecnologie è applicato in modo tale da tutelare sempre la riservatezza e la sicurezza degli elementi documentali oggetto del servizio (documenti e fascicoli conservati) e dei dati personali in essi contenuti: in nessun caso queste informazioni sono trasmesse da Maggioli SPA fuori dal territorio nazionale o ad altro fornitore. Le firme digitali e le marche temporali, utilizzati per attestare l'integrità dei dati archiviati, applicate da Maggioli spa ad ogni indice di conservazione (File IdC) associati ai PdA conservati, sono periodicamente verificati in automatico.

La PEC è utilizzata come canale di comunicazione ufficiale tra

Maggioli spa (conservatore@maggioli.legalmail.it) e
il Cliente (pubblici registri o domicili digitali)

torna al sommario

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.215.200
interamente versato

3.4 Componente applicativa

Il Servizio di conservazione digitale erogato da Maggioli spa utilizza il software LegalArchive® di IFIN Sistemi SRL per la formazione e la verifica periodica dei Pacchetti di Archiviazione (PdA) contenenti le Unità Documentali conservate a norma.

Il software è OAIS compliant e rispondente allo standard di interoperabilità UNI SinCRO; è basato su tecnologia Apache Tomcat, configurato come descritto in questo manuale ed è utilizzato da diversi Sistemi di conservazione digitale italiani, il che rende particolarmente versatile, sicura ed agevole l'integrazione al Sistema di conservazione digitale di Maggioli spa, evitando tra l'altro ogni rischio di lock-in.

Il contratto di partnership tra Maggioli spa e IFIN Sistemi prevede un costante aggiornamento normativo e tecnologico della componente software, la formazione specialistica dei nostri operatori, un supporto applicativo di secondo livello, audit annuali, la possibilità di richiedere personalizzazioni della soluzione applicativa, l'erogazione del Servizio a clienti PA e Privati (nazionali ed esteri) e il deposito delle librerie software presso un noto Studi Notarile che renderà ai partner i sorgenti del software ad esempio in caso IFIN dovesse cessare le sue attività.

Il software di conservazione aggiunge all'interfaccia di comunicazione SFTP, già prevista dal sistema di Maggioli spa, i canali di comunicazione HTTPS (API e GUI): ogni utente autorizzato può accedere al Sistema di conservazione tramite integrazione applicativa oppure tramite l'interfaccia web del Servizio, utilizzando le proprie credenziali personali specifiche, rilasciate dal Conservatore (Maggioli spa) oppure, come opzione aggiuntiva da richiedere specificatamente nell'incarico, utilizzando il proprio profilo SPID "Identità Digitale Uso Professionale Persona Giuridica" che consente di accreditarsi al Sistema per conto dell'Organizzazione di appartenenza e solo a seconda del Ruolo effettivamente ricoperto al momento del tentativo di accesso.

torna al sommario

3.5 Capacity planning

Il Piano per la sicurezza di Maggioli spa indica il metodo di gestione del capacity planning, l'analisi dei rischi applicata alla ISO 27001 e la scalabilità delle soluzioni impostate.

Il capacity planning è monitorato mensilmente al fine di evidenziare eventuali discrepanze tra l'effettivo carico del Sistema e le proiezioni del Piano.

Aggiornato con pianificazione almeno triennale, il Piano è rivisto annualmente in sede di audit e con il Board di Maggioli spa in caso di necessità di ulteriore, anticipata, revisione.

torna al sommario

3.6 Update e change-log

Il Sistema di conservazione è costantemente adeguato rispetto alle norme, alle prassi e agli standard indicati al capitolo 1 di questo Manuale. Le variazioni che impattano sulle specifiche di integrazione applicativa sono comunicate tempestivamente e con il dovuto preavviso ai clienti, mentre non sono notificate altre variazioni (es. normative o infrastrutturali) che possono avere impatto sulla conservazione ma che per competenza, come ad esempio per **gli adempimenti (formazione e gestione) a carico del Produttore, rimangono fuori dal perimetro delle attività iscritte dalla norma al servizio erogato dal conservatore** e su cui comunque Maggioli spa si rende disponibile ad erogare un supporto specialistico ad hoc.

Ogni variazione al Sistema di conservazione segue una procedura di change management che prevede la registrazione dell'intero iter che prevede Richiesta, Analisi di impatto, Programmazione intervento, Verifica esito dell'intervento ed eventuale ripristino.

torna al sommario

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405
Capitale sociale:
Euro 2.215.200
interamente versato

3.7 Attivazione/Disattivazione risorse

Maggioli spa si è dotata di procedure specifiche tese alla corretta selezione, inquadramento ed aggiornamento delle risorse (IT e HR) necessarie al Sistema

torna al sommario

3.8 Supporti removibili, cifratura e trasmissione dati

Il Servizio di conservazione digitale a norma di Maggioli spa NON prevede il ricorso all'utilizzo di dispositivi removibili o altri asset fisici forniti dal cliente come "contenitori di dati" del cliente o di Soggetti terzi.

I dispositivi utilizzati dai nostri operatori per gestire il Sistema o per erogare assistenza ai Clienti hanno tutti dischi cifrati e, eccezion fatta per la modulistica resa a mezzo PEC, non è mai richiesto né necessario far transitare documenti per tramite di un dispositivo o di un servizio o sistema diverso dai nodi di erogazione del Servizio.

La trasmissione di informazioni -da e per- il sistema di conservazione avviene sempre tramite canale cifrato HTTPS o SFTP; inoltre il Cliente può decidere di cifrare a monte le informazioni o i documenti particolarmente sensibili destinati alla conservazione; in quest'ultimo caso il Produttore dovrà avere l'accortezza di conservare, separatamente dalle Unità Documentali in questione, anche le istruzioni e gli strumenti (software e chiavi) necessari a recuperare la forma originaria ed intellegibile dei dati oggetto di conservazione.

torna al sommario

3.9 Gestione file virati

Esclusi i viewer necessari, **è fatto divieto conservare file eseguibili, "documenti illeggibili" oppure file contenenti virus** nel sistema di conservazione digitale di Maggioli spa.

Il Sistema utilizza 3 differenti layer di controllo antivirus

Il primo è eseguito a livello di firewall, in fase di upload – se un file risulta contenente virus (black-list), ne viene impedita la scrittura e il flusso di upload restituisce un errore applicativo al sistema versante, del tutto analogo a quello relativo ad una corruzione dati in fase di trasmissione o di "time-out" per connessione interrotta;

il secondo controllo è eseguito in nell'area di "staging" dei dati in attesa di presa in carico e durante l'elaborazione delle Unità Documentali da conservare – nessun file versato in conservazione è eseguito o aperto in lettura durante la fase di versamento o di messa in conservazione – se l'antivirus intercetta un file virato in questa fase, lo rende inaccessibile (quarantena) al sistema di conservazione e il processo di conservazione avrà come esito "errore in fase di validazione" per la mancata corrispondenza tra indice di versamento e file da conservare

il terzo livello di controllo è applicato agli archivi di conservazione per intercettare eventuali virus che non erano ancora noti al momento del versamento e non sono quindi stati tempestivamente intercettati – in questo caso l'antivirus rinomina e rende inaccessibile il file in questione che non potrà essere aperto o scaricato; ogni controllo automatico ritornerà un "errore di validazione", ma l'assistenza tecnica sarà in grado di estrarre dal log dell'antivirus la relativa annotazione. Il documento bloccato dall'antivirus potrà se richiesto essere ripristinato ovvero definitivamente eliminato semplicemente con una richiesta del Cliente trasmessa al Conservatore a mezzo PEC.

torna al sommario

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.215.200
interamente versato

3.10 Restituzione e dismissione degli asset

Come già anticipato ai capitoli precedenti il Servizio non ricorre all'utilizzo di alcun asset fisico e i datacenter impiegati dedicano delle risorse virtuali al Sistema di conservazione.

Gli asset digitali (le unità documentali, fascicoli o documenti) conservati sono resi al Cliente a richiesta, in Pacchetti di Esibizione durante l'esecuzione del Servizio ovvero con esportazione massiva alla cessazione del rapporto.

Esaurito il periodo dell'incarico i dati conservati sono eliminati dal sistema di conservazione

torna al sommario

3.11 Politiche di backup ed eliminazione dei dati dal sistema

I dati conservati nel Sistema di conservazione digitale e il sistema stesso sono sottoposti a politiche di backup tali da assicurare un RPO di 15 minuti sui dati già conservati.

I backup sono successivamente storicizzati, consolidati ed ottimizzati in modo da poter mantenere offline e ripristinare in caso di necessità l'immagine di ogni archivio, nodo o Tenant anche cessato, risalendo fino ad un anno nel passato.

In caso di definitiva dismissione di un asset IT, il Conservatore applica una idonea politica di reiterata eliminazione e sovrascrittura dei dati tale da rendere irrecuperabile ogni informazione precedentemente in essi archiviata.

torna al sommario

3.12 Alta affidabilità, incident e Disaster recovery

In caso di evento che determini un danno all'integrità, disponibilità o riservatezza dei dati oggetto del servizio, Maggioli spa attiva una procedura di incident-management che prevede la notifica dell'incident ai Soggetti coinvolti, la registrazione dell'evento e di tutte le attività ad esso correlate.

Il Sito primario e il sito secondario sono costantemente allineati ed in caso di disastro o fermo prolungato il Conservatore può attivare la procedura di disaster recovery che prevede l'attivazione un team dedicato al ripristino dell'erogazione del Servizio sul sito secondario.

Se l'incident riguarda anche solo potenzialmente dei dati personali, le notifiche sono inviate anche al Garante e ogni operazione viene coordinata dagli uffici (IT e Organizzativi) preposti.

torna al sommario

3.13 Analisi dei rischi

Le certificazioni necessarie all'erogazione del Servizio richiedono l'applicazione e il costante aggiornamento del documento di Analisi dei rischi, eventualmente disponibile in sede di audit e non esportabile.

I rischi analizzati e trattati con successo per il servizio riguardano diversi ambiti di gestione:

- Organizzazione (ISO 9001; mod.231)
  - Fornitori esterni
  - Formazione
- Cloud e Datacenter (SOA e ISO 20000)
- Sicurezza delle informazioni e dei dati personali (ISO 27001; GDPR)

torna al sommario

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405
Capitale sociale:
Euro 2.215.200
interamente versato

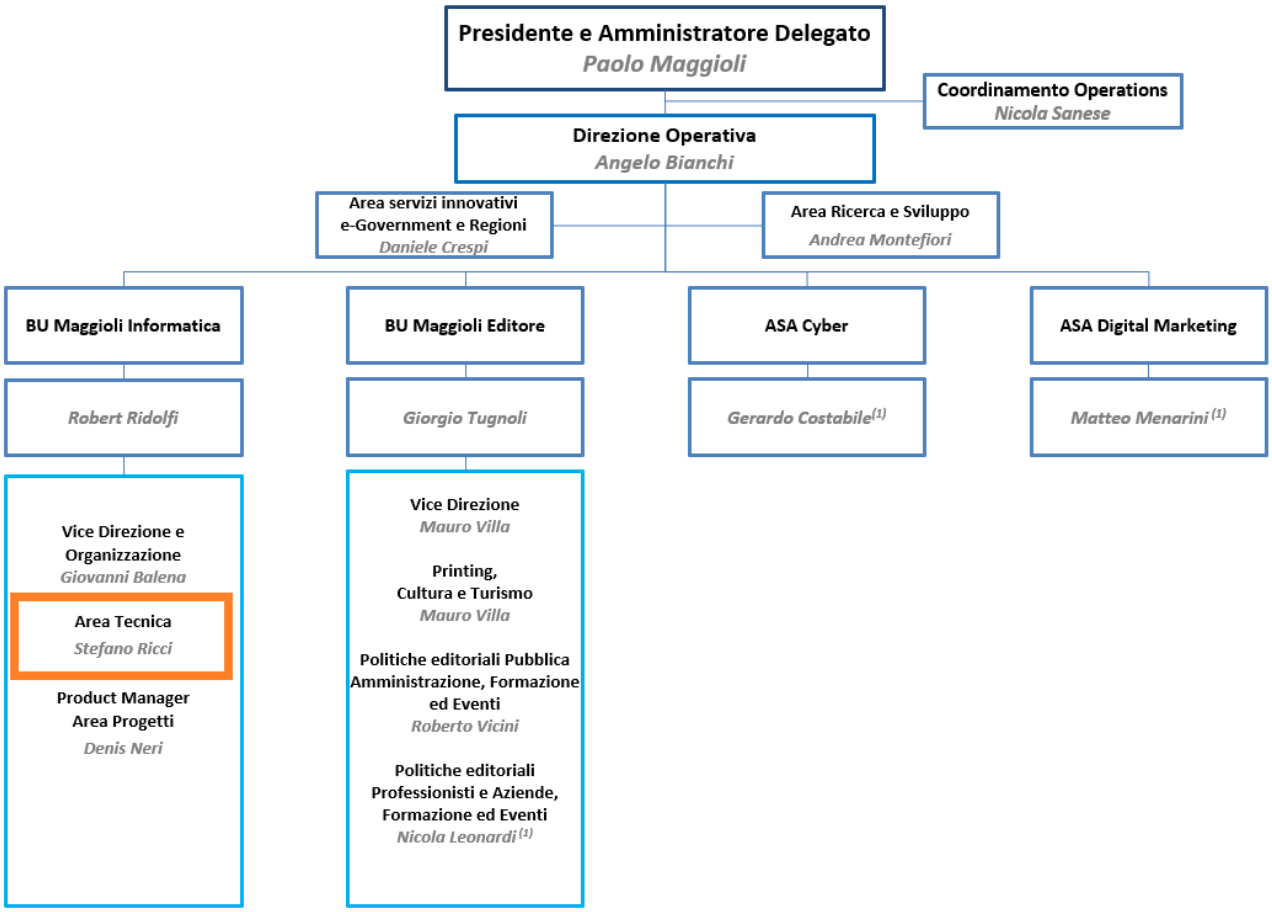
4 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO

Per l'esecuzione attività previste dal Servizio

- Il Cliente/Produttore – Responsabile del Sistema di Gestione Documentale (versante)
- Il Conservatore (Maggioli spa) – Responsabile del Servizio e del Sistema di conservazione digitale

Ognuna delle Organizzazioni coinvolte nell'incarico identifica per competenza e nomina nel proprio organico o con delega i Ruoli di riferimento per le attività previste dal Servizio

Per quanto al Conservatore l'organigramma di riferimento è rappresentato nell'immagine seguente:



2- Organigramma Maggioli spa

torna al sommario

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

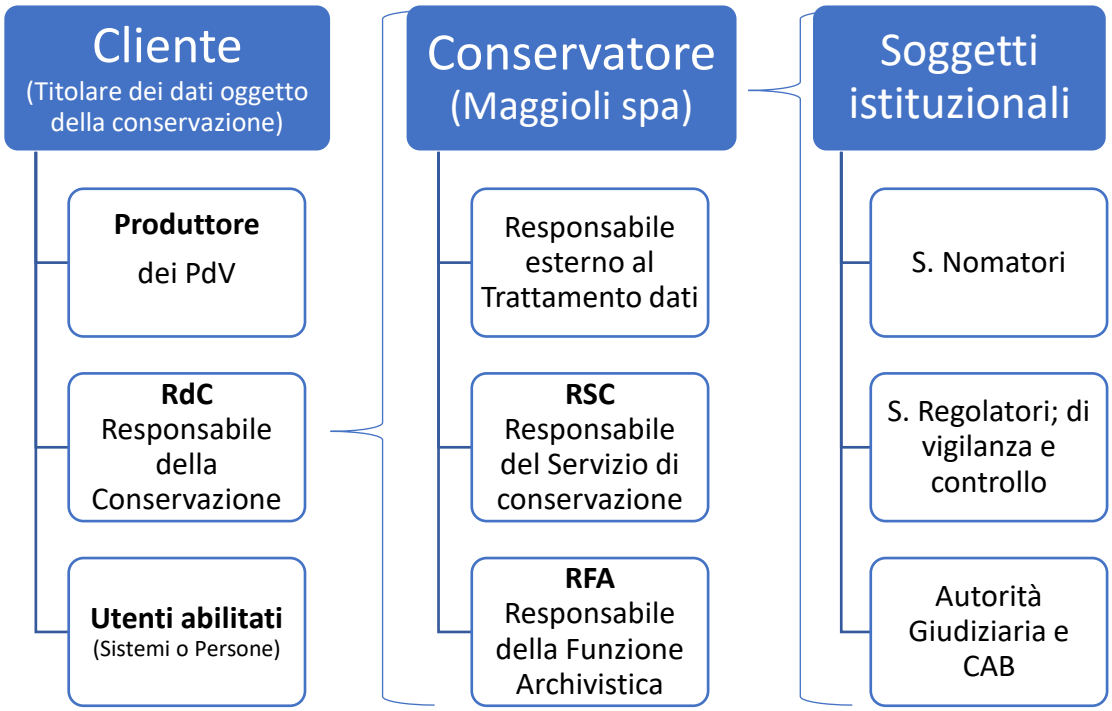
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.215.200
interamente versato

4.1 Ruoli previsti

Nella esecuzione delle attività specifiche, previste dal Servizio di conservazione digitale a norma di Maggioli spa, si interfacciano i ruoli di seguito descritti:



3- Funzioni e Ruoli

I requisiti del processo di conservazione, le responsabilità e i compiti del responsabile della conservazione e del responsabile del servizio di conservazione e le loro modalità di interazione sono formalizzate nell'incarico ovvero nel manuale di conservazione del Cliente, Titolare dell'oggetto della conservazione, e nelle specifiche del contratto di servizio. Tali modalità trovano riscontro anche nel presente Manuale del Servizio del conservatore.

torna al sommario

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405
Capitale sociale:
Euro 2.215.200
interamente versato

4.2 Il Cliente (Responsabile gestione e conservazione)

Il Produttore, Responsabile del Versamento e il Responsabile di conservazione definiscono nel loro Piano di gestione e conservazione documentale le politiche di raccolta, versamento, conservazione e scarto, incluse quelle applicate in Conservazione dal Responsabile del Servizio.

Nella Pubblica Amministrazione Produttore e Responsabile della conservazione sono 2 ruoli (funzioni e persone fisiche) esclusivamente interni all'amministrazione stessa, non delegabili all'esterno e possono coincidere con il medesimo soggetto**; il Responsabile del servizio di conservazione è sempre un soggetto esterno, in organigramma al Soggetto Conservatore che viene incaricato dal Responsabile di conservazione del Cliente all'esecuzione delle attività di conservazione previste dal presente manuale**, limitatamente ai flussi documentali (sorgente, tipologia, quantità e arco temporale) indicati nel modulo "Richiesta di attivazione del Servizio".

torna al sommario

4.3 Il Conservatore (Nomine e Amministratori di sistema)

Conservatore, ma anche CSP qualificato, **Maggioli spa integra i ruoli previsti a suo carico dalla norma con tutte le professionalità comunque ritenute necessarie** e qui riportate:

Nominativo	Ruolo (per il servizio di conservazione)	Inquadramento (organigramma)
Robert Ridolfi	**Responsabile del Servizio di conservazione**	Direttore Maggioli Informatica
Stefania Rampazzo	**Responsabile della funzione archivistica**	Collaboratore esterno
Ernesto Belisario	**(DPO) Responsabile della Protezione dei dati**	Collaboratore esterno
Roberto Piccardi	Responsabile trattamento dati personali	Collaboratore esterno
Beatrice Paccassoni	Responsabile della Sicurezza dei sistemi	Dipendente - Responsabile della Qualità – SGSI
Andrea Furiosi	Product Manager & Sales Account Manager	Collaboratore esterno
Paolo Bianchi	Resp. ufficio ordini e Assistenza clienti	Assistente Direzione
Oscar Bevoni	Responsabile sistemi informativi	Direttore Sistemi Informativi
Fabio Tiralongo	Responsabile sviluppo e manutenzione Amministratore del Sistema di conservazione	Dipendente (B.U. Maggioli Editore)
Federico Berlini	Amministratore del Sistema di conservazione	Dipendente (B.U. Maggioli Editore)
Bruno Cominotti	Amministratore dei Sistemi IT di Maggioli spa	Dipendente Sistemi Informativi, Maggioli spa
Marco Leasi	Amministratore dei Sistemi IT di Maggioli spa	Dipendente Sistemi Informativi, Maggioli spa

4 - Nomine Maggioli spa

4.3.1 Modifiche intercorse alle nomine interne

Dal 1/12/2017 Stefania Rampazzo, archivista esperta e consulente esterno con contratto triennale, sostituisce Elisabetta M.C. Bruno come Responsabile della funzione archivistica

Il 1/12/2017 Roberto Piccardi, consulente privacy per Maggioli spa da oltre 3 anni, è nominato Responsabile trattamento dati personali per il servizio di conservazione

Il 5/05/2022 Robert Ridolfi, direttore e procuratore speciale di Maggioli spa, viene nominato Responsabile del Servizio di conservazione in avvicendamento al Direttore Mauro Villa, già Responsabile di del servizio a partire dal 22/05/2015

torna al sommario

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405
Capitale sociale:
Euro 2.215.200
interamente versato

4.4 Matrice delle responsabilità

La matrice RACI (**R**esponsible, **A**ccountable, **C**onsulted, **I**nformed) descrive per ogni attività prevista o necessaria il

- **R**esponsible = **Responsabile** dell'esecuzione dell'attività
- **A**ccountable = Delegato, responsabile sul risultato atteso (Vicario/Responsabile) delle attività
- **C**onsulted = Funzioni di supporto all'esecuzione o definizione delle attività
- **I**nformed = Funzioni con ruolo di monitoraggio, sorveglianza o intervento

	CLIENTE			CONSERVATORE		
	PRODUTTORE (RGD)	**RdC**	Utente Abilitato (operatore)	**RSC**	**RFA**	**AdS** Amministratori del Sistema
Attività preliminari						
Predisposizione Piano e Manuale di Gestione e conservazione documentale	R	A	I	I	C*	
Redazione del manuale del Servizio di conservazione	I	I	I	R	A	A
Piano per la sicurezza delle informazioni	R	I		A	I	I
Piano per la sicurezza dei Sistemi informativi	R	I		A		I
Incarico per il Servizio di conservazione digitale	C	R	I	A	C*	A
Erogazione del servizio						
Attivazione del Servizio	I	I		R	C	A
Richiesta variazione del servizio	C	R	I	A	C*	A
Adeguamenti del Sistema e del Servizio		I		C	C	R
Monitoraggio del Sistema (disponibilità)		I		I		R
Trasferimento dati in conservazione	R	A	I	I	C*	
Selezione e raccolta UD	A	R	A	I	C*	C*
Caricamento PdV	A	R	A			A
Validazione PdV		R		A		A
Gestione esiti di elaborazione	A	R	A	I		
Archiviazione PdA	I	I		R		A
Accesso agli archivi		R		A		A
Produzione duplicati e copie informatiche	R	I	A	A	C*	A
Gestione dell'obsolescenza tecnologica	R	A		A	C*	
Conversioni e riversamenti	A	R	I	I	C*	
Eliminazione dei dati conservati	A	R		A	C*	A
Tracciatura delle attività eseguite		I	I	R		A
Verifica dell'integrità degli archivi	A	R		R		A
Selezione e scarto di archivio	A	R		A	C*	I
Disattivazione tenant (cessazione)	R	A		R	C*	A

*tramite consulenza o per rimando al presente Manuale

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405
Capitale sociale:
Euro 2.215.200
interamente versato

La "R" evidenziata in rosso indica il Ruolo e l'Organizzazione a cui è iscritta per norma o contratto la Responsabilità sulla corretta esecuzione della fase specifica, anche quando la singola azione o attività può essere delegata ad un altro soggetto "A" o ad un soggetto esterno (es. partner tecnologico)

torna al sommario

5 DETTAGLIO ATTIVITÁ PREVISTE (trattamenti)

Per ognuna della attività previste nell'erogazione del servizio si riporta Descrizione e Responsabile.

torna al sommario

5.1 Trattamento dati

I dati personali gestiti nell'esecuzione del servizio sono sempre:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
b) raccolti per le sole finalità previste per l'erogazione del Servizio e successivamente eliminati in modo da non entrare in contrasto non con tali finalità (nessun un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati");
d) esatti e, se necessario, tempestivamente aggiornati ("esattezza");
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal GDPR a tutela dei diritti e delle libertà dell'interessato ("limitazione della conservazione");
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali ("integrità e riservatezza").

Rispetto ai diritti dell'interessato dal trattamento dei dati personali, diverso dal Titolare degli elementi (e dei dati) trattati nell'erogazione del Servizio, si ricorda che

- le pubbliche autorità e gli altri enti che conservano archivi nel pubblico interesse sono servizi che hanno "l'obbligo legale" di trattare archivi selezionati per la conservazione e la cancellazione di dati personali contenuti in documenti archivistici renderebbe impossibile, per questi organismi, assolvere alla missione istituzionale assegnatagli dalla legge;
- il diritto alla cancellazione delineato dall'art. 17 del GDPR non si applica ai documenti selezionati per la conservazione permanente;
- il diritto di oblio, così come affermato dalla Corte di giustizia della Unione Europea (cioè non cancellazione, ma deindicizzazione dei dati personali) può essere messo in pratica, senza pregiudicare i reciproci compiti istituzionali, deindicizzando o prevenendo in altro modo la ricerca di nomi all'interno dei documenti da parte dei motori di ricerca, senza mettere a rischio la loro integrità e conservazione;
- l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento dei dati personali che lo riguardano, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico (art. 21, c. 6 del GDPR);
- gli Archivi possono impedire la ricerca dei nomi contenuti in un documento pubblicato, mantenendo la possibilità di rintracciarlo utilizzando chiavi di ricerca diverse dai dati personali.

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405
Capitale sociale:
Euro 2.215.200
interamente versato

L'informativa privacy completa è resa disponibile sul sito istituzionale di Maggioli spa, all'indirizzo: https://privacy.maggiolicloud.it/privacy/wwwmaggioli.it

torna al sommario

5.2 Attività preliminari e incarico

L'incarico all'esecuzione previste dal servizio di conservazione digitale è eseguito dal Responsabile della Transizione digitale del Cliente ovvero dal suo Responsabile di conservazione, nell'esecuzione del mandato a lui affidato con tale nomina e secondo quanto disposto dal Responsabile della Gestione Documentale, sentito il parere del Responsabile a trattamento dati, come riportato nel Manuale di gestione documentale del Cliente, Soggetto Produttore e Titolare dei dati oggetto di conservazione.

Il Conservatore può, con attività accessorie e supporto professionale specifico (es. funzione archivistica), supportare il Cliente nell'appurare la congruità dei dispositivi di archivio utilizzati e degli oggetti (nelle fasi di formazione, registrazione, gestione e raccolta), le Unità Documentali, destinati alla conservazione digitale.

torna al sommario

5.3 Attivazione del servizio

Il Conservatore attiva l'istanza di conservazione richiesta dal Cliente appena riceve e verifica come corretta e coerente la necessaria documentazione:

- Modulo di richiesta di attivazione del servizio, nomina del Responsabile del Servizio e del Responsabile esterno al trattamento dati ovvero un atto di incarico completo dei medesimi elementi;
- Contratto predisposto tra le parti (o dal Cliente in caso di PA) ovvero incarico MEPA sottoscritto, accompagnato dalla relativa determinazione;
- Copia sottoscritta dal Cliente (Responsabile di conservazione) del presente manuale che si applica comunque solo per i flussi (tipologie documentali), i tempi e le quantità indicati nel modulo di richiesta di attivazione e nel relativo incarico.

La fase di attivazione è conclusa con l'invio al cliente, mezzo PEC, delle credenziali necessarie all'utilizzo del servizio.

torna al sommario

5.4 Variazione o Estensione del Servizio

In corso di erogazione del servizio o durante le eventuali proroghe attivate, il Cliente può richiedere la variazione dei referenti e degli utenti abilitati da lui indicati, semplicemente trasmettendo al conservatore una PEC a cui allega il relativo modulo firmato dal suo Responsabile di conservazione.

Le variazioni alle nomine interne all'Organizzazione Cliente e soprattutto quelle relative ai Responsabili di gestione e conservazione documentale sono comunicate al Conservatore entro 10 giorni dall'avvenuta modifica; in caso di variazione del Responsabile di conservazione, oltre al modulo previsto, si trasmette al Conservatore anche una copia di questo manuale, sottoscritta dal nuovo Responsabile.

In caso di modifiche, richieste del Cliente, anche tramite nuovi incarichi, volte a modificare i termini del servizio ovvero ad estendere i limiti impostati per l'istanza di conservazione attivata (scadenza, dimensionamento SLOT-GB o flussi coinvolti), il Cliente trasmette al Conservatore un nuovo incarico indicando l'istanza a cui applicarne le disposizioni.

torna al sommario

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405
Capitale sociale:
Euro 2.215.200
interamente versato

5.5 Adeguamento del Sistema

Maggioli spa mantiene il Servizio di conservazione allineato ai requisiti tecnologici, organizzativi e di sicurezza (IT) previsti da AgID per il Sistema di conservazione digitale a norma e i CSP (Cloud Service Provider) qualificati e registrati nel "Marketplace AgID" di riferimento.

Il Conservatore monitora i dati conservati e gli archivi formati nel sistema di conservazione stesso, mentre non interviene per quanto concerne ai sistemi e agli iter esterni al sistema di conservazione e che operano sotto diretto controllo e responsabilità del Produttore.

I responsabili e gli operatori individuati sono selezionati e costantemente formati per il ruolo di competenza; ogni responsabile monitora la variazione alle norme e alle "best-practice" di riferimento per le attività che gli sono assegnate e procede di conseguenza, secondo le procedure disposte dalla propria Organizzazione.

torna al sommario

5.6 Monitoraggio del Sistema (SLA)

Maggioli spa garantisce la disponibilità del servizio per le attività di upload/versamento, ricerca/interrogazione e download/esibizione nei limiti (SLA) concordati in fase di qualificazione, gara o incarico e comunica al cliente eventuali disservizi prolungati.

Se non diversamente specificato, fatti salvi eventi non dipendenti da quanto disposto da Maggioli spa per l'erogazione del servizio e descritto in questo Manuale, i livelli di servizio minimi garantiti ad ogni "istanza" di conservazione sono previsti al 99% ("ggll" = "giornate lavorative nell'anno") nei seguenti casi:

- Up-Time del servizio (raggiungibilità HTTPS/SSH richiesta)
  - **> 99,6%** (ore/ggll/anno);
  - solo sessioni valide e almeno 5 secondi tra le sessioni/chiamate attivate
- Risposta alla Richiesta di attivazione o variazione del Servizio:
  - **entro 10 ggll**
  - dalla ricezione della documentazione completa a mezzo PEC
  - si conclude con l'invio della risposta prevista, stesso mezzo, al Cliente
- Risposta alla Richiesta di Versamento manuale (utente tramite portale WEB del Servizio)
  - Presa in carico immediata (notifica a video)
  - Elaborazione PdV conforme **entro 3 ggll** dalla data "presa in carico"
  - Si conclude con la produzione contestuale di Rapporto di Versamento e indice di conservazione
  - Errori di elaborazione o per PdV non conforme sono notificati entro lo stesso termine.
- Risposta alla Richiesta di Versamento automatizzato (o tramite altro applicativo)
  - "Presa in carico PdV conforme" **entro 15 ggll** dalla cadenza/frequenza di versamento concordata per l'elaborazione applicativa automatizzata
  - termina con la generazione del Rapporto di Versamento (RdV)
  - Elaborazione PdV conforme **entro 3 ggll** dalla "presa in carico" con generazione dell'indice/evidenza di conservazione

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405
Capitale sociale:
Euro 2.215.200
interamente versato

- Errori di elaborazione o per PdV non conforme sono notificati **entro 10 ggll** dalla data di "presa in carico"

- Risposta alla Richiesta di esibizione a norma (portale web o integrazione sicraweb)
  - Presa in carico immediata
  - Esito (email con link per download) entro la giornata lavorativa successiva
  - Notifica di eventuali anomalie **entro 2 ggll**

- Risposta alla Richiesta di assistenza o segnalazione (portale HDM)
  - Presa in carico del ticket (TT) **entro 3 ggll** (TT/anno)
  - Risposta alle richieste di informazioni entro **entro 3 ggll** dalla presa in carico
  - Risoluzione a guasto medio o lieve (parziale indisponibilità) **entro 5 ggll** dalla presa in carico
  - Risposta a guasti gravi (blocco o totale indisponibilità) **entro 2 ggll** con risoluzione nel minor tempo tecnicamente possibile

- Gestione dell'evento "Incident"[6] o "Data breach"[7]
  - Presa in carico (prima comunicazione) **entro il giorno lavorativo successivo**
  - Segnalazioni ai clienti **entro 3 ggll**
  - Chiusura dell'incident **entro 5 ggll**
  - **RTO**[8] (Recovery Time Objective) **1 giorno** lavorativo dalla identificazione dell'evento per riprendere le nuove elaborazioni e **3 giorni** per poter accedere ai dati già conservati al momento dell'evento/incident
  - **RPO**[9] (Recovery Point Objective), massimo **1 giorno**

- Disdetta o richiesta a mezzo PEC di disattivazione del Servizio (istanza) o di un'utenza
  - Presa in carico (eventuale contatto per integrazione documenti) **entro 5 ggll** dalla ricezione della PEC
  - Risposta e applicazione della richiesta **entro 5 ggll** dalla presa in carico (l'effettiva eliminazione dei dati dal sistema segue i tempi tecnici relativi all'attività specifica)

Cambiamenti e migliorie introdotti in seguito ad aggiornamenti delle modalità di funzionamento e fruizione dei servizi sono comunicati entro 30 giorni tramite aggiornamento del presente manuale e, se necessario, sono notificati via PEC alla casella istituzionale di ogni Cliente coinvolto.

In caso di interventi di manutenzione programmata che comportino l'indisponibilità (anche parziale) del servizio, il Conservatore avvisa ogni Cliente coinvolto scrivendo alla PEC istituzionale ovvero al riferimento tecnico indicato in fase di configurazione del servizio.

Il cliente vigila sul rispetto dei livelli di servizio concordati e sulla conformità delle attività eseguite dal Sistema. Maggioli spa rende disponibile su richiesta un account di audit utilizzabile da AgID o altro soggetto preposto per effettuare ogni tipo di verifica che si renderà necessaria sul sistema di conservazione.

Il cliente può inoltrare segnalazioni tramite la piattaforma Assistenza Clienti Maggioli di "issue tracking" che garantisce adeguata visibilità dei processi di ticketing e supporto.

[6] Incident (SGSI) – un evento anomalo, riscontrato nel periodo e nel perimetro di erogazione del servizio, tale da compromettere, anche solo temporaneamente (oltre gli SLA previsti), la disponibilità, l'integrità o la riservatezza dei dati conservati (RID).

[7] Violazione di sicurezza che comporta la sottrazione, l'accesso non autorizzato, la perdita o l'accidentale manomissione/danneggiamento di dati personali, che (non cifrati o pseudonimizzati) presentano per loro natura un rischio elevato per i diritti e le libertà delle persone fisiche.

[8] Tempo massimo necessario a rendere nuovamente disponibili i servizi di conservazione

[9] Tempo massimo indicante le elaborazioni (richieste o dati) che potrebbero essere irrimediabilmente compromesse

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405
Capitale sociale:
Euro 2.215.200
interamente versato

Qualunque altro soggetto debba interfacciarsi con il conservatore può scrivere una email a conservazione@maggioli.it o una PEC a conservatore@maggioli.legalmail.it .

torna al sommario

5.7 Trasferimento dati in conservazione

Il Conservatore attiva per il Cliente le istanze di conservazione ordinate e per ognuna di queste le "Descrizioni Archivistiche" (archivi) necessarie al Cliente. Ogni Descrizione Archivistica può essere alimentata in modalità manuale o automatica (integrazione applicativa), ma sempre sotto la Responsabilità del Produttore e secondo quanto riportato nelle Specifiche tecniche del Servizio e in questo Manuale.

Il Cliente e il Produttore definiscono come trasmettere in conservazione ogni flusso/tipologia documentale oggetto dell'incarico ovvero come raccogliere, inviare e verificare in conservazione gli elementi documentali del Cliente destinati alla conservazione digitale.

Nelle "specifiche tecniche" è descritto come il Sistema di conservazione riceve i dati (PdV) e le richieste, in modo che possa procedere alla loro corretta interpretazione, validazione ed elaborazione.

Sono rifiutati solo i PdV formalmente non validi per via di "tracciati" incompleti o corrotti, ma salvo questi "controlli IT" (*numero massimo di rifiuti previsti = 1*) **il Sistema di conservazione considera**

sempre validi i dati e le sintassi scelti dal Cliente
sempre conformi tutte le Unità Documentali trasmesse dal Produttore nei PdV.

L'attività della Persona o del Sistema (Produttore) incaricato dei versamenti in conservazione inizia dalla selezione e raccolta delle UD (Unità Documentali) da conservare e termina con l'elaborazione degli esiti della conservazione, secondo quanto definito tra Lui e il Cliente, Titolare degli oggetti da conservare.

torna al sommario

5.8 Selezione e raccolta delle UD da conservare

Le evidenze documentali ed i relativi registri e raccolte (fascicoli) sono formate dal Cliente come previsto dall'iter amministrativo specifico e dallo Stesso valorizzate, secondo quanto descritto da AgID nelle Linee Guida di riferimento (formazione, gestione e conservazione dei documenti informatici).

Il Produttore raccoglie gli elementi (le evidenze) documentali in Unità Documentali conformi ed efficaci allo scopo: dimostrare un fatto giuridicamente rilevante per il Cliente.

Ogni Unità Documentale è composta da

1. almeno un file-documento, che contiene le informazioni essenziali (forma e sostanza) a efficace descrizione del fatto
2. eventuali file-allegato, utili ad avvalorare con annotazioni o integrazioni quanto già contenuto nel documento, ovvero a perfezionare (validare e rendere giuridicamente perfetto ed efficace) l'azione o l'atto amministrativo descritto nel documento in oggetto (es. una ricevuta di avvenuta consegna)
3. file-metadati, utile alla valorizzazione/annotazione dei metadati di formazione (es. origine e provenienza), registrazione (es. segnatura) e gestione (es. soggetti)

A seconda della tipologia documentale in trattazione e sempre secondo la scelta del Cliente, che ne riporta i dettagli nel suo Manuale di gestione documentale:

i formati file utilizzati ed inviati in conservazione sono conformi all'allegato 2 delle LLGG AgID sulla formazione gestione e conservazione dei documenti informatici e a quanto indicato nel relativo capitolo di questo Manuale;

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405
Capitale sociale:
Euro 2.215.200
interamente versato

i Metadati di cui all'allegato 5 delle stesse LLGG possono essere conservati come allegato al documento a cui si riferiscono ovvero inseriti nella valorizzazione degli indici di conservazione concordati con il conservatore e riportati al capitolo corrispondente di questo manuale.

torna al sommario

5.9 Generazione PdV e gestione file cifrati

Il Cliente adotta una politica che norma e limita la conservazione agli elementi documentali, originali e completi, strettamente necessari con particolare attenzione a quelli destinati alla conservazione permanente o contenti dati personali, preparando con cura i piani di conservazione che definiscono quali tipologie di fascicoli, documenti e procedimenti debbano essere selezionati per la conservazione.

Il Produttore applica il principio della minimizzazione dei dati, quando crea gli strumenti di ricerca (indici di versamento) per la conservazione digitale, con particolare riguardo ai dati personali e a quelli "più sensibili", relativi alla salute, alla vita sessuale, alle opinioni politiche o ad altre categorie particolari di dati, oppure riguardanti le condanne penali, anche ricorrendo a pseudonimi o altri strumenti di cifratura o Anonimizzazione del dato.

File o porzioni di file (es. metadati) contenenti dati particolarmente critici o sensibili possono essere omessi oppure, se di interesse e quindi da conservare, possono essere cifrati attraverso opportuni strumenti applicativi a patto che, separatamente, siano consegnati in conservazione anche gli strumenti (istruzioni, software, dispositivi e chiavi) necessari a ricostruire il dato originale in caso di accesso o verifica.

torna al sommario

5.10 Caricamento PdV

Il Servizio di conservazione accetta solo dati raccolti e sottomessi al sistema in forma di PdV ovvero Pacchetti (informativi) di Versamento composti da un indice di versamento (file IdV) e file o gruppi di file destinati alla conservazione, raccolti come previsto dalla norma di riferimento in serie oppure fascicoli

L'incarico prevede che gli utenti abilitati, indicati dal Cliente (titolare dei dati da conservare), siano già formati e **competenti sulle fasi di formazione e gestione degli elementi documentali** che devono trasmettere in conservazione.

L'interfaccia web del servizio offre la possibilità di trasmettere dati in conservazione, guidando tramite apposito wizzard la formazione di Pacchetti di Versamento (PdV) idonei. In questo caso l'utente carica uno ad uno i documenti e i file (allegati) da conservare, imputando manualmente e per ogni documento tutti gli indici di conservazione necessari. Agli utenti abilitati è fornito apposito manuale utente, una sessione di formazione e un canale di assistenza specializzata.

L'integrazione applicativa standard prevede l'abilitazione di un canale SFTP, come descritto nelle "specifiche tecniche" del Servizio. Il Produttore trasferisce in conservazione i PdV da lui formati, implementando i necessari strumenti applicativi.

In fase di definizione dell'offerta il Cliente può richiedere altre modalità di integrazione applicativa ad esempio per adattarsi tramite strumenti ad hoc a iter di gestione e conservazione già consolidati.

Per ogni istanza di conservazione (AliasSP o tenant) si può indicare un unico sistema versante "predefinito" e questo determinerà il canale e il metodo di creazione dei PdV utilizzato abitualmente, non che le "regole di

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405
Capitale sociale:
Euro 2.215.200
interamente versato

sedimentazione" dei diversi elementi documentali nell'archivio digitale di deposito del cliente presso Maggioli spa. In ogni caso rimane sempre possibile integrare i dati conservati aggiungendo elementi in "modalità manuale", come anche richiedere di attivare un set di "Descrizioni Archivistiche" (AliasDA) dedicato ad una specifica lavorazione (es. migrazione dati pregressi), aggiuntiva e diversa rispetto al "canale" indicato come "sistema versante" in fase di attivazione.

Raccomandazioni per i trasferimenti di PdV in modalità applicativa

1) verificare di non settare/forzare le date dei file durante il trasferimento SFTP (alcune librerie lo prevedono come impostazione predefinita)
2) La SFTPAREA è un semplice canale di transito per i PdV formati dal Produttore, che spesso il sistema versante usa come "appoggio temporaneo" utile a gestire le proprie code di elaborazione e comporre i pacchetti di versamento previsti per la conservazione a norma.

Ogni sistema versante agisce per conto del Responsabile della gestione documentale del Cliente/Produttore, che deve verificare l'effettiva e completa raccolta e conservazione (non solo trasmissione) dei dati per i quali è prevista la conservazione; **in caso di mancato ritorno positivo entro 45 giorni dalla trasmissione dei dati/file da conservare, il sistema versante può considerare annullato o in errore il trasferimento in conservazione** e procedere di conseguenza.

L'elemento minimo trattato dal sistema di conservazione è il pacchetto informativo (PdV, PdA o PdD); il Sistema di conservazione prevede e traccia le interazioni degli utenti e dei sistemi con i singoli oggetti (documenti o record) conservati nei PdA, ma considera "fuori perimetro" i PdD già scaricati (eliminati) e i file afferenti a PdV non ancora presi in carico e validati (Rapporto di Versamento).

torna al sommario

5.11 Validazione dei PdV

Il Sistema di conservazione ammette nuovi PdV solo tramite i canali, cifrati SSH o HTTPS, indicati ai capitoli precedenti e solo se inoltrati ad "istanze attive".

Se il Tenant ha esaurito lo spazio richiesto (SLOT GB) oppure se ha superato la data limite dell'incarico (scadenza o proroga), il tenant risulta bloccato e il sistema rifiuta l'accettazione di nuovi PdV:

- in modalità SFTP sarà possibile accodare nuovi PdV che saranno presi in carico solo dopo un nuovo incarico ovvero rimossi dopo 60 giorni dalla loro creazione;
- in modalità HTTPS il sistema impedirà l'upload di nuovi PdV.

Rispetto al rapporto Cliente/Fornitore, quindi tra Soggetto Produttore e Soggetto Conservatore, le ultime LLGG AgID, partendo dal CAD e dal recente "Decreto Semplificazioni"[10], hanno riordinato e meglio definito gli aspetti organizzativi e tecnici dell'archivio corrente. Per questa ragione e **per non rischiare di entrare in contrasto con quanto definito dal cliente nel Suo Piano di gestione e conservazione documentale, il servizio di conservazione limita le verifiche sui PdV ricevuti a quanto tecnologicamente necessario ad elaborarli** e renderli poi disponibili al Cliente in PdA (Pacchetti di Archiviazione) correttamente conservati.

I controlli di validazione previsti sui PdV in ingresso sono

ID	Descrizione	Note
RdV.01	Validità (firme digitali e marche manche temporali dei file da conservare)	Disabilitato per impostazione predefinita
RdV.02	Numerazione (ordine, buchi e duplicazioni)	Disabilitato per impostazione predefinita

[10] (D.L. 76/2020), convertito con Legge n. 120/2020

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405
Capitale sociale:
Euro 2.215.200
interamente versato

RdV.03	Integrità (verifica hash calcolato vs "impronta" indicata dal Produttore in IdV)	Attivo
RdV.04	Pattern metadata	Formato campi data ('dd/MM/yyyy') Lunghezza campi stringa max. 240 caratteri
RdV.05	Formati (mime-type) ammessi in conservazione	Attivo

Sono rifiutati (Integrità) i file contenenti virus, macro o altri eseguibili e i file corrotti.
(la violazione di un controllo attivo comporta il rifiuto dell'intero PdV)

Le unità documentali, contenute in PdV rifiutati, sono rinviate in conservazione in nuovi PdV generati dal Produttore a valle della necessaria attività di bonifica.

Ultimo motivo di rifiuto dei PdV in ingresso, sono le richieste di elaborazione extra-soglia ovvero i PdV trasmessi al Sistema dopo la saturazione dello SLOT (GB) richiesto con l'incarico o superata la data di fine incarico; anche in questo caso i dati coinvolti dal rifiuto potranno essere elaborati trasferendoli in nuovi PdV, una volta sanata la questione amministrativa.

In ogni caso il Produttore deve verificare il corretto invio in conservazione dei PdV e di tutte le UD che deve conservare analizzando in dettaglio gli esiti (Rapporti di versamento) prodotti dal Sistema di conservazione come indicato nelle citate specifiche tecniche.

Per impostazione predefinita sono disabilitati blocchi e controlli legati ai vincoli archivistici, tranne nel caso di versamento di fascicoli chiusi (o archivi) e trasferiti completi e in un'unica soluzione.

torna al sommario

5.12 Gestione esiti di elaborazione

Gli esiti di elaborazione sono prodotti dal Sistema di conservazione nei termini riportati al capitolo degli SLA e nel formato reso disponibile nelle "specifiche tecniche" del Servizio.

Il Produttore raccoglie ed elabora gli esiti di conservazione in modo da

1) Fornire al Cliente e al Sistema di Gestione documentale le informazioni di conservazione (URI/URN, UID e Stato) necessarie a recuperare, esibire e gestire (es. scarto) l'evidenza originale conservata;
2) Gestire e bonificare le eventuali anomalie riscontrate in modo da allineare gli elenchi di evidenze prodotte rispetto a quelle correttamente conservate

torna al sommario

5.13 Archiviazione dei dati (PdA)

I PdV ammessi sono archiviati nel sistema di conservazione in forma di PdA, quanti necessari, ognuno di massimo 4 GB o 20'000 documenti. Ogni Pacchetto di Versamento il Pacchetto di Archiviazione è composto da

- ✓ i file-documento e file-allegato trasmessi dal Produttore
- ✓ il file IdC (indice di conservazione UNISinsCRO), firmato in digitale dal Conservatore, completo di marca temporale e dei metadati (informazioni) di conservazione previsti da AgID
- ✓ un file "external-metadata" che riporta gli indici di conservazione indicati dal Produttore (IdV)
- ✓ l'eventuale file-metadati trasmesso dal Produttore e contenente le informazioni (metadati) di formazione, registrazione e gestione di cui all'allegato 5 alle LLGG AgID di riferimento.

I file XML formati dal Sistema di conservazione sono sempre corredati dal relativo XSD e sono descritti nelle specifiche tecniche del Servizio.

Per impostazione predefinita tutti i PdA e tutti gli oggetti in essi raccolti sono archiviati all'interno del sistema di conservazione, in storage (partizioni o archivi) virtuali logicamente riservati al Servizio ed isolati dagli altri sistemi. In fase di definizione dell'offerta il cliente può richiedere per alcuni o per tutti i suoi flussi di conservazione l'utilizzo di storage diversi, anche remoti o cifrati, purché localizzati all'interno del territorio

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405
Capitale sociale:
Euro 2.215.200
interamente versato

nazionale, se destinati a contenere dati personali di cittadini italiani oppure documenti della Pubblica Amministrazione italiana.

I file IdC (indice di conservazione) e RdV (Rapporto di Versamento) prodotti dal Sistema sono sempre inclusi nei PdA estratti, ma sono resi disponibili singolarmente, tramite portale web, al Cliente e a tutti gli operatori (Conservatore e Produttore) coinvolti per le dovute verifiche e le altre attività di competenza.

torna al sommario

5.14 Accesso agli archivi

Gli utenti abilitati, indicati dal Cliente, ricevono le credenziali, personali e non cedibili, necessarie ad accedere con pari profilo e privilegi rispetto al Responsabile di conservazione agli elementi documentali conservati. Ogni altro accesso, fatti salvi quelli operati dalle autorità preposte o dai referenti del Conservatore per le attività previste dal Servizio, sono sempre mediati dal **Cliente** (es. procedura di accesso agli atti) che dispone le opportune misure organizzative e le soluzioni tecnologiche necessarie.

Il Cliente, che detiene parte dei propri fondi documentali nel sistema di conservazione di Maggioli spa, può ricorrere all'integrazione applicativa (API – vedere specifiche tecniche) al fine di abilitare il proprio Sistema di Gestione Documentale o uno strumento dedicato (es. un portale) alla ricerca ed esibizione diretta dei documenti e dei fascicoli nel sistema di conservazione; in questo caso il Produttore potrà disporre di una platea di utenti potenzialmente illimitata, purché identificati ed autenticati come da norma (es. SPID) e tracciando nel proprio SGD o IAM l'attività di questi Soggetti (terzi), anche interni al Produttore Stesso.

torna al sommario

5.15 Produzione duplicati e copie informatiche (PdD)

Gli utenti abilitati, indicati dal Cliente, possono accedere al sistema di conservazione e, seguendo le istruzioni riportate nel "Manuale utente", scaricare i singoli file conservati ovvero richiedere e scaricare un Pacchetto di Distribuzione (PdD), utile per l'esibizione a norma dei documenti informatici conservati.

Il PdD è un file (archivio compresso) formato come aggregazione di PdA e limitato agli elementi documentali selezionati in fase di Richiesta; contiene tutti gli indici e solo i file documento selezionati.

torna al sommario

5.16 Gestione dell'obsolescenza tecnologica (riversamento)

Ognuno per competenza monitora le proprie infrastrutture e sistemi.

Le specifiche di formazione dei documenti e dei PdV evolvono nel tempo a seconda delle indicazioni normative e delle prassi di riferimento:

il Cliente comunica le variazioni proposte al Conservatore che dispone le procedure necessarie;

allo stesso modo il Conservatore può notificare al Cliente le unità documentali a rischio di obsolescenza tecnologica (es. formati file non più "conservabili"), indicando al Cliente la possibile procedura di rientro (es. riversamento).

Altre variazioni IT (infrastrutturali) o procedurali che dovessero avere impatto sulle attività o sui trattamenti previsti per il Servizio sono comunicati tra le parti con preavviso di 6 mesi rispetto alla loro entrata in vigore.

torna al sommario

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.215.200
interamente versato

5.17 Conversioni e riversamenti

Il Sistema di conservazione digitale, salvo che nelle attività disposte dall'antivirus, non altera mai i dati conservati (l'impronta HASH dei file rimane invariata rispetto a quella registrata al momento del versamento in conservazione).

Ogni conversione o nuova versione (es. correzione) dei file o dei documenti conservati è rinviata dal Produttore in conservazione in PdV successivi; in caso di necessità o per sostituire una UD già conservata il cliente può richiedere a mezzo PEC la cancellazione puntuale di UD o interi PdA già in conservazione.

torna al sommario

5.18 Eliminazione dei dati conservati

I dati conservati posso essere eliminati in 3 circostanze:

1. Cessazione del rapporto (istanza) di conservazione
2. Richiesta eliminazione UD da parte del Cliente
3. Scarto d'archivio

L'eliminazione dei dati conservati non comporta storni o riaccrediti al conteggio dei GB versati (SLOT-GB) nell'istanza di conservazione attivata

torna al sommario

5.18.1 Cessazione del rapporto e restituzione asset al Titolare

Esauriti i termini temporali previsti dalla fornitura e dall'incarico, il Cliente ha 3 mesi di tempo per scaricare i dati conservati, procedendo autonomamente alla creazione dei PdD necessari oppure esportando i singoli PdA conservati (le istruzioni di dettaglio sono riportate nel manuale utente) direttamente dal portale web del servizio.

In alternativa ed entro lo stesso termine, il Cliente può richiedere (ordinare) l'esportazione massiva dei dati conservati e in questo caso Maggioli spa attiva una SFTPAREA dedicata all'istanza da eliminare in cui trasferisce i PdA conservati per conto del Cliente; i dati oggetto di esportazione massiva rimangono disponibili in SFTPAREA per massimo 6 mesi e poi sono eliminati.

Esaurito il periodo previsto per lo scarico dei dati, il processo di cessazione prosegue con l'eliminazione dell'istanza di conservazione dal Sistema, cancellando tutti i PdA conservati e i dati (record) relativi.

torna al sommario

5.18.2 Eliminazione UD conservate

Il Responsabile della conservazione del Cliente può chiedere la cancellazione puntuale di UD conservate;

la richiesta (PEC inviata a conservatore@maggioli.legalmail.it) consiste in un allegato pdf completato di firma digitale e contenente i riferimenti univoci degli Oggetti da eliminate (UID) e almeno un parametro di controllo (PID, data conservazione o altro).

Il conservatore può chiedere ulteriori dettagli o conferme via email o telefonicamente ovvero procedere direttamente all'esecuzione dell'operazione richiesta.

La richiesta è conservata nei carteggi relativi al rapporto e portata in annotazione al processo di eliminazione avviato dal Conservatore.

Il Processo di cancellazione di singole UD comporta la "ri-conservazione" del PdA impattato dalla richiesta di modifica, operazione che genera un nuovo Volume/PdA privo degli oggetti eliminati, definitivamente rimossi, ma corredato dal IdC originale e completo del PdA modificato.

torna al sommario

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.215.200
interamente versato

5.18.3 Procedura di Selezione e scarto di archivio

Da eseguirsi anche in conformità a quanto disposta dall'art.21 del Codice sui Beni Culturali.

Conformemente alle citate LLGG, tutti gli elementi documentali (documenti o fascicoli) a conservazione LIMITATA (temporanea) sono trasferiti in conservazione recanti indicazione del tempo massimo di mantenimento previsto in archivio digitale di deposito (retention);

Se non diversamente indicato dal Cliente, tutti gli oggetti trasmessi in conservazione digitale sono considerati "a conservazione PERMANENTE" (retention = '9999');

Quando nel relativo campo (indice) di conservazione è indicata una retention inferiore, il sistema di Conservazione confronta quel termine con la data di riferimento per l'elemento documentale in conservazione e ne riporta gli estremi un file "indice proposta di scarto" trasmesso automaticamente via email alla Persona indicata come Responsabile di conservazione dell'Organizzazione Titolare dell'istanza di conservazione coinvolta e rinviandone a quest'ultimo la puntuale verifica.

Il Cliente, seguendo la propria procedura di selezione e scarto d'archivio, redige un proprio elenco definitivo degli oggetti documentali (già versati in archivio storico; relativi a procedimenti conclusi da oltre 25 anni; ecc.) da eliminare e ne trasmette richiesta a mezzo PEC al Conservatore (o ai suoi conservatori) di riferimento.

Il Titolare (Responsabile di Gestione documentale dell'Organizzazione Titolare) riporta nel suo Manuale di gestione e conservazione documentale la "DESTINAZIONE FINALE" di ogni evidenza documentale prodotta o registrata presso la Sua Organizzazione, in accordo al Massimario di scarto dell'Organizzazione stessa. Questo indica per ogni elemento documentale tempi di conservazione e destinazione finale ovvero come e quando l'elemento documentale cessa di essere di interesse per il Cliente e viene eliminato ovvero trasferito anche per titolarità ad altro soggetto istituzionale preventivamente individuato (es. Archivi centrali dello stato).

Le Unità Documentali per le quali NON è richiesta la cancellazione o lo scarto, sono mantenute in conservazione fino al termine dell'incarico

torna al sommario

5.19 Tracciatura delle attività eseguite

Le registrazioni di accessi, processi e attività riguardanti ogni istanza o oggetto in conservazione sono conservate automaticamente in una apposita descrizione archivistica (LogDiSistema) attivata per default in ogni istanza.

Questi log registrano l'utente (alias + IP) che ha richiesto l'azione, il momento (data-ora), l'oggetto di conservazione impattato (Istanza, Record o UD), la tipologia di attività eseguita e l'esito (OK o ERRORE con dettaglio).

torna al sommario

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.215.200
interamente versato

5.20 Verifica dell'integrità degli archivi (verifiche periodiche)

Ogni responsabile per il Sistema di propria competenza verifica nel tempo la conformità e la validità degli archivi che gestisce:

il Produttore (incaricato) verifica per le Serie e le Raccolte da conservare il loro effettivo esito in conservazione e ne trasmette gli estremi di conservazione al sistema di gestione documentale del Cliente;

Il Cliente (vigilando) verifica l'effettiva e continuata conformità ed erogazione del Servizio

- All'avvio di ogni nuovo "flusso" di versamento in conservazione o in caso di modifica a flussi già attivati, il cliente verifica la coerenza di quanto conservato rispetto all'esito atteso per il processo di invio in conservazione (composizione delle UC e correttezza per forma e contenuto delle informazioni "indici di conservazione");
- Periodicamente, su alcuni oggetti a campione per ogni flusso, la corrispondenza al contesto reale delle proprie procedure di ricerca ed esibizione dei dati conservati;
- Periodicamente e a chiusura delle "code" di versamento in conservazione delle diverse serie e raccolte, la coerenza delle quantità e degli estremi di registrazione degli oggetti destinati alla conservazione.

il Conservatore (incaricato) monitora i PdA conservati e periodicamente ne verifica disponibilità, integrità, intellegibilità e validità

- verificando e in caso rettificando la validità delle firme digitali e delle marche temporali apposte agli IdC;
- confrontando le impronte HASH registrate in IdC, rispetto a quelle ricalcolate sui dati in archivio
- visualizzando dei documenti a campione, in occasione delle sessioni di supporto, assistenza o audit con il Cliente;
- nella gestione dell'obsolescenza tecnologica dei formati file in conservazione.

Se si evidenziano delle anomalie nelle verifiche del Produttore o del Cliente, entro il periodo di validità dell'incarico, queste sono sanate dal Produttore con nuovi invii in conservazione.

Se si evidenziano delle anomalie nelle verifiche del Conservatore, questi procede a sanarle in autonomia, informando il Cliente o il Produttore, solo in caso in cui sia necessario un loro intervento (es. riversamento).

Se l'anomalia è causata da malfunzionamenti o disservizi ascrivibili a Maggioli spa, la quota di SLOT-GB utilizzata nella bonifica dell'anomalia è accreditata all'istanza di conservazione a titolo gratuito e per tutta la durata dell'incarico. N.B. - Le anomalie determinate da eventi non dipendenti dal Conservatore (v. Matrice responsabilità) saranno gestite entro i limiti e le quantità previste dall'incarico ovvero attraverso un incarico "ad integrazione" disposto all'uopo dal Cliente.

torna al sommario

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405
Capitale sociale:
Euro 2.215.200
interamente versato

6 Configurazione del Sistema (il Soggetto Produttore)

L'attivazione prevede la definizione di un Soggetto Produttore (AliasSP) per ogni Cliente e per ogni Suo Sistema "Produttore" di gestione documentale, Versante; questo porta al fatto che, se un'Organizzazione utilizza 3 diversi sistemi documentali (es. segreteria, area02 e area03), questa avrà almeno 3 istanze attive nel sistema di conservazione digitale, ognuna dedicata ai flussi documentali di ogni Ufficio, Area o Sistema "sorgente".

Ogni Soggetto Produttore può essere il "coordinatore" di Soggetti Produttori "figli", che ereditano le medesime regole e strutture, ognuno con propri riferimenti (Persone/Ruoli) e limiti contrattuali.

Per ogni Tenant di conservatore o Soggetto Produttore è necessario individuare almeno

- il Responsabile della conservazione (presso il cliente)
- il Sistema versante (IP, Denominazione e Fornitore)
- un riferimento tecnico per il servizio (presso il cliente)
- Gli utenti abilitati al sistema di conservazione
- Dimensionamento (SLOT GB)
- Durata del servizio
    - data inizio versamenti
    - data inizio documenti (dati pregressi da conservare)
    - data fine versamenti
    - eventuale periodo di mantenimento (retention) dei dati conservati
- Definizione delle Descrizioni Archivistiche che saranno utilizzate per la conservazione digitale

torna al sommario

6.1 Descrizioni Archivistiche

La Descrizione Archivistica (AliasDA) raccoglie e rappresenta un set di regole che si applicano ad una "porzione" specifica dell'archivio digitale di deposito, in conservazione digitale, dedicato e come indicato dal Cliente per la sua istanza (Tenant o SP) di riferimento ed eventualmente limitato ad una **tipologia documentale** specifica.

Il Servizio di conservazione digitale di Maggioli spa prevede 2 Descrizioni Archivistiche principali, da cui il Cliente può scegliere di derivare quelle che andranno a definire i Suo Archivio digitale di deposito

1) Documenti [CAD2018-DOCUMENTI-v3]
2) Raccolte [CAD2018-FASCICOLI-v3]

dove il suffisso V3 rappresenta la III° versione degli indici di conservazione (ex metadati) proposti da Maggioli spa per il Servizio (per i dettagli e le versioni precedenti vedere l'allegato "indici di conservazione").

Documenti informatici e documenti amministrativi informatici condividono in conservazione le medesime "regole di ingaggio", dove per ogni "flusso di conservazione" (tipologia documentale o classificazione) il Cliente decide come comporre la singola Unità (o elemento) Documentale o più semplicemente UD.

Documenti e Fascicoli conservati sono ricercabili per DATA DOCUMENTO e utilizzando gli altri indici di conservazione previsti, compilati in fase di versamento dal Produttore in base a sue proprie regole non necessariamente note al conservatore o allineate alle sintassi proposte da Maggioli spa in questo Manuale.

torna al sommario

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.215.200
interamente versato

6.2 Conservazione di documenti

Si tratta di **Documenti consolidati** (definitivi, non bozze), resi "immodificabili" e quindi trasmessi al sistema di conservazione; rientrano in questa categoria

- Documenti informatici e Documenti amministrativi informatici
- Registri, Repertori e "Libri" (Elenchi di annotazioni o registrazioni)
- Flussi informativi (stream)

È il Cliente che decide come formare ogni UD-Documento ovvero di quanti e quali file debba essere composta per essere giuridicamente perfetta, efficace ed opponibile a terzi in caso di necessità; ad esempio una comunicazione in uscita (allegato), trasmessa a mezzo PEC, potrebbe corrispondere ad una UD composta da

- Metadati UD
  - Documento inviato
  - Ricevuta PEC di accettazione (o non accettazione)
  - Ricevuta PEC di consegna (o di mancata consegna)
- Oppure potrebbe essere composta solo dalla ricevuta di consegna PEC completa, accompagnata dai suoi metadati

La scelta dipende dal cliente e dal sistema di gestione documentale che utilizza, quindi varia a seconda di come archivia i dati nel Suo sistema di gestione documentale, versante.

torna al sommario

6.3 Conservazione di fascicoli

Si tratta di Raccolte ovvero dell'azione amministrativa o di archivio che unisce in un corpo/elemento documentale unico, diverse Unità Documentali che concorrono al raggiungimento del medesimo obbiettivo.

Rientrano in questa categoria

- Fascicoli di affare
- Fascicoli di attività
- Fascicoli di Procedimento (amministrativo)
- Fascicoli di Persona Fisica
- Fascicoli di Persona Giuridica
- Archivi e Database

Le Raccolte devono essere trasmesse in conservazione digitale entro un anno dalla loro chiusura e almeno annualmente anche i fascicoli informatici aperti e le pratiche ancora in trattazione, tramite la conservazione dei documenti che li compongono.

È raccomandato che la conservazione dei fascicoli di procedimento aperti preveda anche il trasferimento annuale in conservazione della "camicia" del fascicolo: un "file-fascicolo", XML sottoscritto in digitale, che riporta le informazioni minime previste da AgID e l'elenco e le coordinate di archivio delle UD, già conservate o meno, raccolte fino a qual momento specifico.

Salvo diversa indicazione il processo di conservazione opera in "conservazione anticipata" ovvero sono attesi in conservazione i documenti del fascicolo "appena consolidati" e solo in seguito il file-fascicolo, prodotto ed inviato in conservazione secondo le politiche del Cliente/Produttore;

in altre circostanze il conservatore riceve fascicoli già formati, chiusi e consolidati: in questo caso il processo di conservazione alimenta il Sistema con 1 un fascicolo per ogni "pacchetto" o Volume ricevuto, archiviando ogni documento o sotto-fascicolo nella descrizione archivistica a cui appartiene.

torna al sommario

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405
Capitale sociale:
Euro 2.215.200
interamente versato

6.4 Metadati, indici di conservazione

Come anticipato il Cliente forma Unità Documentali già conformi: complete dei file necessari alla composizione di documenti informatici giuridicamente perfetti (efficaci) e corredate dei metadati (di formazione, e gestione) propri del contesto di riferimento: Gestione documentale, amministrativa o contabile, corrente.

Il Produttore trasferisce al Sistema di Conservazione le Unità documentali raccolte sul sistema del Cliente e le valorizza con le informazioni "indici di conservazione", utili al Cliente per correlare e reperire gli elementi documentali nel sistema di conservazione

Il Conservatore aggiunge a questi i metadati di conservazione previsti dallo standard UNISinCRO che, firmato e marcato dal conservatore, va a comporre l'indice di conservazione (IdC) necessario per l'esibizione legale a norma dei documenti informatici conservati.

Gli indici in conservazione sono concordati tra Cliente e Conservatore:

- in questo capitolo si riportano le strutture proposte dal Conservatore per la valorizzazione degli "indici in conservazione" di UD-Documento e UD-Fascicolo
- il Produttore verifica con il Cliente e con il Conservatore la struttura proposta e indica per ogni flusso le eventuali variazioni necessarie per il contesto o la tipologia documentale di riferimento
- il Cliente verifica che quanto definito sia coerente con le disposizioni del proprio Piano di gestione e conservazione documentale, riportandovi in dettaglio e per ogni flusso le specifiche di formazione dei PdV e della loro trasmissione in conservazione (composizione, raccolta, versamento)

Nelle specifiche tecniche del Servizio sono disponibili maggiori dettagli, anche in riferimento alle versioni precedenti delle medesime strutture di valorizzazione dati che nel tempo si sono succedute.

torna al sommario

6.4.1 Indici del documento informatico o amministrativo informatico

1. **UFFICIO_RESPONSABILE** (*Soggetto Produttore, Titolare, Archivio*) del documento presso il Soggetto Produttore al momento del trasferimento in conservazione.
   - Formato: Stringa-composta(250) [codice AOO Soggetto Produttore " ; " *Codice iPA* Soggetto Produttore " ; " Denominazione ufficio o *AOO* (se disponibile)]

2. **INDICE_CLASSIFICAZIONE** (*Titolario*) dal piano di classificazione del Soggetto Produttore, indicare TITOLO e CLASSE del documento.
   - Formato: Stringa-composta(250) [*Titolo* (numero "." testo esteso) " - " *Classe* (numero "." testo esteso)]

3. **TIPOLOGIA_DOCUMENTARIA** (*Fattispecie archivistica*) specifica all'interno della classe o sottoclasse di classificazione del documento presso il Soggetto Produttore.
   - Formato: Stringa(250).

4. **DATA_REGISTRAZIONE** è il *RIFERIMENTO TEMPORALE* relativo alla registrazione del documento nell'archivio (repertorio, registro, ecc) del Soggetto Produttore.
   - Formato: DATA(dd/MM/yyyy)

5. **NUMERO_REGISTRAZIONE** è il *CODICE IDENTIFICATIVO del documento nell'archivio (repertorio, registro, ecc) corrente presso il soggetto Produttore*.
   - Formato: Stringa(250).

6. **ID_UNIVOCO_PERSISTENTE** è il codice *Identificativo univoco e persistente* del documento valido all'interno di tutti i fondi archivistici del Soggetto Produttore. Può essere un *URI*.
   - Formato: Stringa(250) [codice di registrazione del documento nell'archivio, repertorio, registro, ecc, del SP]

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405
Capitale sociale:
Euro 2.215.200
interamente versato

7. **TRASMITTENTE** indica la *PERSONA (operatore) o SISTEMA (versante)* che esegue il trasferimento della UD in conservazione per conto del Soggetto Produttore.
   - Formato: Stringa(250)

8. **IMPRONTA** è *l'Impronta HASH* del (1°) file che compone la UD/Documento formata dal SP.
   - Formato: HASH(hex/sha256)

9. **VERSIONE** indica la *versione del documento* all'interno del sistema di conservazione.
   - Formato: Stringa(50)

10. **RESPONSABILE_UO**: *PERSONA, che ha in carico il documento* al momento della messa in conservazione, Responsabile dell'***UFFICIO_RESPONSABILE*** o del *singolo procedimento*.
    - Formato: Stringa-composta(250, persona)

11. **ID_FASCICOLO** è il codice *Identificativo univoco e persistente* del *FASCICOLO* registro, repertorio o serie a cui appartiene la UD trasmessa nel momento di ***DATA_REGISTRAZIONE***
    - Formato: Stringa-composta(250) [come da *Piano di fascicolazione* del SP oppure Codice titolo "." Codice classe ("/" eventuale sotto-classe "." eventuale *Serie*) "." Numero *fascicolo* ("/" eventuale sottofascicolo) "_" ANNO]

12. **OGGETTO** reca un'*indicazione sintetica del contenuto/scopo del DOCUMENTO* (non deve contenere informazioni/dati personali, sensibili). Metadato funzionale a riassumere brevemente il contenuto del documento o comunque a chiarirne la natura.
    - Formato: Stringa(250) [Vedere raccomandazioni AURORA, Università Padova, eventuale normazione specifica, ulteriori limitazioni alla specifica Descrizione Archivistica]

13. **DATA_CHIUSURA** è un RIFERIMENTO TEMPORALE che *rappresenta la prima "DataCerta"* della UD ovvero che a seconda del contesto e con mezzo idoneo (marcatura temporale, registrazione a protocollo, trasmissione a mezzo PEC, ecc) attesta il momento di formazione, chiusura, registrazione, consolidamento o perfezionamento della UD corrispondente a ***IMPRONTA***.
    - Formato: Data(dd/MM/yyyy)

14. **RIFERIMENTI_ESTERNI**: *SOGGETTI e Organizzazioni* non appartenenti al Soggetto Produttore e coinvolti nell'iter di gestione del documento (*mittente*, *destinatari/io*, *controparte*/i, ecc).
    - Formato: Stringa-MultiValore

15. **ALTRI_RIFERIMENTI**: *PERSONE o **altri dettagli aggiuntivi*** a seconda della descrizione archivistica selezionata per il flusso (es. *firmatario/i, CIG, documenti precedenti o susseguenti, numero fattura*, ecc).
    - Formato: Stringa-MultiValore

Gli ultimi 2 sono "campi multi-valore" che è possibile ripetere tante volte quanto necessario a valorizzare correttamente i dati.

N.B. – Per includere negli indici di conservazione anche altre informazioni, relative alle fasi di formazione e gestione (es. dai metadati di cui all'allegato 5 delle LLGG AgID di riferimento), è possibile concordarne di diversi ovvero modificarne, in accordo tra Cliente e Produttore, le regole di compilazione.

torna al sommario

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405
Capitale sociale:
Euro 2.215.200
interamente versato

6.4.2 Indici del fascicolo informatico

1. **UFFICIO_RESPONSABILE** (*Soggetto Produttore, Titolare, Archivio*) dell'ufficio o settore che per ultimo ha avuto in carico il fascicolo (o il procedimento) aperto o che ne ha completato la chiusura.
   - Formato: Stringa(250)

2. **INDICE_CLASSIFICAZIONE** (*Titolario*) dal piano di classificazione del Soggetto Produttore, indicare TITOLO e CLASSE del documento.
   - Formato: Stringa-composta(250) [*Titolo* (numero "." testo esteso) " - " *Classe* (numero "." testo esteso) eventuale "." e numero dell'eventuale *sottoclasse* a cui appartiene il fascicolo]

3. **ID_FASCICOLO** è il codice *Identificativo univoco e persistente del FASCICOLO*, valido all'interno di tutti i fondi archivistici del Soggetto Produttore. Può essere un *URI*.
   - Formato: Stringa-composta(250) [come da Piano di fascicolazione del SP oppure Codice titolo "." Codice classe ("/" eventuale sotto-classe "." eventuale Serie) "." *Numero fascicolo* ("/" eventuale *sottofascicolo*) "_" *ANNO*]

4. **VERSIONE** indica la *versione della UD* all'interno del sistema di conservazione.
   - Formato: Stringa(50)

5. **IMPRONTA** è *l'Impronta HASH* del (1°) file che compone la UD/Fascicolo formata dal SP.
   - Formato: HASH(hex/sha256)

6. **DATA_APERTURA** è un *RIFERIMENTO TEMPORALE* che *rappresenta la data di* chiusura/registrazione del primo documento contenuto nel fascicolo.
   - Formato [data: dd/MM/yyyy]

7. **DATA_CHIUSURA** (SOLO PER I *FASCICOLI CHIUSI*) è un RIFERIMENTO TEMPORALE che *rappresenta la data di* chiusura/registrazione dell'ultimo documento conclusivo o la data del documento che *conclude il rispettivo procedimento amministrativo*.
   - [data: dd/MM/yyyy]

8. **RETENTION** , come da *massimario di scarto* del SP, indica il numero di anni a decorrere da "DATA_CHIUSURA", dopo i quali si potrà valutare l'eventuale scarto dei fascicoli e dei relativi documenti conservati (Indicare "0" per un fascicolo a conservazione perenne).
   - Formato: Stringa(50)

9. **OGGETTO** (*Oggetto del fascicolo* o *soggetto passivo del procedimento*) riporta lo *scopo/contenuto/natura del fascicolo* o dei documenti in esso contenuti nel caso dei sottofascicoli.
   - Formato: Stringa(250)

10. **RPA** (*Responsabile del Procedimento Amministrativo*) è il Direttore responsabile della UOR al momento della messa in conservazione del fascicolo oppure il Funzionario responsabile che ha in carico il procedimento o la corretta formazione e gestione del fascicolo. Ogni qualvolta cambia il RPA il fascicolo informatico deve essere immediatamente trasferito per competenza al nuovo responsabile del procedimento dell'amministrazione che ha aperto il fascicolo.
    - Formato: Stringa-composta(250, persona)

11. **TRASMITTENTE** indica la *PERSONA (operatore) o SISTEMA (versante)* che esegue il trasferimento della UD in conservazione per conto del Soggetto Produttore.
    - Formato: Stringa(250)

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405
Capitale sociale:
Euro 2.215.200
interamente versato

12. **AOO PARTECIPANTI** (Alte Amministrazioni o *Organizzazioni*, di altra AOO), diverse dal Soggetto Produttore che trasmette in conservazione il fascicolo, che hanno collaborato alla formazione del fascicolo stesso (ad esempio se contiene Protocolli provenienti da altri Enti; se il procedimento prevede la *cooperazione* o evidenze di strutture diverse; ecc)
    - Formato: Stringa-MultiValore

13. **RIF_DOCUMENTI** è l'elenco di *UID di conservazione* (o ID_DOCUMENTO) dei documenti conservati e appartenenti al fascicolo
    - Formato: Stringa-MultiValore

14. **RIF_ESTERNI** è l'elenco di UID di conservazione (o ID_DOCUMENTO) dei documenti conservati non appartenenti al fascicolo, ma *correlati* ad esso, ad esempio come allegati non parte integrante ai documenti dell'elenco **RIF_DOCUMENTI**
    - Formato: Stringa-MultiValore

Gli ultimi 3 sono "campi multi-valore" che è possibile ripetere tante volte quanto necessario a valorizzare correttamente i dati.

N.B. – Per includere negli indici di conservazione anche altre informazioni, relative alle fasi di formazione e gestione (es. dai metadati di cui all'allegato 5 delle LLGG AgID di riferimento), è possibile concordarne di diversi ovvero modificarne, in accordo tra Cliente e Produttore, le regole di compilazione.

torna al sommario

6.5 Formati file ammessi in conservazione

Il Cliente definisce per ogni tipologia documentale i formati file idonei alla sua trattazione in gestione corrente e quali deve assumere per poter essere correttamente conservato; alcuni "file" sono formati o registrati nel sistema di gestione documentale già in formato idoneo alla conservazione, mentre altri saranno conservati solo una volta che saranno stati convertiti (riversamento) dal Cliente/Produttore che li raccoglie e trasmette al conservatore.

I formati file che sono in generale da preferire nelle fasi di gestione e conservazione documentale sono quelli indicati da AgID nell'allegato 2 alle LLGG di riferimento; ogni Cliente e ogni tipologia documentale ha però esigenze diverse e peculiari: **il conservatore propone in un allegato specifico (Formati di conservazione) i formati file ammessi dal Sistema di conservatore**; il Cliente definisce quali usare per ogni flusso e lo comunica al Produttore, proponendo al Conservatore la necessità di eventuali variazioni o integrazioni.

L'invio in conservazione di file in formato diverso da quelli previsti comporta il rifiuto dell'intero PdV, che dev'essere quindi ripreso in carico dal Produttore per le conseguenti attività di bonifica e rinvio.

torna al sommario

7 Istruzioni e strutture dati di riferimento

Per tutto quanto non qui riportato, si rimanda al Manuale utente e alle Specifiche tecniche del servizio in allegato a questo Manuale e quindi alle LLGG AgID di riferimento e relativi allegati.

torna al sommario

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.215.200
interamente versato

Manuale della Conservazione

di InfoCert S.p.A.

InfoCert
TINEXTA GROUP

REGISTRO DELLE VERSIONI

N° versione	Data emissione	Modifiche apportate
01	Luglio 2014	Prima versione
02	Novembre 2015	Utilizzo dello schema proposto da AgID
03	Febbraio 2016	Correzioni formali e di layout
04	Marzo 2016	Correzioni formali e di layout
05	Settembre 2017	Glossario, Normativa, Mission, Comunità di riferimento, Riferimenti a policy aziendali interne
05.1	Novembre 2017	Specificità del contratto
06	Luglio 2018	Normativa GDPR, semplificazione glossario e nuovi Responsabili
07	Gennaio 2019	Nuovo logo aziendale
08	Maggio 2019	Nuovo Responsabile sistemi
09	Ottobre 2020	Glossario, nuovi Responsabili, aggiornamento procedure di monitoraggio, semplificazione delle Specificità del contratto
10	Novembre 2020	Ampliamento servizi di storage

INDICE DEL DOCUMENTO

1. SCOPO E AMBITO DEL DOCUMENTO

Il presente documento è il Manuale della Conservazione di InfoCert S.p.A. (Società soggetta a direzione e controllo di TecnoInvestimenti S.p.A.), ai sensi del Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'Amministrazione Digitale di cui al decreto legislativo n. 82 del 2005 pubblicato in GU Serie Generale n.59 del 12-3-2014 - Suppl. Ordinario n. 20.
Il Manuale della Conservazione 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 utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.
In caso di ispezione da parte delle autorità di vigilanza preposte, il Manuale della Conservazione permette un agevole svolgimento di tutte le attività di controllo.

Torna al sommario

2. TERMINOLOGIA (GLOSSARIO, ACRONIMI)

TERMINE	DEFINIZIONE
ACCESSO	Operazione che consente di prendere visione dei documenti informatici.
AFFIDABILITÀ	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.
AGGREGAZIONE DOCUMENTALE INFORMATICA	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.
ARCHIVIO	Complesso dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività.
ARCHIVIO INFORMATICO	Archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche.
AREA ORGANIZZATIVA OMOGENEA	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.
ATTESTAZIONE DI CONFORMITÀ DELLE COPIE PER IMMAGINE SU SUPPORTO INFORMATICO DI UN DOCUMENTO ANALOGICO	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.
AUTENTICITÀ	Caratteristica 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.
CERTIFICAZIONE	Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi.
CLASSIFICAZIONE	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.
CLOUD DELLA PA	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.
CODEC	Algoritmo di codifica e decodifica che consente di generare flussi binari, eventualmente imbustarli in un file o in un *wrapper* (codifica), così come di estrarli da esso (decodifica).
CONSERVATORE	Soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici.
CONSERVAZIONE	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti

CONVENZIONI DI DENOMINAZIONE DEL FILE	Insieme di regole sintattiche che definisce il nome dei file all'interno di un filesystem o pacchetto.
COORDINATORE DELLA GESTIONE DOCUMENTALE	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.
DESTINATARIO	Soggetto o sistema al quale il documento informatico è indirizzato.
DIGEST	Vedi Impronta crittografica.
DOCUMENTO AMMINISTRATIVO INFORMATICO	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
DOCUMENTO ELETTRONICO	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva
DOCUMENTO INFORMATICO	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
DUPLICATO INFORMATICO	Vedi art. 1, comma 1, lett) i quinquies del CAD.
ESEAL	Vedi sigillo elettronico.
ESIBIZIONE	operazione che consente di visualizzare un documento conservato
ESIGNATURE	Vedi firma elettronica.
ESTRATTO DI DOCUMENTO INFORMATICO	Parte del documento tratto dal documento originale
ESTRATTO PER RIASSUNTO DI DOCUMENTO INFORMATICO	Documento nel quale si attestano in maniera sintetica fatti, stati o qualità desunti da documenti informatici.
ESTRAZIONE STATICA DEI DATI	Estrazione di informazioni utili da grandi quantità di dati (es. database, datawarehouse ecc…), attraverso metodi automatici o semi-automatici
EVIDENZA INFORMATICA	Sequenza finita di *bit* che può essere elaborata da una procedura informatica.
FASCICOLO INFORMATICO	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.
FILE	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.
FILE CONTAINER	Vedi Formato contenitore.
FILE WRAPPER	Vedi Formato contenitore.
FILE-MANIFESTO	File che contiene metadati riferiti ad un file o ad un pacchetto di file.
FILESYSTEM	Sistema di gestione dei file, strutturato mediante una o più gerarchie ad albero, che determina le modalità di assegnazione dei nomi, memorizzazione e organizzazione all'interno di uno storage.
FIRMA ELETTRONICA	Vedi articolo 3 del Regolamento eIDAS.
FIRMA ELETTRONICA AVANZATA	Vedi articoli 3 e 26 del Regolamento eIDAS.
FIRMA ELETTRONICA QUALIFICATA	Vedi articolo 3 del Regolamento eIDAS.
FLUSSO (BINARIO)	Sequenza di bit prodotta in un intervallo temporale finito e continuativo che ha un'origine precisa ma di cui potrebbe non essere predeterminato il suo istante di interruzione.

FORMATO CONTENITORE	Formato di file progettato per consentire l'inclusione ("imbustamento" o *wrapping*), in uno stesso file, di una o più evidenze informatiche soggette a differenti tipi di codifica e al quale possono essere associati specifici metadati.
FORMATO DEL DOCUMENTO INFORMATICO	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
FORMATO "DEPRECATO"	Formato in passato considerato ufficiale il cui uso è attualmente sconsigliato a favore di una versione più recente.
FUNZIONI AGGIUNTIVE DEL PROTOCOLLO INFORMATICO	Nel sistema di protocollo informatico, componenti supplementari rispetto a quelle minime, necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni.
FUNZIONI MINIME DEL PROTOCOLLO INFORMATICO	Componenti del sistema di protocollo informatico che rispettano i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445.
FUNZIONE DI *HASH* CRITTOGRAFICA	Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o *digest* (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.
GESTIONE DOCUMENTALE	Processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta, uso, selezione e conservazione dei documenti.
HASH	Termine inglese usato, impropriamente, come sinonimo d'uso di "impronta crittografica" o "*digest*" (vedi).
IDENTIFICATIVO UNIVOCO	Sequenza di numeri o caratteri alfanumerici associata in modo univoco e persistente ad un'entità all'interno di uno specifico ambito di applicazione.
IMPRONTA CRITTOGRAFICA	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di *hash* crittografica a un'evidenza informatica.
INTEGRITÀ	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.
INTEROPERABILITÀ	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.
LEGGIBILITÀ	Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica.
MANUALE DI CONSERVAZIONE	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.
MANUALE DI GESTIONE	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.

METADATI	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.
NAMING CONVENTION	Vedi Convenzioni di denominazione
OGGETTO DI CONSERVAZIONE	Oggetto digitale versato in un sistema di conservazione.
OGGETTO DIGITALE	Oggetto informativo digitale, che può assumere varie forme tra le quali quelle di documento informatico, fascicolo informatico, aggregazione documentale informatica o archivio informatico.
PACCHETTO DI ARCHIVIAZIONE	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel manuale di conservazione.
PACCHETTO DI DISTRIBUZIONE	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione.
PACCHETTO DI FILE (*FILE PACKAGE*)	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.
PACCHETTO DI VERSAMENTO	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione.
PACCHETTO INFORMATIVO	Contenitore logico che racchiude uno o più oggetti di conservazione con i relativi metadati, oppure anche i soli metadati riferiti agli oggetti di conservazione.
PATH	Percorso (*vedi*).
PATHNAME	Concatenazione ordinata del percorso di un file e del suo nome.
PERCORSO	Informazioni relative alla localizzazione virtuale del file all'interno del filesystem espressa come concatenazione ordinata del nome dei nodi del percorso.
PIANO DELLA SICUREZZA DEL SISTEMA DI CONSERVAZIONE	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi.
PIANO DELLA SICUREZZA DEL SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi.
PIANO DI CLASSIFICAZIONE (TITOLARIO)	Struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata.
PIANO DI CONSERVAZIONE	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.
PIANO DI ORGANIZZAZIONE DELLE AGGREGAZIONI DOCUMENTALI	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
PIANO GENERALE DELLA SICUREZZA	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.
PRESA IN CARICO	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione 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.
PROCESSO	Insieme di attività correlate o interagenti che trasformano elementi in ingresso in elementi in uscita.
PRODUTTORE DEI PDV	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.
QSEAL	Sigillo elettronico qualificato, come da art. 35 del Regolamento eIDAS.
QSIGNATURE	Firma elettronica qualificata, come da art. 25 del Regolamento eIDAS.
RAPPORTO DI VERSAMENTO	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.
REGISTRO DI PROTOCOLLO	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.
REGISTRO PARTICOLARE	Registro informatico individuato da una pubblica amministrazione per la memorizzazione delle informazioni relative a documenti soggetti a registrazione particolare.
REGOLAMENTO EIDAS	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.
REPERTORIO	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.
RESPONSABILE DEI SISTEMI INFORMATIVI PER LA CONSERVAZIONE	Soggetto che coordina i sistemi informativi all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID.
RESPONSABILE DEL SERVIZIO DI CONSERVAZIONE	soggetto che coordina il processo di conservazione all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
RESPONSABILE DELLA CONSERVAZIONE	Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.
RESPONSABILE DELLA FUNZIONE ARCHIVISTICA DI CONSERVAZIONE	soggetto che coordina il processo di conservazione dal punto di vista archivistico all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID

RESPONSABILE DELLA GESTIONE DOCUMENTALE	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.
RESPONSABILE DELLA PROTEZIONE DEI DATI	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.
RESPONSABILE DELLA SICUREZZA DEI SISTEMI DI CONSERVAZIONE	soggetto che assicura il rispetto dei requisiti di sicurezza all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
RESPONSABILE DELLO SVILUPPO E DELLA MANUTENZIONE DEL SISTEMA DI CONSERVAZIONE	soggetto che assicura lo sviluppo e la manutenzione del sistema all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
RIFERIMENTO TEMPORALE	Insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC).
RIVERSAMENTO	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.
SCARTO	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.
SERIE	Raggruppamento di documenti con caratteristiche omogenee (vedi anche aggregazione documentale informatica).
***SIDECAR* (FILE)**	File-manifesto (*vedi*).
SIGILLO ELETTRONICO	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.
SISTEMA DI CONSERVAZIONE	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.
SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI	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
TIMELINE	Linea temporale virtuale su cui sono disposti degli eventi relativi ad un sistema informativo o a un documento informatico. Costituiscono esempi molto diversi di *timeline* un file di log di sistema, un flusso multimediale contenente essenze audio\video sincronizzate.
TITOLARE DELL'OGGETTO DI CONSERVAZIONE	Soggetto produttore degli oggetti di conservazione.
TRASFERIMENTO	Passaggio di custodia dei documenti da una persona o un ente ad un'altra persona o un altro ente.
TUDA	Testo Unico della Documentazione Amministrativa, Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni e integrazioni.

UFFICIO	Riferito ad un'area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico.
UTENTE ABILITATO	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.
VERSAMENTO	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

3.1 Normativa di riferimento

Di seguito l'elenco dei principali riferimenti normativi italiani in materia, ordinati secondo il criterio della gerarchia delle fonti:

- Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- Legge 7 agosto 1990, n. 241 e ss.mm.ii. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e ss.mm.ii – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e ss.mm.ii. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e ss.mm.ii. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e ss.mm.ii. (D. Lgs. 26 agosto 2016, n.179) – Codice dell'amministrazione digitale (CAD);
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;

- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche per il protocollo informatico ai sensi degli articoli 40 -bis, 41, 47, 57 -bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Decreto del Ministero dell'Economia e delle Finanze 17 giugno 2014 - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82 del 2005;
- Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.
- eIDAS (electronic IDentification Authentication and Signature) EU Regulation 910/2014 of the European Parliament and of the Council, of 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market.
- GDPR (General Data Protection Regulation) EU Regulation 679/2016 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
- Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici del settembre 2020.

Torna al sommario

3.2 Standard di riferimento

Si riportano di seguito gli standard di riferimento elencati nell'allegato 3 delle citate Regole

Tecniche ai sensi del Codice:

- UNI EN ISO 9001:2015 Sistemi di gestione per la Qualità;
- ISO 14001:2015 Sistema di Gestione Ambientale;
- Norma ETSI 319 401 - Reg. UE 910/2014 – eIDAS (electronic IDentification Authentication and Signature);
- ISO 15489:2014 (cap. 5 Regulatory Environment; cap. 7 Records Management Requirements);
- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ISO/IEC 27017:2015 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud service;
- ISO/IEC 27018:2019 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors;
- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- ETSI TR 101 533-2 V1.3.1 (2012-04) Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- ISO/IEC 20000-1: 2018 Service Management System Requirements
- ISO 15836:2009 Information and documentation - The Dublin Core metadata element

set, Sistema di metadata del Dublin Core.

- UNI 11386:2020 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;

Torna al sommario

3.3 Procedure aziendali interne

Si riportano di seguito i riferimenti alle procedure aziendali interne e alle principali politiche aziendali applicate anche al sistema di conservazione:

- PR/225- Change Management InfoCert
- MG231 – Modello di Gestione e Organizzazione D.Lgs 231/01
- PR/235 Progettare e sviluppare un servizio informatico InfoCert
- MG294 Capacity Management
- MG/325 Gestire Verifiche Ispettive InfoCert
- MG445 – Gestione Documentale InfoCert
- PR456 Problem Management
- Procedura Service Management System – SMS
- Processo MG115/TB02_Processi e Responsabilità_Integrated Management System
- Procedura di hand-over tra conservatori e scarto archivistico in LegalDoc.

Torna al sommario

4. RUOLI E RESPONSABILITÀ

Si riportano di seguito i profili professionali di Responsabilità legate al servizio di conservazione e le rispettive attività di competenza.
Tutti i Responsabili sono assunti a tempo indeterminato.

RUOLI	NOMINATIVI	ATTIVITA'	PERIODI
Responsabile del servizio di Conservazione	Nicola Maccà	• 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. • Definizione delle condizioni generali del contratto di servizio in coordinamento con la funzione legale e la funzione commerciale e funzione	da luglio 2018

RUOLI	NOMINATIVI	ATTIVITA'	PERIODI
		marketing di InfoCert.	
Responsabile Sicurezza dei sistemi per la conservazione	Giovanni Belluzzo	• Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; • Segnalazione delle eventuali difformità al Responsabile del servizio di Conservazione e individuazione e pianificazione delle necessarie azioni correttive.	da luglio 2018
Responsabile funzione archivistica di conservazione	Marta Gaia Castellan	• Definizione e descrizione archivistica dei documenti e delle aggregazioni documentali per la fruizione del patrimonio documentario e informativo conservato. • Definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici. • Analisi archivistica per lo sviluppo di funzionalità del sistema di conservazione. • Collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza. • Definizione delle condizioni	da settembre 2015

RUOLI	NOMINATIVI	ATTIVITA'	PERIODI
		generali del contratto di servizio in coordinamento con la funzione legale e la funzione commerciale e funzione marketing di InfoCert. • Controlli periodici a campione sulla leggibilità dei documenti conservati.	
Responsabile trattamento dati personali	Ilenia Gentilezza	• Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali. • Garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.	da marzo 2020
Responsabile sistemi informativi per la conservazione	Francesco Griselda	• Presidio ed evoluzione dei sistemi informativi per la conservazione nel rispetto delle procedure ISO9001 ISO14000 ISO20000 ISO27000. • Gestione dell'esercizio delle componenti hardware e software di base del sistema di conservazione. • Monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore in collaborazione con Il Responsabile della	da ottobre 2020

RUOLI	NOMINATIVI	ATTIVITA'	PERIODI
		manutenzione del sistema di conservazione. • Segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di Conservazione e individuazione e pianificazione delle necessarie azioni correttive. • Pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione. • Controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di Conservazione. • Coordinamento dello sviluppo e manutenzione delle componenti hardware e software di base del sistema di conservazione.	
Responsabile sviluppo e manutenzione del sistema di conservazione	Lucia Bortoletto	• Sviluppo e manutenzione del sistema di conservazione nel rispetto delle procedure ISO9001 ISO14000 ISO20000 ISO27000. • Coordinamento dello sviluppo e manutenzione delle componenti software del sistema di conservazione. • Pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione.	da luglio 2018

RUOLI	NOMINATIVI	ATTIVITA'	PERIODI
		• Monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione. • Interfaccia con l'ente produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche in collaborazione con il Responsabile funzione archivistica di conservazione. • Gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.	

Di seguito sono storicizzate le figure professionali che hanno ricoperto ruoli di responsabilità precedentemente:

RUOLI	NOMINATIVI PRECEDENTI	PERIODI
Responsabile sistemi informativi per la conservazione	Stefano Mameli	da maggio 2019 a ottobre 2020
Responsabile trattamento dati personali	Valentina Zoppo	da luglio 2018 a marzo 2020

RUOLI	NOMINATIVI PRECEDENTI	PERIODI
Responsabile sistemi informativi per la conservazione	Nicolò Poniz	da luglio 2018 a maggio 2019
Responsabile sviluppo e manutenzione del sistema di conservazione	Nicola Maccà	da gennaio 2013 a luglio 2018
Responsabile sistemi informativi per la conservazione	Massimo Biagi	da marzo 2014 a luglio 2018
Responsabile funzione archivistica di conservazione precedente	Silvia Loffi	da dicembre 2014 ad agosto 2015
Responsabile trattamento dati personali	Alfredo Esposito	da gennaio 2011 a luglio 2018
Responsabile Sicurezza dei sistemi per la conservazione	Alfredo Esposito	da gennaio 2011 a luglio 2018
Responsabile del servizio di Conservazione	Antonio Dal Borgo	da luglio 2008 a luglio 2018
Responsabile del servizio di Conservazione	Pio Barban	da luglio 2007 a luglio 2008

Torna al sommario

5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Profilo di InfoCert

Denominazione sociale	InfoCert S.p.A.
Sede Legale:	Piazza Sallustio, 9, 00187 Roma Tel.+39 06 836691
Sedi Operative:	• Piazza da Porto, 3, 35131 Padova • Via Via Carlo Bo, 11, 20143 Milano • Via Marco e Marcelliano, 45, 00147 Roma Tel: +39 06836691
Sito web	www.infocert.it
e-mail	info@infocert.it
PEC	infocert@legalmail.it
Codice Fiscale / Partita IVA	07945211006
Numero REA	RM – 1064345

InfoCert si pone sul mercato europeo come Trust Service Provider altamente specializzato, leader del mercato italiano nei servizi di digitalizzazione e dematerializzazione, nonché una delle principali Certification Authority a livello europeo, fornendo servizi di Posta Elettronica Certificata, Firma Avanzata e Digitale, Conservazione Digitale dei documenti e gestore accreditato AgID dell'identità digitale di cittadini e imprese, in conformità ai requisiti regolamentari e tecnici dello SPID (Sistema Pubblico per la gestione dell'Identità Digitale).

Da sempre la mission aziendale è credere nel futuro e nella trasformazione digitale, per questo dedichiamo la nostra esperienza, la nostra capacità di innovazione e la nostra passione per l'eccellenza, a tutti coloro che, in Italia e nel mondo, ricercano sicurezza e affidabilità nelle soluzioni digitali. Investiamo in ricerca e sviluppo per dare vita a nuove idee che supportino i nostri clienti nella costruzione di modelli e processi di business innovativi e conformi alle

normative, guidandoli verso una efficace trasformazione digitale e un futuro maggiormente sostenibile per le aziende, le persone e la realtà sociale.

La mission aziendale si declina anche nel servizio di Conservazione digitale: innovazione, sicurezza, affidabilità e conformità normativa, con lo scopo di assicurare la corretta gestione, archiviazione e conservazione dei documenti informatici di diversi soggetti produttori, assicurando l'esibizione a norma dei documenti conservati e la consulenza specialistica su progetti di paperless design.

InfoCert dal 2014 è tra le prime aziende italiane accreditate dall'Agenzia per l'Italia Digitale (AgID) come Conservatore, requisito normativo necessario per erogare servizi di Conservazione digitale per la Pubblica Amministrazione.

Inoltre, dal 2019, InfoCert ha ottenuto la qualifica AgID Cloud Marketplace (CSP Tipo B Infrastruttura e SaaS per LegalDoc).

La comunità di riferimento del servizio di Conservazione digitale di InfoCert è un gruppo identificato di clienti e di potenziali utenti in grado di comprendere un determinato set di informazioni: si tratta di un'unica comunità, ben definita, ma con alcune differenziazioni interne (multiple user communities), a seconda del mercato di riferimento (Pubblica Amministrazione centrale e locale, Sanità, Industry, Banking, Pharma, Utilities, Insurance, Ordini e Associazioni, PMI, liberi professionisti).

Il fine ultimo del servizio di Conservazione digitale è rendere i Pacchetti di Distribuzione ricercabili, esibibili, leggibili, integri, affidabili, autentici e fruibili dagli utenti della comunità di riferimento, attraverso la mediazione del soggetto produttore, in ottemperanza ai principali standard internazionali di records management (OAIS ISO14721 e ISO15489).

InfoCert è costantemente impegnata nel monitoraggio della propria comunità designata, al fine di acquisire nuove informazioni o esigenze o standard tecnologici, anche con lo scopo di combattere l'obsolescenza tecnologica. Per maggiori dettagli si rimanda al Service Management System.

InfoCert, inoltre, nello svolgimento delle proprie attività, ha conseguito le seguenti certificazioni:

- ISO 14001:2015 (Sistema di Gestione Ambientale)
- ISO/IEC 20000-1:2011 (Gestione dei Servizi Informatici)
- UNI EN ISO 9001:2015 (Sistemi di gestione per la qualità);
- ISO/IEC ISO 27001:2013 (Sistemi di gestione della sicurezza delle informazioni).
- ISO/IEC ISO 27017 e ISO/IEC ISO 27018 relativamente al Servizio di conservazione digitale a norma di documenti informatici erogato in modalità Cloud (SaaS) e relativi servizi di infrastruttura (IaaS privato).

InfoCert ha adottato il modello di organizzazione e controllo [MG231/01] di cui al D.lgs. del 08 giugno 2001 n.231 allo scopo di prevenire i reati per i quali la legge in questione prescrive la responsabilità amministrativa dell'impresa.

Il modello adottato da InfoCert rappresenta un'ulteriore garanzia dell'azienda in termini rigore, trasparenza e senso di responsabilità nella gestione dei processi interni e nei rapporti con il mondo esterno.

Il modello prevede l'istituzione di un Organismo di Vigilanza, la gestione di un processo formativo/informativo, la adozione di un Codice Etico e la definizione di un Sistema Sanzionatorio.

InfoCert si è dotata, inoltre, di un Integrated Management System per la gestione dei processi e delle responsabilità aziendali. Il documento MG115/TB02 descrive la mappatura dei processi aziendali in termini di ambiti di processo, procedure, ownership, modelli di gestione, pianificazioni, erogazioni, approvvigionamenti, controlli, governance e sicurezza.

Torna al sommario

5.2 Organigramma

L'organigramma di InfoCert è stato depositato presso AgID durante le procedure di accreditamento. Di seguito sono riportate le figure di responsabilità che intervengono nei processi e nelle attività di Conservazione.

Torna al sommario

5.3 Strutture organizzative

Nel processo di conservazione digitale intervengono numerosi soggetti, a differenti livelli e con diverse responsabilità, sintetizzate nella tabella seguente e dettagliate per singola attività.

Responsabilità Attività	Responsabile del servizio della Conservazione	Responsabile della funzione archivistica	Responsabile del trattamento dei dati personali	Responsabile della sicurezza dei sistemi per la conservazione	Responsabile dei sistemi informativi per la conservazione	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Soggetto Produttore
1. Condizioni Generali di Contratto	R						
2. Richiesta di attivazione	R	V	V	V	V	V-E	
3. Atto di affidamento	R						
4. Specifiche Tecniche di integrazione	V			A	A	R-E	
5. Impegno alla riservatezza	V		R	A			
6. Acquisizione del documento da conservare	R				E	V	
7. Metadatazione ed archiviazione	A	R			E	V	
8. Eventuale attestazione della conformità di quanto memorizzato nel documento d'origine da parte di un PU	R						

Responsabilità Attività	Responsabile del servizio della Conservazione	Responsabile della funzione archivistica	Responsabile del trattamento dei dati personali	Responsabile della sicurezza dei sistemi per la conservazione	Responsabile dei sistemi informativi per la conservazione	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Soggetto Produttore
9. Creazione del pacchetto di versamento							R
10. Invio al sistema di conservazione del pacchetto di versamento							R
11. Validazione Del pacchetto di versamento	R				E	V	
12. Generazione del pacchetto di archiviazione	R				E	V	
13. Memorizzazione e creazione “copia di sicurezza”	R			V	E	V	
14. Invio dell'IPdA al soggetto Produttore	R					E	
15. Scarto dei pacchetti di archiviazione	R	V			A	E	
16. Chiusura del servizio di conservazione al termine di un contratto	R	V			A	E	
17. Conduzione e manutenzione del	A				R	E	

Responsabilità Attività	Responsabile del servizio della Conservazione	Responsabile della funzione archivistica	Responsabile del trattamento dei dati personali	Responsabile della sicurezza dei sistemi per la conservazione	Responsabile dei sistemi informativi per la conservazione	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Soggetto Produttore
sistema di conservazione							
18. Monitoraggio del sistema di conservazione	**A**	**V**			**R**	**E**	
19. Change management		**V**		**V**	**A**	**R**	
20. Verifica periodica di conformità a normativa e standard di riferimento	**A**	**R**	**V**	**V**	**A**		

[**R**-responsabile; **E**-esegue; **V**- verifica; **A**-approva]

I Soggetti Produttori affidano in outsourcing il servizio di conservazione a InfoCert S.p.A., che assume le responsabilità della conservazione in accordo con quanto previsto dai documenti contrattuali descritti al capitolo 10 'Specificità del Contratto' e dagli articoli 5 e 6 del DPCM del 3 dicembre 2013.

Tutte le verifiche in carico al Responsabile del servizio della Conservazione sono garantite anche dal servizio di auditing interno. Il processo di conservazione è normalmente effettuato da procedure totalmente automatizzate, che non necessitano dell'intervento di altri soggetti o delegati. InfoCert si riserva, come specificato nelle Condizioni generali del Contratto, la possibilità di avvalersi di partner tecnologici per l'esecuzione di operazioni, singole attività, servizi relativi a funzioni o fasi del processo di conservazione, a terzi soggetti, fornitori esterni, che per conoscenza, esperienza, capacità e affidabilità forniscano idonee garanzie.

Torna al sommario

6. OGGETTI SOTTOPOSTI A CONSERVAZIONE

In generale si definisce 'pacchetto' un contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare.

I pacchetti (versamento/archiviazione/distribuzione) sono contrattualizzati con il Soggetto Produttore e si basano sui documenti che fanno parte delle 'Specificità del Contratto'.

Per "pacchetto di versamento" si intende l'insieme di documenti che il Soggetto Produttore invia al sistema di conservazione in un'unica sessione (login/logout).

Per "pacchetto di archiviazione" si intende un pacchetto informativo composto dalla trasformazione di pacchetti di versamento, depositato nei data center InfoCert descritto nelle 'Specificità del Contratto' SPT/NDOC- Specifiche tecniche per l'integrazione. Ad ogni documento il Sistema di conservazione associa un file XML, detto Indice del Pacchetto di Archiviazione (Indice di Conservazione UNI SInCRO). L'insieme degli Indici del Pacchetto di Archiviazione associati ai file componenti un pacchetto di versamento è detto Rapporto di Versamento.

Per "pacchetto di distribuzione" si intende un pacchetto informativo inviato dal sistema di conservazione all'utente in risposta a una sua richiesta, ovvero è la risposta alla ricerca effettuata dal Soggetto Produttore tramite interfaccia disponibile, che porta all'esibizione del documento conservato. Il documento da esibire è accompagnato sempre dall'IPdA.

Nel sistema, ad oggi, il "pacchetto di distribuzione" coincide con il "pacchetto di archiviazione".

Eventuali specificità sono concordate con il Soggetto Produttore e descritte nelle 'Specificità del Contratto' SPT/NDOC- Specifiche tecniche per l'integrazione e AL/NDOC – Allegato Tecnico al Contratto LegalDoc.

Torna al sommario

6.1 Oggetti conservati

Tipologie documentali, metadati e formati sono sempre concordati con il Soggetto Produttore, e vengono elencati nelle 'Specificità del Contratto' - 'Dati Tecnici di attivazione'.

I visualizzatori dei formati standard, previsti nell'allegato 2 del DPCM 3 dicembre 2013, sono automaticamente assegnati all'atto dell'attivazione del proprio ambiente di conservazione e sono forniti da InfoCert al Soggetto Produttore all'atto di attivazione del servizio. Tutti i documenti inviati in conservazione saranno associati al visualizzatore configurato per il particolare formato.

Formato	Estensione	MIME-Type	Standard
PDF o PDF/A	.pdf	application/pdf;NA	ISO 32000-1 (PDF), ISO 19005-1:2005 (vers. PDF 1.4), ISO 19005-2:2011 (vers. PDF 1.7)
TIFF	.tif	image/tiff;NA	ISO 12639(TIFF/IT); ISO 12234 (TIFF/EP)
XML	.xml	text/xml;1.0	
TXT	.txt	text/plain;NA	

Conservare documenti in altri formati (jpeg, Open Document Format, eml, DICOM, ecc..) è sempre possibile.

Qualora un Soggetto Produttore necessiti di formati aggiuntivi rispetto a quelli standard, dovrà segnalarlo nei 'Dati Tecnici di attivazione' (compresi nelle 'Specificità del Contratto') ed eventualmente conservare gli appositi visualizzatori in una sezione predefinita dell'ambiente assegnato.

I formati aggiuntivi devono essere concordati, dunque, tra il Soggetto Produttore e InfoCert in fase contrattuale e non è possibile caricare visualizzatori per formati non preventivamente concordati e configurati nel sistema.

I visualizzatori di formati aggiuntivi ai predefiniti devono essere inviati dal Soggetto Produttore prima di iniziare la conservazione dei documenti (il sistema accetta i documenti in conservazione anche se il visualizzatore non è caricato, ma finché non viene caricato non è possibile effettuare l'esibizione dei documenti). Il caricamento di un visualizzatore per un particolare mime/type va effettuato una sola volta, ulteriori caricamenti per lo stesso mime/type verranno identificati come aggiornamenti di versione del visualizzatore.

Di seguito è riportata la tabella di sintesi del processo di caricamento dei visualizzatori, inoltre per ognuna delle attività elencate saranno descritte le attività di dettaglio, seguendo lo schema: input\dettaglio delle attività\output.

Responsabilità **Attività**	Responsabile del servizio della Conservazione	Responsabile della funzione archivistica	Responsabile del trattamento dei dati personali	Responsabile della sicurezza dei sistemi per la conservazione	Responsabile dei sistemi informativi per la conservazione	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Soggetto Produttore
1. Creazione del file dei parametri di upload, del file della scheda tecnica e predisposizione dei file del visualizzatore.							**R**
2. Invio della richiesta al sistema di conservazione.							**R**
3. Validazione delle informazioni presenti nei file della richiesta	**R**				**E**	**V**	
4. Caricamento del visualizzatore, creazione del file IPdA, marcatura temporale e firma digitale	**R**				**E**	**V**	

Responsabilità Attività	Responsabile del servizio della Conservazione	Responsabile della funzione archivistica	Responsabile del trattamento dei dati personali	Responsabile della sicurezza dei sistemi per la conservazione	Responsabile dei sistemi informativi per la conservazione	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Soggetto Produttore
dello stesso ed invio al soggetto Produttore.							

[**R**-responsabile; **E**-esegue; **V**- verifica; **A**-approva]

Torna al sommario

6.2 Pacchetto di versamento

Di seguito è riportata la tabella di sintesi del processo di versamento del pacchetto, inoltre per ognuna delle attività elencate saranno descritte le attività di dettaglio, seguendo lo schema input\dettaglio delle attività\output.

Responsabilità Attività	Responsabile del servizio della Conservazione	Responsabile della funzione archivistica	Responsabile del trattamento dei dati personali	Responsabile della sicurezza dei sistemi per la conservazione	Responsabile dei sistemi informativi per la conservazione	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Soggetto Produttore
1. Invio al sistema di conservazione del pacchetto di versamento.							**R**
2. Validazione del pacchetto di	**R**				**E**	**V**	**R**

Responsabilità Attività	Responsabile del servizio della Conservazione	Responsabile della funzione archivistica	Responsabile del trattamento dei dati personali	Responsabile della sicurezza dei sistemi per la conservazione	Responsabile dei sistemi informativi per la conservazione	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Soggetto Produttore
versamento.							
3. Generazione del pacchetto di archiviazione.	**R**				**E**	**V**	
4. Memorizzazione e creazione “copia di sicurezza”.	**R**			V	**E**	**V**	
5. Invio dell'IPdA al Soggetto Produttore.	**R**						

L'art. 7 comma c) del DPCM del 3 dicembre 2013 introduce, inoltre, l’obbligo di generare il Rapporto di Versamento.

L’insieme degli Indici del Pacchetto di Archiviazione associati ai file componenti un pacchetto di versamento è detto Rapporto di Versamento.

Il Rapporto di Versamento attesta l'avvenuta presa in carico da parte del sistema di conservazione del pacchetto di versamento inviato dal Produttore ed è l’insieme degli Indici dei Pacchetti di Archiviazione prodotti per ogni singolo documento oggetto di versamento (per i dettagli tecnici si rimanda a ‘Specificità del Contratto’ SPT/NDOC- Specifiche tecniche per l’integrazione).

Il rifiuto dei pacchetti di versamento avviene nella modalità descritta nelle ‘Specificità del Contratto’ SPT/NDOC- Specifiche tecniche per l’integrazione e con le casistiche definite SPT/NDOCERR – Descrizione dei codici di errore di LegalDoc.

Le eventuali personalizzazioni specifiche di un contratto sono descritte nei documenti elencati e descritti nel capitolo 10 - 'Specificità del Contratto'.

Torna al sommario

6.3 Pacchetto di archiviazione

Per "pacchetto di archiviazione" si intende un pacchetto informativo composto dalla trasformazione di pacchetti di versamento, depositato nei data center InfoCert descritto nelle 'Specificità del Contratto' SPT/NDOC- Specifiche tecniche per l'integrazione. Ad ogni documento il Sistema di conservazione associa un file XML, detto Indice del Pacchetto di Archiviazione. L'insieme degli Indici del Pacchetto di Archiviazione associati ai file componenti un pacchetto di versamento è detto Rapporto di Versamento.

L'Indice del Pacchetto di Archiviazione è un file in formato XML, marcato temporalmente e firmato digitalmente dal Responsabile del servizio della Conservazione, generato dal sistema, che contiene i metadati in formato UNI SInCRO e le informazioni di conservazione del documento e viene con esso conservato.

In particolare, nel file sono riportati:

- informazioni sull'applicazione che ha generato l'IPdA
- il token del documento (ovvero il suo identificativo univoco)
- l'operazione eseguita (conservazione, rettifica, scarto e cancellazione)
- il bucket (ovvero l'area di conservazione) associato al Soggetto Produttore e la policy utilizzata
- il nome dei file che compongono il pacchetto, incluso il file dei parametri di conservazione ed il file di indici, e le rispettive impronte
- eventuali informazioni relative al documento rettificante e rettificato
- il tempo di creazione (timestamp) del file IPdA
- l'impronta di Hash del documento.

L'insieme degli IPdA di un pacchetto di versamento formano il Rapporto di versamento di cui all'art. 9, comma d) del DPCM del 3 dicembre 2013.

Il file IPdA è reso disponibile con il documento di riferimento ad ogni operazione di conservazione e richiesta di esibizione.

Torna al sommario

6.4 Pacchetto di distribuzione

Il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, al documento informatico conservato, attraverso la produzione di un pacchetto di distribuzione.

Le procedure di esibizione permettono di estrarre dal sistema un pacchetto di distribuzione per cui sia stata completata correttamente la procedura di conservazione, utilizzando il relativo token (ovvero l'identificativo univoco del documento da esibire) o utilizzando uno o più metadati versati.

Insieme ai file costituenti il pacchetto di distribuzione, sono rese disponibili anche le informazioni che qualificano il processo di conservazione, ossia il file IPdA e un'Attestazione di corretta conservazione e datacertazione firmata dal Responsabile del servizio di Conservazione.

Non è possibile esibire parti singole di documento.

L'esibizione può restituire i pacchetti in tre modalità differenti: in un pacchetto di distribuzione in formato zip contenente al suo interno tanti pacchetti quanti sono i documenti da esibire, in un unico pacchetto di distribuzione in formato zip, oppure un file alla volta (quest'ultima modalità deve essere compatibile con il client di esibizione dell'utente).

Le procedure del sistema mantengono e aggiornano ad ogni nuovo invio il database di tutti i token; il database viene interrogato ad ogni richiesta di rettifica, scarto e cancellazione, ricerca ed esibizione confrontando il token inviato con quelli memorizzati. La procedura assicura di agire solamente sul documento richiesto, e solamente se in possesso dei dovuti profili di autorizzazione.

L'esibizione del pacchetto di distribuzione ottenuto tramite interrogazione al sistema di conservazione rappresenta un'esibizione completa, legalmente valida ai sensi del secondo comma dell'articolo 10 del DPCM del 03 dicembre 2013 e dell'articolo 5 del DMEF del 17 giugno 2014.

Un apposito strumento di esibizione e verifica, anche detto “Esibitore a Norma”, permette di richiamare agevolmente un documento conservato e consente di ottenere in modo automatico sia la verifica delle firme digitali e delle marche temporali apposte che le verifiche di integrità dei documenti conservati e di tutti gli altri elementi conservati.

Si rimanda al ‘MU/ESIB Manuale Utente Esibitore LegalDoc’ – ‘Specificità del Contratto’ per il dettaglio delle funzionalità di verifica del sistema.

Torna al sommario

7. IL PROCESSO DI CONSERVAZIONE

Il sistema di conservazione è erogato in modalità SaaS (Software as a Service) secondo uno schema di Business Process Outsourcing (BPO) e permette di mantenere e garantire nel tempo l'integrità, la leggibilità e la validità legale di un documento informatico, nel rispetto della normativa vigente.

Il sistema consente le funzionalità di:

- **accettazione del pacchetto di versamento**, formato dal documento da conservare e dai metadati ad esso associati;
- **conservazione del pacchetto di archiviazione**: il documento, ricevuto nei Data Center di InfoCert in formato digitale statico non modificabile, viene conservato a norma di legge per tutta la durata prevista ed è contenuto in un pacchetto di archiviazione;
- **rettifica del pacchetto di archiviazione**: un documento inviato in conservazione può essere rettificato dall'invio di un documento successivo. La rettifica è una modifica logica, nel pieno rispetto del principio di tracciabilità e la rettifica si applica al pacchetto di archiviazione;
- **scarto/cancellazione del pacchetto di archiviazione:** in caso un documento sia stato versato per errore. La cancellazione è una modifica logica, nel pieno rispetto del principio di tracciabilità e si applica al pacchetto di archiviazione; per la cancellazione fisica di pacchetti di archiviazione ritenuti privi di valore amministrativo e di interesse storico-culturale dal Produttore, occorre formulare apposita richiesta a InfoCert (scarto archivistico);
- **ricerca dei documenti conservati**: l'utente autorizzato può eseguire una ricerca tra i documenti conservati trasversalmente sulle classi documentali, utilizzando uno o più metadati popolati in fase di caricamento;
- **esibizione del pacchetto di distribuzione:** il documento richiesto via web viene richiamato direttamente dal sistema di conservazione digitale ed esibito, con garanzia della sua opponibilità a terzi; attraverso l'Esibitore di LegalDoc è possibile visualizzare e scaricare sia il documento conservato che gli altri documenti a corredo della corretta conservazione (file di indici, file di parametri, Indice del Pacchetto di Archiviazione);
- **visualizzazione delle statistiche di conservazione**;
- **caricamento dei visualizzatori**: è previsto il deposito dei visualizzatori da parte del Soggetto Produttore qualora la tipologia dei file conservati non sia quella standard, definita in fase di attivazione del sistema.

Il sistema di conservazione, quindi, integra il sistema di gestione del Soggetto Produttore, sia esso un'azienda o un ente locale, e ne estende i servizi con funzionalità di stoccaggio digitale (archivio di deposito).

Le fasi di creazione, utilizzo e archiviazione dei documenti sono organizzate liberamente, in quanto il servizio interviene solamente nella fase di conservazione e solamente per i documenti che il Soggetto Produttore sceglie di conservare.

Torna al sommario

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

Di seguito è riportata la tabella che descrive l'acquisizione dei pacchetti, seguendo lo schema: input\dettaglio delle attività\output.

ATT.1 Invio al sistema di conservazione del pacchetto di versamento

INPUT	*Documento da inviare al sistema di conservazione tramite il pacchetto di versamento*	
Sistema di gestione documentale del Soggetto Produttore		Invocazione del sistema di conservazione da parte del sistema di gestione, secondo lo standard descritto nelle SPT/NDOC – Specifiche tecniche per l'integrazione di LegalDoc.
		Autenticazione al sistema LegalDoc mediante credenziali (username/password) e ottenimento dell'identificativo di sessione (IdSessionId)
		Trasmissione del pacchetto di versamento costituente il documento (file di dati, il file di indici del documento e il file dei parametri di conservazione) secondo le modalità di trasmissione descritte nelle SPT/NDOC – Specifiche tecniche per l'integrazione di LegalDoc.
OUTPUT	*pacchetto di versamento inviato*	

Per maggiori dettagli si rimanda al documento “SPT/NDOC – Specifiche tecniche per l'integrazione di LegalDoc” – ‘Specificità del Contratto’.

Torna al sommario

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

ATT.1 Validazione del pacchetto di versamento

INPUT	*Pacchetto di versamento*
Sistema di conservazione	Generazione dell'impronta di ogni file costituente il documento e confronto con la corrispondente impronta inviata dal Soggetto Produttore, a garanzia dell'integrità del documento ricevuto. In caso di esito negativo delle verifiche, rigetto del documento con invio al sistema di gestione del Soggetto Produttore dell'errore intercorso. In questo caso, termine del flusso.
	Controllo dei valori indicati dal Soggetto Produttore nel file dei parametri di conservazione: verifica della policy dichiarata, verifica della congruenza dei tipi di file inviati (mimetype), verifica dell'univocità del file all'interno del path (cartella) indicato.
	Controllo dei valori indicati dal Soggetto Produttore nel file di indici del documento: validazione dei tracciati dei file di indice, verifica della correttezza della classe documentale, verifica della compatibilità fra policy dichiarate e policy configurate, verifica degli indici obbligatori (esistenza, valorizzazione, non duplicazione, correttezza del tipo di file, controllo numerico). I valori espressi nel file di indici vengono confrontati con la configurazione presente nelle apposite tabelle presenti nel database LegalDoc.
	Aggiornamento dei database del sistema con i dati relativi al documento e ai file che lo compongono per il mantenimento della tracciabilità delle operazioni.

OUTPUT	*pacchetto di versamento verificato*

Torna al sommario

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

Le fasi previste sono la memorizzazione, la creazione del file IPDA e la marcatura temporale dello stesso.

ATT.1 Generazione del pacchetto di archiviazione

INPUT	*Pacchetto di archiviazione*
Sistema di conservazione	Eventuale apposizione della firma digitale sul file di dati, cioè sul documento da conservare (se prevista da accordi contrattuali appositi esplicitati nei 'Dati Tecnici di attivazione', che fanno parte delle 'Specificità del contratto')
	Creazione del file XML IPdA (Indice del Pacchetto di Archiviazione) contenente: le informazioni sul processo di conservazione (in particolare sul software LegalDoc), le policy ed il bucket (area di conservazione) utilizzati, il nome e le impronte dei file costituenti il documento e l'identificativo (token) assegnato al documento,
	Marcatura e firma da parte del Responsabile del servizio della Conservazione del file IPdA. Copia del file sul supporto primario.
	Indicizzazione del documento conservato al fine di poter reperire lo stesso in seguito.
	Aggiornamento del database del sistema interessato alle modifiche di cui sopra.

OUTPUT	*pacchetto di archiviazione*

ATT.2 Memorizzazione e creazione copia di sicurezza

INPUT	*Pacchetto di archiviazione*	
		Memorizzazione del pacchetto di archiviazione su supporto magnetico, mediante un sistema di archiviazione permanente dei contenuti digitali
		Inserimento nelle tabelle di interfaccia del sistema di archiviazione permanente delle informazioni di puntamento dei file, al fine di poter reperire gli stessi in seguito.
		La procedura di creazione della copia di sicurezza avviene in maniera automatica e gestita dal sistema di Storage.
OUTPUT	*Documenti conservati*	

ATT.3 Invio dell'IPdA al soggetto Produttore

INPUT	*File IPdA*	
		Invio dell'esito e del file IPdA al soggetto Produttore.
OUTPUT	*Esito conservazione inviato*	

Torna al sommario

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

All'interno delle 'Specificità del Contratto' SPT/NDOCERR – Descrizione dei codici di errore di LegalDoc è presente la griglia riassuntiva dei codici errore che il servizio LegalDoc restituisce

in seguito a situazioni che impediscono la corretta e completa esecuzione del servizio richiesto. La griglia riporta le seguenti informazioni:

- Codice di errore - codifica abbreviata dell'errore avvenuto
- Messaggio di errore - breve descrizione dell'errore avvenuto

I campi codice e descrizione vengono inseriti nel corpo della risposta HTTP.

L'assistenza LegalDoc è contattabile mediante ticket https://help.infocert.it/

Torna al sommario

7.5 Preparazione e gestione del pacchetto di archiviazione

Di seguito è riportata la tabella che descrive la gestione dei pacchetti di archiviazione, seguendo lo schema: input\dettaglio delle attività\output.

ATT.1 Verifica del pacchetto di versamento

INPUT	*Pacchetto di versamento*	
Sistema di conservazione	1	Generazione dell'impronta di ogni file costituente il documento e confronto con la corrispondente impronta inviata dal soggetto Produttore, a garanzia dell'integrità del documento ricevuto. In caso di esito negativo delle verifiche, rigetto del documento con invio al sistema di gestione del soggetto Produttore dell'errore intercorso. In questo caso, termine del flusso.
	2	Controllo dei valori indicati dal soggetto Produttore nel file dei parametri di conservazione: verifica della policy dichiarata, verifica della congruenza dei tipi di file inviati (mimetype), verifica dell'univocità del file all'interno del path (cartella) indicato.
	3	Controllo dei valori indicati dal soggetto Produttore nel file di indici del documento: validazione dei tracciati dei file di indice, verifica della correttezza della classe documentale, verifica della compatibilità fra policy dichiarate e policy configurate, verifica degli indici obbligatori (esistenza, valorizzazione,

		non duplicazione, correttezza del tipo di file, controllo numerico). I valori espressi nel file di indici vengono confrontati con la configurazione presente nelle apposite tabelle presenti nel database LegalDoc.
	4	Aggiornamento dei database del sistema con i dati relativi al documento e ai file che lo compongono per il mantenimento della tracciabilità delle operazioni.
OUTPUT	*pacchetto di versamento verificato*	

ATT.2 Formazione del pacchetto di archiviazione

INPUT	*Pacchetto di archiviazione*	
Sistema di conservazione	1	Eventuale apposizione della firma digitale sul file di dati (se prevista da accordi contrattuali)
	2	Creazione del file XML IPdA (Indice del Pacchetto di Archiviazione) contenente: le informazioni sul processo di conservazione (in particolare sul software LegalDoc), le policy ed il bucket (area di conservazione) utilizzati, il nome e le impronte dei file costituenti il documento e l'identificativo assegnato al documento,
	2	Marcatura e firma da parte del Responsabile del servizio di Conservazione del file IPdA. Copia del file sul supporto primario.
	3	Indicizzazione del documento conservato al fine di poter reperire lo stesso in seguito.
	4	Aggiornamento del database del sistema interessato alle modifiche di cui sopra.
OUTPUT	*pacchetto di archiviazione*	

ATT.3 Memorizzazione del pacchetto di archiviazione

INPUT	*Pacchetto di archiviazione*	
Sistema di conservazione	1	Memorizzazione del pacchetto di archiviazione su supporto magnetico, mediante un sistema di archiviazione permanente dei contenuti digitali
	2	Inserimento nelle tabelle di interfaccia del sistema di archiviazione permanente delle informazioni di puntamento dei file, al fine di poter reperire gli stessi in seguito.
	3	La procedura di creazione della copia di sicurezza avviene in maniera automatica e gestita dal sistema di Storage.
OUTPUT	*Documenti conservati*	

Torna al sommario

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

ATT1. Ricerca del documento da esibire

INPUT	*Lista di token archiviati dal sistema*	
Sistema di Gestione documentale del Soggetto Produttore		Ricerca negli archivi del sistema del token relativo al documento da esibire attraverso le procedure previste dai sistemi di gestione.
		Restituzione del token corretto.
OUTPUT	*Token relativo al documento da esibire*	

ATT2. Richiesta di esibizione del documento conservato

INPUT	*Richiesta di esibizione da eseguire*
Sistema di Gestione documentale del Soggetto Produttore	Autenticazione al sistema LegalDoc mediante credenziali (username/password) e ottenimento dell'identificativo di session (ldSessionId).
	Invocazione del servizio di esibizione del sistema di conservazione secondo le modalità descritte nelle 'Specificità del Contratto' SPT/NDOC – Specifiche tecniche per l'integrazione di LegalDoc. In questa chiamata viene utilizzato il token ricavato in precedenza.
OUTPUT	*Richiesta di esibizione eseguita*

ATT.3 Accettazione della richiesta da parte del sistema di conservazione

INPUT	*Richiesta di esibizione*
Sistema di conservazione	Ricezione della richiesta di esibizione del documento.
	Controllo di corrispondenza tra il token inviato dal Soggetto Produttore e quelli dei documenti conservati.
OUTPUT	*Richiesta di esibizione presa in carico*

ATT.4 Risposta del sistema di conservazione ed esibizione del documento

INPUT	*Richiesta di esibizione acquisita*
	Ricerca dei file costituenti il documento e dei file attestanti il processo di conservazione corrispondenti al token inviato e preparazione del pacchetto di distribuzione.
	Invio della risposta al sistema del Soggetto Produttore.

OUTPUT	*Documento esibito*

Torna al sommario

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

Per duplicato si intende il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario.

Per copia si intende il documento informatico avente contenuto identico al documento da cui è tratto, ma con forma diversa.

La conservazione avviene su supporto primario e su supporto secondario, quindi con duplicazione automatica. Come descritto in seguito, tali supporti sono magnetici ad alte capacità e performance, che garantiscono la ridondanza interna del dato. È inoltre eseguito un backup periodico su tape magnetico.

La creazione di copie informatiche, invece, in caso di adeguamento del formato rispetto all'evoluzione tecnologica sarà presa in carico dal Responsabile del servizio della Conservazione e dalle figure professionali coinvolte nel processo di conservazione in base alle specifiche del formato in questione e al know-how tecnologico a disposizione. A fronte di questa analisi sarà progettata una soluzione di concerto con il Soggetto Produttore del formato più idoneo per permettere la leggibilità del documento conservato.

Possono essere generati anche duplicati o copie attraverso l'Esibitore o su supporto ottico, su specifica richiesta del Soggetto Produttore. Nel primo caso il Produttore/Utente agisce autonomamente con apposite credenziali attraverso l'Esibitore di LegalDoc. Nel secondo caso il Soggetto Produttore inoltra la richiesta ai suoi riferimenti abituali (help desk o account) che poi provvedono alla veicolazione verso gli operatori interni.

L'intervento di un Pubblico Ufficiale per attestare la conformità di una copia all'originale avviene secondo quanto previsto dagli articoli 22 e 23 del Codice e dalle Regole Tecniche del DPCM del 13 novembre 2014 - Regole tecniche in materia di formazione, trasmissione, copia,

duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

Torna al sommario

7.8 Scarto dei pacchetti di archiviazione

In LegalDoc esistono due diverse metodologie di 'cancellazione':

1. Cancellazione logica: eliminazione di un documento versato in conservazione per errore materiale, gestita in autonomia solo dal Soggetto Produttore (attraverso apposite chiamate WS), per cui il documento cancellato è ancora consultabile dall'Utente (compare con lo 'stato': 'cancellato'), in ossequio al principio di tracciabilità informatica.

2. Cancellazione fisica o scarto archivistico: eliminazione vera e propria di un documento o di un pacchetto di archiviazione e di qualsiasi duplicato prodotto durante le attività di conservazione, sia dal punto di vista logico che dal punto di vista fisico, per cessata rilevanza ai fini amministrativi, legali o di ricerca storica, ai sensi del Codice Privacy, del GDPR e del Codice dei beni culturali. Questa attività è espressamente richiesta a InfoCert dal Soggetto Produttore, mediante apposita lista debitamente firmata (anche attraverso apposite chiamate WS).

Per gli enti pubblici e per gli archivi privati dichiarati di notevole interesse storico, le proposte di scarto sono sottoposte a nulla osta delle soprintendenze archivistiche o delle commissioni di sorveglianza di competenza. La stesura di 'Piani di Conservazione' (detti anche 'Massimari di selezione e scarto'), la selezione dei documenti da scartare e la procedura di sdemanializzazione e approvazione ministeriale sono in capo al Soggetto Produttore, che può avvalersi del supporto della Digital Consulting di InfoCert.

La distruzione degli eventuali supporti ottici rimovibili di back-up è effettuata mediante strumentazione adeguata e seguendo le procedure definite per lo smaltimento dei rifiuti prodotti.

Il Responsabile del servizio della Conservazione mantiene traccia delle richieste di scarto ricevute e correttamente eseguite, e vengono redatti Attestati di scarto firmati digitalmente dal Responsabile del servizio.

Per ulteriori dettagli si rimanda all'apposito documento interno 'Procedura di hand-over tra conservatori e scarto archivistico in LegalDoc'.

Torna al sommario

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

Nel caso il Soggetto Produttore decida di rescindere o interrompere il contratto di affidamento del servizio di conservazione, il Responsabile del servizio della Conservazione provvede a comunicare al Soggetto Produttore la lista dei pacchetti di archiviazione conservati.

Il soggetto produttore può effettuare il download dei propri Pacchetti di Distribuzione in autonomia, attraverso la procedura di esibizione, o richiedendo il servizio di restituzione al proprio commerciale di riferimento (su supporto da concordare in base a volume ed esigenze).

Se i supporti sono removibili, i documenti contenuti sono criptati e compressi con password apposita e non devono contenere nel dorso o nella custodia nessun riferimento al soggetto produttore o al contenuto.

Il soggetto produttore provvederà a inviare anche copia della liberatoria denominata 'MODULO DI RESTITUZIONE DATI – SERVIZIO LEGALDOC' sottoscritta digitalmente dal Responsabile della Conservazione interno. Al termine della procedura di hand over verso il nuovo Conservatore per rescissione o risoluzione del contratto di servizio, i pacchetti conservati verranno cancellati da LegalDoc.

Insieme ai veri e propri documenti conservati, sono rese disponibili anche le informazioni e i documenti a corredo della corretta conservazione.

Gli archivi di conservazione generati dal sistema InfoCert sono conformi allo standard di interoperabilità UNI SInCRO: l'interrogazione di tali archivi restituisce le informazioni secondo il suddetto standard.

L’adozione di tale standard permette l’interoperabilità e la trasferibilità dei dati in modo semplificato.

Per ulteriori dettagli si rimanda all’apposito documento interno ‘Procedura di hand-over tra conservatori e scarto archivistico in LegalDoc’.

Torna al sommario

8. IL SISTEMA DI CONSERVAZIONE

La descrizione dell'architettura generale del sistema di conservazione è stata depositata in AgID in fase di accreditamento.

Il sistema è organizzato su più siti (Padova, Modena, Milano).

Il sistema di conservazione è implementato da un'applicazione software appositamente sviluppata a tale scopo (applicazione Java in architettura distribuita, ossia costituita da molteplici componenti) e da una serie di servizi di interesse generalizzato condivisi con altre applicazioni (marca temporale, HSM, supporti di conservazione, PEC).

Il sistema è reso in modalità SaaS (Softwareas a Service) e consente al Soggetto Produttore di accedere ai sistemi di conservazione dei documenti informatici su un elaboratore elettronico, gestito da InfoCert e fisicamente posto nei locali di quest'ultima, in conformità a quanto descritto nei documenti delle 'Specificità del Contratto'.

Il sistema è accessibile dalla apposita URL di rete e il Soggetto Produttore richiama il sistema di conservazione secondo le modalità concordate.

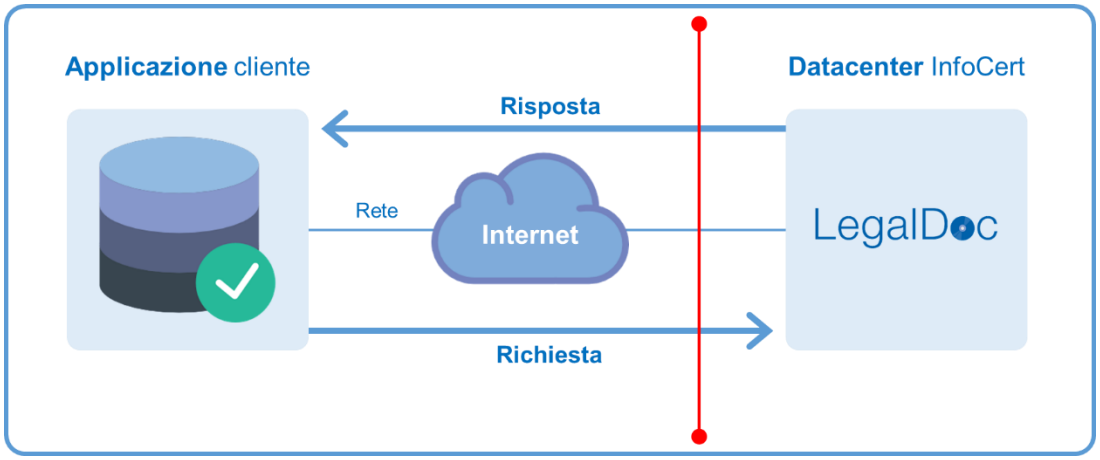


Figura 1 Rappresentazione del servizio attraverso la rete

Dal punto di vista architetturale LegalDoc è realizzato utilizzando la tecnologia dei Web Services.

I Web Services di LegalDoc sono implementati secondo architettura REST su protocollo HTTPS.

LegalDoc è dotato anche di un'interfaccia (LegalDoc WEB) utilizzata sia per il versamento manuale di alcune tipologie documentali, sia per la ricerca e l'esibizione a norma di documenti conservati.

L'esibitore è un'applicazione in tecnologia web, che permette ad un utente, precedentemente definito e in possesso delle debite autorizzazioni e credenziali, di accedere al sistema di conservazione LegalDoc da un qualsiasi computer, purché collegata in rete.

Attraverso l'esibizione a norma diventa possibile:

- estrarre un documento e visualizzarlo a video;
- produrre copia cartacea o su altro supporto informatico del documento;
- estrarre i visualizzatori memorizzati nel sistema di conservazione permettendone l'installazione sulla stazione dove si sta svolgendo l'esibizione;
- prendere visione dei file a corredo che formano il pacchetto di distribuzione e che qualificano il processo di conservazione attestandone il corretto svolgimento (Indice di Conservazione UNI SINCRO, altrimenti detto Indice del Pacchetto di Archiviazione, File di parametri, File di indici, File di dati, Attestato di conservazione);
- verificare la validità delle firme digitali e delle marche temporali apposte nel processo di conservazione;
- verificare l'integrità del documento.

Il sistema è protetto da firewall ed implementa un sistema di back-up dei dati memorizzati.

Torna al sommario

8.1 Componenti Logiche

Il servizio LegalDoc è basato su tecnologia REST e svolge le operazioni di conservazione, esibizione, rettifica, cancellazione e ricerca.

Torna al sommario

8.2 Componenti Tecnologiche

8.2.1 Firewall

I firewall assicurano la difesa del perimetro di sicurezza tra il sistema e il mondo esterno, nonché tra i sistemi dedicati all'erogazione del sistema e i sistemi che interfacciano i dispositivi sicuri per la generazione della firma digitale.

I firewall sono configurati in alta affidabilità e costantemente aggiornati per assicurare i massimi livelli di protezione possibile.

Torna al sommario

8.2.2 Back-up

L'intero sistema di conservazione viene interessato periodicamente da processi di back-up completo dei documenti, delle evidenze qualificanti il processo, dei database di gestione del sistema e di ogni altra informazione necessaria per la sicurezza.

Torna al sommario

8.2.1 Dispositivo HSM di firma digitale dei pacchetti

Al buon esito del processo di conservazione, il Responsabile del servizio della Conservazione di InfoCert appone la propria firma digitale su ogni pacchetto di archiviazione, mediante un sistema di firma digitale automatica erogato dalla Certification Authority InfoCert, che si avvale di un dispositivo crittografico ad altre prestazioni Hardware Security Module e di un certificato qualificato di firma appositamente generato e su cui ha pieno controllo.

Torna al sommario

8.2.2 Servizio di marcatura temporale dei pacchetti

Per l'emissione delle marche temporali il sistema si avvale del servizio di marcatura di InfoCert, Certification Authority accreditata, compliant eIDAS. La marca temporale viene richiesta al TSS (Time Stamping Service) che la restituisce firmata con un certificato emesso dalla TSA (Time Stamping Authority) di InfoCert. Il root-certificate della TSA è depositato presso AgID. Il TSS è sincronizzato via radio con l'I.N.RI.M di Torino (Istituto Nazionale di Ricerca Metrologica, già Istituto Elettrotecnico Nazionale "Galileo Ferraris") ed è protetto contro la manomissione della sincronizzazione mediante misure fisiche e logiche, nel pieno rispetto delle norme di legge.

Torna al sommario

8.3 Componenti Fisiche

InfoCert, in accordo con i Soggetti Produttori e come previsto dalle Condizioni Generali del Contratto si avvale di partner tecnologici per le componenti fisiche del data center.

Torna al sommario

8.3.1 Sistema Storage

Il sistema di conservazione di InfoCert e dei suoi partner tecnologici supporta la memorizzazione dei file sia su storage magnetici ad alte performance che su sistema *Object Storage S3*. Tali storage, scelti tra i primari fornitori di tecnologie presenti sul mercato, garantiscono adeguati requisiti di affidabilità e di ridondanza interna del dato e rispondono all'esigenza di memorizzazione a lungo termine dei *fixed content*, ossia dei file che devono essere conservati con garanzia nel tempo di integrità e disponibilità del contenuto.

Per garantire la riservatezza vengono applicate appropriate politiche sulle autorizzazioni che prevedano la cifratura dei documenti che contengono dati sensibili ed eventualmente anche degli altri.

I sistemi di storage sono stati valutati da InfoCert e dai suoi partner tecnologici sotto molteplici profili e, in virtù delle loro caratteristiche fisiche e architetturali, sono ritenuti idonei ad essere utilizzati nel sistema di conservazione.

Nell'ambito del sistema di conservazione, lo storage magnetico ad alte performance rappresenta sia il supporto primario di conservazione posto fisicamente presso la sede InfoCert di Padova, sia il supporto secondario posto nel sito di *disaster recovery* di Modena.

I due sistemi sono interconnessi mediante collegamenti ad alta velocità dedicati, completamente ridondati e protetti da misure di sicurezza. I collegamenti consentono la replicazione dei dati conservati eliminando il rischio di distruzione di tutte le copie delle informazioni in caso di danno irreparabile a livello di sito.

Questo secondo sistema funge anche da copia di sicurezza.

L'allineamento tra il sito primario e il sito secondario avviene coerentemente con le politiche generali di *Disaster Recovery* definite in InfoCert che garantiscono RTO e RPO inferiori alle 48 ore.

Per il sistema di *Object Storage S3* InfoCert si avvale dei servizi cloud computing *Amazon Web Services (AWS)* che garantisce la ridondanza e il rispetto delle misure di sicurezza.

Torna al sommario

8.3.2 Sincronizzazione dei sistemi

Tutti i server di InfoCert, attraverso il protocollo NTP (Network Time Protocol), sono sincronizzati sul “tempo campione” fornito dall’Istituto di Ricerca Metrologica – INRIM (già Istituto Elettrotecnico Nazionale “Galileo Ferraris”), abilitato a fornire il “tempo campione” ai sensi dell’articolo 2, comma 2, lettera b) del D.M. 30 novembre 1993, n. 591 “Regolamento concernente la determinazione dei campioni nazionali di talune unità di misura del Sistema internazionale (SI) in attuazione dell’art. 3 della L. 11 agosto 1991, n.273. La sincronizzazione è protetta da misure di sicurezza fisiche e logiche documentate per impedirne la manomissione.

Il meccanismo di allineamento temporale tra i sistemi fornisce la certezza della successione temporale degli avvenimenti nel sistema. La sincronizzazione delle macchine

infatti, genera dei file di log temporalmente omogenei tra loro, che permettono di ricostruire con certezza l'ordine di accadimento degli eventi intervenuti a tutti i livelli del sistema, e di individuare la sequenza di svolgimento delle varie operazioni.

Torna al sommario

8.4 Procedure di gestione e di evoluzione

Il sistema di conservazione di InfoCert e il processo da questi implementato rispondono interamente alle norme di legge che regolano la materia.

La progettazione e il continuo miglioramento del sistema di conservazione sono il frutto di una intensa opera di confronto tra le professionalità e le competenze delle diverse funzioni aziendali, al fine di giungere all'erogazione di un sistema pienamente conforme alle norme, architetturalmente stabile, affidabile, e che garantisca elevati livelli di servizio all'utente in condizioni di assoluta sicurezza, certezza degli accessi e tracciabilità delle operazioni.

Punto fondante del processo di progettazione è l'attenta disamina delle norme, al fine di definire puntualmente i requisiti legali che il sistema deve possedere per assicurare la corretta implementazione della conservazione.

Il rispetto dei requisiti di legge è la condizione imprescindibile per l'erogazione del servizio. Oltre a questi sono definiti ulteriori requisiti funzionali, di architettura e di connettività e interoperabilità. I requisiti funzionali, individuati dal gruppo di competenza, rispondono all'obiettivo di offrire al Soggetto Produttore le funzionalità da questi richieste, mentre i requisiti di architettura e di interoperabilità rispondono alla necessità di sviluppare e mantenere un sistema stabile, in linea con le evoluzioni tecnologiche e capace di interfacciarsi con gli altri sistemi sviluppati dall'azienda, sfruttando le economie di scala e di conoscenza.

I Responsabili InfoCert, infatti, sono costantemente impegnati nell'attività di 'technology watch' attraverso la partecipazione a gruppi di lavoro nazionali e internazionali, forum e associazioni di settore con lo scopo di monitorare e prevenire l'obsolescenza tecnologica sia logica che fisica.

Torna al sommario

8.4.1 Criteri di organizzazione del contenuto

Gli oggetti della conservazione sono trattati dal sistema di conservazione in pacchetti informativi in cui i documenti sono corredati da tutta una serie di metadati. I documenti inviati al sistema di conservazione, infatti, vengono aggregati secondo criteri di omogeneità secondo le informazioni di configurazione definite in fase contrattuale. In particolare, vengono concordati i parametri fondamentali (bucket, policy, classi documentali) con i quali sono organizzati i documenti presi in carico, per consentire la maggiore interoperabilità possibile tra i sistemi di conservazione.

Se le tipologie documentali conservate sono di tipo sanitario (es. referti, immagini diagnostiche, ecc..) si provvede alla conservazione in ambienti separati e cripatati, in ottemperanza della normativa sulla privacy e sulla data protection.

Torna al sommario

8.4.2 Organizzazione dei supporti

Come atto conclusivo della procedura di conservazione, i documenti vengono memorizzati nel sistema di storage, contenenti tutti i documenti inviati in conservazione e i relativi file IPdA in conformità alle Regole AgID, OAIS e UNI SInCRO.

Torna al sommario

8.4.3 Archivio dei viewer consegnati dal Soggetto Produttore

InfoCert ha stabilito dei formati standard per i documenti da inviare in conservazione, dettagliati nei ‘Dati Tecnici di attivazione’ a disposizione del Soggetto Produttore e nel DPCM del 3 dicembre 2013, per i quali l'azienda definisce e mette a disposizione dei Soggetti Produttori i relativi viewer, mantenendoli aggiornati. Al momento dell'attivazione del servizio, il Soggetto Produttore verifica che i documenti inviati siano nel formato standard e siano leggibili con il software definito da InfoCert.

Se un Soggetto Produttore ha l'esigenza di inviare in conservazione documenti in formati differenti da quelli definiti standard, provvede a fornire ad InfoCert, tramite apposita funzionalità dell'applicativo dell’interfaccia di LegalDoc, il relativo software di visualizzazione.

Se il Soggetto Produttore invia documenti in formato non standard senza depositare il relativo visualizzatore, oppure nel caso di invio di documenti in modalità cifrata, è sua cura la conservazione degli strumenti necessari per la decifratura e/o la visualizzazione di quanto conservato.

Il Responsabile del servizio della Conservazione mantiene i programmi consegnati in un apposito database sottoposto a un periodico processo di back-up; in questo processo, il Responsabile è supportato dalle apposite procedure automatiche del sistema.

Torna al sommario

8.4.4 Archivio dell'hardware e del software obsoleto

La tenuta di un archivio dell'hardware e dei sistemi operativi ormai obsoleti ma necessari alla visualizzazione dei documenti conservati non è esplicitamente prevista dalla norma, ma è un'attività che si desume dall'obbligo di tenuta dell'archivio dei software nelle eventuali diverse versioni, e a questo direttamente correlata e fa parte delle misure per combattere l'obsolescenza dei formati, citate all'art. 7 comma 1 lettera g) dal Decreto 2013.

Il progresso tecnologico dei sistemi, tuttavia, può portare all'impossibilità di utilizzare i viewer definiti dal Soggetto Produttore, se divenuti obsoleti, sulle macchine di ultima generazione, rendendo di fatto impossibile la presa di conoscenza del contenuto del documento e inficiandone così la validità legale nel tempo. Per far fronte a questo rischio, il Responsabile del servizio della Conservazione mantiene un archivio di tutte le componenti hardware e software non più compatibili con i programmi di visualizzazione garantiti e/o depositati dal Soggetto Produttore, nel caso questi siano i soli strumenti che consentono di rendere leggibile i documenti conservati associati a tale viewer.

Torna al sommario

9. MONITORAGGIO E CONTROLLI

InfoCert possiede un sistema di gestione integrato che risponde attualmente ai requisiti delle norme ISO 9001, 27001, 20000 e 14001.

È inoltre un Qualified Trust Service Provider (ETSI EN 319 401) per i servizi di certificazione qualificata di: firme elettroniche, sigilli elettronici, validazione temporale e autenticazione siti web.

Particolare attenzione viene quindi posta nel mantenimento di livelli di servizio. attraverso l'dozione di un modello di Service Management System conforme alla citata norma ISO/IEC 20000 ha permesso infatti di:

- mappare ed integrare i Livelli di Servizio (SLA) garantiti ai clienti in relazione ai Livelli di servizio operativi garantiti internamente e quelli contrattuali garantiti dai fornitori;
- strutturare e governare la catena di composizione del valore dei servizi;
- ottimizzare la gestione dei processi aziendali integrando processi produttivi con processi di business fornendo un modello per la gestione sui servizi erogati;
- facilitare l'allineamento tra i requisiti del cliente e l'offerta InfoCert impostando/definendo accordi di servizio formalizzati e misurabili (SLA) e garantiti;
- garantire un controllo dei fornitori che concorrono alla erogazione dei nostri servizi;
- migliorare la qualità dei servizi di business erogati.

Di seguito lo schema rappresentativo del Modello adottato da InfoCert:

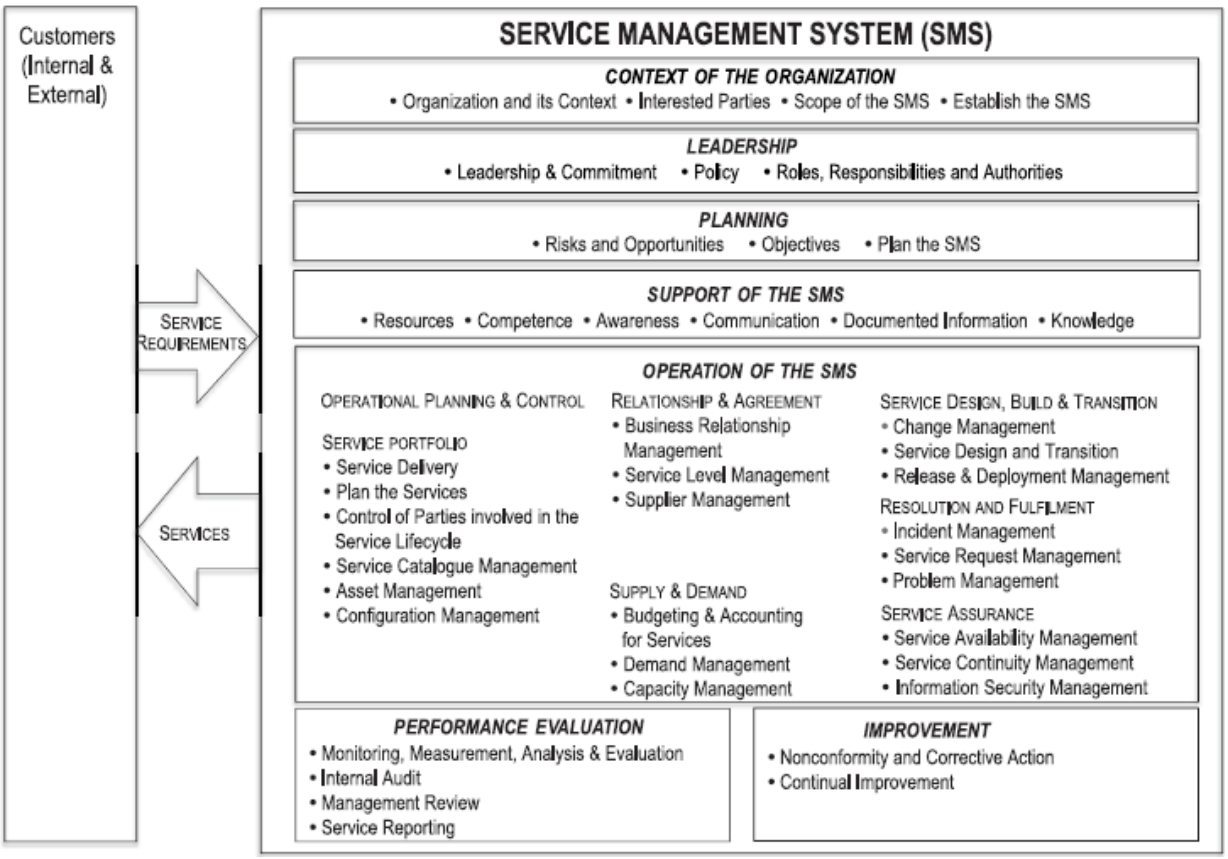


Figura 2 Rappresentazione grafica processi della norma ISO/IEC 20000:11

Le attività di istituzione, attuazione, monitoraggio e sviluppo del Service Management System-SMS seguono il modello ciclico PDCA che si sviluppa nelle seguenti fasi:

- istituzione del sistema - SMS (Plan) in cui si definiscono e si pianificano le politiche e i requisiti per la gestione dei servizi inerenti il campo di applicazione; si stabiliscono gli obiettivi di gestione del servizio a tutti i livelli pertinenti.
- implementazione ed attuazione del sistema-SMS (Do) e dei processi di design, transition, delivery e improvement continuo dei servizi sulla base di quanto definito nel

service management plan, con particolare attenzione al controllo delle modifiche al SMS valutando e limitando I rischi.

- azioni di monitoraggio e revisione del sistema-SMS (Check);
- attuazione di misure a miglioramento del sistema-SMS (Act) ove sono pianificate e attuate idonee azioni correttive sulla base dei risultati della fase precedente.

Il processo di gestione dei Livelli di Servizio [Service Level Management] è considerato un processo cardine del Service Management System in quanto ha effetto sui tre obiettivi principali quali:

- allineare i servizi di business con i bisogni correnti e futuri del cliente
- coordinare i requisiti del mercato sui servizi offerti con gli obbiettivi aziendali
- migliorare la qualità dei servizi di business erogati
- fornire attraverso gli SLA una base per la determinazione del valore del servizio.

Nello specifico InfoCert ha definito degli SLA baseline di riferimento in relazione ai seguenti KPI (Key Performance Indicator):

- Orario di servizio
- Disponibilità di servizio.

Torna al sommario

9.1 Procedure di monitoraggio

La soluzione di monitoraggio, nel seguito denominata TMS, è fornita dal Gruppo Sintesi che si occupa della completa gestione di tutta la piattaforma.

TMS si occupa di monitorare e misurare tutto lo stack tecnologico usato per erogare i servizi InfoCert, infatti non è solo in grado di dire se un servizio o un particolare componente hardware stanno funzionando correttamente, ma è anche in grado di misurarne le risorse utilizzate e le performance.

La piattaforma è costruita a partire da una versione customizzata del noto software open source Nagios e per rilevare i dati dai diversi componenti utilizza diverse tecnologie (SNMP, NRPE, Sahi, ecc.), inoltre, è stata sviluppata l'integrazione con la piattaforma di controllo *Cloudwatch*, tool nativo di AWS consente di avere il pieno controllo e la gestione delle metriche di tutte le componenti presenti in cloud I monitoraggi possono essere eseguiti in modalità attiva (quindi la piattaforma interroga puntualmente le diverse componenti) oppure in modalità passiva (ovvero sono le singole componenti che inviano dati alla piattaforma, senza il bisogno di venire interrogate da essa).

L'infrastruttura di monitoraggio, ad oggi, è composta da:

- due apparati fisici (denominati probe) posizionati all'interno del Data Center,
- una probe posizionata all'interno dei locali della CA,
- un'altra probe posizionata nel sito di DR.

Alle quattro probe fisiche si aggiunge un pool di macchine virtuali posizionate nella server farm di *Clouditalia* e la piattaforma *Cloudwatch* posizionata in AWS Le probe fisiche si occupano di effettuare i monitoraggi sull'infrastruttura ed i servizi ospitati nei locali nei quali sono installate mentre le macchine virtuali si occupano di effettuare le navigazioni dei servizi sia da rete interna che tramite internet, *Cloudwatch* invece gestisce i monitoraggi di tutte le metriche infrastrutturali presenti in AWS. Tutti i dati raccolti vengono infine centralizzati su una piattaforma resa disponibile online per una veloce e facile consultazione degli stessi.

Oltre alle misurazioni effettuate sull'infrastruttura e la verifica del traffico dati tra il cloud e il DC, il sistema di monitoraggio è in grado di misurare anche le performance dei servizi, infatti tramite le navigazioni effettuate dalle macchine virtuali si riesce a capire se un servizio è disponibile e anche quanto tempo impiega per effettuare una certa elaborazione.

Con tutti i dati raccolti si popola una base di dati in ottica di Business Intelligence che risulta di fondamentale importanza per la redazione della reportistica riguardante gli SLA dei vari servizi ma anche, e soprattutto, per supportare i processi di decisione aziendale.

La soluzione di monitoraggio fin qui descritta risulta indispensabile per individuare tempestivamente eventuali anomalie sui servizi erogati da InfoCert, ma soprattutto è in grado di segnalarci su quale dei molti componenti che compongono un servizio andare a concentrare l'azione correttiva per una rapida risoluzione degli incident.

Torna al sommario

9.1.1 Processi di monitoraggio del sistema di conservazione

Il monitoraggio del sistema di conservazione si esplica su due diversi livelli operativi:

- sistema di monitoring della disponibilità del sistema
- sistema di monitoring dell'integrità degli archivi.

Torna al sommario

9.1.2 Monitoring della disponibilità del sistema

Tale operazione viene svolta coerentemente con le procedure di monitoring generali di InfoCert. In particolare, tutte le componenti costituenti il sistema di conservazione, ovvero i servizi applicativi, i processi di elaborazione batch e le interfacce per l'utente finale sono monitorate con i tool definiti nella piattaforma di monitoraggio TMS precedentemente descritta.

A fronte di anomalie rilevate lo strumento invia delle segnalazioni al Service Desk InfoCert che le gestisce in conformità ai processi di Incident Management e, se necessario, Problem Management. Tali processi sono descritti nelle procedure che definiscono il Sistema di gestione integrato InfoCert.

Torna al sommario

9.2 Verifica dell'integrità degli archivi

Il sistema di memorizzazione utilizzato, grazie alle caratteristiche intrinseche dei supporti, alla configurazione architetturale e alle procedure di memorizzazione permanente dei dati, garantisce l'immodificabilità, l'integrità, la leggibilità e la reperibilità nel sistema di quanto conservato, ai fini della corretta esibizione.

Il sistema mantiene traccia di tutte le operazioni effettuate sui documenti in appositi file di log.

Inoltre, è garantita la tracciatura di tutti i documenti richiamati dal Soggetto Produttore mediante interrogazione al sistema e conseguentemente esibiti, che rappresenta un'ulteriore prova di leggibilità, effettuata direttamente dal Soggetto Produttore.

In aggiunta, come descritto dall'art. 7 comma 1 lettera g) del DPCM del 3 dicembre 2013, "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", InfoCert, per rispondere a tali richieste, ha attivato sottosistemi di controllo automatico dedicati alla simulazione della navigazione nel sistema e delle operazioni che effettua l'utente, svolgendo controlli di coerenza dei dati e attività di ripristino da situazioni di errore.

In ogni occasione in cui il file viene copiato o spostato di posizione, funzionalità automatiche verificano che le sue dimensioni non siano mutate durante lo spostamento e che non siano intervenute alterazioni, che possano inficiarne la visualizzazione.

Il Responsabile del servizio della Conservazione, come descritto nell'art. 7 comma 1 lettera f) "assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità" dei documenti conservati con procedure automatiche e manuali, al fine di prevenire il rischio che i documenti non possano essere visualizzabili, inficiando il mantenimento della loro validità legale nel tempo.

L'apposita procedura, detta verificatore, esegue il test di leggibilità binaria mediante il continuo calcolo delle impronte dei documenti conservati, con successivo confronto con l'hash del documento contenuto nel file delle direttive della conservazione inviato dal Soggetto Produttore. Se la procedura non registra differenze tra i due hash, il documento è inalterato rispetto a quanto trasmesso dal Produttore.

Vengono eseguiti i seguenti passi operativi:

- verifica della validità della firma digitale e della marcatura temporale apposte all'atto della conservazione dal Responsabile del servizio della Conservazione sul file IPdA e, se presenti, verifica della firma digitale e della marcatura temporale del documento;
- calcolo dell'impronta del documento e confronto con quella contenuta all'interno del file IPdA;

- generazione di un report che viene automaticamente sottoposto alla conservazione nell'area dedicata al Responsabile del servizio della Conservazione (quindi a sua volta firmato e marcato temporalmente dal Responsabile del servizio della Conservazione stesso).

La procedura appena descritta viene applicata sia sul supporto primario sia su quello secondario.

In caso di anomalie, se il documento risulta corrotto in uno dei due repository, il sistema tenta il ripristino automatico con il dato presente nel repository integro. Se invece ambedue le copie sono alterate, viene inviato un alert al Responsabile del servizio della Conservazione, che tenterà il ripristino manuale partendo da un'altra sorgente (per esempio le copie di backup). Se nessuna sorgente è disponibile viene redatto un verbale di incidente, sottoscritto e conservato dal Responsabile del servizio della Conservazione per attestare la situazione rilevata. Analoga procedura viene applicata in caso di perdita di tutte le copie del dato.

Periodicamente, il sistema produce dei report di sintesi dell'attività di verifica svolta.

In aggiunta alla verifica automatica dell'integrità binaria, il Responsabile del servizio della Conservazione e i suoi Responsabili incaricati sono dotati di apposita strumentazione (detta CORE, Console del Responsabile), con credenziali dedicate, con la quale procedono manualmente e periodicamente ad una verifica campionaria di leggibilità dell'archivio documentale conservato, scegliendo ed esibendo casualmente un campione di documenti presenti nel sistema di conservazione.

Viene poi redatto automaticamente un verbale che attesta l'elenco dei documenti visualizzati, successivamente sottoscritto e conservato dal Responsabile del servizio della Conservazione nell'area appositamente creata nel sistema di conservazione.

9.3 Controlli

Oltre ai monitoraggi appena descritti, il sistema di conservazione implementa numerosi sotto-processi dediti al controllo del corretto svolgimento dei processi, segnalando eventuali errori o anomalie al Soggetto Produttore o al personale incaricato dell'amministratore del sistema.

I controlli effettuati si distinguono nelle tre tipologie: controlli di versamento, controlli di

processo e controlli periodici.

Torna al sommario

9.3.1 Controlli di versamento

In fase di versamento dei pacchetti in LegalDoc vengono automaticamente eseguiti dei controlli, preventivamente concordati con il soggetto Produttore nelle 'Specificità del contratto' all'attivazione del servizio e che riguardano:

- abilitazione utenza al versamento;
- validità sessione in uso (di default della durata di un'ora tra login e logout);
- struttura del file di Parametri (contenente le informazioni per la leggibilità nel tempo del documento da conservare);
- struttura del file di Indici (contente i metadati del documento da conservare, alcuni dei quali obbligatori, in coerenza con i 'Dati Tecnici di attivazione');
- mime type dichiarato in coerenza con i 'Dati Tecnici di attivazione';
- dimensione massima del documento da conservare (di default 256 megabyte, variabile su richiesta);
- presenza nello stesso path dello stesso nome-file (su richiesta);
- validità del certificato qualificato di firma digitale con cui è sottoscritto il documento da conservare (su richiesta).

InfoCert non effettua controlli sull'eventuale presenza di virus nei pacchetti di versamento, che sono conservati in LegalDoc alla stregua di tutti gli altri file.

Torna al sommario

9.3.2 Controlli di processo di progettazione e sviluppo dei servizi

L'organizzazione garantisce che non vengano rilasciati prodotti/servizi per i quali non siano state completate le attività di controllo della qualità citate nelle relative procedure di rilascio.

Per maggiori dettagli si rimanda a "PR/235 Progettare e sviluppare un servizio informatico InfoCert", "PR/225- Change Management InfoCert", "Service Management System-SMS".

Torna al sommario

9.3.3 Monitoraggio e registrazioni durante il ciclo produttivo

Lungo l'intero ciclo produttivo si effettuano i controlli al fine di verificare la conformità del prodotto e del processo a quanto previsto dalle procedure applicabili.

Nelle procedure “PR/235 Progettare e sviluppare un servizio informatico InfoCert” e “PR/225- Change Management InfoCert” sono indicate le fasi specifiche per i controlli, i test e le misurazioni del prodotto/servizio in termini di ciclo di vita, tecniche, metriche del SW, gestione dei controlli, dello “sforzo/effort”, tenuta in controllo dei costi e dei tempi di realizzazione, la definizione dei mezzi e delle risorse necessarie.

Il prodotto/servizio è oggetto di un processo progressivo di accettazione: le registrazioni documentano la conformità del prodotto ai criteri di accettazione e indicano la persona che autorizza il rilascio.

Il prodotto/servizio è predisposto per la consegna al cliente ad esito positivo delle prove, controlli e collaudi. I prodotti che non superano le prove, i controlli e i collaudi sono sottoposti alla procedura per il trattamento dei prodotti non conformi.

Torna al sommario

9.3.4 Monitoraggio e registrazioni per collaudo finale

Il prodotto/servizio corrispondente ai requisiti contrattuali è oggetto di un processo progressivo di accettazione che viene attivato in occasione di ogni consegna ufficiale al Produttore, o di una accettazione globale fatta alla fine del processo produttivo secondo quanto previsto dalla procedura.

Torna al sommario

9.3.5 Controlli periodici

In InfoCert è attiva una struttura appositamente preposta alla supervisione e controllo della gestione dei problemi e del rispetto dei livelli del sistema per tutte le applicazioni.

La struttura si avvale di un gruppo di lavoro trasversale all'azienda ed effettua la raccolta dei dati relativi al funzionamento dei servizi.

Il gruppo si riunisce con una periodicità mensile al fine di individuare le cause dei malfunzionamenti registrati nel periodo, analizzare le soluzioni contingenti adottate per il superamento del problema e sviluppare eventuali proposte per rimedi strutturali.

Torna al sommario

9.4 Soluzioni adottate in caso di anomalie

Ad ogni semestre il Responsabile del servizio della Conservazione effettua un riesame generale del sistema insieme ai soggetti incaricati, al fine di accertare la conformità del sistema al livello atteso, analizzare le cause di eventuali incidenti o disservizi e promuovere attività di prevenzione o miglioramento.

Qualora necessario, una riunione di riesame può essere indetta a fronte di particolari eventi (ad esempio, a titolo non esaustivo, cambi tecnologici, normativi o di requisiti funzionali, stagionalità di carico elaborativo, arrivo consistente e non pianificato di nuova clientela, ecc.).

Torna al sommario

9.4.1 Auditing generale del sistema

Il Programma di AUDIT aziendale è attuato secondo le procedure del Sistema Integrato di Gestione.

Gli Audit sono condotti, sempre secondo le citate procedure, con il fine di determinare se i processi aziendali:

- sono in accordo con quanto previsto nei documenti di riferimento
- sono compliant alla normativa di riferimento
- sono compliant agli standard adottati dal sistema di conservazione
- sono attuati efficacemente
- sono idonei al conseguimento degli obiettivi della Qualità e miglioramento servizi

In ogni processo aziendale, le modalità di audit sono improntate alle indicazioni dello standard UNI EN ISO 19011 ed hanno per oggetto:

- strutture organizzative
- risorse utilizzate
- procedure
- processi
- prodotti e i risultati dell'attività
- documentazione
- addestramento
- segnalazioni dei clienti e terze parti.

Le attività di audit sono in capo all'Area Management System che le esegue direttamente o le delega a personale esterno qualificato.

Oltre alle verifiche ispettive sopra descritte indirizzate al Sistema Gestione Qualità, sono pianificati e condotti audit su tutti gli altri componenti del Sistema di Gestione Integrato (SGSI-ISO 27001, SMS-ISO 20000, SGA-ISO14001, Verifiche di interoperabilità condotte da AgID, Privacy, Sicurezza Fisica, M231/01 ecc.).

Relativamente al SGA-ISO14001 l'attività di audit comprende anche la verifica di conformità legislativa.

Relativamente al SGA-ISO14001 l'attività di audit comprende anche la verifica di conformità legislativa.

Il processo prevede inoltre la gestione controllata di tutti gli Audit esterni svolti dagli Enti istituzionali, relativi ai Sistemi di Gestione ed ai Prodotti/Servizi certificati.

A fronte di non conformità rilevate in sede di verifica ispettiva, il Responsabile della Struttura Organizzativa valutata definisce un piano di attuazione delle azioni correttive o migliorative richieste.

Il Responsabile delle verifiche e ispezioni (auditing) pianifica e implementa processi di audit che coinvolgono aspetti di processo, organizzazione, tecnologici e logistici. L'obiettivo è accertare la conformità del sistema alle leggi, ai regolamenti, al contratto, alla

documentazione generale del sistema, ai principi che ispirano il sistema qualità e al presente Manuale della Conservazione.

L'audit è un processo fondamentale per lo screening del sistema, in quanto consente l'individuazione delle aree critiche d'intervento e la pianificazione dei necessari interventi sul sistema, ragion per cui è svolto periodicamente.

Torna al sommario

9.4.2 Incident management

L'ambito completo del processo si applica alla gestione degli incidenti informatici che possono interessare uno o più servizi tecnologici eventualmente interconnessi ed è formalmente descritto dalla procedura 'PR455-Incident Management InfoCert'. La procedura definisce anche la metodologia di assegnazione della gravità di un incidente e della relativa priorità di gestione in base alla matrice di analisi di impatto/urgenza effettuata utilizzando le informazioni sul servizio di riferimento e sui relativi SLA del servizio o nelle istruzioni /policy specifiche relative alla sicurezza informatica.

Urgenza ⇨ Impatto⇩	ALTA	MEDIA	BASSA
ALTO	Critica	Alta	Media
MEDIO	Alta	Media	Bassa
BASSO	Media	Bassa	Molto bassa

L'impatto è definito in base alla BIA [Business Impact Analisys] del servizio.

L'urgenza è dettata dallo SLA di disponibilità del servizio.

Il processo di gestione degli incidenti, condotto secondo le raccomandazioni delle Best Practice ITIL e in conformità alle norme ISO 27001, si focalizza sulle modalità di gestione e di ripristino tempestivo degli incidenti informatici.

Il modello organizzativo prevede che il supporto specialistico sistemistico sia gestito dall'area di Product Factory che gestisce il ciclo di vita dell'incidente con gli strumenti per la rilevazione e tracciamento degli eventi.

Il processo d'Incident Management, che ha lo scopo di minimizzare impatti e tempi di disservizio, alimenta il processo di Problem Management (PR456), che a sua volta ha lo scopo di prevenire il verificarsi e il ripetersi di tali errori.

A tale scopo il Problem Management cerca di individuare la causa principale degli incidenti e ne attua le opportune azioni preventive, correttive e/o migliorative.

I processi di Incident Management e Problem Management sono soggetti a un miglioramento continuativo.

Il Responsabile del servizio della Conservazione mantiene il verbale degli incidenti e delle contromisure attuate sono inviate al sistema di conservazione.

Torna al sommario

10. SPECIFICITÀ DEL CONTRATTO

I servizi sono regolati dai seguenti documenti contrattuali, che contengono e descrivono tutte le esigenze richieste dai Soggetti Produttori.

La documentazione contrattuale e tecnica elencata è resa disponibile all'atto del perfezionamento dell'accordo di servizio al Produttore.

1. ***Condizioni Generali di Contratto*** che regola la vendita del servizio di conservazione nelle diverse modalità di erogazione;
2. ***Richiesta di attivazione*** che comporta l'adesione al servizio e disciplina le condizioni economiche;
3. ***Dati tecnici per l'attivazione*** con cui il Soggetto Produttore fornisce tutte le informazioni necessarie su tipologie documentali, metadati e credenziali di accesso di cui necessita;
4. ***File di configurazione*** redatto da InfoCert all'attivazione del servizio, contiene i dati di configurazione del soggetto produttore, delle user d'accesso, delle policy associate e delle tipologie documentali, comprensivi di metadati e formati configurati;
5. ***Atto di affidamento*** che rappresenta la formalizzazione dell'affidamento ad InfoCert del processo di conservazione, la nomina del Responsabile del trattamento dei dati personali ai sensi del Regolamento UE n. 679/2016 GDPR, e stabilisce espressamente quali attività di fatto vengano assunte da InfoCert e quali, al contrario, rimangano a carico dell'affidatario, Soggetto Produttore, come stabilito dagli articoli 5 e 6 del DPCM del 3 dicembre 2013;
6. ***Specifiche Tecniche di integrazione (sia per i web services che per LegalDoc Connector)*** che fornisce tutte le informazioni tecniche necessarie ad operare l'integrazione tra i Sistemi di Gestione documentali del Produttore e il sistema di conservazione di InfoCert;
7. ***Impegno alla riservatezza***;
8. ***Allegato Tecnico*** che descrive le modalità di fornitura del servizio e l'infrastruttura tecnico-tecnologica utilizzata per la sua erogazione;

9. ***Manuale Utente*** che risponde alla necessità di documentare operativamente il processo dal punto di vista del Produttore/Utente;
10. ***Descrizione dei codici di errore*** per fornire una casistica esaustiva dei possibili messaggi di errore del servizio di conservazione e delle azioni che è necessario intraprendere per porvi rimedio.

La documentazione relativa alle procedure e/o ai processi interni di InfoCert, invece, è resa disponibile solo su esplicita richiesta del Soggetto Produttore e all'atto del perfezionamento di una specifica NDA (non-disclosure agreement).

Per i Soggetti Produttori con una infrastruttura tecnologica complessa viene redatto un '**Manuale dei processi per la conservazione**', che rimanda al presente Manuale per quanto riguarda le sezioni standard (es. Struttura organizzativa e Ruoli di responsabilità del Conservatore, Dettaglio tecnico del sistema di conservazione e trattazione dei pacchetti di archiviazione, Monitoraggio e controlli del Conservatore), e dettaglia le specificità del singolo Produttore (es. modalità di versamento o esibizione, tipologie documentali, metadati scelti, infrastrutture tecnologiche particolari).

Torna al sommario

MANUALE DEL SISTEMA DI CONSERVAZIONE

Sommario

Indice delle figure

Registro delle versioni

Revisione	Data	Motivo Revisione	Redatto da	Approvato da
1.0	03/10/2009	Emissione	Resp. funzione archivistica	Resp. servizio di conservazione
2.0	12/02/2010	Aggiornamento funzionalità	Resp. funzione archivistica	Resp. servizio di conservazione
3.0	20/06/2010	Aggiornamento funzionalità	Resp. funzione archivistica	Resp. servizio di conservazione
4.0	28/09/2010	Aggiornamento funzionalità	Resp. funzione archivistica	Resp. servizio di conservazione
5.0	15/10/2010	Aggiornamento funzionalità	Resp. funzione archivistica	Resp. servizio di conservazione
6.0	10/02/2011	Modifica gestione anomalie – Ampliamento funzionalità Unistorage	Resp. funzione archivistica	Resp. servizio di conservazione
7.0	20/05/2011	Aggiornamento composizione societaria Unimatica-RGI	Resp. funzione archivistica	Resp. servizio di conservazione
8.0	30/11/2012	Aggiornamento Data Center	Resp. funzione archivistica	Resp. servizio di conservazione
8.1	11/12/2012	Personalizzazioni	Resp. funzione archivistica	Resp. servizio di conservazione
8.2	20/06/2013	Aggiornamento compiti e responsabilità della conservazione	Resp. funzione archivistica	Resp. servizio di conservazione
8.3	04/07/2013	Aggiornamento normative	Resp. funzione archivistica	Resp. servizio di conservazione
8.4	05/02/2014	Aggiornamento normative	Resp. funzione archivistica	Resp. servizio di conservazione
8.5	11/02/2014	Aggiornamento Data Center	Resp. funzione archivistica	Resp. servizio di conservazione
8.6	05/03/2014	Adeguamento normative	Resp. funzione archivistica	Resp. servizio di conservazione
8.7	17/02/2015	Adeguamento DPCM 03/12/2013	Resp. funzione archivistica	Resp. servizio di conservazione
8.8	15/10/2015	Passaggio alla ISO 27001:2013	Resp. funzione archivistica	Resp. servizio di conservazione
8.9	20/01/2016	Adeguamento Schema Manuale della conservazione AgID	Resp. funzione archivistica	Resp. servizio di conservazione
9.0	11/04/2017	Modifica ruolo Responsabile della Funzione Archivistica	Resp. funzione archivistica	Resp. servizio di conservazione
9.1	14/06/2017	Aggiornamento definizioni per termine “Produttore”	Resp. funzione archivistica	Resp. servizio di conservazione
9.2	05/10/2017	· Aggiornamento Server farm · Visualizzazione di 200 risultati da portale	Resp. funzione archivistica	Resp. servizio di conservazione
9.3	20/10/2017	· Capitolo Trasparenza · Aggiornamento elenco formati · Aggiunto testo alternativo mancante su alcune immagini · Sostituita immagine 7 precedentemente con parti nascoste	Resp. funzione archivistica	Resp. servizio di conservazione
9.4	25/10/2018	· Aggiornamento par. 1.1 adeguamento GDPR · Modifica ruolo Privacy Manager cap. 4 · Aggiornamento tabella normativa par. 3.1 · Aggiunto ruolo DPO al par.4.1	Resp. funzione archivistica	Resp. servizio di conservazione

Revisione	Data	Motivo Revisione	Redatto da	Approvato da
9.5	29/01/2019	· Recepimento N.C. AgID Recepimento Oss. Audit interno · Aggiornamento Nomina ad Interim Responsabile della funzione archivistica · Aggiornamento proc. Gestione Incident par. 8.1.3	Res. funzione archivistica	Resp. servizio di conservazione
9.6	19/04/2019	· Revoca nomina ad Interim per la Responsabilità della funzione archivistica · Aggiornamento nomina ad interim DPO	Res. funzione archivistica	Resp. servizio di conservazione
9.7	27/09/2019	· Aggiornamento Ruoli (Delegato Responsabile del servizio di conservazione – Responsabile dello sviluppo e della manutenzione – Responsabile dei sistemi informative – DPO) · Aggiornamento proc. Gestione Incident par. 8.1.3 · Aggiornamento estensioni ISO 27017 – 27018 · Aggiornamento descrizione par. 7.5 Rifiuto PDV	Res. funzione archivistica	Resp. servizio di conservazione
9.8	20/12/2019	· Aggiornamento capp. 4 e 5 a seguito della sostituzione del Delegato alla Responsabilità del servizio di conservazone, della Responsabile della funzione archivistica e della Responsabile dello sviluppo e manutenzione · 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 incident di sicurezza.	Res. funzione archivistica	Resp. servizio di conservazione
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	Res. funzione archivistica	Resp. servizio di conservazione
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)	Res. funzione archivistica	Resp. servizio di conservazione
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)	Res. funzione archivistica	Resp. servizio di conservazione

1. Scopo e ambito del documento

Il presente documento costituisce il Manuale del servizio di conservazione erogato da Unimatica-RGI 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-RGI, 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-RGI, a partire dalla data di sottoscrizione del contratto, il Soggetto produttore, nella sua qualità di Titolare del trattamento, affida a Unimatica-RGI, 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-RGI deve attenersi:

1. Unimatica-RGI 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-RGI 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-RGI 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-RGI, nella sua qualità di Responsabile del trattamento, in particolare è tenuta a:

a) effettuare tutte le operazioni in termini di mansioni, definendo regole e modelli di comportamento che assicurino la riservatezza e il rispetto del divieto di comunicazione e diffusione dei dati ai quali si ha accesso;

b) trattare direttamente, o per il tramite dei propri dipendenti, collaboratori esterni, consulenti, etc. - designati autorizzati al trattamento - i dati personali del Soggetto produttore, Titolare del trattamento, 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, nonché, infine, dalle presenti istruzioni;
c) non 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;
d) collaborare con il Titolare per garantire la puntuale osservanza e conformità alla normativa in materia di protezione dei dati personali;
e) incaricare per iscritto i soggetti che abbiano le caratteristiche di Responsabili di Sistema e di Amministratori di Sistema, tenerne l'elenco aggiornato a disposizione del Soggetto produttore e fornirne eventualmente copia a semplice richiesta dello stesso;
f) adottare, se del caso, adeguate misure di sicurezza, in modo da ridurre al minimo i rischi di distruzione e perdita, anche accidentale dei dati/documenti stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
g) informare immediatamente il Soggetto produttore di qualsiasi richiesta o comunicazione da parte dell'Autorità Garante e/o Giudiziaria, per concordare congiuntamente l'evasione delle stesse;
h) collaborare con il Soggetto produttore per l'attuazione delle prescrizioni eventualmente impartite dall'Autorità Garante;
i) comunicare al Soggetto produttore qualsiasi accadimento che possa compromettere il corretto trattamento dei dati personali;
j) segnalare eventuali criticità al Soggetto produttore che possono mettere a repentaglio la sicurezza dei dati, al fine di consentire idonei interventi da parte dello stesso;
k) prestare particolare attenzione all'eventuale trattamento di dati personali rientranti nelle categorie particolari e/o relative a condanne penali o reati degli interessati conosciuti, anche incidentalmente, in esecuzione dell'incarico affidato, procedendo alla loro raccolta e archiviazione 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.
5. 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.
6. Unimatica-RGI, nella sua qualità di Responsabile esterno del trattamento, si impegna a notificare al Soggetto produttore, Titolare del trattamento, senza ingiustificato ritardo dall'avvenuta conoscenza, e comunque entro 24 ore dalla scoperta con comunicazione da inviarsi all'indirizzo PEC del Soggetto produttore, (salvo diversa email indicata) ogni violazione dei dati personali (*data breach*). Unimatica-RGI si impegna a prestare ogni più ampia assistenza al Soggetto produttore al fine di consentirgli di assolvere agli obblighi di cui agli artt. 32 - 34 del GDPR.
Una volta definite le ragioni della violazione, Unimatica-RGI di concerto con il Soggetto produttore e/o altro soggetto da quest'ultimo indicato, si attiverà per implementare nel minor tempo possibile tutte le misure di sicurezza fisiche e/o logiche e/o organizzative atte ad arginare il verificarsi di una nuova violazione della stessa specie di quella verificatasi.
7. In esecuzione degli accordi in essere con il Soggetto produttore, Unimatica-RGI potrà affidare l'esecuzione - parziale o totale - delle relative attività 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, Unimatica-RGI , nella sua qualità di Responsabile esterno del trattamento, provvede personalmente a designare Responsabile 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 Soggetto produttore tramite il seguente link: https://www.unimaticaspa.it/it/gdpr-elenco-sub-responsabili.
8. Unimatica-RGI assicura che nessun dato personale potrà essere trasferito all'esterno dell'Area Economica Europea (EEA).

9. 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-RGI si rende disponibile a collaborare con il Soggetto produttore stesso fornendogli tutte le informazioni necessarie a soddisfare le eventuali richieste ricevute in tal senso.
10. Unimatica-RGI – 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.
11. Unimatica-RGI 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.
12. 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-RGI 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-RGI 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 sono disponibili:

- i contatti principali quali telefono, fax, email ed indirizzo.
- La certificazione per la Qualità ISO 9001:2015 (Unimatica-RGI 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-RGI 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-RGI sta implementando 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, verrà aggiunta alle altre presenti nella sezione Trasparenza.

Negli anni, il settore Conservazione di Unimatica-RGI 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-RGI 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, e della Privacy (ISO 27001, ISO 9001, ISO 14001) 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-RGI 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-RGI 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

La terminologia e gli acronimi utilizzati in questo manuale richiamano quelli elencati *nell'Allegato 1 Glossario dei termini e degli acronimi* alle Linee guida per la formazione, gestione e conservazione dei documenti informatici al quale si rimanda.

Torna al sommario

3. Normativa e standard di riferimento

Il sistema di conservazione sviluppato da Unimatica-RGI 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
Codice Civile	[Libro Quinto del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle Scritture contabili], art. 2215 bis – Documentazione informatica.
RD 1163/1911	Regolamento per gli archivi di Stato
DPR 1409/1963	Norme relative all'ordinamento ed al personale degli archivi di Stato
Legge 241/1990	Nuove norme sul procedimento amministrativo
DPR 445/2000	Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
DPR 37/2001	Regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli uffici dello Stato
D.lgs 196/2003	Recante il Codice in materia di protezione dei dati personali
D.lgs 42/2004	Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002,n.137
Legge 9 gennaio 2004, n. 4 aggiornata dal decreto legislativo 10 agosto 2018, n. 106	Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici
D.lgs 82/2005 e ss.mm.ii.	Codice dell'amministrazione digitale
D.lgs 33/2013	Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni
DPCM 22 febbraio 2013	Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71
DPCM 21 marzo 2013	Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni;

Reg. UE 910/2014	In materia di identificazione elettronica e servizi fiduciari per le transazionielettroniche nel mercato interno e che abroga la direttiva 1999/93/CE - Regolamento eIDAS;
Circolare 40 e 41 del 14 dicembre 2015 della Direzione generale degli archivi	Autorizzazionealla distruzione di originali analogici riprodotti secondo le regole tecniche di cui al DPCM 13.11.2014 econservati secondo le regole tecniche di cui al DPCM 13.12.2013;
Reg. UE 679/2016 (GDPR)	Relativo alla protezione delle persone fisiche con riguardo al trattamento deidati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
Circolare 18 aprile 2017 n. 2/2017 dell'Agenzia per l'Italia Digitale	Recante le misure minime disicurezza ICT per le pubbliche amministrazioni;
Circolare n. 2 del 9 aprile 2018	Recante i criteri per la qualificazione dei Cloud Service Provider per laPA;
Circolare n. 3 del 9 aprile 2018	Recante i criteri per la qualificazione di servizi SaaS per il Cloud dellaPA;
Reg. UE 2018/1807	Relativo a un quadro applicabile alla libera circolazione dei dati non personalinell'Unione europea;
DPCM 19 giugno 2019 n. 76	Regolamento di organizzazione del Ministero per i beni e le attivitàculturali, degli uffici di diretta collaborazione del Ministro e dell'Organismo indipendente di valutazione dellaperformance.
Linee guida AgID ed Allegati	Linee guida sulla Formazione, Gestione, Conservazione dei documenti informatici Allegato 1 Glossario dei termini e degli acronimi Allegato 2 Formati di File e Riversamento Allegato 3 Certificazione di processo Allegato 4 Standard e specifiche tecniche Allegato 5 Metadati
Regolamento AgID ed Allegati	Regolamento sui criteri di conservazione Allegato A Requisiti per l'erogazione del servizio di conservazione per conto delle pubbliche amministrazioni Allegato B Piano di cessazione del servizio di conservazione dei documenti informatici

Torna al sommario

3.2. Standard di Riferimento

Sigla	Titolo standard
UNI 11386	Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.
ISO 14721	OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione.
ISO 15836	Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core
ISO/TR 18492	Long-term preservation of electronic document-based information.
ISO 20652	Space data and information transfer systems - Producer-Archive interface - Methodology abstract standard.
ISO 20104	Space data and information transfer systems — Producer-Archive Interface Specification (PAIS).
ISO/CD TR 26102	Requirements for long-term preservation of electronic records.
SIARD	Software Independent Archiving of Relational Databases 2.0 Ministère de la

	culture et de la communication, Service interministériel des Archives de France, Standard d'échange de donnéès pour l'archivage. Transfert – Communication – Élimination – Restitution - Modification, ver. 2.1, 2018
METS	Metadata Encoding and Transmission Standard
PREMIS	PREservation Metadata: Implementation Strategies.
EAD (3)/ISAD (G)	
EAC (CPF)/ISAAR (CPF)/NIERA (CPF)	
SCONS2/EAG/ISDIAH	

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 della 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**, identificato come l'insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti.

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

Unimatica-RGI 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;
- giostione 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-RGI è **Silvano Ghedini**.

Nello svolgere le attività del processo di conservazione, Silvano Ghedini ha delegato l'esercizio complessivo di queste a **Paolo Vandelli** e **Cecilia Canova.**

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-RGI 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-RGI è **Massimo Ortensi**.

Privacy manager il quale si occupa di garantire:

- il rispetto delle vigenti disposizioni in materia di trattamento dei dati personali
- che il trattamento dei dati affidati dai Produttori dei PDV avvenga nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.

Il **Privacy manager di conservazione** nominato da Unimatica-RGI è **Silvano Ghedini**.

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-RGI 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.

La **Responsabile dello sviluppo e manutenzione del sistema di conservazione** nominata da Unimatica-RGI è **Annachiara Coviello**.

Nell'attribuire ruoli e responsabilità Unimatica-RGI 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-RGI, 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-RGI è **Anna Veltri.**

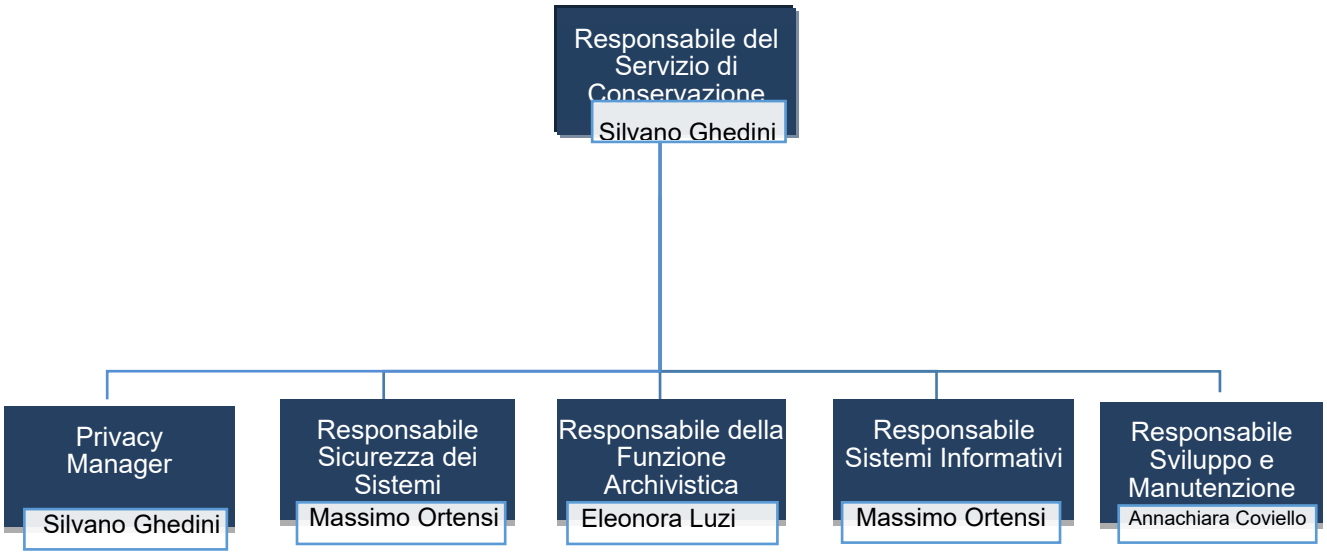
Torna al sommario

5. Struttura organizzativa per il servizio di conservazione

Il presente capitolo ha lo scopo di illustrare la struttura organizzativa del settore conservazione di Unimatica-RGI. 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[1] delle funzioni e delle responsabilità che intervengono nel processo di conservazione.

Torna al sommario

5.1. Organigramma



Torna al sommario

[1] 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[2].	Gli oggetti versati vengono trasformati in PdA contenenti, oltre agli oggetti da conservare, l'IdPA[3] 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	Prima della scadenza del periodo di conservazione, Unimatica-RGI contatta il Soggetto produttore il quale in caso di rescissione del contratto comunicherà in forma scritta la decisione. Unimatica-RGI eliminerà fisicamente i PdA. Per i PdA provenienti da enti pubblici o da archivi privati per i quali è stato	RSC RFA PM

[2] 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).
[3] Indice del pacchetto di archiviazione.

		dichiarato l'interesse culturale si terrà conto dei massimari di scarto di questi e della decisione ultima della Soprintendenza archivistica.	
6	Chiusura del servizio di conservazione (al termine di un contratto)	Il Soggetto produttore comunicherà ad Unimatica-RGI la rescissione del contratto.	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-RGI 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[4],

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-RGI 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-RGI 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-RGI, 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

[4] 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"

schemi si rimanda alle schede di dettaglio presenti all'interno dell'*Allegato 5* alle Linee guida e 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.

É 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: heck 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.

Tracciature 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.

É 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.

Tracciature 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-RGI, 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-RGI 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 ingestion (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 l'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-RGI 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[5]:

- l'oggetto o gli oggetti da conservare;

[5] Sono elencate le caratteristiche indicate nell'allegato 4 al DPCM 3 dicembre 2013 Regole tecniche in materia di sistema di conservazione.

- 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.

L'esibizione del materiale di interesse avviene via interfaccia web o mediante memorizzazione su supporto ottico. La descrizione dettagliata delle procedure è indicata nel capitolo 7 "Il processo di erogazione del servizio di conservazione", Fase 6.
Per quanto riguarda i Pacchetti di distribuzione memorizzati su supporto ottico, questi coincidono con i Pacchetti di archiviazione, come previsto delle Regole tecniche in materia di sistemi di conservazione, ma saranno corredati di informazioni aggiuntive necessarie per la creazione dei DVD, CD, ecc. nel caso di richiesta di esibizione da parte dell'Utente.

UniStorage consente la produzione di supporti rimovibili che possono essere forniti all'Utente.
In ogni supporto vengono trasferiti Pacchetti di distribuzione chiamati "Registrazioni", contenenti sia gli oggetti che l'insieme delle evidenze di conservazione.
La registrazione generata è auto-esplicativa, intendendo con questo che i dati sono affiancati da indici e informazioni di riferimento tali da poter permettere la comprensione del contenuto anche da programmi esterni al sistema di conservazione.
La registrazione è contenuta in una directory, il cui nome contiene un'indicazione del blocco dei documenti e data/ora dell'inizio della creazione della registrazione stessa.

Contenuto della directory della registrazione:

- file README.txt
- file autorun
- icona
- directory chrome
- directory chrome_profile
- directory viewer

I vari Pacchetti di distribuzione a seconda delle dimensioni possono venire raggruppati in volumi auto consultanti, la struttura dei volumi è la seguente:

Figura 1 - Struttura volumi

All’interno della directory viewer avremo una directory contenente i documenti suddivisi per Pacchetti. Questi volumi sono auto consultanti e permettono la ricerca e visualizzazione dei documenti conservati, i metadati associati e le marche di conservazione.

Torna al sommario

7. Il processo di erogazione del servizio di conservazione

Il processo di conservazione eseguito da Unimatica-RGI adotta il modello standard OAIS - Open Archival Information System[6] 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[7], il Soggetto conservatore provvederà a creare i Pacchetti di distribuzione in una forma tale che venga garantita la corretta visualizzazione di questi.

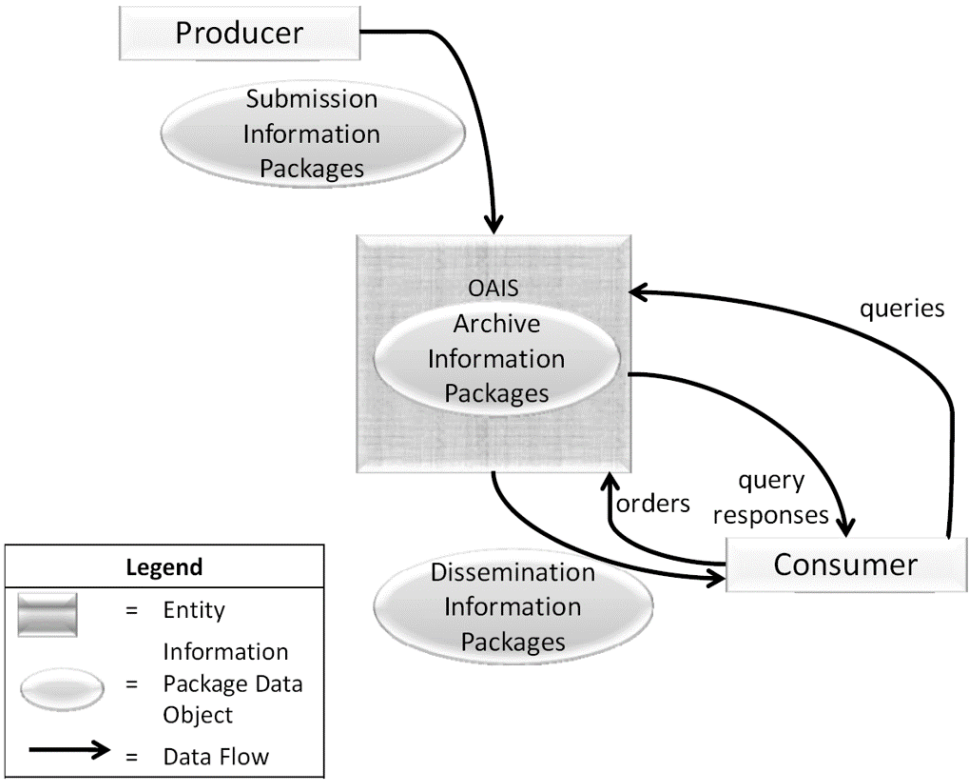


Figura 2 - Modello OAIS

Torna al sommario

[6] L'Open Archival Information System è lo standard ISO per la conservazione a lungo termine di archivi digitali.
[7] 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

7.1 Il processo di conservazione

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

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

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

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-RGI

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-RGI

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-RGI, 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-RGI 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:
    - *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
    - *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.
    - *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-RGI attesta esclusivamente la corretta esecuzione del processo di conservazione secondo la normativa vigente in materia di conservazione. Unimatica-RGI 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-RGI 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 duplice canale:

- via web: i Soggetti produttori titolari dei documenti potranno ricercare e visualizzare tutti i documenti conservati direttamente sul portale di Unimatica-RGI 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 maggiore chiarezza si precisa che al fine di garantire una veloce e corretta visualizzazione dei documenti conservati, tramite ricerca libera il portale permette la visualizzazione di 200 risultati. Per la ricerca di tutti gli altri documenti sarà necessario valorizzare 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 'Funzionalita_portale'. Vengono inoltre resi disponibili servizi web (Web Services) per le eventuali integrazioni con i portali dei Soggetti produttori.

- copia del documento su supporto ottico. La descrizione dettagliata circa la visualizzazione dei Pacchetti di distribuzione mediante supporto ottico è presente nel capitolo 6 Oggetti sottoposti a conservazione, paragrafo 6.5.

La struttura architetturale 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 ottico, 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[8] il Soggetto produttore richieda la presenza di un pubblico ufficiale, Unimatica-RGI 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

[8] "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."

7.9 Scarto dei Pacchetti di archiviazione

Sette mesi prima della scadenza del periodo di conservazione dei documenti stabilito dal contratto, Unimatica-RGI comunica al Soggetto produttore, in modalità certa, che in assenza di ulteriori comunicazioni, trascorsi i termini previsti, provvederà alla cancellazione dei documenti.
In caso di proroga della conservazione, Unimatica-RGI rinnova la marca temporale sui documenti per il periodo richiesto (uno o più anni).

Le attività di scarto dei Pacchetti di archiviazione vengono svolte sulla base di accordi tra il Responsabile del servizio di conservazione di Unimatica-RGI e il soggetto produttore. Il responsabile del servizio è tenuto a generare l'elenco dei pacchetti di archiviazione contenenti i documenti destinati allo scarto e ad inviarlo al soggetto produttore 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.

In caso degli 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[9].

Il Titolare dell'oggetto di conservazione, una volta effettuate le verifiche e/o ricevuta l'autorizzazione da eventuali parti coinvolte, che può essere concessa anche solo su una parte dell'elenco proposto, provvede a trasmetterlo al conservatore affinché provveda alla distruzione dei pacchetti di archiviazione.

Unimatica-RGI provvede a tracciare tutte le operazioni mediante la produzione di informazioni essenziali sullo scarto, inclusi gli estremi della richiesta di nulla osta allo scarto e il conseguente provvedimento autorizzatorio.

I documenti e le aggregazioni documentali informatiche scartate da Unistorage vengono distrutti anche su tutti i sistemi di backup.

Al termine delle operazioni di distruzione dal sistema di conservazione dei pacchetti di archiviazione scartati, Unimatica-RGI provvede a comunicare in via ufficiale il termine delle operazioni al Titolare dell'oggetto che provvederà a sua volta a notificarlo a chi di competenza

Torna al sommario

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

Unimatica-RGI, 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.

[9] 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).

Torna al sommario

7.11 Chiusura del contratto

Il Soggetto produttore, 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-RGI utilizzando una delle modalità di seguito indicate:

1. Invio dell'originale cartaceo con firma autografa tramite posta all'indirizzo:
   Unimatica-RGI S.p.A.
   Via Cristoforo Colombo, 21
   40131 Bologna

2. Invio dell'originale firmato digitalmente dal rappresentante legale, all'indirizzo di posta elettronica certificata (PEC): fatturaelettronica@pec.unimaticaspa.it

Il soggetto produttore che intende disdire il servizio di conservazione a norma dei documenti informatici affidato alla società Unimatica-RGI può scegliere di:

- mantenere la conservazione a norma dei documenti informatici già versati in conservazione fino al termine precedentemente concordato mantenendo la possibilità di utilizzare le credenziali di accesso al sistema per i soli scopi di consultazione

- non mantenere la conservazione a norma dei documenti informatici già versati in conservazione e di procedere allo scarto degli stessi e quindi disattivare le credenziali di accesso al sistema per i soli scopi di consultazione. L'Utente pertanto, dalla data della disdetta esonera la società Unimatica-RGI da ogni adempimento e responsabilità in merito alla custodia e conservazione dei documenti informatici versati in conservazione ed interessati dal servizio.

  I documenti informatici che sono stati oggetto di conservazione a norma possono essere restituiti, a richiesta, all'utente su supporto ottico 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-RGI In particolare, verranno descritte, a titolo esemplificativo ma non esaustivo, le misure di sicurezza tecniche e organizzative adeguate adottate da Unimatica-RGI 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-RGI 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 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 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 uno 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[10], Eliminazione delle cause[11], Ripristino[12].

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

[10] **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.
[11] **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.
[12] **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.

- De-duplicazione del dato ad alta velocità
- Replica efficiente in rete
- Scalabilità dell'infrastruttura

L'architettura di backup utilizza 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

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 rimuovibili) 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-RGI
- DB Postgres[nella modalità export DB]

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

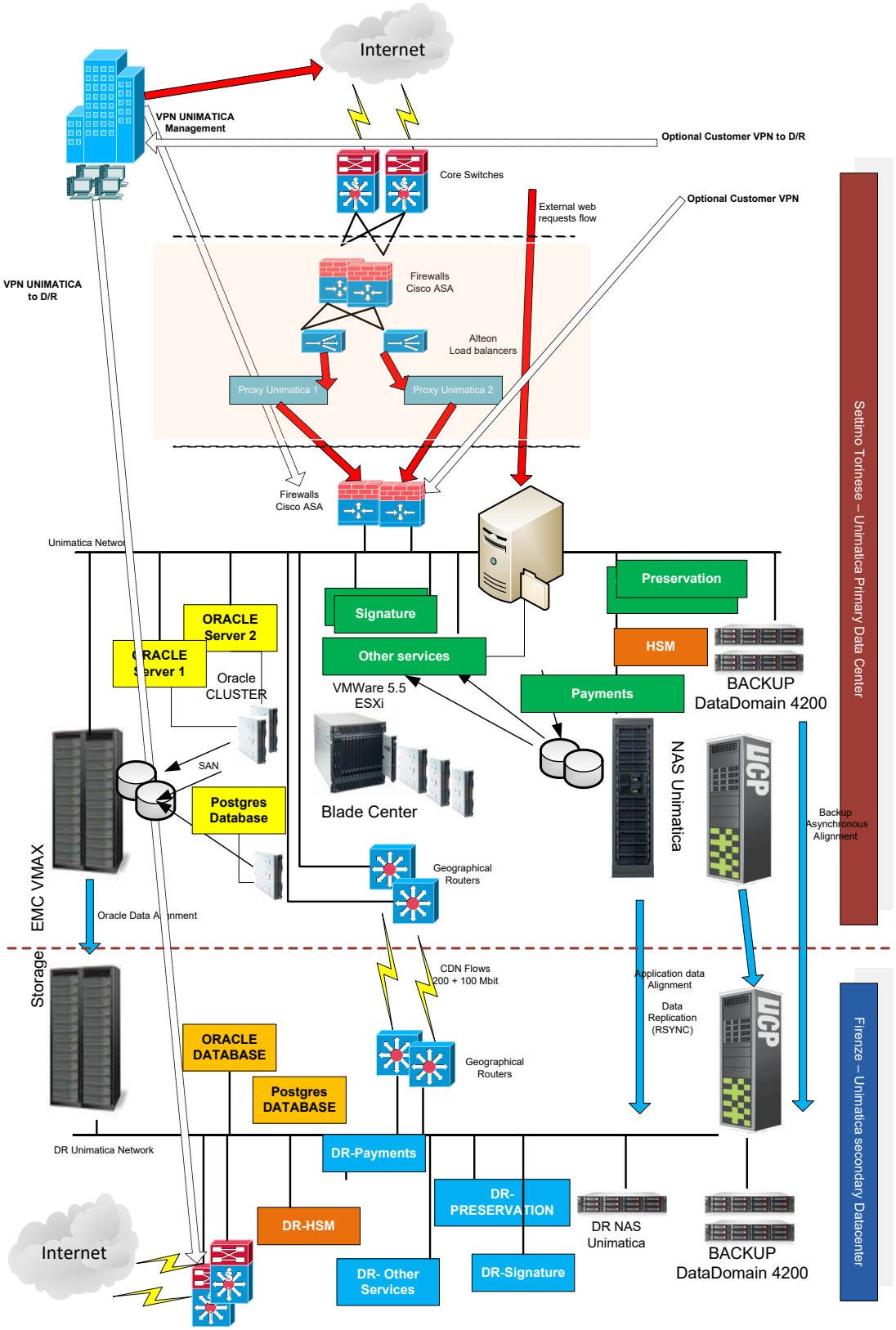
- Media Tempo di presa in Carico Service Request
- Media Tempo di Chiusura Service Request

Torna al sommario

10. La server farm di Unimatica-RGI

Dal punto di vista infrastrutturale, i data center dai quali Unimatica-RGI 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:



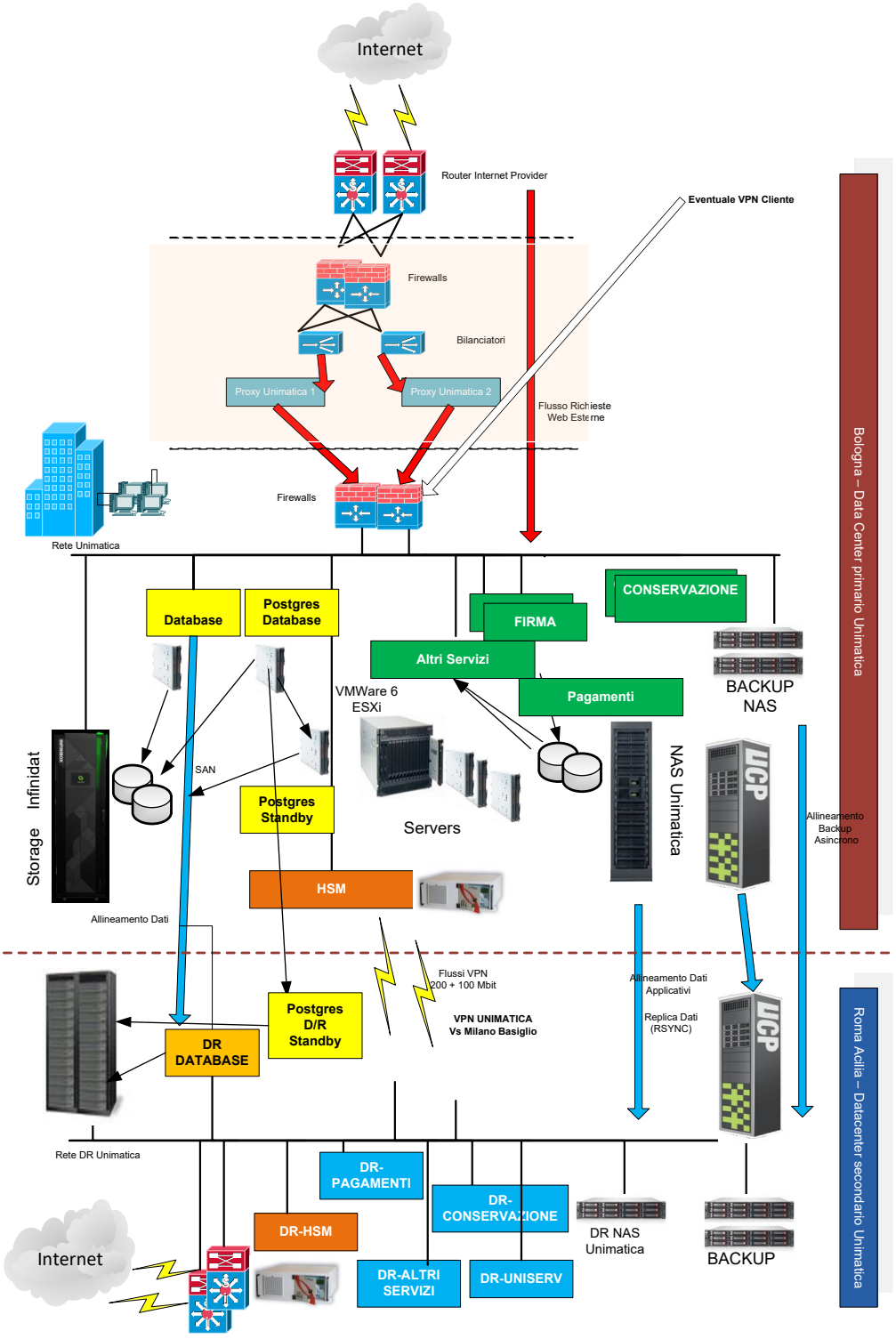


Figura 3 - Architettura di conservazione

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-RGI, 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 seguente 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-RGI, 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.
- ‘Funzionalita_portale'.
- Elenco delle modifiche apportate al Manuale della conservazione e dei documenti obsoleti.

Torna al sommario