



CITTÀ DI AULLA

Medaglia d'Oro al Merito Civile

Provincia di Massa-Carrara

Regione Toscana

MANUALE DI CONSERVAZIONE

dei documenti informatici

Adottato ai sensi dell'art. 44 del D.Lgs. 82/2005 (CAD)
e delle Linee Guida AgID sulla formazione, gestione e conservazione
dei documenti informatici

Versione 01 – 30/06/2026

Approvato con Deliberazione di Giunta Comunale n. 90 del 30/06/2026

Controllo delle versioni

Versione	Data	Descrizione della modifica	Redazione / Approvazione
01	30/06/2026	Prima emissione	Responsabile della conservazione

Indice

1. Scopo e ambito di applicazione	4
2. Terminologia: acronimi e definizioni	5
3. Normativa e standard di riferimento.....	6
4. Ruoli e responsabilità.....	7
5. Modello organizzativo e affidamento del servizio	11
6. Oggetti sottoposti a conservazione.....	13
7. Il pacchetto informativo	15
8. Il processo di conservazione	16
9. Modello di funzionamento del sistema di conservazione	18
10. Modalità di esibizione.....	20
11. Sicurezza del sistema di conservazione.....	21
12. Selezione e scarto dei documenti informatici	22
13. Tempi di conservazione e versamento.....	23
14. Pubblicazione e aggiornamento del Manuale	24
15. Allegati	25

1. Scopo e ambito di applicazione

1.1 Scopo del documento

Il presente Manuale di conservazione descrive il sistema di conservazione adottato dal Comune di Aulla, in qualità di Titolare dell'oggetto della conservazione, e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli da essi svolti, il modello di funzionamento, la descrizione del processo, delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica nel tempo del funzionamento del sistema di conservazione.

Il documento è redatto in conformità a quanto previsto dal par. 4.7 delle **Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici**, in vigore dal 1^o gennaio 2022, ed è parte integrante del sistema documentale dell'Ente unitamente al Manuale di gestione documentale e al Piano di conservazione (massimario di selezione e scarto).

1.2 Ambito di applicazione

Il Manuale si applica a tutti i documenti informatici e alle aggregazioni documentali informatiche (fascicoli e serie) prodotti, ricevuti e gestiti dall'Area Organizzativa Omogenea «AOO – Comune di Aulla» (codice AOO: A0E768A), destinati alla conservazione ai sensi dell'art. 44 del CAD.

Esso disciplina le attività e le responsabilità connesse al trasferimento degli oggetti documentali nel sistema di conservazione, alla loro presa in carico, gestione, esibizione ed eventuale scarto, nel caso — adottato dall'Ente — di affidamento del servizio a un conservatore accreditato presso AgID.

1.3 Modalità di gestione e aggiornamento

Il Manuale è un documento informatico soggetto a revisione periodica. Il Responsabile della conservazione ne cura l'aggiornamento in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti, secondo quanto indicato al cap. 14. Ogni revisione è tracciata nella tabella di controllo delle versioni.

2. Terminologia: acronimi e definizioni

2.1 Acronimi

Acronimo	Significato
AgID	Agenzia per l'Italia Digitale
AOO	Area Organizzativa Omogenea
CAD	Codice dell'Amministrazione Digitale (D.Lgs. 7 marzo 2005, n. 82)
PdA	Pacchetto di Archiviazione (AIP)
PdD	Pacchetto di Distribuzione (DIP)
PdV	Pacchetto di Versamento (SIP)
RdC	Responsabile della conservazione
RGD	Responsabile della gestione documentale
RSC	Responsabile del servizio di conservazione (presso il conservatore)
RFA	Responsabile della funzione archivistica (presso il conservatore)
TUDA	Testo Unico Documentazione Amministrativa (DPR 28 dicembre 2000, n. 445)

2.2 Definizioni

Per le definizioni dei termini tecnici utilizzati nel presente Manuale si rinvia integralmente all'Allegato 1 – Glossario delle Linee Guida AgID. Si richiamano di seguito, per immediatezza di lettura, i termini essenziali:

- **Conservazione:** insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione, garantendo nel tempo autenticità, integrità, affidabilità, leggibilità e reperibilità degli oggetti conservati.
- **Pacchetto informativo:** contenitore logico che racchiude uno o più oggetti da conservare (documenti, dati, metadati). Si distingue in pacchetto di versamento, di archiviazione e di distribuzione.
- **Rapporto di versamento:** documento informatico che attesta l'avvenuta presa in carico, da parte del sistema di conservazione, di uno o più pacchetti di versamento.
- **Titolare dell'oggetto della conservazione:** soggetto produttore degli oggetti destinati alla conservazione; nel presente Manuale, il Comune.

3. Normativa e standard di riferimento

3.1 Principali riferimenti normativi

- **D.Lgs. 7 marzo 2005, n. 82** – Codice dell'Amministrazione Digitale (CAD) e s.m.i., in particolare artt. 34, 43 e 44.
- **DPR 28 dicembre 2000, n. 445** – Testo Unico delle disposizioni in materia di documentazione amministrativa, in particolare artt. 61, 67 e 68.
- **Linee Guida AgID** – sulla formazione, gestione e conservazione dei documenti informatici (in vigore dal 1^o gennaio 2022) e relativi allegati.
- **D.Lgs. 22 gennaio 2004, n. 42** – Codice dei beni culturali e del paesaggio, in particolare artt. 21, 30, 40 e 41.
- **D.Lgs. 14 marzo 2013, n. 33** – Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni (art. 9).
- **Regolamento (UE) 2016/679 (GDPR)** – e D.Lgs. 30 giugno 2003, n. 196 – Protezione dei dati personali.
- **Regolamento (UE) n. 910/2014 (eIDAS)** – Identificazione elettronica e servizi fiduciari per le transazioni elettroniche.

3.2 Standard di riferimento

- **ISO 14721:2012 (OAIS)** – Open Archival Information System, modello di riferimento per i sistemi di conservazione.
- **UNI 11386 – Standard SInCRO** – Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (struttura del pacchetto di archiviazione).
- **ISO 15489** – Records management.
- **ETSI** – Specifiche tecniche in materia di firme e sigilli elettronici (CAAdES, PAdES, XAdES).

4. Ruoli e responsabilità

4.1 I soggetti del processo di conservazione

I ruoli individuati nel processo di conservazione, ai sensi del par. 4.5 delle Linee Guida AgID, sono i seguenti:

- **Titolare dell'oggetto della conservazione**
- **Produttore dei pacchetti di versamento (PdV)**
- **Utente abilitato**
- **Responsabile della conservazione**
- **Conservatore**

4.2 Titolare dell'oggetto della conservazione

Il ruolo di Titolare dell'oggetto della conservazione è svolto dal Comune di Aulla (sede legale piazza Gramsci n. 1, Aulla (MS); codice fiscale e partita IVA n. 00102940459; PEC comune.aulla@postacert.toscana.it; codice AOO A0E768A; codice IPA **c_i462a**). Il Titolare utilizza, già al momento della formazione dei documenti, le modalità e i formati individuati nel presente Manuale, in conformità alle Linee Guida AgID, e definisce i tempi di conservazione e di scarto dei propri documenti nel Piano di conservazione.

4.3 Produttore dei PdV / Responsabile della gestione documentale

Il Produttore dei PdV pur essendo il Comune di Aulla il processo viene svolto automaticamente dal sistema. Il **Responsabile della gestione documentale** dell'Ente, individuato nella persona della Dott.ssa Luciana Micheletti, Dirigente del 2° Settore «Servizi Finanziari e alla Città» verifica il buon esito delle operazioni. Il Produttore genera e trasmette al sistema di conservazione i pacchetti di versamento nelle modalità e con i formati concordati con il conservatore e verifica il buon esito dell'operazione di trasferimento.

4.4 Responsabile della conservazione

Il Responsabile della conservazione è un ruolo previsto dall'organigramma dell'Ente, ricoperto da un dirigente o funzionario interno formalmente designato e in possesso di idonee competenze giuridiche, informatiche ed archivistiche. Può coincidere con il Responsabile della gestione documentale.

Soggetto designato: Dott.ssa Luciana Micheletti, Dirigente del 2° Settore «Servizi Finanziari e alla Città», nominata con Decreto del Sindaco n. 7 del 18/07/2024 (atto con cui è altresì nominata Responsabile della Transizione Digitale ai sensi dell'art. 17 del CAD).

Ai sensi del par. 4.6 delle Linee Guida AgID, il Responsabile della conservazione in particolare:

Attività	Conservatore Maggioli	Responsabile della conservazione
1. definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione;		

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 presente Manuale;		
4. genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal Manuale;		
5. effettua il monitoraggio della corretta funzionalità del sistema di conservazione;		
6. effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti e delle aggregazioni documentarie;		
7. adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e l'obsolescenza dei formati;		
8. provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico		
9. adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione;		
10. assicura, ove richiesto, la presenza di un pubblico ufficiale e l'assistenza agli organismi di verifica e vigilanza;		
11. predispone il presente Manuale e ne cura l'aggiornamento periodico.		

In caso di affidamento del servizio a un conservatore accreditato, le predette attività, ad esclusione del versamento agli Archivi di Stato di cui alla lett. l) del par. 4.6, possono essere in tutto o in parte affidate al **Responsabile del servizio di conservazione** del conservatore, fermo restando che il Responsabile della conservazione dell'Ente conserva la titolarità e la responsabilità complessiva del processo.

4.5 Utente abilitato

L'utente abilitato può richiedere al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse, nei limiti previsti dalla legge e secondo le modalità stabilite nel presente Manuale e nel contratto/convenzione di servizio. Sono utenti abilitati dall'Ente, oltre al Responsabile della conservazione:

- Dott.ssa Samanta Baldi
- Dott.ssa Enrica Traghella

4.6 Conservatori accreditati

Il Comune di Aulla si avvale di **due conservatori**, ciascuno per le tipologie documentali indicate al cap. 6.1: il sistema di conservazione DAX della Regione Toscana per gli atti amministrativi, e Maggioli S.p.A. per il protocollo, i repertori e i flussi finanziari e demografici (versati tramite il sistema versante hyperSIC di APKAPPA).

4.6.1 DAX – Sistema di conservazione della Regione Toscana

Elemento	Dato
Denominazione del servizio	DAX – Sistema di conservazione della Regione Toscana (accesso per il referente dell'Ente tramite il portale SISE – Sistema Informativo Situazione Enti)
Conservatore (titolare del servizio)	Regione Toscana – P. IVA 01386030488
Natura del rapporto	Servizio pubblico regionale; adesione al Contratto Quadro Regione Toscana – Soggetto Aggregatore (logica pubblico-pubblico)
Gestione, manutenzione ed evoluzione	RTI affidatario del Contratto Quadro: Engineering Ingegneria Informatica S.p.A. (mandataria, C.F. 00967720285) – DocLife S.r.l. (mandante, C.F./P. IVA 01856380504)
Responsabile del servizio di conservazione	Anna Fuggi
Infrastruttura	Data Center regionale TIX – Tuscany Internet eXchange, sul territorio nazionale
Accesso al servizio	Portale SISE: https://condidoc.regione.toscana.it/dax_sise/ – autenticazione SPID/CIE/CNS
Riferimento al manuale del conservatore	Manuale di conservazione di Regione Toscana (sistema DAX) «Manuale Utente Referente dell'Ente» DAX/SISE v. 1.3

4.6.2 Maggioli S.p.A.

Elemento	Dato
Denominazione	Maggioli S.p.A.
Forma giuridica / sede legale	Società per azioni – Via del Carpino, 8 – 47822 Santarcangelo di Romagna (RN); R.E.A. di Rimini n. 219107
Partita IVA / C.F.	P. IVA 02066400405 / C.F. 06188330150
Estremi accreditamento AgID	Conservatore già accreditato AgID; CSP qualificato; Servizio di conservazione iscritto tra i Servizi SaaS del Marketplace AgID, ai sensi della Det. AgID n. 455/2021
Responsabile del servizio di conservazione	Dott. Robert Ridolfi

Riferimento al manuale del conservatore	«Manuale del Servizio di conservazione digitale di Maggioli spa», versione 05.02 del 20/06/2023 (cod. 04-03-06-02)
---	--

4.7 Tabella riepilogativa delle responsabilità

Soggetto	Principali responsabilità	Attribuzione
Titolare	Definizione tipologie, formati, tempi di versamento e scarto	Comune di Aulla
Produttore PdV	Generazione e trasmissione dei PdV; verifica esito versamento	RGD – L. Micheletti
Responsabile della conservazione	Politiche, governo del processo, rapporto di versamento, monitoraggio	L. Micheletti
Conservatore – atti amministrativi	Gestione tecnica del sistema di conservazione, PdA, PdD, sicurezza	DAX – Regione Toscana
Conservatore – protocollo, repertori, flussi finanziari e demografici	Gestione tecnica del sistema di conservazione, PdA, PdD, sicurezza	Maggioli S.p.A.

4.8 Deleghe

Il Responsabile della conservazione, sotto la propria responsabilità, può delegare lo svolgimento di proprie attività o parte di esse a uno o più soggetti dotati di specifiche competenze. La delega, riportata nel presente Manuale, individua le funzioni e le competenze delegate: non sono presenti deleghe.

5. Modello organizzativo e affidamento del servizio

5.1 Modello organizzativo adottato

Ai sensi dell'art. 34, comma 1-bis, del CAD, il processo di conservazione può essere svolto all'interno o all'esterno della struttura organizzativa dell'Ente. Il Comune di Aulla ha adottato un modello di conservazione affidata in modalità totale all'esterno, articolato su **due conservatori accreditati presso AgID**: il sistema DAX della Regione Toscana per gli atti amministrativi e Maggioli S.p.A. per il protocollo, i repertori e i flussi finanziari e demografici. Restano in capo all'Ente i ruoli interni e non delegabili di Produttore/Responsabile della gestione documentale e di Responsabile della conservazione, nonché gli obblighi di cui al cap. 13.

5.2 Affidamento ai conservatori accreditati

I requisiti del processo di conservazione, le responsabilità e i compiti del Responsabile della conservazione e dei Responsabili del servizio di conservazione, nonché le loro modalità di interazione, sono formalizzati nel presente Manuale e nei rispettivi atti di affidamento, e trovano riscontro nei manuali di conservazione dei due conservatori (Manuale di conservazione di Regione Toscana per il sistema DAX e Manuale del Servizio di conservazione digitale di Maggioli spa, v. 05.02). Per la parte affidata a Maggioli, l'affidamento è perfezionato per il tramite del Committente APKAPPA S.r.l., gestore del Sistema versante hyperSIC.

5.3 Estremi degli atti di affidamento

5.3.1 DAX – Regione Toscana

Elemento	Dato
Tipologia di atto	Atto di adesione al rinnovo del Contratto Quadro Regione Toscana – Soggetto Aggregatore (Lotto 1 «Sistema di Conservazione»); Accordo di Servizio Enti allegato
Estremi del Contratto Quadro	CIG 8551248914; atto di rinnovo del 05/05/2025 (n. 9157 Rep. e n. 5703 Racc.), ai sensi dell'art. 54 del D.Lgs. 50/2016; affidatario RTI Engineering Ingegneria Informatica S.p.A. – DocLife S.r.l.
Decorrenza e durata	Adesione con decorrenza 05/05/2025, termine alla scadenza dell'atto di rinnovo (24 mesi dal 04/05/2025)
Importo della manifestazione di interesse	€ 343,47 oltre IVA
Sottoscrizione / autorizzazione	Dott.ssa Luciana Micheletti, Dirigente del 2° Settore «Servizi Finanziari e alla Città», autorizzata con Decreto Sindacale n. 7 del 25/05/2023
RUP dell'atto di adesione	E.Q. Samanta Baldi – samanta.baldi@comune.aulla.ms.it – tel. 0187 400231

5.3.2 Maggioli S.p.A.

Elemento	Dato
Tipologia di atto	Affidamento del servizio di conservazione digitale a norma (adesione per il tramite del Committente APKAPPA S.r.l.)

Estremi e data	Determinazione di affidamento n. 1103 del 09/08/2024 – CIG B2327A3DD6 – contratto/offerta Maggioli n. 0001311205
Durata e scadenza	Affidamento fino al 31/12/2026, prorogabile nei termini previsti dal manuale del conservatore
Dimensionamento (SLOT)	Limite massimo stimato pari a 50 GB
Attività affidate al servizio di conservazione	Presa in carico e validazione dei PdV, generazione e gestione dei PdA, produzione dei PdD ed esibizione, conservazione e verifiche periodiche, gestione dell'obsolescenza tecnologica, eliminazione dei dati su disposizione del Titolare (cfr. matrice RACI del manuale del conservatore)
RdC dell'Ente riportato negli atti	Dott.ssa Luciana Micheletti – luciana.micheletti@comune.aulla.ms.it – tel. 0187 400253 – PEC comune.aulla@postacert.toscana.it

6. Oggetti sottoposti a conservazione

6.1 Tipologie documentali e aggregazioni

Sono sottoposti a conservazione i seguenti oggetti digitali, con i relativi metadati:

- i documenti informatici e i documenti amministrativi informatici;
- le aggregazioni documentali informatiche (fascicoli e serie), con i riferimenti che identificano univocamente i singoli oggetti documentali;
- gli archivi informatici, con i metadati associati.

Le tipologie documentali trattate dall'Ente e i relativi tempi di conservazione sono individuati nel Piano di conservazione allegato al Manuale di gestione. Si riportano di seguito le classi documentali oggetto degli affidamenti, con la relativa Descrizione Archivistica (AliasDA) e il conservatore di destinazione:

Tipologia documentale	Descrizione Archivistica (AliasDA)	Formato prevalente	Conservatore
Protocollo Generale	AAGG-PG-DOCUMENTI	PDF/A	Maggioli S.p.A.
Registri giornalieri di protocollo	AAGG-PG-REGISTRI	PDF/A	Maggioli S.p.A.
Deliberazioni	AAGG-ATTI-DELIBERAZIONI	PDF/A – P7M	DAX – Regione Toscana
Determinazioni	AAGG-ATTI-DETERMINAZIONI	PDF/A – P7M	DAX – Regione Toscana
Decreti	AAGG-ATTI-DECRETI	PDF/A – P7M	DAX – Regione Toscana
Atti di liquidazione	AAGG-ATTI-LIQUIDAZIONI	PDF/A	DAX – Regione Toscana
Provvedimenti amministrativi	AAGG-ATTI-PROVVEDIMENTI	PDF/A	DAX – Regione Toscana
Ordinanze	AAGG-ATTI-ORDINANZE	PDF/A	DAX – Regione Toscana
Altri atti amministrativi	AAGG-ATTI-AMMINISTRATIVI	PDF/A	DAX – Regione Toscana
Altri repertori	AAGG-RD-REPERTORI	PDF/A	Maggioli S.p.A.
Contratti e scritture private	AAGG-RD-CONTRATTI	PDF/A – P7M	Maggioli S.p.A.
Lotti di fatture non protocollati	AAGG-RD-FATTUREPA	XML	Maggioli S.p.A.
Notifiche SEND / atti dei Messi	AAGG-RD-DOCUMENTI	PDF/A	Maggioli S.p.A.
Flussi OPI (Tesoreria, SIOPE+)	TEI-FLUSSI-OPI	XML	Maggioli S.p.A.
Fascicolo elettorale	DEM-FE-DOCUMENTI	PDF/A	Maggioli S.p.A.
Indice generale demografici	DEM-RD-REPERTORI	PDF/A	Maggioli S.p.A.

I metadati di ciascuna tipologia sono valorizzati ai sensi dell'Allegato 5 alle Linee Guida AgID (cfr. cap. 6.3). Gli atti amministrativi sono versati al sistema DAX della Regione Toscana tramite Pacchetto di Versamento (SIP); le restanti tipologie sono versate a Maggioli S.p.A. tramite il sistema versante hyperSIC di APKAPPA.

6.2 Formati

I formati dei documenti destinati alla conservazione sono conformi a quanto indicato nell'Allegato 2 «Formati di file e riversamento» delle Linee Guida AgID, privilegiando formati aperti, standardizzati e idonei a garantire la leggibilità nel tempo (in via prioritaria PDF/A, XML, TIFF, JPEG2000, formati firmati CAdES/PAdES/XAdES). I formati ammessi dal sistema di conservazione sono indicati nell'allegato «Formati di conservazione» del manuale del conservatore.

6.3 Metadati

A ciascun oggetto sono associati i metadati previsti dall'Allegato 5 «Metadati» delle Linee Guida AgID per la relativa classe documentale. I metadati minimi sono valorizzati in fase di formazione e trasmessi con il pacchetto di versamento; in caso di mancata valorizzazione dei metadati obbligatori il pacchetto può essere rifiutato dal sistema di conservazione. Le strutture degli indici di conservazione differiscono per conservatore: per il sistema DAX della Regione Toscana il SIP è descritto nel SIPManifest secondo le specifiche regionali e lo standard UNI 11386 (SInCRO); per Maggioli si applicano le Descrizioni Archivistiche «CAD2018-DOCUMENTI-v3» e «CAD2018-FASCICOLI-v3» (cfr. cap. 6.4 del manuale Maggioli). Per le tipologie versate a Maggioli i metadati sono valorizzati sul Sistema versante hyperSIC di APKAPPA S.r.l.

6.4 Eccezioni

Non sono presenti eccezioni

7. Il pacchetto informativo

Gli oggetti della conservazione sono trattati dai sistemi di conservazione in pacchetti informativi, distinti in pacchetti di versamento, di archiviazione e di distribuzione.

7.1 Pacchetto di versamento (PdV/SIP)

Il pacchetto di versamento è il contenitore inviato dal Produttore al sistema di conservazione secondo le modalità e i formati definiti nel presente Manuale; è composto da un indice di versamento e dai file destinati alla conservazione. Gli atti amministrativi sono versati al sistema DAX della Regione Toscana come SIP (Submission Information Package), corredato del relativo SIPManifest, e l'esito è notificato dal sistema (cfr. report «Versamenti», «Errori di conferimento» ed «Errori di presa in carico» del portale SISE). Le restanti tipologie sono trasmesse a Maggioli S.p.A. tramite il Sistema versante hyperSIC di APKAPPA su canale cifrato SFTP o HTTPS, secondo le Specifiche tecniche di versamento del conservatore.

7.2 Pacchetto di archiviazione (PdA)

Il pacchetto di archiviazione è generato dal sistema di conservazione conformemente alle specifiche della norma **UNI 11386 – SInCRO**, a garanzia dell'interoperabilità tra sistemi di conservazione. Il sistema DAX della Regione Toscana genera il PdA secondo le specifiche regionali; il sistema di Maggioli forma PdA contenenti al massimo 4 GB o 20.000 documenti, ciascuno corredato dall'indice di conservazione (file IdC) firmato digitalmente e marcato temporalmente dal conservatore, prodotto

tramite il software LegalArchive® di IFIN Sistemi S.r.l. La struttura dati di dettaglio è descritta nei rispettivi manuali di conservazione.

7.3 Pacchetto di distribuzione (PdD)

Il pacchetto di distribuzione è prodotto dal sistema di conservazione ai fini dell'esibizione richiesta dall'utente abilitato, secondo le modalità indicate al cap. 10.

8. Il processo di conservazione

Il processo di conservazione, conforme al par. 4.8 delle Linee Guida AgID, si articola nelle fasi di seguito descritte.

8.1 Presa in carico e versamento dei PdV

Il trasferimento dell'oggetto nel sistema di conservazione avviene mediante generazione di un PdV nelle modalità e con i formati previsti al cap. 7. Il sistema di conservazione acquisisce il PdV per la sua presa in carico.

8.2 Verifica dei PdV

Il sistema verifica che il PdV e gli oggetti digitali in esso contenuti siano coerenti con le modalità previste dal Manuale e con i formati indicati nell'Allegato 2 delle Linee Guida AgID.

8.3 Accettazione e rifiuto dei PdV

In presenza di anomalie rilevate in sede di verifica, il sistema rifiuta il PdV. Ai sensi delle Linee Guida AgID il numero massimo di rifiuti non può essere inferiore a 3; superato tale limite il conservatore non è più tenuto ad accettare quell'oggetto in conservazione. Per il sistema DAX della Regione Toscana gli esiti negativi sono classificati come «errori di conferimento» ed «errori di presa in carico», consultabili dal referente dell'Ente sul portale SISE; per Maggioli si applicano i controlli di validazione tecnologici sui PdV in ingresso (integrità/hash, pattern dei metadati, formati ammessi) di cui al cap. 5.11 del relativo manuale. Le unità documentali contenute in PdV rifiutati sono rinviate in conservazione in nuovi PdV a valle dell'attività di bonifica. Numero massimo di rifiuti concordato 3.

8.4 Rapporto di versamento

Il sistema genera, anche in modo automatico, il rapporto di versamento relativo a uno o più PdV, univocamente identificato e contenente un riferimento temporale espresso in UTC e una o più impronte calcolate sull'intero contenuto del pacchetto. Il rapporto di versamento è sottoscritto con firma digitale o firma elettronica qualificata o avanzata dal Responsabile della conservazione o dal Responsabile del servizio di conservazione, ove previsto.

8.5 Generazione e gestione del PdA

Il pacchetto di archiviazione è preparato, sottoscritto con firma digitale/firma elettronica qualificata o avanzata, ovvero con sigillo elettronico, e gestito secondo le specifiche della struttura dati di cui all'Allegato 4 delle Linee Guida AgID. Maggioli appone su ciascun indice di conservazione (IdC) firma digitale e marca temporale erogate da TSP italiani qualificati eIDAS, e archivia i PdA in storage logicamente riservati e isolati, ubicati sul territorio nazionale.

8.6 Produzione del PdD ed esibizione

Il pacchetto di distribuzione è preparato e sottoscritto (o sigillato) secondo le modalità indicate nel Manuale ai fini dell'esibizione richiesta dall'utente abilitato. Ai fini dell'interoperabilità tra sistemi di conservazione, i PdD possono contenere uno o più pacchetti di archiviazione.

8.7 Produzione di duplicati e copie

Su richiesta degli utenti abilitati il sistema produce duplicati informatici o copie informatiche, in conformità alle Linee Guida AgID.

8.8 Riversamento

Al fine di adeguare i formati alle esigenze conservative di leggibilità nel tempo, il sistema produce copie informatiche mediante attività di riversamento, in base alle indicazioni dell'Allegato 2 delle Linee Guida AgID.

9. Modello di funzionamento del sistema di conservazione

Capitolo a contenuto prevalentemente parametrico (dati dei conservatori). In caso di affidamento esterno è ammesso il rinvio ai manuali di conservazione dei conservatori per le parti di loro competenza: il Manuale di conservazione di Regione Toscana (sistema DAX) e relativa documentazione (Manuale Utente Referente dell'Ente SISE v. 1.3) e il Manuale del Servizio di conservazione digitale di Maggioli spa, v. 05.02, con i relativi allegati (Specifiche tecniche di versamento, Formati di conservazione, Indici di conservazione).

9.1 Componenti logiche

Il sistema DAX della Regione Toscana acquisisce i SIP versati dagli Enti, ne verifica conferimento e presa in carico, genera i PdA e ne consente l'esibizione; il referente dell'Ente monitora versamenti, errori ed esiti tramite il portale SISE. Il sistema di conservazione di Maggioli S.p.A. gestisce i pacchetti informativi (PdV, PdA, PdD) tramite workflow di presa in carico, validazione, archiviazione, esibizione e verifica, con formazione e verifica periodica dei PdA mediante il software LegalArchive® di IFIN Sistemi S.r.l. (OAIS compliant, UNI SInCRO). In entrambi i sistemi l'accesso avviene tramite canali cifrati e utenti profilati secondo il principio del minimo privilegio.

9.2 Componenti tecnologiche

Entrambi i servizi sono erogati in modalità cloud sul territorio nazionale. Le firme digitali e le marche temporali apposte agli indici di conservazione sono erogate da Trust Service Provider italiani qualificati ai sensi del Regolamento eIDAS. Il sistema di Maggioli applica tre livelli di controllo antivirus (firewall in upload, area di staging, archivi di conservazione).

9.3 Componenti fisiche e infrastrutture

Ai sensi del par. 4.9 delle Linee Guida AgID, i dati e le copie di sicurezza sono materialmente conservati sul territorio nazionale; i servizi cloud sono qualificati e presenti nel Catalogo dei servizi Cloud per la PA.

Conservatore / Sito	Ubicazione
DAX – Regione Toscana	Data Center regionale TIX – Tuscany Internet eXchange, sul territorio nazionale
Maggioli – sito primario	Milano Campus Data4 (eLogic S.r.l.) – Via Monzoro 101-105, 20007 Cornaredo (MI)
Maggioli – sito secondario	DC Mantova (Gruppo Maggioli) – Via Pietro Verri 27, 46100 Mantova (MN)

I datacenter di Maggioli sono di proprietà della stessa o di sue controllate, iscritti come CSP qualificati AgID; il sito primario e il secondario sono costantemente allineati, con RPO di 15 minuti e procedura di disaster recovery. Il sistema DAX è erogato dall'infrastruttura regionale della Toscana.

9.4 Ubicazione e conservazione dei dati

Tutti i PdA e gli oggetti in essi raccolti sono archiviati all'interno del sistema di conservazione, in storage virtuali logicamente riservati al Servizio e isolati dagli altri sistemi, ubicati sul territorio nazionale. L'accesso ai dati presso la sede del Titolare avviene tramite portale web del Servizio e/o integrazione applicativa, con credenziali personali rilasciate agli utenti abilitati dall'Ente.

9.5 Procedure di gestione ed evoluzione

Ogni variazione al sistema di conservazione segue una procedura di change management (richiesta, analisi di impatto, programmazione, verifica, eventuale ripristino). Le variazioni che impattano sulle specifiche di integrazione applicativa sono comunicate ai clienti con adeguato preavviso e tramite aggiornamento del manuale del conservatore.

10. Modalità di esibizione

Fermi restando gli obblighi di esibizione previsti dalla normativa vigente, il sistema di conservazione consente ai soggetti autorizzati l'accesso diretto, anche da remoto, agli oggetti digitali conservati, attraverso la produzione di pacchetti di distribuzione. Nel caso di affidamento esterno del servizio, le modalità di esibizione sono concordate tra le parti e indicate nei rispettivi manuali.

Modalità di accesso ed esibizione adottate: per gli atti conservati nel sistema DAX, accesso del referente dell'Ente al portale SISE (https://condidoc.regione.toscana.it/dax_sise/) tramite SPID/CIE/CNS, con consultazione di versamenti, report ed esiti; per le tipologie conservate da Maggioli, accesso al portale web del Servizio con credenziali personali e non cedibili (profili base/avanzato) e/o integrazione applicativa via API. In entrambi i casi gli utenti abilitati possono scaricare i singoli file conservati o richiedere un Pacchetto di Distribuzione (PdD) per l'esibizione a norma. Gli accessi sono profilati dal Responsabile della conservazione dell'Ente e tracciati nei log dei rispettivi sistemi.

11. Sicurezza del sistema di conservazione

11.1 Piano della sicurezza

Il Responsabile della conservazione, di concerto con il Responsabile della sicurezza e con il Responsabile della transizione digitale, e acquisito il parere del Responsabile della protezione dei dati personali, predispone — nell'ambito del piano generale della sicurezza — il piano della sicurezza del sistema di conservazione, mettendo in atto misure tecniche e organizzative adeguate al rischio ai sensi dell'art. 32 del Regolamento (UE) 2016/679 e in aderenza alle «Misure minime di sicurezza ICT per le pubbliche amministrazioni».

11.2 Misure di sicurezza adottate

Nel caso di affidamento esterno, le misure di sicurezza fisica e logica dei sistemi di conservazione sono descritte nei manuali dei rispettivi conservatori, cui si rinvia. Il sistema DAX è erogato dall'infrastruttura regionale della Toscana (Data Center TIX) con le misure di sicurezza previste dal manuale di conservazione di Regione Toscana. Maggioli S.p.A. opera con un Sistema di Gestione per la Sicurezza delle Informazioni certificato ISO/IEC 27001, oltre alle certificazioni ISO 9001 e ISO/IEC 20000-1 e all'adozione del Modello 231/2001; applica segregazione fisica e logica del sistema di conservazione, cifratura dei canali (HTTPS/SFTP) e dei dispositivi, politiche di backup con RPO di 15 minuti, controlli antivirus su tre livelli e procedure di incident management e disaster recovery. Il Responsabile della sicurezza dei sistemi (CISO) di Maggioli è il Dott. Luca Castellano.

11.3 Trattamento dei dati personali e violazioni

Il trattamento dei dati personali nell'ambito dei sistemi di conservazione è conforme al Regolamento (UE) 2016/679. È predisposta la procedura da adottare in caso di violazione dei dati personali ai sensi degli artt. 33-34 del medesimo Regolamento. Gli atti di disciplina del trattamento differiscono per conservatore:

- DAX – Regione Toscana: il rapporto è di natura pubblico-pubblico ed è disciplinato dall'Accordo di Servizio Enti e dalla relativa documentazione del Contratto Quadro regionale (non da una nomina commerciale ex art. 28).
- Maggioli S.p.A.: nomina del Comune di Aulla a Maggioli S.p.A. quale Responsabile esterno del trattamento ex art. 28 GDPR, in riferimento al contratto/offerta n. 0001311205, sottoscritta dal Titolare il 26/06/2026; il Responsabile della protezione dei dati (DPO) del conservatore è il Dott. Ernesto Belisario.

Il Titolare del trattamento per l'Ente è il Comune di Aulla, nella persona del Sindaco Avv. Roberto Valettini.

12. Selezione e scarto dei documenti informatici

12.1 Criteri e tempi

La selezione e lo scarto dei pacchetti di archiviazione sono definiti dal Titolare dell'oggetto di conservazione secondo quanto indicato dal Piano di conservazione, nel rispetto della normativa sui beni culturali.

12.2 Procedura di scarto e autorizzazione

Il Responsabile della conservazione genera l'elenco dei pacchetti di archiviazione contenenti i documenti destinati allo scarto e, verificato il rispetto dei termini temporali stabiliti dal Piano di conservazione, lo comunica al Responsabile della gestione documentale. In caso di affidamento esterno, l'elenco proposto è generato dal sistema di conservazione e trasmesso al Responsabile della conservazione per la puntuale verifica.

Lo scarto è subordinato al rilascio dell'autorizzazione da parte della **Soprintendenza archivistica e bibliografica della Toscana** (per il tramite della Direzione generale Archivi nei casi previsti). Le proposte di scarto di pacchetti contenenti documenti sottratti alla libera consultabilità sono autorizzate dal Ministero dell'Interno. Ricevuta l'autorizzazione, il Titolare procede alla distruzione dei pacchetti, anche per il tramite del conservatore; l'operazione è tracciata mediante appositi metadati e ha efficacia al completo aggiornamento delle copie di sicurezza. I documenti scartati sono distrutti anche in tutti i sistemi gestiti dal Titolare.

13. Tempi di conservazione e versamento

Ai sensi del par. 4.7 delle Linee Guida AgID, resta fermo l'obbligo del Comune di individuare e pubblicare i tempi di versamento, le tipologie documentali trattate, i metadati, le modalità di trasmissione dei PdV e le tempistiche di selezione e scarto dei propri documenti informatici. Almeno una volta all'anno il Responsabile della gestione documentale trasmette al sistema di conservazione i fascicoli e le serie documentarie, anche relativi a procedimenti non conclusi (art. 44, comma 1-bis, CAD).

I tempi di conservazione delle singole tipologie documentali sono indicati nel **Piano di conservazione** (massimario di selezione e scarto) allegato al Manuale di gestione documentale, cui si rinvia. Per l'affidamento in essere i flussi sono trasmessi in conservazione con retention a conservazione illimitata (retention = 0), salvo diversa indicazione dell'Ente. Quadro di sintesi:

Tipologia documentale	Tempo di versamento	Tempo di conservazione
Registro giornaliero di protocollo	entro il giorno lavorativo successivo	illimitato
Protocollo generale e atti amministrativi	tempestivo, comunque entro un anno	illimitato
Lotti di fatture / flussi OPI (SIOPE+)	periodico secondo flusso	10+1 anni
Altri flussi affidati	tempestivo, comunque entro un anno	illimitato

14. Pubblicazione e aggiornamento del Manuale

Il Comune redige, adotta con provvedimento formale e pubblica sul proprio sito istituzionale il presente Manuale di conservazione. La pubblicazione è realizzata in una parte chiaramente identificabile dell'area «Amministrazione trasparente» prevista dall'art. 9 del D.Lgs. 33/2013.

Il Manuale è aggiornato a cura del Responsabile della conservazione in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti, ovvero al variare del conservatore affidatario del servizio. Ogni aggiornamento è adottato con provvedimento formale, tracciato nella tabella di controllo delle versioni e ripubblicato.

15. Allegati

Costituiscono allegati e parte integrante del presente Manuale:

Allegato 1 - Decreto del Sindaco n. 7 del 18/07/2024 – nomina del Responsabile della transizione digitale e del Responsabile della conservazione (Dott.ssa Luciana Micheletti)

Allegato 2 - Affidamento del servizio di conservazione – Determinazione n. 1103 del 09/08/2024, CIG B2327A3DD6, contratto/offerta Maggioli n. 0001311205

Allegato 3 - Nomina di Maggioli S.p.A. quale responsabile del trattamento ex art. 28 GDPR (sottoscritta il 26/06/2026)

Allegato 4 - Manuale del Servizio di conservazione digitale di Maggioli spa, v. 05.02 del 20/06/2023, e relativi allegati (Formati di conservazione, Indici di conservazione, Specifiche tecniche di versamento)

Allegato 5 - Piano di conservazione (massimario di selezione e scarto)

Allegato 6 - Affidamento del servizio di conservazione – Determinazione n. 1223 del 16/09/2025, CIG B7F02FD93C - Adesione contratto quadro fra Regione Toscana – Soggetto Aggregatore e RTI Engineering Ingegneria Informatica spa

Allegato 7 - Manuale di conservazione DAX – Regione Toscana.



CITTA' DI AULLA

Medaglia d'Oro al Merito Civile

Provincia di Massa Carrara

DECRETO DEL SINDACO

**DECRETO DEL SINDACO / 7
del 18/07/2024**

OGGETTO:

NOMINA DEL RESPONSABILE DELLA TRANSIZIONE DIGITALE E DEL DIFENSORE CIVICO PER IL DIGITALE

Soggetti destinatari:

Dott.ssa Luciana Micheletti , Dott.ssa Laura Castagna

IL SINDACO

Avv. VALETTINI ROBERTO

Le firme, in formato digitale, sono state apposte sull'originale del presente atto ai sensi dell'art. 24 del D.Lgs. 07.03.2005, n. 82 e s.m.i. (CAD). Il presente atto è conservato in originale negli archivi informatici del Comune di Aulla, ai sensi dell'art. 22 del D.Lgs. 82/2005.

IL SINDACO

PREMESSO

-Che il nuovo CAD (ed. CAD 3.0), di cui al D.Lgs. 82/2005 e successive modifiche e integrazioni, con i suoi principi generali e le collegate regole tecniche, è l'asse portante e lo strumento operativo per attuare "la transizione alla modalità operativa digitale", principio espressamente richiamato dall'art. 1, c. 1 lett. n) della l. 124/2015 e negli artt. 13 e 17, comma 1, dello stesso CAD;

-Che il processo di riforma della pubblica amministrazione pone in capo ad ogni Ente la necessità di garantire l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione, centralizzando in capo ad un ufficio unico il compito di accompagnare la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione, con l'obiettivo generale di realizzare un'amministrazione digitale e aperta, dotata di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità;

VISTO l'art. 17 del CAD rubricato "Strutture per l'organizzazione, l'innovazione e le tecnologie, che disciplina puntualmente la figura del "Responsabile della transizione digitale" cui sono attribuiti importanti compiti di coordinamento e di impulso ai processi di reingegnerizzazione dei servizi;

DATO ATTO

-che i processi e i procedimenti attivi devono essere conformi alla normativa in materia di pubblicità e trasparenza di cui al D.Lgs. 33/2013, come revisionato a seguito dell'entrata in vigore del D.Lgs. 97/2016 cd. Freedom of Information Act (FOIA);

-che è specifico obiettivo dell'Amministrazione garantire la trasparenza dell'azione amministrativa anche attraverso il miglioramento dell'informatizzazione dei processi, e che gli obiettivi di pubblicità e trasparenza risultano direttamente collegati alle misure previste nel vigente Piano trasparenza e anticorruzione;

CONSIDERATE le competenze possedute dai Dirigenti e le ripartizioni interne delle funzioni nelle diverse Aree in cui la struttura comunale è suddivisa;

DATO ATTO che occorre nominare un Responsabile della Transizione Digitale in possesso di adeguate competenze ed esperienza;

RITENUTO di

-nominare Responsabile della Transizione Digitale, la Dott.ssa Luciana Micheletti, Dirigente del 2°Settore "Servizi Finanziari e alla Città", in virtù delle comprovate competenze tecnologiche, di informatica giuridica e manageriali, come richieste dall'art. 17 del CAD vigente,

-assegnare il compito di Difensore civico per il digitale alla D.ssa Laura Castagna, Segretario Generale dell'Ente, in possesso di adeguati requisiti di terzietà, autonomia ed imparzialità;

VISTO il Decreto Legislativo 18.08.2000, n. 267 "Testo Unico delle Leggi sull'ordinamento degli Enti Locali" e successive modifiche e integrazioni e in particolare gli articoli 50,97, 107 e 109;

DECRETA

- Di individuare e nominare, ai sensi dell'art. 17 del Codice dell'Amministrazione Digitale, quale Responsabile della Transizione Digitale, la Dott.ssa Luciana Micheletti, Dirigente del 2°Settore "Servizi Finanziari e alla Città", in possesso di comprovate competenze tecnologiche, di informatica giuridica e manageriali, come richieste dall'art. 17 del CAD vigente;

- Di nominare altresì la Dirigente suddetta quale Responsabile della Conservazione dei Documenti Informatici;

- Di nominare, inoltre, sulla base dello stesso disposto di cui all'art. 17 del CAD, il Segretario Comunale D.ssa Laura Castagna, quale Difensore Civico per il Digitale ossia il soggetto in possesso di adeguati requisiti di terzietà, autonomia e imparzialità cui chiunque può inviare segnalazioni e reclami relativi ad ogni presunta violazione del Codice dell'Amministrazione Digitale (CAD) e di ogni altra norma in materia di digitalizzazione ed innovazione della pubblica amministrazione;

- Di dare atto che per l'attribuzione delle responsabilità di cui al presente decreto non viene corrisposto compenso aggiuntivo in quanto resta ricompreso nella retribuzione di posizione già in godimento;

- Di trasmettere il presente atto a tutti i Dirigenti dell'Ente;

- Di pubblicare il presente atto all'albo on line per 15 giorni e sul Sito Web – Amministrazione Trasparente.

IL SINDACO
Avv. Roberto Valettini



CITTA' DI AULLA

Medaglia d'Oro al Merito Civile

Provincia di Massa Carrara

SERVIZI FINANZIARI E ALLA CITTA'

BILANCIO E CONTABILITA'

DETERMINAZIONE N. 1103 Del 09/08/2024

OGGETTO:

**ASSISTENZA, MANUTENZIONE E AGGIORNAMENTO SOFTWARE GESTIONALI E
CONSERVAZIONE ARCHIVI DIGITALI AREA FINANZIARIA E PROTOCOLLO TRIENNIO
2024-2026 - CIG: B2327A3DD6 – AFFIDAMENTO ALLA DITTA APKAPPA SRL**

FIRMATO
IL DIRIGENTE
MICHELETTI LUCIANA

Le firme, in formato digitale, sono state apposte sull'originale del presente atto ai sensi dell'art. 24 del D.Lgs. 07.03.2005, n. 82 e s.m.i. (CAD). Il presente atto è conservato in originale negli archivi informatici del Comune di Aulla, ai sensi dell'art. 22 del D.Lgs. 82/2005.

OGGETTO: ASSISTENZA, MANUTENZIONE E AGGIORNAMENTO SOFTWARE GESTIONALI E CONSERVAZIONE ARCHIVI DIGITALI AREA FINANZIARIA E PROTOCOLLO TRIENNIO 2024-2026 - CIG: B2327A3DD6 – AFFIDAMENTO ALLA DITTA APKAPPA

IL DIRIGENTE DEL 2° SETTORE

Visto il Decreto Sindacale n. 7 del 25.05.2023 ad oggetto: “incarico della Direzione del 2° Settore "Servizi Finanziari e alla Città" al Dirigente Dott.ssa Luciana Micheletti”;

Vista la deliberazione di Consiglio Comunale n. 39 del 29/11/2023 ad oggetto: “APPROVAZIONE DOCUMENTO UNICO DI PROGRAMMAZIONE (DUP) 2024-2026”;

Vista la deliberazione di Consiglio Comunale n. 1 del 13/01/2024 ad oggetto: “APPROVAZIONE DEL BILANCIO DI PREVISIONE FINANZIARIO 2024-2026 (ART. 151 DEL D.LGS. N. 267/2000 E ART. 10, D.LGS. N. 118/2011)”;

Premesso che con determinazione dirigenziale n.1150/2023 veniva affidata alla Ditta APKAPPA SRL per il periodo 01.01.2023-31.12.2023 il contratto di assistenza e manutenzione degli applicativi prodotti dalla Ditta APKAPPA SRL, utilizzati dai vari servizi comunali e la conservazione a norma degli archivi digitali del “Servizio Protocollo” e del “Servizio Finanziario”;

Vista la propria determinazione n. 813 del 21.06.2024, con la quale si stabiliva di procedere all'affidamento del servizio di aggiornamento, assistenza e manutenzione dei software in uso c/o l'Ente per il triennio 2024-2026 come di seguito dettagliati e la conservazione a norma degli archivi digitali del “Servizio Protocollo” e del “Servizio Finanziario” per il triennio 2024-2026:

- Area Finanziaria – Tributi;
- Area Protocollo/Interoperabilità;
- Area Demografica;
- Gestione Archivio digitale/Cartografia
- Cittadino digitale – APP.IO
- Cloud Procedurale – area Fin – Tri;
- Pago PA;
- Piano sicurezza
- Pubblicazioni WEB

per l'importo annuo di € 20.950,00 oltre iva di legge per i sopra elencati applicativi/servizi installati presso il Comune di Aulla e per l'importo annuo di € 1.400,00 oltre iva di legge per la conservazione a norma degli archivi digitali 2024-2026 (50GB), per un importo complessivo triennale di € 67.050,00 oltre iva di legge, mediante ordine diretto d'acquisto sul mercato elettronico della Pubblica Amministrazione, per la categoria “Servizi ICT, servizi di manutenzione, assistenza tecnica e gestione”;

Dato atto che è stata individuata la Ditta “APKAPPA s.r.l.”, con sede in Reggio Emilia, quale fornitrice del materiale sopradescritto;

Visto l'ordine diretto di acquisto sul MEPA - Mercato elettronico della Pubblica Amministrazione n. 694858 del 21/06/2024;

Considerato che per gli affidamenti di importo pari o superiori a € 40.000,00 è obbligatorio verificare l'assenza delle cause di esclusione ex artt. 94 e 95 del D. Lgs. 36/2023 mediante il Fascicolo Virtuale dell'Operatore Economico (FVOE), come sancito dalla Delibera Anac n. 262/2023, che permette alle Stazioni

Appaltanti e agli Enti aggiudicatori l'acquisizione dei documenti a comprova del possesso dei requisiti di carattere generale, tecnico-organizzativo ed economico-finanziario per l'affidamento dei contratti pubblici;

Costatato che, ai sensi dell'art. 17, comma 5, il presente provvedimento è già efficace in quanto, a seguito degli accertamenti condotti mediante la consultazione del Fascicolo Virtuale dell'Operatore Economico (FVOE), il citato operatore economico risulta in possesso dei requisiti di carattere generale e speciale prescritti dal d.lgs. n. 36/2023;

Accertata la regolarità del DURC della ditta "APKAPPA s.r.l.", con sede in Via Francesco Albani – 20149 MILANO (MI), rilasciato dall'INAIL (prot. n.43923282 del 30/05/2024) con scadenza validità il 27/09/2024

Dato atto che il presente affidamento è assoggettato a tutte le norme sulla tracciabilità dei pagamenti, come previste dall'art. 3 della legge 136/2010 e che il relativo codice CIG è il seguente: B2327A3DD6;

DETERMINA

- 1) Di affidare alla ditta "APKAPPA s.r.l.", con sede in Via Francesco Albani – 20149 MILANO (MI), la fornitura di servizio di aggiornamento, assistenza e manutenzione dei software in uso c/o l'Ente come di seguito dettagliati e la conservazione a norma degli archivi digitali del "Servizio Protocollo" e del "Servizio Finanziario" per il triennio 2024-2026, per l'importo complessivo di € 67.050,00 oltre iva di legge:
 - Area Finanziaria – Tributi;
 - Area Protocollo/Interoperabilità;
 - Area Demografica;
 - Gestione Archivio digitale/Cartografia
 - Cittadino digitale – APP.IO
 - Cloud Procedurale – area Fin – Tri;
 - Pago PA;
 - Piano sicurezza
 - Pubblicazioni WEB
- 2) Di dare atto che la prenotazione di spesa di € 67.050,00 oltre iva di legge, per complessivi € 81.801,00, assunta con determinazione n. 813 del 21/06/2024, viene trasformata in impegno definitivo di €81.801,00 a favore della Ditta "APKAPPA s.r.l.", con il seguente cronoprogramma di spesa:
 - € 27.267,00 annualità 2024
 - € 27.267,00 annualità 2025
 - € 27.267,00 annualità 2026
- 3) Di dare atto che il Responsabile Unico del Procedimento è la dipendente BALDI SAMANTA;
- 4) Di dare atto che il presente affidamento è già efficace, in quanto sono stati verificati i requisiti di ordine generale e speciale in capo alla ditta "APKAPPA s.r.l.";
- 5) Di dare atto dell'assenza di conflitto di interessi del Dirigente/Responsabile del Procedimento dell'atto, ai sensi dell'art. 6 bis L. 241/1990, così come introdotto dalla L. 190/2012.
- 6) Di dare atto che contro il presente provvedimento è ammesso ricorso al Tribunale Amministrativo Regionale competente, entro il termine di 60 giorni o, in alternativa, ricorso straordinario al Presidente della Repubblica, entro 120 giorni.

Il Dirigente del 2° Settore
Dott.ssa Luciana Micheletti

**Nomina a Responsabile Esterno del Trattamento ai sensi del Regolamento Europeo Privacy -
GDPR 2016/679 art. 28**

COMUNE DI AULLA

quale *Titolare del trattamento dei dati personali (di seguito “Titolare”)*, ai sensi e per gli effetti dell’art. 4.7 del GDPR 2016/679, in riferimento all’affidamento avente ad oggetto il servizio di Conservazione di Maggioli S.p.a. stipulato con APKAPPA n. contratto/offerta [0001311205](#)

Premesso che

ha valutato che Maggioli S.p.A. sotto il profilo della strutturazione, dell’organizzazione di mezzi e uomini, delle conoscenze, competenze e Know how disponibili possiede i requisiti di affidabilità, capacità ed esperienza tali da fornire l’idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza

Tutto ciò premesso,

DESIGNA

Maggioli S.p.A. in virtù dell’art. 28 del Reg. UE 2016/679 quale *Responsabile del trattamento dei dati personali (di seguito “Responsabile”)*.

Il Trattamento è affidato esclusivamente con le finalità proprie del *Titolare*, al fine di consentire l’esecuzione delle attività affidate a Maggioli S.p.A.

Si rileva che Maggioli S.p.A. esegue il trattamento dei dati personali di titolarità del *Titolare* esclusivamente come conseguenza delle attività e finalità strettamente inerenti allo svolgimento dell’affidamento citato in premessa.

Nell’espletamento dell’incarico, il *Responsabile* dovrà attenersi alle disposizioni vigenti disposte dalla legislazione in materia e specificatamente il trattamento dovrà essere realizzato in osservanza delle norme Regolamento Europeo Privacy (GDPR) 2016/679 e delle apposite prescrizioni che verranno impartite dal *Titolare*.

Il trattamento è affidato esclusivamente con le finalità proprie del *Titolare* e cioè di consentire l’esecuzione delle attività del fornitore dei servizi sopra elencati.

Sia il *Titolare* che il *Responsabile*, sono tenuti ad attuare le misure tecniche ed organizzative tenendo conto dello stato dell’arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche per quanto previsto agli articoli 32-33 e 35-36 del GDPR. Inoltre devono ottemperare a specifici requisiti previsti dal GDPR per ridurre i rischi del trattamento e assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; assicurare la capacità di ripristinare tempestivamente la disponibilità e l’accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l’efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

OBBLIGHI DEL RESPONSABILE

Il *Responsabile* ha anche altri obblighi specifici:

- I dati personali dei quali il *Responsabile* verrà a conoscenza sono di proprietà del *Titolare*; il *Responsabile*, pertanto, potrà tenerne copia solo per l’espletamento dei compiti affidati e limitatamente al tempo strettamente necessario a svolgere le operazioni consentite.

- Il *Responsabile* ha l'obbligo specifico di attenersi al divieto di comunicazione non espressamente autorizzata e di diffusione a qualsiasi titolo dei dati personali, nonché al divieto di utilizzo autonomo per finalità diverse rispetto a quanto qui specificato. Inoltre i dati personali saranno trattati da personale opportunamente informato e/o incaricato dal *Responsabile*.

- (Qualora la natura dell'incarico prevedesse l'intervento di Amministratori di sistema) Il *Responsabile* provvede all'osservanza di quanto stabilito dal provvedimento a carattere generale - 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" (G.U. n. 300 del 24/12/2008) e successive modifiche, emesso dall'autorità Garante per la protezione dei dati personali.

- (Qualora la natura dell'incarico prevedesse l'intervento di Amministratori di sistema) Il *Responsabile* adotta le misure tecniche ed organizzative del menzionato provvedimento, con riferimento: alla conservazione presso la propria organizzazione degli estremi identificativi delle persone preposte quali amministratori di sistema ed autorizzate quali incaricati al trattamento designati, le nomine degli stessi come amministratori di sistema secondo quanto previsto dal suddetto provvedimento e l'applicazione diligente dello stesso;

- (Qualora la natura dell'incarico prevedesse l'intervento di Amministratori di sistema) Il *Responsabile* secondo quanto stabilito dal provvedimento in materia di Amministratori di Sistema, comunicherà al *Titolare* i nominativi dei soggetti designati quali amministratori di sistema, che opereranno con tale qualifica presso la struttura del *Titolare* per le attività limitate all'affidamento. L'archiviazione dei log secondo quanto previsto dal provvedimento 27 novembre 2008 in termini di amministratori di sistema è a carico del *Titolare*.

- Il *Responsabile* fornisce se richiesto le Linee Guida per il Trattamento dei Dati Personali ai sensi del GDPR 2016/679.

- All'interno dell'organizzazione del *Responsabile* i dati potranno essere trattati soltanto da soggetti che dovranno utilizzarli per l'esecuzione delle prestazioni oggetto dei servizi affidati dal *Titolare*. Il *Responsabile* dovrà impartire ai suddetti soggetti autorizzati al trattamento, ogni necessaria istruzione (anche per iscritto) in merito al corretto utilizzo di tutti gli apparati di sistema ed informatici coinvolti in operazioni di trattamento di dati personali e mantenere la lista degli autorizzati al trattamento aggiornata. Il *Responsabile* dovrà inoltre vigilare sul rispetto delle istruzioni impartite ai propri autorizzati al trattamento.

- Il personale dipendente e/o i collaboratori che saranno incaricati dal *Responsabile* di svolgere le prestazioni assicureranno serietà ed affidabilità e saranno debitamente formati ed informati sulle modalità del trattamento, sui rischi che incombono sui dati e sui profili della vigente normativa.

- Il *Responsabile* deve rispettare, salvo diversa prescrizione scritta del *Titolare*, quanto previsto all'articolo 28 paragrafi 2,3,4. In particolare in riferimento a quanto previsto dal paragrafo 3 alle lettere a, b, c, d, e, f, g, h.

- Nel caso in cui il *Responsabile*, per l'esecuzione dell'attività, ritenga opportuno o necessario nominare altri Responsabili (c.d. *Subresponsabili*) è autorizzato sin d'ora a nominarli, con l'obbligo di darne notizia al *Titolare*.

A tale fine il responsabile mette a disposizione del titolare la lista dei *Subresponsabili* al seguente link <https://assistenza.maggioli.it/privacy/> . La lista è tenuta costantemente aggiornata dal responsabile e può essere consultata in ogni momento dal titolare che potrà prendere visione di modifiche e sostituzioni. Il titolare autorizza sin d'ora i responsabili elencati potendo richiedere informazioni di dettaglio all'indirizzo privacy@maggioli.it

Nel caso in cui il *Responsabile* ricorra a un altro soggetto per l'esecuzione di specifiche attività di trattamento per conto del Titolare, sarà tenuto a imporre su tale *altro Responsabile del trattamento* gli stessi obblighi in materia di protezione dei dati contenuti nella presente nomina, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento.

Qualora l'*altro Responsabile* ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile iniziale conserva nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi dell'altro Responsabile.

- Il *Titolare* autorizza sin d'ora il *Responsabile* a trasferire, qualora necessario, i dati personali trattati per suo conto al di fuori dello Spazio Economico Europeo. In tale ipotesi, il *Responsabile* dovrà assicurare e garantire che il trattamento avvenga verso Paesi terzi e Organizzazioni internazionali che garantiscano un livello di sicurezza e protezione adeguato, basando il trasferimento stesso su una decisione di adeguatezza della Commissione UE o su altri meccanismi di garanzia (quali ad esempio Clausole Contrattuali Standard o Binding Corporate Rules) oppure su una delle deroghe previste dalla normativa vigente.

- Il *Responsabile* dovrà garantire i diritti spettanti agli interessati al trattamento e stabiliti dal GDPR 679/2016, in tal senso il *Responsabile* si impegna a comunicare immediatamente al *Titolare* qualsiasi richiesta di esercizio diritti pervenuta da un interessato, al fine di consentire al *Titolare* la possibilità di fornire riscontro all'interessato.

ADEMPIMENTI DEL RESPONSABILE IN CASO DI DATA BREACH

Il *Responsabile* si è dotato di un proprio modello per la gestione di violazione dei dati personali e provvederà ad informare entro 24 ore, in forma scritta, il *Titolare*. Tale comunicazione sarà in linea con quanto previsto dagli articoli 33, 34 del GDPR.

Il *Responsabile* del trattamento procederà con le operazioni di trattamento dei dati personali in presenza delle misure di sicurezza richieste ai sensi e per gli effetti dell'art. 32 del GDPR e valutate dal *Responsabile* in base al contesto del trattamento. Le misure di sicurezza adottate sono quelle dichiarate in appositi documenti (tra cui il questionario di qualifica del fornitore allegato) messi a disposizione del *Titolare*.

DURATA E CESSAZIONE DEL TRATTAMENTO

Il presente accordo avrà la durata del contratto al quale si riferisce.

Nel caso in cui la cessazione delle Operazioni di Trattamento da parte del *Responsabile* configuri una cessazione del trattamento, questi provvede a notificarlo per iscritto con congruo anticipo al *Titolare* per l'adozione degli opportuni provvedimenti di Legge.

All'atto della cessazione, per qualsiasi causa, delle operazioni di trattamento da parte del *Responsabile*, quest'ultimo, trascorsi dodici mesi, provvede alla integrale distruzione dei dati inerenti alla privacy, fatta eccezione per la documentazione amministrativa la cui tenuta è gestita in ottemperanza agli obblighi di conservazione stabiliti per legge.

Inoltre il *Responsabile* sarà autorizzato a trattare i dati per conto del *Titolare* - anche ai fini dell'erogazione del servizio - nel periodo intercorrente tra la cessazione di un contratto e le conseguenti attività di migrazione, per un periodo non superiore a dodici mesi dalla cessazione degli effetti del contratto.

VERIFICHE DEL TITOLARE DEL TRATTAMENTO

Il *Titolare*, come previsto dalla vigente normativa, sarà chiamata ad esercitare vigilanza e controllo sull'osservanza delle istruzioni impartite e delle vigenti disposizioni in materia di trattamento dei dati personali.

L'attività di verifica potrà concretizzarsi attraverso la richiesta al *Responsabile* di compiere attività di autovalutazione rispetto alle misure di sicurezza adottate, all'osservanza delle misure impartite, fornendone, a richiesta, documentazione scritta.

Il *Titolare* ha il diritto di esercitare controlli o attività di audit, presso le sedi del *Responsabile*, finalizzati ad una verifica della puntuale applicazione delle istruzioni impartite, nonché della conformità alla legge delle operazioni di trattamento. Tali controlli saranno effettuati previa comunicazione al *Responsabile* stesso, da comunicarsi con congruo anticipo (almeno con sette giorni di anticipo).

ULTERIORI DISPOSIZIONI

Il *Responsabile*, con l'accettazione della presente nomina, si impegna a tenere indenne il *Titolare* da ogni responsabilità, costo, spesa o altro onere, discendenti da pretese, azioni o procedimenti di terzi a causa della violazione da sua parte o di suoi dipendenti e/o collaboratori o sub responsabili degli obblighi a proprio carico in base alla presente nomina e/o della violazione delle prescrizioni contenute nel Regolamento Europeo 2016/679.

Il *Titolare* tiene indenne e manlevato il *Responsabile* da ogni perdita, costo, spesa, multa e/o sanzione, danno e da ogni responsabilità di qualsiasi natura connessa al trattamento dei dati personali effettuato dal *Responsabile* nel rispetto e nella piena osservanza di tutte le istruzioni e prescrizioni impartite dal *Titolare* con la presente nomina e per qualsiasi responsabilità connessa al trattamento dei dati personali e per operazioni al trattamento per cui lo stesso non è espressamente nominato *Responsabile*. Il *Titolare* tiene altresì indenne e manlevato il *Responsabile* da eventuali pretese di terzi che dovessero lamentare l'illegittimo trattamento dei loro dati personali effettuato dal *Responsabile* su richiesta del *Titolare*.

Per tutto quanto non espressamente specificato in questa scrittura, il *Titolare* ed il *Responsabile* si atterranno in generale a quanto previsto dalla vigente disciplina in materia di dati personali, Reg. UE 2016/679.

Luogo e Data

AULLA - 26/06/2026

Firma Il Titolare del trattamento

Firma Il Responsabile del trattamento

Maggioli S.p.A.

Firmato digitalmente



Roberto Valettini
26/06/2026 12:08:14 UTC+0200



Luciana Micheletti
26/06/2026 13:22:12 UTC+0200



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 CAD¹

"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: 05.02	04-03-06-02	Data approvazione: 20/06/2023
Redazione	Fabio Tiralongo	Responsabile Sviluppo e Manutenzione del Servizio
Revisione	Andrea Furiosi	Product Manager
Revisione ed approvazione	Robert Ridolfi	Responsabile del Servizio di conservazione
Verifica		
Visto		
Approvazione	Robert Ridolfi	

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"

Allegati:

- Formati di conservazione v3
- Indici di conservazione (ex-metadati) v5
- Specifiche tecniche di versamento in conservazione 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 v1.2

Registro delle variazioni al Manuale:

Versione	Data revisione	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
5.1	31/01/2023	Aggiornamento dell'organigramma per il servizio e codifica (interna) del documento	
5.2	20/06/2023	Revisione Generale	

SOMMARIO P.TE 1 (CARATTERISTICHE GENERALI)

1	SCOPO E AMBITO	5
1.1	Norme e standard di riferimento	6
1.2	Terminologia (glossario e acronimi)	9
1.3	Oggetto del servizio (Mission)	11
1.4	Destinatari del Servizio	11
1.5	Soggetti coinvolti	12
1.6	Descrizione del Servizio	13
1.7	Attività accessorie	14
1.8	Cambio di mission (cessazione del Servizio)	14
2	PERIMETRO DI EROGAZIONE DEL SERVIZIO	15
2.1	Durata del rapporto (attivazione istanza)	15
2.2	<i>Limiti all'erogazione del Servizio</i>	16
2.3	<i>Sospensione, prosecuzione e cessazione del rapporto</i>	16
2.4	Alert previsti	17
3	CARATTERISTICHE TECNICHE E TECNOLOGICHE	18
3.1	Datacenter	18
3.2	Segregazione dei sistemi	18
3.3	Firme digitali, PEC e Marcatura temporale	18
3.4	Componente applicativa	19
3.5	Capacity planning	19
3.6	Update e change-log	19
3.7	Attivazione/Disattivazione risorse	20
3.8	Supporti removibili, cifratura e trasmissione dati	20
3.9	Gestione file virati	20
3.10	Restituzione e dismissione degli asset	21
3.11	Politiche di backup ed eliminazione dei dati dal sistema	21
3.12	Alta affidabilità, incident e Disaster recovery	21
3.13	Analisi dei rischi	21
4	STRUTTURA ORGANIZZATIVA PER IL SERVIZIO	22
4.1	Ruoli previsti	23
4.2	Il Cliente (Responsabile gestione e conservazione)	24
4.3	Il Conservatore (Nomine e Amministratori di sistema)	24
4.4	Matrice delle responsabilità	25

SOMMARIO P.TE 2 (SPECIFICITÀ DEL SERVIZIO)

5	DETTAGLIO ATTIVITÀ PREVISTE (trattamenti)	26
5.1	Trattamento dati.....	27
5.2	Attività preliminari e incarico.....	27
5.3	Attivazione del servizio	27
5.4	Variazione o Estensione del Servizio.....	28
5.5	Adeguamento del Sistema	28
5.6	Monitoraggio del Sistema (SLA).....	28
5.7	Trasferimento dati in conservazione	30
5.8	Selezione e raccolta delle UD da conservare	31
5.9	Generazione PdV e gestione file cifrati.....	31
5.10	Caricamento PdV.....	32
5.11	Validazione dei PdV.....	33
5.12	Gestione esiti di elaborazione.....	34
5.13	Archiviazione dei dati (PdA)	34
5.14	Accesso agli archivi.....	34
5.15	Produzione duplicati e copie informatiche (PdD)	35
5.16	Gestione dell'obsolescenza tecnologica (riversamento)	35
5.17	Conversioni e riversamenti	35
5.18	Eliminazione dei dati conservati	35
5.19	Tracciatura delle attività eseguite.....	37
5.20	Verifica dell'integrità degli archivi (verifiche periodiche)	38
6	Configurazione del Sistema (il Soggetto Produttore)	39
6.1	Descrizioni Archivistiche	39
6.2	Conservazione di documenti.....	40
6.3	Conservazione di fascicoli	40
6.4	Metadati, indici di conservazione	41
6.5	Formati file ammessi in conservazione.....	44
7	Istruzioni e strutture dati di riferimento	44

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 AgID². 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 Sistema³ 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, Fascicolo 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 differenzia "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 obiettivo specifico e condiviso (v. Manuale di gestione e conservazione documentale del Cliente/Produttore)

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 requisiti 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
Reg. UE 2018_1807	Regolamento relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea

[torna al sommario](#)

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 2024-2026	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
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](#)

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 Archival 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 Guide : 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](#)

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 conservare 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.

MANUALE DEL SERVIZIO DI CONSERVAZIONE

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 obiettivo o nell'erogazione di un servizio
Servizio	Erogazione di uno o 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 logica 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, contenente 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](#)

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".

1.5 Soggetti coinvolti

Rinviano 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 dedicati 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](#)

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 trasmesse in conservazione **in Pacchetti di Versamento (PdV)**, accompagnate dagli [indici di conservazione](#) previsti per la relativa fattispecie.

I PdV ammessi in conservazione sono 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](#)

1.7 Attività accessorie

Fuori dal perimetro 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 perimetro 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 sede 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](#)

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

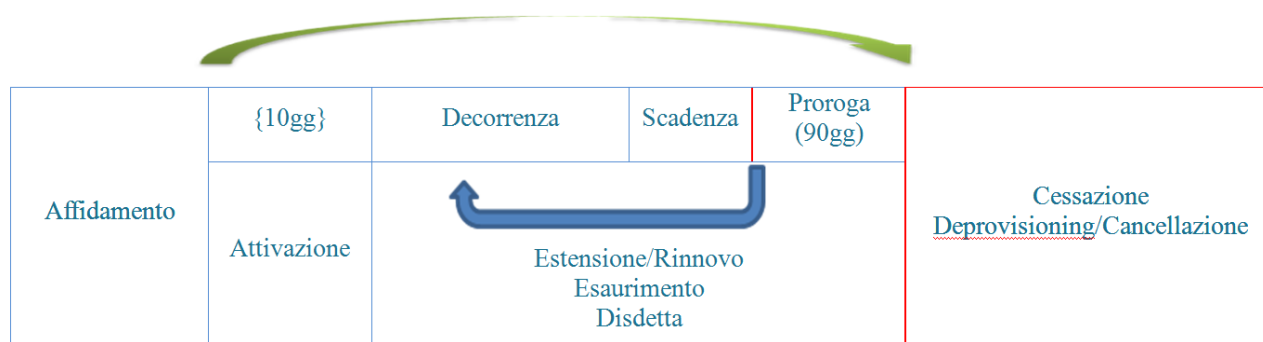
- un **ordine** (o atto equivalente) che dettaglia tempi, importi economici e quantità di dati concordati;
- un atto, o modulo di **richiesta di attivazione** che dettaglia i flussi documentali e i Soggetti coinvolti;
- la sottoscrizione per accettazione integrale di **questo Manuale e dei suoi allegati**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

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.

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](#)

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](#).

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](#)

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](#)

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](#)

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](#)

4 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO

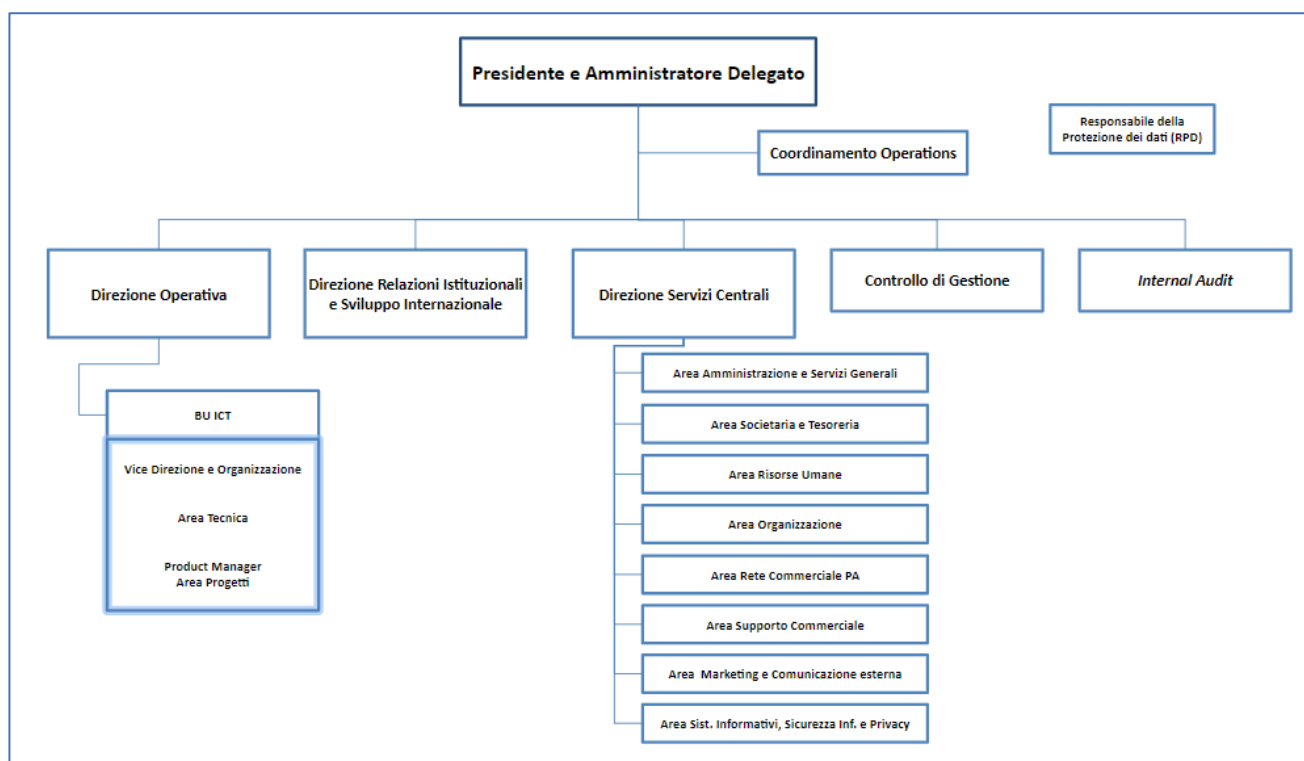
Per l'esecuzione attività previste dal Servizio

- 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:

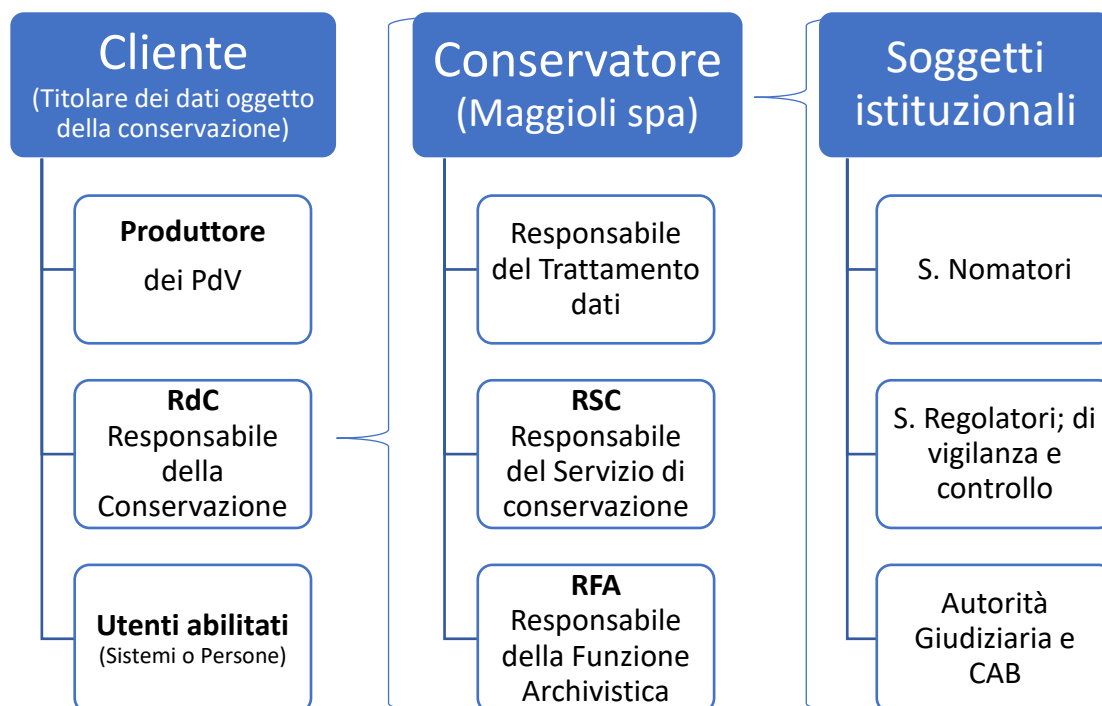
2- Organigramma Maggioli spa



[torna al sommario](#)

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](#)

4.2 Profili utente

Il Sistema di conservazione applica il **principio di minimo privilegio** e quello di ereditarietà dei permessi:

Gli Utenti sono Attori abilitati ad interagire con il Sistema; Gli Attori possono essere Persone fisiche oppure Applicazioni o Sistemi esterni indicati dal Responsabile di Conservazione di ogni Organizzazione coinvolta e possono agire limitatamente agli archivi dell’istanza di riferimento per l’organizzazione e in base al loro Ruolo.

Il conservatore dispone di Utenti con ruolo di Gestione (accedono ai log e ai processi, ma non ai dati) e Amministrazione (possono attivare istanze, utenti e accedere ai dati), mentre i clienti possono avere Utenti base o avanzati (solo ricerca o ricerca più versamento manuale) e utenti che operano in integrazione applicativa, con le stesse limitazioni degli utenti avanzati; gli Enti istituzionali e di controllo possono disporre di utenze “demo” (funzionalità complete, ma accesso limitato a dati fittizi) oppure eseguire verifiche più approfondite con il supporto degli Amministratori del Sistema del Conservatore

[torna al sommario](#)

4.3 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](#)

4.4 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 B.U. ICT
Stefania Rampazzo	Responsabile della funzione archivistica	Collaboratore esterno
Ernesto Belisario	(DPO) Responsabile della Protezione dei dati	Collaboratore esterno
Luca Castellano	Responsabile della Sicurezza dei sistemi	Direttore Sistemi informativi e Sicurezza (CISO)
Andrea Furiosi	Product Manager & Sales Account Manager	Collaboratore esterno
Alessandro Urbinati	Resp. ufficio ordini e commesse	Dipendente (B.U. ICT)
Miriam Saladino	Resp. Assistenza clienti	Dipendente (B.U. ICT)
Oscar Bevoni	Responsabile sistemi informativi	Responsabile infrastrutture e Data Center
Fabio Tiralongo	Responsabile sviluppo e manutenzione Amministratore del Sistema di conservazione	Dipendente (B.U. ICT)
Matteo Aletta	Amministratore del Sistema di conservazione	Dipendente (B.U. ICT)
Marco Leasi	Amministratore dei Sistemi IT di Maggioli spa	Dipendente Sistemi Informativi, Maggioli spa

4 - Nomine Maggioli spa

4.5 Matrice delle responsabilità

La matrice RACI (Responsible, Accountable, Consulted, Informed) descrive per ogni attività prevista o necessaria il

- Responsible = **Responsabile** dell'esecuzione dell'attività
- Accountable = Delegato, responsabile sul risultato atteso (Vicario/Responsabile) delle attività
- Consulted = Funzioni di supporto all'esecuzione o definizione delle attività
- Informed = 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

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](#)

4.6 Il Responsabile del Servizio di conservazione

- 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.

[torna al sommario](#)

4.7 Il Responsabile della Funzione Archivistica

- Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato;
- definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici;
- monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione;
- collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.

[torna al sommario](#)

4.8 Amministratori del Sistema

Sono gli unici operatori, appositamente formati e nominati, autorizzati da Maggioli spa ad accedere al sistema di conservazione e ai dati in esso conservati.

[torna al sommario](#)

4.9 Modifiche intercorse alle nomine interne

È importante che il sistema di conservazione storicizzi e riporti nei Pacchetti di archiviazione prodotti la corretta e corrente definizione dei Ruoli, presso il Soggetto Produttore, quanto presso il Conservatore.

Il Cliente (Soggetto Produttore) ha il dovere di comunicare il più tempestivamente possibile al Conservatore ogni variazione intercorsa alle nomine indicate.

4.9.1 Variazione delle Nomine a Responsabile di Conservazione presso Maggioli spa

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](#)

5 DETTAGLIO ATTIVITÀ PREVISTE (trattamenti)

Per ognuna della attività previste nell'erogazione del servizio si riporta Descrizione e [Responsabile](#).

In generale il Servizio di conservazione applica il **principio di minimizzazione dei dati** ovvero consente di trasmettere in conservazione tutte le informazioni previste dal Soggetto Produttore, ma utilizza ed indicizza solo quelle minime, e concordate, necessarie all'erogazione del servizio (corretta registrazione dei dati conservati e disponibilità delle evidenze documentali prodotte)

[torna al sommario](#)

5.1 Trattamento dati

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

- trattati in modo lecito, corretto e trasparente;
- raccolti per le sole finalità previste per l'erogazione del Servizio;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati");
- 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 ("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").

L'informativa privacy completa è resa disponibile sul sito istituzionale di Maggioli spa, all'indirizzo: https://assistenza.maggioli.it/wp-content/uploads/2023/09/Maggioli-SpA_Informativa-Privacy-Clienti_01.01.2020.pdf

[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 del 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](#)

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% ("ggl" = "giornate lavorative nell'anno") nei seguenti casi:

INDICATORI DI PERFORMANCE (SISTEMA)

- **Up-Time** del servizio (raggiungibilità HTTPS/SSH richiesta)
 - > **99,5%** (ore/ggl/anno);
 - solo sessioni valide e almeno 5 secondi tra le sessioni/chiamate attivate

MANUALE DEL SERVIZIO DI CONSERVAZIONE

- 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
 - 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**

INDICATORI DI GESTIONE (SERVIZIO)

- Risposta alla Richiesta di **attivazione o variazione del Servizio** [\[PEC\]](#):
 - **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 assistenza o segnalazione** ([portale HDM](#))
 - Presa in carico del ticket (TT) **entro 3 ggll** (TT/anno)
 - Risposta alle **richieste di informazioni** **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**
 - **RTO⁸ (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
 - **RPO⁹ (Recovery Point Objective), massimo 1 giorno**

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

- Disdetta o richiesta di **disattivazione** del Servizio (istanza) o di un'utenza **[PEC]**:
 - 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 un adeguato monitoraggio dei processi di ticketing e supporto.

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. segnatrice) 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;

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 contenuti 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 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
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](#)

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

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 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](#)

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 possono 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 eliminare (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](#)

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.

MANUALE DEL SERVIZIO DI CONSERVAZIONE

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](#)

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](#)

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](#)

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 obiettivo.

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](#)

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]

MANUALE DEL SERVIZIO DI CONSERVAZIONE

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](#)

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)

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.

N.B: i file vuoti (dimensione pari a 0b), non hanno mime-type o formato associato e non possono per tanto essere validati/inviati in conservazione

[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](#)



CITTA' DI AULLA

Medaglia d'Oro al Merito Civile

Provincia di Massa Carrara

SERVIZI FINANZIARI E ALLA CITTA'

BILANCIO E CONTABILITA'

DETERMINAZIONE N. 1223 Del 16/09/2025

OGGETTO:

**AFFIDAMENTO GESTIONE, ASSISTENZA E MANUTENZIONE CONSERVAZIONE
DOCUMENTALE - ADESIONE CONTRATTO QUADRO FRA REGIONE TOSCANA - SOGGETTO
AGGREGATORE E RTI ENGINEERING INGEGNERIA INFORMATICA SPA LOTTO 1 - CIG
CONTRATTO QUADRO N. 8551248914. CIG DERIVATO N. B7F02FD93C.**

FIRMATO
IL DIRIGENTE
MICHELETTI LUCIANA

Le firme, in formato digitale, sono state apposte sull'originale del presente atto ai sensi dell'art. 24 del D.Lgs. 07.03.2005, n. 82 e s.m.i. (CAD). Il presente atto è conservato in originale negli archivi informatici del Comune di Aulla, ai sensi dell'art. 22 del D.Lgs. 82/2005.

OGGETTO: AFFIDAMENTO GESTIONE, ASSISTENZA E MANUTENZIONE CONSERVAZIONE DOCUMENTALE - ADESIONE CONTRATTO QUADRO FRA REGIONE TOSCANA - SOGGETTO AGGREGATORE E RTI ENGINEERING INGEGNERIA INFORMATICA SPA LOTTO 1 - CIG CONTRATTO QUADRO N. 8551248914. CIG DERIVATO N. B7F02FD93C.

IL DIRIGENTE

PREMESSO il Decreto Sindacale n. 7 del 25.05.2023 ad oggetto: "incarico della Direzione del 2° Settore "Servizi Finanziari e alla Città" al Dirigente Dott.ssa Luciana Micheletti";

VISTE:

- la deliberazione di Consiglio Comunale n. 33 del 29/11/2024 ad oggetto: "APPROVAZIONE DEL DOCUMENTO UNICO DI PROGRAMMAZIONE (DUP) 2025/2027 E RELATIVI ALLEGATI.";
- la deliberazione di Consiglio Comunale n. 43 del 30/12/2024 ad oggetto: "APPROVAZIONE DEL BILANCIO DI PREVISIONE FINANZIARIO 2025-2027 (ART. 151 DEL D.LGS. N. 267/2000 E ART. 10, D.LGS. N. 118/2011);

VISTI:

- l'art. 9 del D.L. n. 66/2014, convertito con modificazioni dalla L. 23 giugno 2014, n. 89, secondo cui i soggetti aggregatori, tra cui rientra la Regione Toscana - Dir. Gen. Organizzazione - Settore Contratti, possono stipulare, per gli ambiti territoriali di competenza, le convenzioni di cui all'art. 26 comma 1 della Legge 488/1999;
- l'art. 42 della L.R. 38/2007 secondo cui è consentito alla Regione di assumere le funzioni di centrale di committenza nei confronti delle amministrazioni pubbliche per gli appalti di forniture e servizi di interesse generale;
- l'articolo 1 comma 512 ss. della legge 28 dicembre 2015, n. 208, secondo cui le amministrazioni pubbliche provvedono ai propri approvvigionamenti esclusivamente tramite gli strumenti di acquisto e di negoziazione di Consip Spa o dei soggetti aggregatori, ivi comprese le centrali di committenza regionali, per i beni e i servizi disponibili presso gli stessi soggetti;

RICORDATO l'art. 44 del D.Lgs. 82/2005 ed in particolare il comma 1ter secondo cui: *"Il sistema di conservazione dei documenti informatici assicura, per quanto in esso conservato, caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità, secondo le modalità indicate nelle Linee guida"*;

Vista la determinazione n.1932 del 30/12/2022, con la quale è stato affidato alla ditta engineering ingegneria informatica s.p.a la *"Fornitura di un sistema per la gestione di archivio in ambito RTRT, comprendente la conservazione a lungo termine per gli archivi digitali (DAX)"*, mediante il sistema telematico acquisti regionali della toscana – START – aderendo al contratto fra Regione Toscana e Engineering Ingegneria Informatica S.p.A. (capogruppo) c.f. 00967720285, per gli esercizi 2022/2024;

RILEVATA la necessità di continuare a garantire e mantenere la conservazione documentale comprensiva di servizi di gestione dell'archivio, help desk e supporto;

DATO ATTO CHE:

- è attivo su START un contratto quadro per la *"Gestione, assistenza, manutenzione, evoluzione del Sistema di Conservazione di Regione Toscana (Sistema di Conservazione) - Lotto 1 CIG 8551248914"* stipulato da Regione Toscana con la Società ENGINEERING – Ingegneria Informatica S.p.a.;

- è stata presentata una manifestazione di interesse a Regione Toscana in data 04/05/2025 per un importo di € 343,47 oltre IVA pari ad € 419,03, allegata al presente provvedimento quale parte integrante;
- l'importo suddetto è per l'utilizzo di 201 GB di spazio a disposizione per la conservazione/archiviazione dei documenti per coprire le esigenze fino al 04/05/2027;
- sono stati compilati i moduli atto di adesione e modulo d'ordine, qui allegati parti integranti e sostanziali;

RITENUTO necessario, pertanto, aderire al contratto quadro per la *"Gestione, assistenza, manutenzione, evoluzione del Sistema di Conservazione di Regione Toscana (Sistema di Conservazione) - Lotto 1 CIG 8551248914"* stipulato da Regione Toscana con la Società ENGINEERING – Ingegneria Informatica S.p.a. per un importo di € 343,47 oltre IVA 22%, come da contratto e tabella economica allegati al presente provvedimento;

DATO ATTO, inoltre, che sono allegati al presente atto i seguenti documenti da trasmettere alla Regione Toscana mediante START successivamente all'esecutività del presente provvedimento:

- atto di adesione
- modulo di ordine;

RITENUTO pertanto necessario, a seguito di quanto sopra esposto, procedere all'affidamento alla ditta Engineering Ingegneria Informatica S.p.A. mediante il Sistema Telematico Acquisto Regionale della Toscana – START – aderendo al contratto fra Regione Toscana e Engineering Ingegneria InformaDca S.p.A. (capogruppo) c.f. 00967720285 e di provvedere ad assumere il necessario impegno di spesa per un importo di 343,47 oltre IVA 22%, per complessivi € 419,03, per le annualità 2025/2027;

DATO ATTO che:

- il CIG del contratto Quadro è 8551248914 e il CIG derivato è: B7F02FD93C;
- è stata verificata la regolarità del DURC prot. INAIL_49500756 del 13/06/2025 con scadenza il 11/10/2025;

VISTO:

- il D.Lgs. n. 36/2023 "Codice dei contratti pubblici";
- gli artt. 107 – 183 e 192 del D.Lgs. 267/2000;
- il vigente Regolamento Comunale di contabilità;
- lo Statuto del Comune di Aulla;

DETERMINA

1. di dare atto che la premessa è parte integrante e sostanziale del presente provvedimento, per cui si intende qui integralmente trascritta e ne costituisce la motivazione;
2. di aderire al Contratto Quadro stipulato per la *"Gestione, assistenza, manutenzione, evoluzione del Sistema di Conservazione di Regione Toscana (Sistema di Conservazione) - Lotto 1 CIG 8551248914"* stipulato da Regione Toscana con l'RTI Società ENGINEERING – Ingegneria Informatica S.p.a. di Roma - P.IVA 05724831002 per la fornitura dei servizi di mantenimento e conservazione documentale, comprensivi di gestione archivio, help desk e supporto, per le annualità 2025 – 2027 per un importo complessivo di €343,47 oltre IVA e così per complessivi € 419,03;

3. di dare atto che sono allegati al presente provvedimento i seguenti documenti, facenti parte integrante e sostanziale del presente atto, approvati da Regione Toscana sul negozio elettronico del portale START in data 08/08/2025:

- contratto, tabella economica;
- manifestazione di interesse;
- schema di atto di adesione e del modulo d'ordine;

4. di impegnare a favore del RTI Engineering SpA la somma complessiva di € 419,03 IVA inclusa, con imputazione sui capitoli del bilancio finanziario 2025/2027 indicati nel parere di regolarità contabile reso dal Responsabile del servizio finanziario, con esigibilità sugli esercizi finanziari 2025, 2026 e 2027, con il seguente cronoprogramma di spesa:

- € 167,39 sull'esercizio 2025;
- € 184,46 sull'esercizio 2026;
- € 67,18 sull'esercizio 2027 fino al 04/05/2027;

6. di dare atto che, ai sensi e per gli effetti dell'art. 5 della L. 241/1990 e dell'art. 31 del D. Lgs.n. 50/2016, il responsabile del procedimento, con esclusione dell'adozione del provvedimento finale la cui responsabilità è in capo al Dirigente, è dipendente Samanta Baldi;

7. di dare atto che la prestazione oggetto del contratto è riconducibile ad un contratto pluriennale necessario per garantire la continuità dei servizi, per cui, ai sensi dell'art. 183, comma 6, lett. a) del T.U.E.L. è possibile assumere la relativa obbligazione in esercizi successivi a quello in corso;

8. di dare atto che il presente provvedimento assume la valenza di decisione di contrarre, di cui all'art. 17, comma 1, del D.Lgs 36/2023, ai sensi del comma 2 del medesimo articolo;

9. di dare atto che i pagamenti avverranno mediante atto di liquidazione redatto ai sensi dell'art.184 del D. Lgs. n. 267/2000;

10. di dare atto che il contenuto della presente determinazione è soggetto agli ulteriori e specifici obblighi di pubblicazione previsti dal D.Lgs 33/2013;

11. di dare atto che, ai fini del controllo preventivo di regolarità amministrativa e contabile di cui all'art. 147 bis, comma 1, del D.Lgs. n. 267/2000:

- il parere di regolarità tecnica è rilasciato con la sottoscrizione del presente atto da parte del Dirigente del 2° Settore.
- il parere di regolarità contabile è rilasciato con l'apposizione del visto contabile attestante la copertura finanziaria ex art. 183, comma 7 del D.Lgs. 267/2000 da parte del Responsabile del servizio finanziario.

IL DIRIGENTE DEL 2° SETTORE
(D.ssa Luciana Micheletti)



Manuale di conservazione

REVISIONI DEL DOCUMENTO

Data	Versione	Elenco Modifiche	Compilato	Verificato	Validato
2015-10-30	1.0	Prima emissione	Andrea Panichi (Direttore Esecuzione Regione)	Anna Fuggi (Responsabile servizio DigiDoc)	Laura Castellani (RUP Regione Toscana)
2015-12-18	2.0	Recepiti osservazioni AGID del 24/11/2015	Andrea Panichi (Direttore Esecuzione Regione)	Anna Fuggi (Responsabile servizio DigiDoc)	Laura Castellani (RUP Regione Toscana)
2016-01-26	3.0	Recepiti osservazioni AGID del 21/01/2016	Andrea Panichi (Direttore Esecuzione Regione)	Anna Fuggi (Responsabile servizio DigiDoc)	Laura Castellani (RUP Regione Toscana)
2016-02-08	3.1	Recepiti osservazioni AGID del 05/02/2016	Andrea Panichi (Direttore Esecuzione Regione)	Anna Fuggi (Responsabile servizio DigiDoc)	Laura Castellani (RUP Regione Toscana)
2018-01-12	3.2	Cambio sito DR – cambio responsabile sicurezza- cambio hypertix con gestore TIX	Andrea Panichi (Direttore Esecuzione Regione)	Anna Fuggi (Responsabile servizio DigiDoc)	Laura Castellani (RUP Regione Toscana)
2018-03-02	3.3	Dettagli sui log	Andrea Panichi (Direttore Esecuzione Regione)	Anna Fuggi (Responsabile servizio DigiDoc)	Laura Castellani (RUP Regione Toscana)
2019-10-23	3.4	Precisazioni sui log come richiesto da ISO/IEC 27017 e 27018. Modifica del Responsabile trattamento dati personali e del Responsabile della Sicurezza	Andrea Panichi (Direttore Esecuzione Regione)	Anna Fuggi (Responsabile servizio DigiDoc)	Sergio Papiani (RUP Regione Toscana)



2022-01-01	4.0	Revisioni a seguito degli adeguamenti alle Linee Guida AgID	Andrea Panichi (Direttore Esecuzione Regione)	Anna Fuggi (Responsabile servizio DigiDoc)	Sergio Papiani (RUP Regione Toscana)
2022-04-08	4.1	Modifica del Responsabile funzione archivistica di conservazione	Andrea Panichi (Direttore Esecuzione Regione)	Anna Fuggi (Responsabile servizio DigiDoc)	Sergio Papiani (RUP Regione Toscana)

INDICE

1	Scopo e ambito del documento.....	5
2	Terminologia (glossario e acronimi).....	5
2.1	ACRONIMI.....	5
2.2	Glossario.....	7
3	Normativa e standard di riferimento.....	16
3.1	Normativa di riferimento.....	16
3.2	Standard di riferimento.....	17
4	Ruoli e responsabilità.....	18
4.1	Il Responsabile del servizio di conservazione.....	21
4.2	Formazione.....	23
5	Struttura organizzativa per il servizio di conservazione.....	24
5.1	Strutture organizzative.....	25
5.1.1	Regione Toscana.....	25
5.1.2	Gestore del TIX.....	25
5.1.3	RTI DAX.....	26
6	Oggetti sottoposti a conservazione.....	27
6.1	Oggetti conservati.....	27
6.2	Pacchetto di versamento.....	28
6.3	Pacchetto di archiviazione.....	29
6.4	Pacchetto di Distribuzione.....	30
6.5	Formati.....	31
6.6	Metadati conservati.....	31
6.7	Tempi di conservazione.....	32
7	IL PROCESSO DI CONSERVAZIONE.....	32
7.1	Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico.....	34
7.2	Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti.....	36
7.2.1	Controllo impronta del pacchetto di versamento.....	36



7.2.2	Controllo dell'identità del soggetto produttore del pacchetto.....	36
7.2.3	Controllo delle Firme Digitali.....	37
7.2.4	Controllo dei Formati digitali.....	39
7.2.5	Controllo della Presenza di Macro e Codice Eseguitibile.....	42
7.2.6	Controllo dei Metadati.....	42
7.2.7	Controllo Impronta.....	43
7.3	Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico 44	
7.3.1	Rinnovo marche temporali in scadenza.....	44
7.4	Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie.....	45
7.5	Preparazione e gestione del pacchetto di archiviazione.....	45
7.5.1	Creazione Indice di Conservazione.....	46
7.5.2	Certificazione pacchetto (firma e apposizione riferimento temporale).....	47
7.6	Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione.....	48
7.6.1	Funzionalità di ricerca.....	48
7.6.2	Funzionalità di esibizione.....	50
7.7	Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti.....	53
7.8	Scarto dei pacchetti di archiviazione.....	54
7.8.1	Cancellazione di pacchetti di archiviazione inviati per errore.....	55
7.9	Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori.....	56
7.10	Riversamento.....	56
8	Il sistema di conservazione.....	57
8.1	Componenti Logiche.....	57
8.2	Componenti Tecnologiche.....	58
8.2.1	Software di base.....	58
8.2.2	Framework di sviluppo utilizzati.....	59
8.3	Componenti Fisiche.....	59
8.3.1	Componenti HW.....	62
8.4	Procedure di gestione e di evoluzione.....	62
8.4.1	Procedure per la conduzione e manutenzione dell'infrastruttura hardware (manutenzione evolutiva e correttiva).....	63
8.4.2	Procedure per la gestione e conservazione dei log (anche in accordo con il Titolare degli oggetti di conservazione).....	64

9	Monitoraggio e controlli.....	65
9.1	Procedure di monitoraggio.....	65
9.2	Procedure di monitoraggio per il cliente.....	66
9.3	Verifica dell'integrità degli archivi.....	66
9.4	Soluzioni adottate in caso di anomalie.....	67

INDICE DELLE FIGURE

Figura 1 :	La figura mostra l'organizzazione del servizio di Conservazione, in base ai ruoli svolti dai diversi soggetti coinvolti nella erogazione.....	24
Figura 2:	La figura rappresenta il flusso con cui un documento viene versamento del documento nel sistema di conservazione.....	35
Figura 3:	la figura rappresenta la modalità di visualizzazione di un documento, a seguito di ricerca nel sistema di conservazione.....	49

1 Scopo e ambito del documento

Il presente documento costituisce il Manuale di Conservazione adottato da Regione Toscana per il processo di conservazione della documentazione digitale ai sensi della vigente normativa in materia elencata nell'apposito capitolo del presente documento.

Il manuale comprende tutte le informazioni previste dall'Agenzia per l'Italia Digitale per quanto concerne le tipologie documentali oggetto di conservazione: all'ampliarsi e/o al variare di tali tipologie il manuale verrà aggiornato per recepire tutte le informazioni aggiornate relative al trattamento delle tipologie oggetto di conservazione.

Si precisa che, per garantire la protezione di informazioni riservate, i dettagli relativi a argomenti che riguardano aspetti delle specifiche forniture del servizio di conservazione, come anche alcune informazioni previste all'interno del manuale, non saranno inseriti nel presente manuale, ma saranno sviluppati in documenti specifici (ad es. "Proposta tecnica" o "Piano della Sicurezza"), depositati in sede di presentazione della domanda di accreditamento, per i quali non sussiste obbligo di pubblicazione.

Torna all' [INDICE](#)

2 Terminologia (glossario e acronimi)

Torna all' [INDICE](#)

2.1 ACRONIMI

ACRONIMO	DEFINIZIONE
ACL	Access Control List
AIP	Archival Information Package (ex OAIS), ovvero il pacchetto di archiviazione ex DPCM 3 Dicembre 2013
AgID	Agenzia per l'Italia Digitale
AOO	Area Organizzativa Omogenea
CA	Certification Authority
CAD	Codice dell'Amministrazione Digitale, ovvero D.lgs 7 marzo 2005, n.82 e successive modificazioni e integrazioni
CAdES	CMS (Cryptographic Message Syntax) Advanced Electronic Signatures

ACRONIMO	DEFINIZIONE
CNS	Carta Nazionale dei Servizi provvista almeno del certificato di autenticazione (recante il codice fiscale del titolare)
DB	Database
DIP	Dissemination Information Package (ex OAIS), ovvero il pacchetto di distribuzione DPCM 3 Dicembre 2013
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
GDPR	Regolamento (UE) N° 679/2016 del Parlamento Europeo e del Consiglio, del 27 aprile 2016 ("General Data Protection Regulation"), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE
GUI	Graphical User Interface
FTP server	programma che permette di accettare connessioni in entrata e di comunicare con un Client attraverso il protocollo FTP
HSM	Hardware Security Module
ORM	Object-relation Mapping
OAIS	Open Archival Information System, standard ISO 14721:2002
PAdES	PDF Advanced Electronic Signatures
PEC	Posta Elettronica Certificata
SdI	Sistema di Interscambio (per le fatture elettroniche destinate alle pubbliche amministrazioni)
SIP	Submission Information Package (ex OAIS), ovvero il pacchetto di versamento DPCM 3 Dicembre 2013
SSO	Single Sign On
TSA	TimeStamping Authority
UI	User Interface
UO	Unità organizzativa (cfr glossario)
URI	Uniform Resource Identifier
XAdES	XML Advanced Electronic Signatures

ACRONIMO	SIGNIFICATO
RT	Regione Toscana

Torna all' [INDICE](#)

2.2 Glossario

Obiettivo di questo glossario è quello di definire il significato con il quale alcuni termini “chiave” ricorrenti saranno utilizzati all’interno del presente documento. Le definizioni, nel rispetto della terminologia tecnica di riferimento e delle prescrizioni normative, sono quelle effettivamente utilizzate all’interno del sistema di conservazione.

TERMINE	DEFINIZIONE
Accesso	Operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia 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



TERMINE	DEFINIZIONE
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.
Base di dati	Collezione di dati registrati e correlati tra loro
CAD	Decreto legislativo 7 Marzo 2005, n. 82 e successive modificazioni e integrazioni
CAdES	CMS Advanced Electronic Signatures – Formato di firma che può essere apposto su qualsiasi tipo di file. Genera una busta genera una busta crittografica contenente il file originale. Si presenta come un file la cui estensione è p7m
Certificazione	Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi.
Certificato di firma	Certificato destinato alla generazione delle firme apposte ai documenti digitali.
Certificato di marcatura temporale	Certificato destinato alla generazione di marche temporali.
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.
Conservatore	Soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici.



TERMINE	DEFINIZIONE
Conservazione	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governare la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione
Coordinatore della gestione documentale	Responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50, comma 4 del Testo Unico nei casi di amministrazioni che abbiano istituito più Aree Organizzative Omogenee
Copia analogica del documento informatico	Documento analogico avente contenuto identico a quello del documento informatico da cui è tratto
Destinatario	Identifica il soggetto/sistema al quale il documento informatico è indirizzato
DOI	Digital Object Identifier
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.
Esibizione	Operazione che consente di visualizzare un documento conservato
Estratto per riassunto di documento informatico	Documento nel quale si attestano in maniera sintetica fatti, stati o qualità desunti da documenti informatici.
Evidenza informatica	Sequenza di simboli binari, ossia 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
Firme multiple	Firme digitali apposte da diversi sottoscrittori allo stesso documento.
Firme parallele	Firme apposte da differenti soggetti al medesimo documento digitale utilizzando una sola busta crittografica.



TERMINE	DEFINIZIONE
Firme verticali	Firme apposte da differenti soggetti, l'una ad un documento firmato in precedenza da un altro soggetto, creando delle buste crittografiche innestate l'una dentro l'altra.
Formato del documento informatico	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
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.
Identificativo univoco	Sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione
Immodificabilità	Caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso
Impronta crittografica	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di hash crittografica a un'evidenza informatica
Indice di conservazione	Evidenza informatica che elenca in forma strutturata – xml - le impronte, gli identificativi e le informazioni descrittive dei documenti digitali sottoposti insieme a processo di conservazione. Tale file è conforme al UNI 11386:2020 Standard SInCRO ed è firmato digitalmente dal responsabile del servizio di conservazione e marcato temporalmente.
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.



TERMINE	DEFINIZIONE
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.
ISBN	International Standard Book Number
Leggibilità	Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica.
Log di sistema	Registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati
Manuale di conservazione	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.
Marca temporale	Evidenza informatica che consente di rendere opponibile a terzi un riferimento temporale. La marca temporale può essere solamente rilasciata da una Time Stamping Authority
Memorizzazione	Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici
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.
Oggetto di conservazione	Oggetto digitale versato in un sistema di conservazione



TERMINE	DEFINIZIONE
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 versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato 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
PADES	PDF Advanced Electronic Signatures– Formato di firma che può essere apposto esclusivamente sul tipo di file pdf.
Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza
Piano della sicurezza del sistema di gestione informatica dei documenti	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi nell'ambito dell'organizzazione di appartenenza
Piano di conservazione	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 generale della sicurezza	Documento per la pianificazione delle attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza

TERMINE	DEFINIZIONE
Posta elettronica certificata	Sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici
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.
Produttore dei PdV	Persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con il responsabile della gestione documentale
Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore
Registrazione informatica	Insieme delle informazioni risultanti da transazioni informatiche o dalla presentazione in via telematica di dati attraverso moduli o formulari resi disponibili in vario modo all'utente
Registro particolare	Registro informatico individuato da una pubblica amministrazione per la memorizzazione delle informazioni relative a documenti soggetti a registrazione particolare, ai sensi dell'articolo 53, comma 5 del D.P.R. 28 dicembre 2000, n. 445
Registro di protocollo	Registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti
Repertorio informatico	Registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche con cui si formano altri atti e documenti o indici di atti e documenti secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica



TERMINE	DEFINIZIONE
Responsabile della gestione documentale	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 conservazione	Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia
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 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 del trattamento dei dati	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento dei dati personali
Responsabile della sicurezza	Soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza
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
Riferimento temporale	Informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento
Scarto	Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico-culturale.
Scheda documento	Nel sistema DAX è un Aggregato logico costituito da uno o più documenti digitali e/o analogici che sono considerati come un tutto unico e come tali costituiscono l'oggetto di una singola descrizione: nel caso in cui sia formato da più documenti uno di essi si configura come "primario" e gli altri sono gli "allegati" che trovano il loro significato compiuto solo in relazione al primario. E' l'unità minima, concettualmente non divisibile, di cui è composto l'archivio.



TERMINE	DEFINIZIONE
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
Staticità	Caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione
Tag	Marcatori (etichette) per assegnare una semantica al testo nei file xml
Testo Unico	Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 e successive modificazioni
Titolare dell'oggetto di conservazione	Soggetto produttore degli oggetti di conservazione
Transazione informatica	Particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche alla base dati
Unità di aggregazione	Nel sistema DAX è un aggregato logico di schede documento collegate tra loro che si forma nell'archivio corrente e che può costituire un'unità di versamento in conservazione. Il fascicolo che scaturisce da un procedimento amministrativo è il caso più comune di unità di aggregazione, altri esempi sono costituiti dalle serie tipologiche (delibere, contratti ecc).
Unità organizzativa	Qualsiasi articolazione di un'Area Organizzativa Omogenea, ovvero un nodo della struttura gerarchica – mappa organizzativa - in cui si organizza un'Amministrazione
URI	Uniform Resource Identifier
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

TERMINE	DEFINIZIONE
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 all' [INDICE](#)

3 Normativa e standard di riferimento

Torna all' [INDICE](#)

3.1 Normativa di riferimento

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

- [1] Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- [2] Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- [3] Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- [4] Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- [5] Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali;
- [6] Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;

- [7] Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
- [8] 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, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;
- [9] Reg. UE 910/2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE - Regolamento eIDAS;
- [10] Reg. UE 679/2016 (GDPR), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- [11] Linee Guida sulla formazione, gestione e conservazione dei documenti informatici adottate da AgID con determinazione n. 407/2020 e successivamente aggiornate e rilasciate con determinazione 37172021.

Torna all' [INDICE](#)

3.2 Standard di riferimento

Di seguito sono riportati gli standard ai quali si fa riferimento per il Manuale di Conservazione (si rimanda all'allegato 4 alle Linee guida AgID "Standard e specifiche tecniche")

- ISO 14721 OASIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ISO/IEC 27001, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- ETSI TR 101 533-2 V1.3.1 (2012-04) Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;

- UNI 11386 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 15836 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.
- Moreq - Model Requirements for Electronic Records Management
- Pronom - registro internazionale sui formati idonei alla conservazione a lungo termine

Torna all' [INDICE](#)

4 Ruoli e responsabilità

Il Servizio di Conservazione gestito da Regione Toscana è basato su un modello organizzativo descritto nel successivo capitolo 5.

I ruoli che intervengono nella erogazione del servizio, con le pertinenti responsabilità, sono elencati nella tabella di seguito e assegnati a risorse che rispondono ai requisiti espressi da AgID, così come ufficializzati nel documento “Profili Professionali”.

RUOLO	NOMINATIVO	ATTIVITÀ DI COMPETENZA	PERIODO NEL RUOLO	EVENTUALI DELEGHE
Responsabile del servizio di conservazione	Anna Fuggi	• 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; • approvazione autorizzazioni al sistema.	Dal 20/10/2015	Ivan Ricotti; Antonella Ghisaura; Laura Castellani <i>(per approvazione modifiche sistema, dal 12/01/2018 al 09/06/2019);</i> Andrea Panichi <i>(per approvazione modifiche sistema, dal 12/01/2018),</i> Angelo Marcotulli <i>(per approvazione modifiche sistema, dal 10/06/2019)</i>
Responsabile Sicurezza dei sistemi per la conservazione	Leonardo Borselli	• 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.	Dal 01/01/2022	N/A



RUOLO	NOMINATIVO	ATTIVITÀ DI COMPETENZA	PERIODO NEL RUOLO	EVENTUALI DELEGHE
Responsabile funzione archivistica di conservazione	Antonella Ghisaura	- Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; - definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici; - monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione; - collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.	Dal 08/04/2022	Ivan Ricotti.
Responsabile trattamento dati personali	Sergio Papiani	- garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; - garanzia che il trattamento dei dati affidati dagli Enti Produttori avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza	Dal 23/09/2019	N/A
Responsabile sistemi informativi per la conservazione	Andrea Panichi	- Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione; - monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore; - segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive; - pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione; - controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.	Dal 20/10/2015	N/A



RUOLO	NOMINATIVO	ATTIVITÀ DI COMPETENZA	PERIODO NEL RUOLO	EVENTUALI DELEGHE
Responsabile sviluppo e manutenzione del sistema di conservazione	Rosario Graziano	• Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione; • pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione; • monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione; • interfaccia con l'ente produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche; • gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.	Dal 08/04/2022	N/A

Alcuni ruoli sono cambiati nel tempo. Nominativi che hanno svolto in precedenza i ruoli indicati sono:

RUOLO	NOMINATIVO	PERIODO NEL RUOLO
Responsabile Sicurezza dei sistemi per la conservazione	Sandro Piana	Dal 20/10/2015 al 25/09/2017
Responsabile Sicurezza dei sistemi per la conservazione	Marco Barbalinardo	Dal 26/09/2017 al 2/10/2019
Responsabile Sicurezza dei sistemi per la conservazione	Angelo Marcotulli	Dal 3/10/2019 al 31/12/2021
Responsabile sviluppo e manutenzione del sistema di conservazione	Valentina Martinucci	Dal 20/10/2015 al 07.04.2022
Approvazione autorizzazioni al sistema	Paola Collesei	Dal 11/10/2016 al 10/01/2018
Delegato Responsabile del servizio di conservazione Delegato Responsabile funzione archivistica di conservazione	Marcello Serenetti	Dal 20/10/2015 al 10/01/2018
Responsabile trattamento dati personali	Laura Castellani	Dal 20/10/2015 al 09/06/2019
Delegato Responsabile del servizio di conservazione	Laura Castellani	Dal 12/01/2018 al 9/06/2019
Responsabile trattamento dati personali	Angelo Marcotulli	Dal 10/06/2019 al 22/09/2019
Delegato Responsabile del servizio di conservazione	Angelo Marcotulli	Dal 10/06/2019 al 22/09/2019
Responsabile funzione archivistica di conservazione	Anna Fuggi	Dal 20/10/2015 al 07/04/2022

Torna all' [INDICE](#)

4.1 Il Responsabile del servizio di conservazione

Nel presente paragrafo sono dettagliate le competenze del Responsabile del servizio di conservazione, affidate dal Responsabile della conservazione, interno al soggetto produttore, al Responsabile del servizio di conservazione che opera presso il soggetto conservatore secondo quanto previsto dal decreto [8].

- Definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente;
- gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
- genera il rapporto di versamento con sigillo qualificato con marcatura temporale, secondo le modalità previste dal manuale di conservazione;
- genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata o sigillo qualificato, nei casi previsti dal manuale di conservazione;
- effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
- assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
- al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;
- provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
- adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12 decreto [8];
- assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
- assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
- provvede, per gli organi giudiziari e amministrativi dello Stato, al versamento dei documenti conservati all'archivio centrale dello Stato e agli archivi di Stato secondo quanto previsto dalle norme vigenti;

- predispone il manuale di conservazione di cui all'art. 8 del decreto [8]e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.
- Definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti (analogici o informatici) da conservare, della quale tiene evidenza. Organizza conseguentemente il contenuto dei supporti ottici e gestisce le procedure di sicurezza e di tracciabilità che ne garantiscono la corretta conservazione, anche per consentire l'esibizione di ciascun documento conservato;
- archivia e rende disponibili, con l'impiego di procedure elaborative, relativamente ad ogni supporto di memorizzazione utilizzato, le seguenti informazioni:
 1. descrizione del contenuto dell'insieme dei documenti;
 2. estremi identificativi del responsabile del servizio di conservazione;
 3. estremi identificativi delle persone eventualmente delegate dal responsabile del servizio di conservazione, con l'indicazione dei compiti alle stesse assegnati;
 4. indicazione delle copie di sicurezza;
- mantiene e rende accessibile un archivio del software dei programmi in gestione nelle eventuali diverse versioni;
- verifica la corretta funzionalità del sistema e dei programmi in gestione;
- adotta le misure necessarie per la sicurezza fisica e logica del sistema preposto al processo di conservazione e delle copie di sicurezza dei supporti di memorizzazione;
- richiede la presenza di un pubblico ufficiale nei casi in cui sia previsto il suo intervento, assicurando allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
- definisce e documenta le procedure di sicurezza da rispettare per l'apposizione del riferimento temporale;
- verifica periodicamente, con cadenza non superiore a cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti.

Il responsabile del procedimento di conservazione può delegare in tutto o in parte le proprie attività ad una o più persone che, per competenza ed esperienza, garantiscano la corretta esecuzione delle operazioni ad esse delegate.

Il responsabile del servizio di conservazione richiede l'intervento del Pubblico Ufficiale nei casi previsti, assicurando allo stesso l'assistenza e le risorse necessarie all'espletamento delle attività al medesimo attribuite.

Il Responsabile del servizio di Conservazione non è responsabile del contenuto dei singoli documenti né degli indici (attributi) associati a ciascun Documento. La conformità dei documenti trasmessi ai corrispondenti originali è assicurata da formale autorizzazione alla Conservazione da parte del Produttore, eseguita mediante la sottoscrizione del contratto per la fornitura del servizio.

Il responsabile del servizio di conservazione è tenuto ad operare d'intesa con:

- il responsabile del trattamento dei dati personali
- il responsabile della sicurezza
- il responsabile dei sistemi informativi
- il coordinatore della gestione documentale, salvo che il ruolo sia ricoperto dallo stesso responsabile del servizio di conservazione
- i responsabili designati per ciascuno dei sistemi/applicativi abilitati a versare in conservazione la documentazione: per poter versare in conservazione ciascun sistema/applicativo deve essere a ciò abilitato attraverso apposita procedura che prevede di poter indicare il responsabile di riferimento del sistema/applicativo quale figura che il RdC può interpellare per qualsiasi problematica inerente la documentazione versata in conservazione dal sistema/applicativo stesso; qualora tale responsabile non sia designato il coordinatore della gestione documentale e il responsabile del cliente che ha versato la documentazione sono i soggetti tenuti a fornire al RdC tutte le informazioni richieste.

Torna all' [INDICE](#)

4.2 Formazione

Per il responsabile del servizio di conservazione è previsto uno piano di formazione allo scopo di adeguare il percorso formativo alle nuove eventuali esigenze di legge e di business. Tale percorso prevede la partecipazione ad eventuali corsi di aggiornamento e seminari periodici sul tema della conservazione digitale, corsi di formazione sulla sicurezza delle informazioni e sulla privacy.

Torna all' [INDICE](#)

5 Struttura organizzativa per il servizio di conservazione

Il servizio di Conservazione erogato dalla Regione Toscana si configura in armonia al seguente schema:

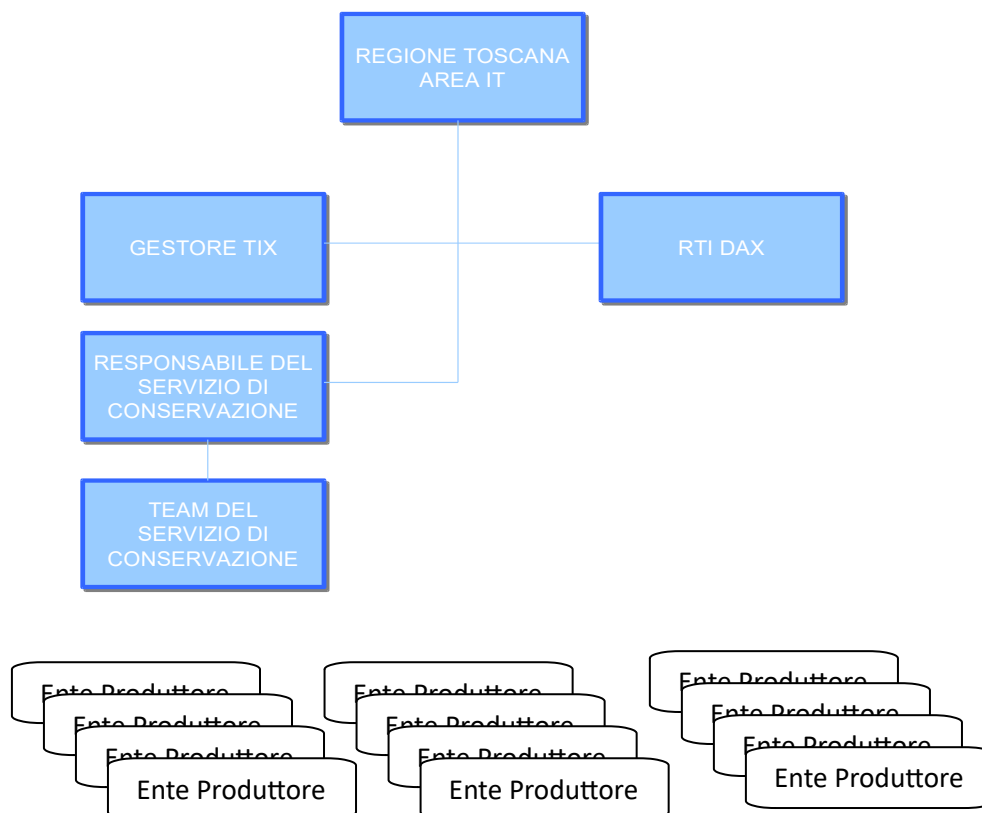


Figura 1 : La figura mostra l'organizzazione del servizio di Conservazione, in base ai ruoli svolti dai diversi soggetti coinvolti nella erogazione

Quanto sopra riportato dimostra la segregazione dei compiti all'interno del servizio di conservazione. In particolare:

- le figure di responsabilità descritte nel capitolo precedente sono ricoperte da persone distinte;
- le persone addette alla conduzione delle applicazioni e alla conduzione dei sistemi sono distinti;
- l'organizzazione dello sviluppo e manutenzione è in carico ad azienda certificata come conservatore, che pertanto garantisce le opportune separazioni tra sviluppatori, manutentori, tester e sistemisti.

Torna all' [INDICE](#)

5.1 Strutture organizzative

Torna all' [INDICE](#)

5.1.1 Regione Toscana

L'area IT di Regione Toscana, tra le altre responsabilità relative alle infrastrutture IT e alla gestione dei sistemi informativi in uso, si configura come Soggetto che coordina il Servizio di Conservazione che viene utilizzato sia all'interno della Regione stessa, sia dagli Enti Locali del territorio toscano che, poiché Regione Toscana svolge il ruolo di Centrale di committenza ai sensi dell'art. 33 del D.Lgs. 163/2006 e dell'art. 42 della L.R. 38/2007, possono aderire ai contratti regionali e quindi avvalersi della piattaforma Digidoc adottata dalla Regione per la Conservazione.

In tal senso, l'area IT della Regione Toscana ha le seguenti responsabilità:

- interfacciare gli Enti Locali, nelle fasi di adesione al contratto di servizio;
- Relazionarsi con gli outsourcer incaricati della gestione delle infrastrutture tecnologiche su cui si attesta il Servizio di Conservazione, per i diversi aspetti relativi alla gestione dell'infrastruttura fisica (in carico al Gestore TIX) e della piattaforma applicativa (in carico alla RTI DAX);
- Cooperare con il Responsabile della Conservazione, nelle diverse fasi di messa in piedi, erogazione ed eventuale dismissione del servizio stesso;
- Nominare ufficialmente le risorse che ricoprono i ruoli previsti dalla Normativa AgID per il Servizio di Conservazione.

Torna all' [INDICE](#)

5.1.2 Gestore del TIX

Il Gestore del TIX attualmente eroga presso il TIX (Tuscany Internet eXchange) servizi per conto di Regione Toscana o per altri Enti ed è incaricato da Regione Toscana stessa, con la stipula di un apposito contratto di Outsourcing, di gestire l'infrastruttura fisica (CED) su cui si attesta il servizio di Conservazione, in termini di:

- monitoraggio della disponibilità di sistemi e rete, secondo i Livelli di Servizio stabiliti contrattualmente con Regione Toscana;
- monitoraggio della connettività;
- gestione sistemistica di reti e sistemi (attività di Amministratore di Sistema);

- ricezione e gestione delle segnalazioni di malfunzionamenti riconducibili all'infrastruttura IT a perimetro, collaborando con le altre strutture organizzative coinvolte nel servizio di Conservazione per individuare e risolvere le cause di tali malfunzionamenti;
- gestione degli apparati di sicurezza in termini di:
 - Firewall;
 - Intrusion Detection System;
 - Gestione centralizzata log degli accessi ai sistemi ed agli apparati;
 - Bandwidth management;
- gestione di:
 - sistemi di storage di classe enterprise;
 - virtual tape library per backup ed archiving.

Il Gestore TIX opera in via di San Piero a Quaracchi 250, Firenze.

Torna all' [INDICE](#)

5.1.3 RTI DAX

Il Raggruppamento di Imprese (RTI) DAX è incaricato da Regione Toscana, (attraverso la stipula di apposito contratto di outsourcing), della messa in opera e successiva manutenzione del sistema per la gestione di Archivio e di Conservazione. Il Raggruppamento è inoltre incaricato dalla Regione di fornire le risorse adeguate a gestire il Servizio di Conservazione in esercizio.

Le principali responsabilità in carico al Raggruppamento sono:

- assicurare la disponibilità delle licenze del Software DigiDoc, secondo quanto riportato nel Contratto di Outsourcing con Regione Toscana;
- supportare l'installazione e la manutenzione della piattaforma DigiDoc in ambiente di "staging" (collaudo) e successivamente in esercizio, secondo le modalità descritte nell'Accordo di Servizio tra Regione Toscana ed il fornitore della piattaforma DigiDoc;
- effettuare gli interventi di manutenzione ordinaria, correttiva e di adeguamento (per le applicazioni e i componenti di sistema, escluso l'hardware e lo strato di virtualizzazione), anche per quanto riguarda la sicurezza, in armonia a quanto previsto nell'Accordo di Servizio tra Regione Toscana e il fornitore della piattaforma DigiDoc;
- fornire a Regione Toscana la documentazione tecnica a corredo del software, sia in sede di prima installazione, sia in occasione di interventi di manutenzione (correttiva e/o adeguativa) come previsto dalle procedure di Regione Toscana e del fornitore della piattaforma DigiDoc;

- assicurare a Regione Toscana la disponibilità delle risorse adeguate a ricoprire i ruoli di cui al capitolo 5, le quali opereranno per conto della Regione Toscana, come definito nell'ambito del Contratto siglato tra Raggruppamento e Regione.

Torna all' [INDICE](#)

6 Oggetti sottoposti a conservazione

Torna all' [INDICE](#)

6.1 Oggetti conservati

Il servizio offerto da Regione Toscana permette potenzialmente il trattamento e la conservazione di

- documenti informatici e documenti amministrativi informatici
- aggregazioni documentali informatiche.

Il cliente che intende usufruirne, deciderà per quali oggetti digitali (rappresentati nel DAX come schede documento e unità di aggregazione) attivare il servizio di conservazione e, una volta comunicate a Regione Toscana, collaborerà con il team DigiDoc nelle operazioni di definizione del relativo trattamento.

Per ogni caso specifico, ossia per ogni Titolare i cui documenti vengano presi in carico, Regione Toscana individua le classi documentali e i dati o attributi specifici da associare a ciascuna di esse. In questa fase, con le scadenze da concordare; saranno ad esempio precisati i tempi di conservazione, la periodicità di invio dei documenti al sistema di conservazione, l'intervallo di tempo intercorrente tra la presa in carico e la chiusura del pacchetto di archiviazione.

La classe documentale racchiude tutte le caratteristiche comuni ad uno specifico tipo di documento da sottoporre a conservazione, definendone quindi le informazioni indispensabili per qualificarlo ed identificarne gli elementi distintivi. L'elenco e le caratteristiche delle classi documentali vengono precisate di caso in caso, in collaborazione con il Soggetto Produttore; a titolo esemplificativo, tuttavia, le classi più comunemente trattate sono documenti del ciclo attivo (Fatture Clienti, Libri e Registri, etc.), del ciclo passivo (Fatture di Acquisto, etc.) e documenti del lavoro (LUL) e dagli Atti amministrativi.

Il dettaglio delle informazioni sopra indicate, concordate con il soggetto produttore, viene riportato nella documentazione scambiata con il singolo Ente produttore.

Torna all' [INDICE](#)

6.2 Pacchetto di versamento

Il Pacchetto di versamento è il pacchetto informativo proveniente dal soggetto produttore e versato nel sistema di conservazione. Le modalità di versamento sono concordate e descritte nell'accordo di servizio.

Fra i diversi aspetti da concordare, i principali sono:

- le tipologie di documenti da conservare,
- metadati,
- eventuali informazioni extra,
- i formati da adottare per ogni classe/tipo di documento,
- le modalità e canali di trasferimento dei documenti nell'archivio (ws, ftp, http) ed ulteriori.

Il responsabile del servizio di conservazione coordina l'intero processo e si accerta del rispetto delle regole fissate negli specifici accordi di servizio. Sono conservati i seguenti oggetti: documenti informatici, documenti amministrativi informatici e fascicoli informatici e per ciascuno di queste tipologie di oggetti sono previsti determinati requisiti da rispettare per la corretta esecuzione della procedura di conservazione.

Con l'entrata in vigore delle nuove linee guida, a partire dal 1° gennaio 2022, il sistema di Conservazione della Regione Toscana DAX ha introdotto una serie di modifiche in materia di formati documentali accettati (si rimanda all'allegato 2 Linee Guida AgID "Formati di file e riversamento") e metadati necessari per l'invio in conservazione (si rimanda all'allegato 5 Linee Guida "Metadati"), per il dettaglio dei quali si rimanda ai rispettivi paragrafi del presente manuale.

Il pacchetto di versamento è corredato da un file xml - SIPManifest.xml, il cui schema è fornito nell'allegato *Allegato1 – SIPManifest.v.2.0.pdf* - che contiene sia le descrizioni della documentazione che i puntatori e le impronte dei file che compongono la documentazione digitale da inviare in conservazione. In caso di documentazione già inviata in conservazione e di cui si devono solo aggiornare dati e/o file, per le unità di descrizione - schede documento, unità di aggregazione di documenti ecc - e i documenti digitali da aggiornare si rimanda al documento di Specifiche tecniche. La responsabilità del produttore è quella di provvedere e monitorare il corretto funzionamento dell'integrazione tra i sistemi producer e il sistema di conservazione.

E' altresì a cura del produttore fare quanto necessario per assicurarsi che:

- tutta la documentazione venga inviata in conservazione correttamente "tipizzata" nel pacchetto di versamento secondo quanto specificato nell'accordo di servizio, cosicché dalla

tipologia specificata il sistema di conservazione sia in grado di impostare correttamente sia il termine entro cui obbligatoriamente deve essere effettuato il processo di conservazione che il termine fino cui decorre l'obbligo di conservazione della documentazione;

- tutta la documentazione sia inviata al sistema di conservazione in tempo utile affinché la conservazione possa avvenire nel rispetto delle tempistiche imposte dalla normativa vigente e secondo quanto concordato negli accordi di servizio;
- la documentazione venga inviata in conservazione corredata almeno dei metadati obbligatori previsti dal profilo specifico della tipologia documentale specificata;

Per quanto concerne gli allegati delle fatture

- nel caso delle fatture attive in base alle nuove regole tecniche della fatturazione elettronica gli eventuali allegati, recanti ad esempio il dettaglio di ciò che viene fatturato, sono inglobati all'interno della fatturaPA (*embedded* in base 64 nell'xml della fattura stessa), e dato che la fattura è firmata digitalmente sono inviati in conservazione come parte integrante del documento xml principale della fattura (esattamente come ricevuti dal SdI); tuttavia per garantire una maggior leggibilità vengono anche versati in conservazione come documenti distinti (allegati) della scheda documento della fattura, "estraendoli" dall'xml firmato in cui sono inglobati;
- nel caso delle fatture attive è previsto che eventuali allegati a corredo della fattura siano descritti nel pacchetto di versamento come documenti allegati della scheda documento di cui la fattura è il documento principale

Per quanto concerne eventuali ricevute/notifiche provenienti o inviate al SdI a fronte di una data fattura passiva o lotto di fatture ricevuto, esse vengono versate in conservazione come schede documento distinte dalla fattura o lotto a cui fanno riferimento, creando una relazione con la scheda documento della fatturaPA cui sono relative (attraverso gli appositi tag di relazione tra schede documento previsti dal tracciato xsd del pacchetto di versamento).

Torna all' [INDICE](#)

6.3 Pacchetto di archiviazione

L'elaborazione del pacchetto di versamento verifica dati e file dei documenti versati al fine di stabilire quali dei documenti del pacchetto possano esser presi in carico da DigiDoc e quali vadano rifiutati (vi può essere anche una presa in carico parziale). Al termine di questa elaborazione i risultati e i dettagli dei controlli effettuati su tutti i documenti del pacchetto, sia quelli accettati che

quelli rifiutati, sono riportati nel rapporto di versamento (SIPResult.xml, il cui schema è fornito nell'allegato *Allegato2 - SIPResult (Rapporto di Versamento).pdf*) che viene restituito al versatore e al tempo stesso diviene esso stesso oggetto di conservazione in DigiDoc.

Il Pacchetto di Archiviazione (PdA) o Archival Information Package (AIP) secondo la terminologia OAIS, viene generato dal sistema a conclusione del processo di verifica e presa in carico degli item – schede documento e unità di aggregazione – del PdV e si ottiene dalla trasformazione di uno o più pacchetti di versamento. Esso contiene:

- I documenti conservati nel formato utilizzato all'atto del versamento;
- Il file indice IPdA firmato e marcato temporalmente: esso è un file XML formato secondo le regole tecniche definite nella norma UNI 11386:2020 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali; nella sezione MoreInfo prevista dallo standard contiene per ciascun documento del PdA:
 - il corrispondente tag *Item* del SIPManifest.xml con cui il documento è stato versato in conservazione (per dettagli si rimanda all'allegato *Allegato1 – SIPManifest.v.2.0.pdf*);
 - il corrispondente tag del *Item* del SIPResult.xml, ovvero il rapporto di versamento, contenente l'esito dei controlli effettuati sul documento (per dettagli si rimanda all'allegato *Allegato2 - SIPResult (Rapporto di Versamento).pdf*).

Torna all' [INDICE](#)

6.4 Pacchetto di Distribuzione

Il Pacchetto di distribuzione (PdD) o Dissemination Information Package (DIP) secondo la terminologia OAIS, consente di rispettare l'obbligo di esibizione dei documenti conservati; esso viene generato dal Sistema a partire dai Pacchetti di archiviazione conservati ed è finalizzato a mettere a disposizione degli Utenti, in una forma idonea alle specifiche esigenze di utilizzo, gli oggetti sottoposti a conservazione. Un pacchetto di distribuzione può coincidere con un pacchetto di archiviazione, ma è possibile gestire la produzione di pacchetti di distribuzione specifici in relazione a particolari esigenze. In relazione alle sue caratteristiche e agli utilizzi a cui è destinato, il Pacchetto di distribuzione può essere generato al momento della richiesta da parte di un Utente e non conservato nel Sistema.

Torna all' [INDICE](#)

6.5 Formati

L'allegato 2 alle Linee Guida "Formati di file e riversamento" presenta un elenco dettagliato dei formati dei file con cui vengono rappresentati i documenti informatici, specificando, per ciascuno di questi, se è idoneo o meno per la conservazione nel lungo periodo.

L'adeguamento del sistema DAX su questo tema ha previsto:

- l'introduzione di nuovi formati o nuove estensioni e mimetype a formati già presenti in configurazione;
- l'accettazione di quei formati considerati da AgID non più idonei alla conservazione. In questo caso specifico, nel rapporto di versamento sarà incluso un messaggio di warning che indicherà il conferimento di formato documentale escluso da AgID in ambito di conservazione.

Negli accordi di servizio con ogni ente sarà definito l'elenco dei formati dei documenti che il soggetto produttore vuole conservare nell'archivio digitale.

L'elenco dei principali formati che saranno accettati dal DAX, a partire dal 1° gennaio 2022 e l'elenco dei formati esclusi da AgID per la conservazione, ma che continueranno ad essere accettati dal sistema DAX, sono stati riportati nell' *Allegato5 - ElencoFormatiDigitali.v.1.0.pdf*).

Torna all' [INDICE](#)

6.6 Metadati conservati

Il sistema di conservazione consente di gestire tutti i metadati obbligatori previsti dalla normativa vigente ai quali vanno aggiunti quelli presenti negli accordi specifici.

In particolare, tutti i metadati definiti nel nuovo allegato 5 alle Linee guida AgID vengono inclusi all'interno del descrittore del pacchetto di versamento (SIPManifest.xml); la loro definizione è quella di AgID sia nella sintassi che nella semantica. Vengono ridefinite le tipologie documentali attualmente accettate dal DAX e le relative schede tecniche sono state adeguate.

Le versioni attuali delle tipologie documentali continueranno ad essere accettate: in caso di conferimento di documenti afferenti a tali versioni di tipologie, nel rapporto di versamento sarà incluso un messaggio di warning che segnalerà il conferimento in deroga alla normativa AgID.

Saranno definiti, sempre nel rapporto di versamento, nuovi messaggi di warning in caso di:

- Documento dichiarato firmato dall'Ente versatore (tramite apposito metadato obbligatorio definito da AgID) ma che non risulti firmato o il caso inverso;

- Formato del documento dichiarato dall'Ente versatore (tramite apposito metadato obbligatorio definito da AgId) non conforme al reale formato del documento.

Per entrambi i casi d'uso precedenti, il conferimento della documentazione avrà sempre esito positivo, salvo che non siano presenti altri errori.

Torna all' [INDICE](#)

6.7 Tempi di conservazione

Il sistema di conservazione consente di gestire i tempi entro cui è necessario mettere in conservazione e quelli per cui è necessario conservare i documenti. Tali informazioni sono fornite dal produttore all'atto del versamento e indicate nelle schede anagrafiche per ogni tipologia documentale.

La permanenza in conservazione è specificata nei "Piani di conservazione", che indicano, tipologia per tipologia, i tempi (p.e. le delibere sono mantenute per sempre).

I tempi di conservazione sono un metadato della tipologia documentale. Per ogni PdV l'ente produttore specifica, tra i metadati, il tempo di conservazione. Pertanto, le eventuali modifiche di politica sono in carico al produttore.

Ciò detto è responsabilità fondamentale del produttore indicare correttamente la tipologia documentale: in caso di mancata o errata attribuzione della tipologia il sistema di conservazione non potrà procedere all'avvio e mantenimento della conservazione secondo le corrette tempistiche.

Il tempo di conservazione di tutte le tipologie documentali dei cicli attivo e passivo di fatturazione è configurato a 10 anni.

Torna all' [INDICE](#)

7 IL PROCESSO DI CONSERVAZIONE

DigiDoc adotta lo standard ISO 14721:2003, comunemente noto come OAIS (Open Archival Information System), che costituisce lo standard di riferimento per qualsiasi sistema si occupi di digital preservation.

La soluzione, nel pieno rispetto della normativa in materia e degli standard internazionali di riferimento, assicura la gestione di tutti i processi inerenti alla conservazione quali:

- Processo di Amministrazione: preparazione dell'ambiente, intendendo con ciò la messa a punto del contesto operativo, finalizzata alla predisposizione degli elementi necessari alla creazione, gestione, archiviazione e conservazione dei documenti (massimario di scarto, formati, metadati associati ai documenti ...);
- Processo di Invio in Conservazione: trasferimento del documento al Sistema di Conservazione.
- Processo di Controllo: verifica che il documento abbia i requisiti per essere accettato dal sistema di conservazione
- Processo di Conservazione e fruizione della memoria digitale.
- Processo di Consultazione: ricerca della documentazione conservata da parte di soggetti abilitati.

Le funzionalità gestite dal sistema permettono di garantire:

- l'identificazione certa del soggetto che ha formato il documento e dell'AOO di riferimento
- l'integrità del documento
- la leggibilità e l'agevole reperibilità dei documenti e dei relativi metadati
- il rispetto della normativa nazionale sulla conservazione, con adeguamento alla variazione delle norme
- la prevenzione della obsolescenza hw e sw, attraverso adeguamenti continui dell'HW e del SW e attraverso riversamenti sostitutivi dei documenti digitali;
- il rispetto del trattamento dei dati e della tutela dei dati tramite la registrazione e conservazione in un sistema di audit unico in grado di restituire dati di sintesi, ma interrogabili a più livelli di dettaglio;
- il tracciamento di ogni accesso, variazione e intervento sul sistema: accessi, modifiche tecnologiche, aggiornamenti dei metadati e dei documenti digitali.
- l'ampliamento e l'aggiornamento della lista dei formati digitali ammessi;
- la ricezione, il mantenimento, l'aggiornamento e la conservazione di tutti i metadati relativi alla documentazione dell'archivio.

Torna all' [INDICE](#)

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

Il processo di invio in conservazione inizia con l'invocazione da parte di un sistema/applicativo del soggetto produttore del web service di receiveSIP esposto da DigiDoc.

Tale servizio prevede l'invio in conservazione di una collezione di uno o più documenti o aggregati di documenti attraverso un attachment, il Submission Information Package (SIP) di OAIS, che è un file compresso – zip o tar.gz – contenente:

- un file xml *SIPManifest.xml* che contiene sia i metadati del/i documenti e loro aggregati (fascicoli, serie ecc) da inviare in conservazione, sia le impronte e gli URI (percorsi relativi all'interno del file archivio) dei file associati ai documenti;
- i file che compongono i documenti digitali da inviare in conservazione (che possono essere o meno firmati digitalmente).

Per ogni item – i.e. documento o aggregato di documenti – presente nel SIP il sistema del produttore deve specificare nel SIPManifest.xml un identificativo univoco attraverso cui può richiederne in seguito degli aggiornamenti o l'esibizione. Infatti, lo stesso servizio di receiveSIP consente anche di inviare ad DigiDoc solo degli aggiornamenti dei metadati e/o l'aggiunta di allegati della documentazione già inviata in conservazione. In questo caso l'attachment contiene solo il SIPManifest.xml, se si devono rettificare, aggiornare o versionare solo dei metadati, ed eventualmente anche i file da rettificare o versionare. Peraltro, l'identificativo che il soggetto produttore deve specificare per ogni item (univoco solo limitatamente a quelli degli item inviati dal dato sistema) serve anche affinché DigiDoc possa controllare se un dato sistema ha già inviato un dato item in modo da non accettarlo in conservazione qualora quel soggetto produttore lo stia inviando una seconda volta (senza indicare che si tratta di un aggiornamento).

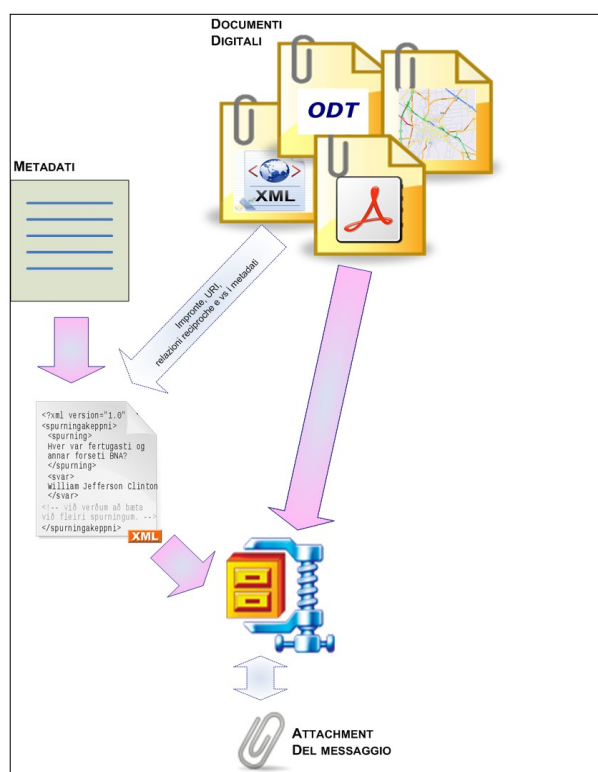


Figura 2: La figura rappresenta il flusso con cui un documento viene versamento del documento nel sistema di conservazione

Gli estremi di ciascun SIP ricevuto, tra cui il produttore e l'identificativo univoco assegnatogli dal produttore, sono memorizzati insieme al numero di registrazione, in apposito registro dei SIP, assegnatogli da DigiDoc stesso. Associato a questo record viene archiviato e avviato alla conservazione il corrispondente SIPManifest.xml.

Sia i file che le strutture dati dei SIP sono oggetto delle procedure di back-up adottate per tutti i dati e i file archiviati in DigiDoc.

Una volta che il pacchetto di versamento è stato preso in carico dal Sistema di Conservazione, il sistema produttore riceve un ticket attraverso cui può in seguito richiedere l'esito dell'invio di quel SIP, vale a dire il rapporto di versamento: stato di trasmissione/elaborazione e dettaglio dell'elaborazione, ovvero cosa è stato accettato in conservazione e cosa no e perché. Infatti, il processo di invio in conservazione della documentazione nel suo complesso prevede una modalità di interazione che è asincrona, dato che i documenti inviati in un unico SIP possono essere molti o di dimensioni ragguardevoli e che la verifica del SIP da parte del Sistema di Conservazione può richiedere un certo tempo di elaborazione.

Torna all' [INDICE](#)

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

Quando la documentazione inviata in conservazione arriva al modulo di elaborazione dei pacchetti di versamento, il modulo si occupa per prima cosa di effettuare i controlli dei metadati e dei file del SIP pervenuto: la documentazione che non supera i controlli “bloccanti” non può essere ammessa in conservazione. Il sistema DigiDoc compie le seguenti classi di controlli dettagliati nei seguenti paragrafi:

- Controllo dell’identità del soggetto produttore del pacchetto;
- Controllo delle Firme Digitali;
- Controlli dei Formati digitali;
- Controllo della Presenza di Macro e Codice Eseguitabile;
- Controllo dei Metadati;
- Controllo impronta.

Torna all’ [INDICE](#)

7.2.1 Controllo impronta del pacchetto di versamento

Per evitare eventuali alterazioni, al produttore del pacchetto di versamento viene richiesto di inserire l’impronta. Il sistema DigiDoc, all’atto del versamento, calcola l’impronta e la confronta con quella inserita dal produttore. Se le due stringhe non coincidono, il pacchetto viene rifiutato.

Torna all’ [INDICE](#)

7.2.2 Controllo dell’identità del soggetto produttore del pacchetto

Il versamento di un pacchetto può avvenire solo fornendo una coppia di credenziali – userid e password – che vanno specificate nell’header del messaggio con cui il pacchetto viene inviato a DigiDoc: tali credenziali sono state precedentemente generate e memorizzate da DigiDoc associandole ai dati anagrafici – denominazione, codice fiscale, partita IVA, codice IPA se trattasi di PA ecc - del Titolare degli oggetti di conservazione a cui sono state rilasciate. Inoltre, nel SIPManifest.xml sono previsti come dati obbligatori – si veda *Allegato1- SIPManifest.v2.0.pdf* (Indice di Versamento) per maggiori dettagli – i dati identificativi del soggetto che ha prodotto il pacchetto. Quando riceve un pacchetto di versamento il primo controllo effettuato da DigiDoc è quello relativo alle credenziali di autenticazione inviate e subito dopo quello che il soggetto produttore specificato nel SIPManifest.xml sia quello corrispondente alle credenziali verificate.

Torna all' [INDICE](#)

7.2.3 Controllo delle Firme Digitali

I controlli sulla/e firme digitali e sulle relative marche temporali, sono i seguenti:

- la firma non deve precludere la leggibilità del documento, per cui se il documento firmato è una busta crittografica quale una busta p7m o CAdES, la busta deve poter essere aperta: il mancato superamento di tale controllo impedisce l'accettazione in conservazione;
- le eventuali marche temporali associate alle firme devono essere valide, ovvero: integre, di formato ammesso dalla normativa, emesse da una TSA accreditata da AgID, firmate da un certificato valido e non revocato né sospeso alla data della marca, non ancora scadute: qualora alcuni di questi controlli non siano superati ciò non preclude l'accettazione in conservazione ma dà solo luogo a degli avvertimenti restituiti nel rapporto di versamento;
- la busta crittografica deve essere in uno dei formati ammessi dalla normativa italiana (quella in vigore alla data del riferimento temporale associato al documento firmato - una marca temporale o una data, quale la data di protocollo del documento, associata al documento digitale nel SIPManifest – ovvero, in assenza di questo riferimento temporale, alla data di esecuzione del controllo) e deve risultare integra: il mancato superamento di tale controllo impedisce l'accettazione in conservazione;
- i certificati di firma devono essere attendibili, ovvero emessi da CA accreditate da AgID: qualora il controllo non sia superato ciò non preclude l'accettazione in conservazione ma dà solo luogo a degli avvertimenti restituiti nel rapporto di versamento;
- i certificati di firma non devono risultare scaduti alla data del riferimento temporale associato al documento firmato ovvero, in assenza di questo riferimento temporale, alla data di esecuzione del controllo: qualora il controllo non sia superato ciò non preclude l'accettazione in conservazione ma dà solo luogo a degli avvertimenti restituiti nel rapporto di versamento;
- i certificati di firma non devono risultare revocati o sospesi alla data del riferimento temporale associato al documento firmato ovvero, in assenza di questo riferimento temporale, alla data di esecuzione del controllo: qualora il controllo non sia superato ciò non preclude l'accettazione in conservazione ma dà solo luogo a degli avvertimenti restituiti nel rapporto di versamento.

Il Sistema di Conservazione è in grado di verificare tutti i tipi e i formati di firme digitali e marche temporali ammessi dalla normativa italiana, e si adegua nel tempo ad ogni cambio normativo in materia di firma digitale.

Dunque, ad oggi è in grado di verificare:

- controfirme, firme parallele e firme multiple
- le buste crittografiche: p7m (PKCS#7 e CAdES); PDF (PAdES); XML (XAdES)
- le modalità di imbustamento (enveloped, enveloping, detached)
- le eventuali marche temporali associate alle firme, di qualunque dei formati ammessi (tsr, tsd, tst), sia detached che embedded nella busta crittografica.

Trattandosi di un sistema pensato per la conservazione a lungo termine, e che quindi ha un'attesa di vita molto lunga, è progettato per poter effettuare controlli diversi sui tipi e i formati di firme e marche accettati, a seconda del riferimento temporale dei documenti: in questo modo tiene conto del fatto che ciò che è stato validamente firmato secondo la normativa vigente quando la firma è stata apposta, può non essere conforme alla norma vigente al momento del suo invio in conservazione.

Il sistema traccia tutti i controlli effettuati e i relativi esiti (corredandoli del timestamp in cui li ha effettuati). In particolare, dato che il servizio di verifica firma restituisce tutti i dati ottenuti dall'analisi della busta crittografica - superamento o meno dei vari gradi di validità; estremi degli intestatari dei certificati di firma e delle CA che li hanno emessi; timestamp delle eventuali marche temporali associate; tipo di busta crittografica ecc – tutti questi dati vengono memorizzati nel pacchetto di archiviazione del documento.

Da notare in particolare che il servizio di verifica delle firme digitali:

- consente di specificare un riferimento temporale – quale una data di registrazione a protocollo – rispetto al quale deve essere effettuata la verifica della firma: in questo modo viene soddisfatto il requisito di legge che prevede di considerare altri riferimenti temporali, oltre alle marche, come riferimenti temporali opponibili a terzi;
- quando la verifica della firma viene fatta rispetto ad una data passata, indicata da una marca temporale o da un altro riferimento temporale, il sistema valuta la validità del formato della busta crittografica rispetto a quella data (ad esempio una busta p7m non CAdES che utilizza ancora l'algoritmo SHA-1 per il calcolo dell'impronta può risultare comunque valida purché riferita ad una data antecedente 30/6/2010);
- anche il periodo di validità delle marche temporali viene valutato rispetto alla loro data di emissione (la norma ha cambiato nel tempo il periodo di validità minimo richiesto alle TSA);
- grazie ad un archivio storico di CRL che viene man mano incrementato – ogni qual volta, nel verificare una firma, si scarica o si aggiorna una CRL – è in grado di verificare lo stato di revoca e sospensione di un certificato di firma a cui sia associato un riferimento temporale così addietro nel tempo che la relativa CRL non è più pubblicata (la norma impone alle CA di

mantenere le CRL solo fino allo scadere dei certificati con cui sono stato firmati i certificati di firma che rimandano alle CRL).

Torna all' [INDICE](#)

7.2.4 Controllo dei Formati digitali

Su ciascun documento digitale inviato in conservazione il sistema di conservazione effettua il controllo del formato: se il formato non è riconosciuto o non è tra quelli ammessi l'intera scheda documento cui appartiene il documento digitale non viene accettata in conservazione. Tale controllo si basa sul contenuto del file e non sull'estensione del nome file (che potrebbe non essere indicata o peggio essere discordante rispetto al formato effettivo del file). In particolare, nel caso di documenti che sono buste crittografiche - p7m, tsd, m7m - il formato che viene riconosciuto è quello del documento con il contenuto informativo depurato dalle eventuali buste crittografiche: il sistema prima procede allo "sbustamento" (se necessario anche ricorsivamente) ed una volta che è arrivato ad un file che non è più una busta crittografica procede al riconoscimento del formato di quel file.

Il servizio di verifica formati del Sistema di Conservazione è ad oggi in grado di riconoscere con un buon grado di affidabilità i seguenti formati:

- PDF e PDF/A;
- tutti i formati della suite MS Office (inclusi Power Point, Visio e Project);
- tutti i formati della suite Open Office;
- I formati immagine più diffusi;
- xml, ascii (txt, csv, ecc);
- i formati audio e video più diffusi;
- gli archivi compressi;
- mail in formato eml.

Il formato eml di fatto è un formato archivio/busta che a loro volta contengono delle parti con dei loro formati. Quindi quando vengono verificati, come nel caso delle buste crittografiche, il servizio di verifica formato va a verificare anche i contenuti del file archivio e delle parti della busta eml (attachment e body): se questi sono riconosciuti e ammessi il file archivio o eml è ammissibile in conservazione, altrimenti no. È anche gestita la verifica ricorsiva dei formati dei file contenuti se nel file archivio/eml vi sono dei file/attachment che sono a loro volta file archivio o e-mail. Il fatto che il

servizio di verifica formato sia in grado di riconoscere e verificare il contenuto di questi formati “contenitore”, anche nel caso di annidamenti di buste, mette il Sistema di Conservazione nella condizione di poter accettare in conservazione:

- e-mail firmate;
- ricevute PEC, ovvero e-mail che in genere contengono a loro volta, come attachment, l’e-mail di cui sono la ricevuta: possono essere documenti che è importante conservare in quanto a norma di legge costituiscono un riferimento temporale opponibile a terzi (riferimento utilizzabile, per esempio. per il documento firmato che è stato inviato in uscita tramite PEC e il cui invio ha dato luogo a quella ricevuta);
- archivi compressi per i quali esiste solo una descrizione complessiva, come documento semplice, e non quelle singoli file componenti.

Una volta che il formato di un documento inviato in conservazione è stato riconosciuto viene sottoposto ad un filtro ulteriore che analizza il formato utilizzando detector diversi e specifici a seconda del formato riconosciuto: attraverso tale analisi il Sistema di Conservazione può determinare la versione del formato, laddove prevista e altre utili informazioni, che andranno ad arricchire i metadati dell’AIP del documento (in particolare la sezione delle informazioni di stabilità, come definite da OAIS).

Tenuto conto che i formati ad oggi riconosciuti dal Sistema di Conservazione, in un’ottica di conservazione a lungo termine, non sono tutti ugualmente idonei alla conservazione, i formati che effettivamente il sistema di conservazione accetterà e che saranno indicati negli accordi di servizio seguiranno formati caratterizzati dai seguenti aspetti:

- aperti;
- ben documentati;
- standard, possibilmente de-jure;
- non proprietari;
- largamente diffusi;
- indipendenti dalla piattaforma;
- che permettono di includere nei file l’insieme di metadati - self-documentation - che ne descrivono il contenuto e il processo di produzione, fornendo anche i dettagli tecnici per la loro rappresentazione negli ambienti tecnologici del futuro;
- che non possano contenere macroistruzioni o per i quali siano disponibili strumenti efficaci per rilevare con sufficiente sicurezza la presenza di macroistruzioni;

- che non prevedano meccanismi tecnici di protezione e di limitazione sull'utilizzo;
- accessibili e robusti;
- caratterizzati da un'elevata stabilità (backward e forward compatibility).

È buona norma considerare che i formati per cui siano disponibili viewer o reader solo per una o poche piattaforme, anche se non vietati e quindi inseribili nel set dei formati ammessi, andranno comunque evitati quanto più possibile, perché utilizzarli corrisponderebbe a creare una limitazione forte sulla capacità dei sistemi e client fruitori di riprodurre i documenti, e di conseguenza sulla capacità del sistema di conservarli.

Infine, si è stabilito che tra i formati che non devono comunque essere accettati in conservazione, vi siano quelli per i quali, sui registri internazionali di formati – quali UDFR e PRONOM – sia indicata una data di obsolescenza o di prevista/avvenuta cessazione di supporto. È responsabilità del RdSC ed eventuali suoi delegati verificare gli aggiornamenti dei formati in suddetti registri al fine di configurare correttamente il set di formati ammessi in conservazione, procedere ad eventuali procedure di riversamento di quanto già conservato in quel formato nonché dare indicazioni ai produttori e in particolare al coordinatore della gestione documentale in merito a quali formati abbandonare perché a rischio di obsolescenza.

Una volta che il formato di un documento inviato in conservazione sia stato riconosciuto viene sottoposto ad un filtro ulteriore che analizza il formato utilizzando detector diversi e specifici a seconda del formato riconosciuto.

Nel dettaglio del formato sono inoltre presenti:

- tutti i dati previsti per la descrizione dei formati nei registri internazionali quali PRONOM e UDFR;
- l'identificativo – obbligatorio - assegnato al formato in uno dei registri appena menzionati.

Torna all' [INDICE](#)

7.2.4.1 Funzionalità di configurazione

Il sistema consente di configurare per ciascun formato ammesso i seguenti dati di dettaglio:

- nome ed eventuale versione del formato: è questa la coppia che lo identifica univocamente tra tutti gli altri formati censiti;
- estensione principale dei file del dato formato: tale estensione sarà quella che verrà aggiunta in automatico ai nomi dei file accettati in conservazione qualora i nomi originali

specificati nel tracciato di versamento/trasferimento non abbiano estensione o ne abbiano una ma non congruente con quella/e previste per il formato effettivo dei file;

- lista dei viewer/reader che sono utilizzabili per il rendering dei file del dato formato.

Torna all' [INDICE](#)

7.2.5 Controllo della Presenza di Macro e Codice Eseguitibile

Sui documenti digitali inviati in conservazione sono effettuati i controlli per verificare la presenza di parti variabili – macro – e codice eseguibile/dinamico; infatti questi elementi, qualora presenti, non solo danno luogo a sottoscrizione non valida se il file è firmato digitalmente, ma rendono comunque il documento non ammissibile in conservazione in quanto perde le sue caratteristiche di documento così come sancito dalla norma: non è un documento un oggetto che non si presenta sempre uguale nel tempo. Inoltre, le macro e il codice eseguibile/dinamico sono i principali veicoli di virus e altri elementi potenzialmente nocivi, se non per il sistema di conservazione in sé, quantomeno per i client che dovessero richiedere l'esibizione di documentazione contenente malware.

Il controllo della presenza di macro viene effettuato su tutti i formati MS Office e Open Office che sono quelli che contemplano tale rischio, mentre la presenza di parti di codice eseguibile o dinamico (ad esempio javascript) viene verificata sul formato pdf che la consente (salvo se PDF/A).

Torna all' [INDICE](#)

7.2.6 Controllo dei Metadati

Per garantire la qualità dei metadati contenuti nel SIPManifest, il sistema di conservazione è in grado di effettuare sui metadati di ogni item tutti i seguenti tipi di controlli:

- di obbligatorietà: verifica la presenza di taluni metadati (o loro combinazioni) in assenza dei quali l'item non può essere accettato in conservazione;
- di correttezza sintattica: effettua controlli formali – di tipo e formato, di appartenenza ad un certo range/set predefinito di valori ecc – su tutti i metadati;
- di unicità: il sistema è in grado di verificare, sulla base di alcuni dati del SIPManifest che fanno parte delle informazioni di identificazione di OAIS, se un certo documento o unità di aggregazione di documenti è già stato inviato in conservazione o risulta descritto più volte nello stesso SIPManifest (nel qual caso può dar luogo ad un errore bloccante o solo ad un avvertimento).

Il nucleo base dei controlli sui metadati è prestabilito per tutti gli Enti che utilizzano DigiDoc: si tratta dei controlli che sono indispensabili a garantire la corretta conservazione della documentazione, così come regolata dalle norme e intesa e realizzata dal sistema. A questo nucleo base di controlli ogni Ente può aggiungerne altri, anche specializzati per le diverse tipologie documentali, in modo da rafforzare e modulare il filtro di ciò che DigiDoc può prendere in carico.

Le obbligatorio/vincoli del nucleo base di controlli sui metadati sono i seguenti:

- è obbligatorio specificare un identificativo (univoco per il sistema che invia) per ogni documento o aggregato di documenti;
- è obbligatorio specificare un'etichetta/segnetura per ogni documento o aggregato di documenti (nel caso di documento protocollato potrebbero essere gli estremi di protocollo, nel caso di un fascicolo archivistico la sua segnetura basata sulla classifica e l'anno di apertura);
- è obbligatorio specificare un'intitolazione ovvero una descrizione/oggetto per ogni aggregato di documenti o singolo documento;
- è obbligatorio specificare almeno un riferimento cronologico (data di acquisizione/produzione/registrazione a protocollo; data/anno di apertura o chiusura del fascicolo, ecc.) per ogni documento o aggregato di documenti;
- è obbligatorio specificare la tipologia documentale e il tempo o termine di conservazione se non desumibile da nessuno degli elementi precedenti. Se il tempo è specificato sul documento o aggregato inviato, non può essere inferiore ma solo superiore a quello stabilito da eventuali regole del massimario di selezione e scarto applicabili a quel documento o aggregato.

Torna all' [INDICE](#)

7.2.7 Controllo Impronta

Il sistema calcola l'impronta dei file e la confronta con quella dichiarata nel SipManifest.xml. Se le due stringhe non coincidono, viene segnalato nel rapporto di versamento.

Torna all' [INDICE](#)

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

Gli audit dei controlli effettuati, con dettaglio di esiti ed eventuali risultati (ad esempio nel caso della verifica della validità delle firme, tra i risultati vi sono i dati dei certificati di firma) vengono memorizzati per tutti gli item del SIP, sia quelli accettabili che quelli rifiutati, andando a costituire il “rapporto di versamento” SIPResult.xml, il cui schema è fornito nell’allegato *Allegato2 – SIPResult (Rapporto di Versamento).pdf*. Il rapporto di versamento, rilasciato dunque dal sistema di conservazione come esito del conferimento del pacchetto di versamento e sottoscritto con sigillo qualificato, viene esso stesso archiviato e avviato alla conservazione per tempo illimitato. Come detto in precedenza anche il SIPManifest.xml viene archiviato e avviato alla conservazione, il tutto al fine di attestare nel tempo il flusso di tutto ciò che è arrivato in conservazione e come tale flusso è stato trattato. Più precisamente il rapporto di versamento SIPResult.xml viene archiviato collegandolo al relativo pacchetto di versamento attraverso l’inserimento della sua impronta, data e ora di generazione e URI nella stessa tabella di archiviazione dei dati dei SIP.

E’ a cura del sistema produttore che ha inviato il SIP richiedere, attraverso polling, il rapporto di versamento di ciascuno dei SIP inviati fintantoché essi non risultino disponibili, ed è altresì responsabilità del RdSC e suoi delegati accertarsi della corretta e tempestiva (compatibilmente con il carico di lavoro del sistema di conservazione) produzione dei rapporti di versamento di ogni SIP ricevuto nonché della loro messa in conservazione unitamente al SIPManifest.xml.

DigiDoc esegue appositi controlli sui documenti versati propedeutici all’accettazione del documento in conservazione di seguito descritti.

Torna all’ [INDICE](#)

7.3.1 Rinnovo marche temporali in scadenza

DigiDoc prevede un controllo periodico dei pacchetti per verificare se le marche temporali apposte sugli Indici di Conservazione firmati vanno rinnovate perché prossime alla naturale scadenza.

A valle di questa verifica per ogni Indice di Conservazione la cui marca temporale è in scadenza DigiDoc può:

- a) rinnovare la marcatura in modo automatico, richiedendo una nuova marca ad una delle TSA accreditate: la marca viene apposta sull’Indice di Conservazione già firmato e marcato, in modo da garantire la non soluzione di continuità del processo di conservazione;
- b) far rifirmare e marcare l’Indice già firmato e marcato

Nello scenario b) apposita GUI pone i volumi da rimarcare, previa nuova firma, all'evidenza dell'RdSC.

Torna all' [INDICE](#)

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

Se un pacchetto di versamento non supera uno dei controlli previsti, viene rifiutato e non viene caricato nel sistema. I seguenti controlli, se non vengono superati, generano uno scarto del pacchetto:

- Verifica impronta (hash) del pacchetto;
- Apertura della busta crittografica dei file firmati;
- Conformità del formato della busta crittografica dei file firmati alla normativa italiana;
- Formati dei documenti digitali;
- Incompletezza o assenza dei metadati.

Viene prodotto un report dello scarto in cui viene riportato il timestamping in cui è avvenuto il controllo ed un dettaglio dei controlli effettuati ed il loro esito.

Non esistono meccanismi di correzione automatica degli errori.

Torna all' [INDICE](#)

7.5 Preparazione e gestione del pacchetto di archiviazione

I documenti contenuti nel SIP che superano tutti i controlli (salvo quelli eventualmente "elusi" dal Soggetto Produttore) entrano nel sistema di conservazione.

Per facilitare la verifica, il contenuto degli elenchi è presentato nelle seguenti sezioni distinte:

- Unità archivistiche;
- "documenti sciolti": unità documentarie non versate all'interno di un'unità archivistica in esso contenuti

I documenti digitali accettati vengono consolidati attraverso l'aggregazione dei documenti stessi in insiemi logici chiamati pacchetti in consolidamento (ovvero pacchetti non ancora chiusi, vedi §

successivo). Già al momento dell'accettazione in conservazione per ogni scheda documento e ogni unità di aggregazione sia tutti i dati presenti nel SIPManifest.xml che quelli frutto dei controlli vengono "impacchettati" in xml, a formare i pacchetti di archiviazione, e in questa forma archiviati sullo storage del sistema di conservazione. Sul database relazionale vengono memorizzati i puntatori ai pacchetti di archiviazione conservati su storage. Al tempo stesso i dati di descrizione di ciascun item versato e accettato vengono inseriti nella banca dati relazionale del Sistema di Conservazione.

E' possibile configurare:

- sia i trigger di innesco automatico della creazione degli Indici di Conservazione, quali i seguenti:
 - quando sono stati accumulati un determinato numero o una determinata dimensione di documenti;
 - con una certa cadenza temporale, ad esempio settimanale o mensile;
- sia i vincoli da rispettare nella creazione dei pacchetti quali:
 - Aggregazione per classe documentale;
 - Aggregazione per formato digitale;
 - Aggregazione per applicazione.

Quando c'è un nuovo documento "da consolidare" il sistema verifica se c'è un pacchetto ancora in consolidamento in cui quel documento può essere inserito tenuto conto dei vari criteri di formazione dei pacchetti: se non c'è, ne istanzia uno nuovo e vi inserisce il documento. In questo processo di consolidamento, se nei metadati del documento è specificata, in apposito tag del SIPManifest, l'appartenenza ad un aggregato, ad esempio un fascicolo, il sistema di conservazione cerca di mantenerlo "unito" nella formazione dei pacchetti, cercando di mettere nello stesso pacchetto tutti i documenti relativi allo stesso aggregato (compatibilmente con gli altri criteri di creazione pacchetto configurati). Lo stesso fa per i documenti relativi alla medesima scheda documento (es file principale di una registrazione di protocollo e suoi allegati).

Torna all' [INDICE](#)

7.5.1 Creazione Indice di Conservazione

L'attività di creazione degli Indici di Conservazione conformi al UNI 11386:2020 Standard SInCRO, è svolta per lo più in modo automatico, ma se necessario, in rari casi, può essere forzata manualmente dal RdSC o suo delegato.

Quando viene predisposto l'Indice di Conservazione, il pacchetto cambia stato da "in consolidamento" (aperto) a "chiuso": non vi si possono più aggiungere documenti e il file xml dell'Indice, una volta completato, è disponibile in apposita interfaccia WEB per essere firmato e marcato temporalmente dal RdSC o suo delegato.

La chiusura manuale di un pacchetto può comunque essere fatta in qualsiasi momento dal RdSC o suo delegato; egli dispone di un'apposita GUI attraverso cui non solo vede e può chiudere manualmente tutti i pacchetti in consolidamento ma può anche procedere a mano a modificare la composizione – i documenti – dei pacchetti in consolidamento o a creare nuovi pacchetti.

Negli indici di conservazione, oltre alle impronte e ai dati identificativi dei documenti digitali vengono riportati:

- gli URI che puntano allo stream dei componenti digitali di ciascun documento sullo storage del sistema: l'URI permette il reperimento certo dei file ma non è un path assoluto, cosicché qualora i file dovessero essere riversati (riversamento diretto) su altro storage l'URI può non cambiare, il che costringerebbe a riformare e certificare nuovamente i pacchetti contenenti quei documenti;
- nel tracciato dell'Indice per ogni documento viene riportato l'XML che costituisce il pacchetto di archiviazione della scheda documento di appartenenza (quello anche archiviato su storage): in questo modo, attraverso la firma e marcatura, viene anche congelata la situazione dei dati del documento alla data di inizio della conservazione. Qualora i dati di un documento fossero aggiornati a seguito dell'invio di un SIP con aggiornamento dei dati del documento, i dati aggiornati verranno riportati nella banca dati relazionale e nell'AIP conservato su storage, mentre l'Indice di Conservazione attraverso cui è conservato il documento resterà invariato, quale fotografia dello stato del documento al momento dell'avvio della conservazione.

Torna all' [INDICE](#)

7.5.2 Certificazione pacchetto (firma e apposizione riferimento temporale)

La fase di certificazione del pacchetto ha come scopo quello di completare il processo di conservazione, perfezionando l'Indice di Conservazione attraverso l'apposizione della firma digitale del RdSC e l'apposizione di un riferimento temporale.

Le attività di certificazione dei pacchetti avviene tramite l'individuazione da parte del Sistema di Conservazione dei pacchetti chiusi che devono essere firmati.

Una volta che il Responsabile del servizio di conservazione o suo delegato ha firmato il pacchetto, se il pacchetto, in base alla normativa vigente, prevede una seconda firma dell'Indice di Conservazione

(da parte di un notaio o di un pubblico ufficiale), il Sistema di Conservazione gestisce anche questa casistica e inserisce il pacchetto che manca della seconda firma in un apposito elenco di pacchetti in attesa della seconda firma.

Quando sull'Indice di Conservazione viene apposta una delle firme previste nella busta crittografica viene inserito il riferimento temporale – signing time – che attesta quando è stata effettuata la firma. Il tipo di firma che viene apposta è CadES-BES con profilo specifico della conservazione a lungo termine.

A questo punto il processo di conservazione è concluso ai sensi di quanto previsto dalla norma.

Torna all' [INDICE](#)

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

7.6.1 Funzionalità di ricerca

Le GUI del portale DigiDoc consentono di ricercare la documentazione presa in carico da DigiDoc attraverso tutti i dati specificati nel pacchetto di versamento nonché attraverso i dati acquisiti dai documenti durante il loro ciclo di vita in DigiDoc (data di versamento in conservazione, data di accettazione in conservazione, data inizio conservazione ecc).

Le GUI di ricerca sono progettate e realizzate per offrire un accesso:

- sicuro;
- semplice;
- guidato;
- adeguato alle esigenze.

La sicurezza dell'accesso è garantita attraverso:

- accesso autenticato alle GUI del portale;
- gestione delle richieste di accesso alla documentazione e del relativo iter;
- gestione di diversi livelli di sicurezza sulla documentazione.

Attraverso questi meccanismi il sistema garantisce che ognuno acceda solo alla documentazione e alle informazioni cui è autorizzato.

La semplicità dell'accesso è principalmente ottenuta attraverso l'adozione del motore di indicizzazione con cui vengono indicizzati i documenti digitali che alcuni metadati generali contenuti

nel SIPManifest.xml. Al tempo stesso DigiDoc permette di adeguare la modalità di accesso alle esigenze di chi ricerca: infatti consente di impostare filtri di ricerca “strutturati” – con operatori di uguaglianza, somiglianza, maggiore, minore, compreso tra, valorizzato e non valorizzato su alcuni metadati della documentazione conservata, inclusi quelli specifici di certe tipologie documentali.

Dalla lista dei risultati che rispondono ai criteri di ricerca impostati, è possibile accedere al dettaglio dei singoli documenti visualizzando:

- il/i file che compongono il documento;
- i principali metadati trasmessi dal versatore (Oggetto del documento/Intitolazione/ Tipologia Documentale/Identificativo);
- metadati espressi dal sistema in fase di versamento (Data invio in conservazione/Identificativo associato dal sistema di conservazione e trasmesso via rapporto di versamento);
- l’esito dei singoli controlli eseguiti;
- le informazioni del pacchetto di appartenenza del documento (stato del pacchetto, descrizione, data creazione, ecc.).

L’accesso ai documenti è riservato agli utenti autorizzati, secondo le regole impostate nel sistema.

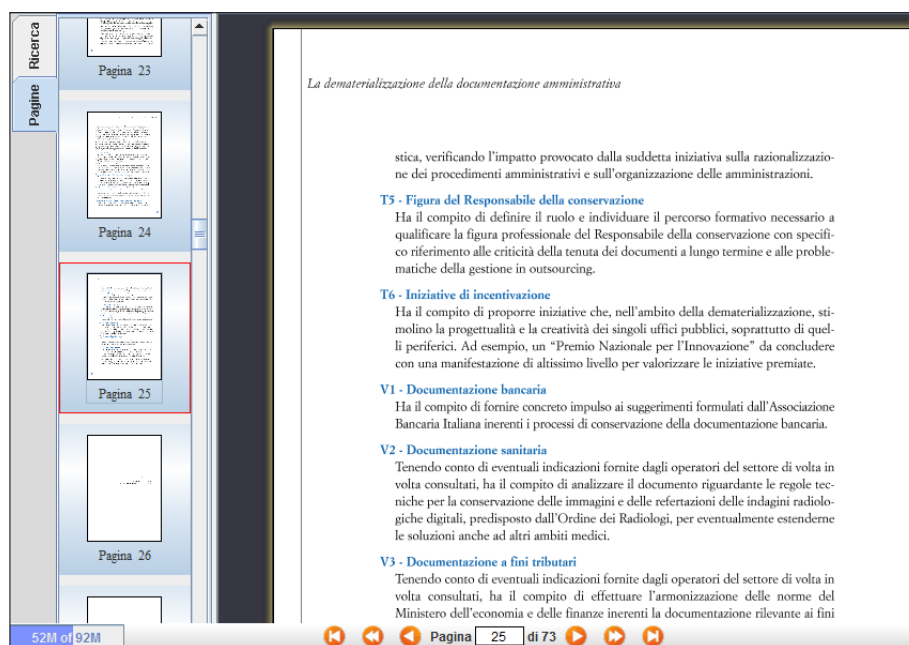


Figura 3: la figura rappresenta la modalità di visualizzazione di un documento, a seguito di ricerca nel sistema di conservazione

Torna all' [INDICE](#)

7.6.2 Funzionalità di esibizione

Per l'esibizione dei documenti conservati nelle forme prescritte dalla norma il sistema di conservazione ad oggi provvede:

- in cooperazione applicativa, dei web service che in modo completamente automatizzato consentono di recuperare uno o più documenti conservati da parte del sistema/applicativo che li ha versati in conservazione o altri applicativi con opportuni diritti di accesso, unitamente, se richiesti, alle prove di conservazione (Indice di Conservazione firmato e marcato) e/o all'attestato di conformità all'originale conservato;
- attraverso le web GUI con cui RdSC e suoi delegati nonché personale abilitato dei soggetti produttori possono visionare la documentazione conservata.

Per entrambe le modalità, al pacchetto di distribuzione sarà apposto il sigillo qualificato.

Torna all' [INDICE](#)

7.6.2.1 Esibizione in cooperazione applicativa

Si tratta della modalità tramite cui i sistemi o applicativi che hanno inviato in conservazione i loro documenti possono ottenere dal Sistema di Conservazione, in cooperazione applicativa, l'esibizione di uno o più documenti conservati.

Tale modalità di esibizione viene implementata attraverso servizi – web services – in cui i DIP restituiti sono realizzati ancora una volta come dei file archivio – zip o tar.gz – che contengono:

- un file manifest.xml con i metadati del documento e i puntamenti ai suoi componenti digitali;
- i componenti digitali del documento.

L'esibizione tramite cooperazione applicativa prevede di poter specificare le seguenti opzioni:

- indicazione se è richiesto anche l'Indice di Conservazione attestante che il documento è conservato secondo norma.

L'esibizione tramite cooperazione applicativa può essere eseguita per più documenti con un'unica invocazione del servizio. Infatti nella richiesta di esibizione si può indicare anche:

- una lista di documenti;
- uno o più aggregati di documenti (fascicoli, cartelle, serie, ecc.).

Per l'esibizione in cooperazione applicativa è prevista una duplice modalità di interazione per il sistema/applicativo che sottomette la richiesta:

- sincrona, quando il richiedente resta in attesa della risposta contenente il DIP. Consente l'esibizione di un solo documento alla volta, ed è ammessa solo per documenti di dimensione inferiore ad una soglia prestabilita; qualora la dimensione del documento richiesto superi il valore soglia la richiesta viene respinta;
- asincrona, quando a fronte dell'invocazione del servizio il richiedente ottiene solo un ticket di richiesta con il quale, in un momento successivo, va a richiedere lo stato della sua richiesta e l'eventuale risultato – il DIP – qualora la richiesta sia stata evasa.

L'xml di richiesta delle due modalità, con le possibili opzioni previste, sono rispettivamente i tag RequestEsibizioneSync e RequestEsibizioneAsync dell'xsd RequestEsibizione.xsd la cui documentazione di dettaglio è nell'allegato *Allegato3 - RequestEsibizione.pdf*.

L'xml di risposta nelle due modalità nonché quello del manifest del DIP (nel caso di esibizione asincrona), sono rispettivamente descritti dai tag ResponseEsibizioneSync, ResponseEsibizioneAsync, ResponseGetDIP e DIP dell'xsd ResponseEsibizione.xsd la cui documentazione di dettaglio è nell'allegato *Allegato4 - ResponseEsibizione.pdf*.

Torna all' [INDICE](#)

7.6.2.2 Esibizione on-line

Questa modalità di esibizione prevede che dalle GUI web di DigiDoc si visualizzi il documento direttamente all'interno della pagina web. Tale modalità di esibizione è disponibile solo per i documenti in formati pdf o formati Office e ascii convertibili in PDF: infatti prevede la conversione in pdf effettuata a carico del sistema di conservazione.

Se il documento è firmato digitalmente e in particolare se si tratta di una busta crittografica di tipo p7m o tsd o m7m, il sistema esibisce il contenuto della busta depurato della/e firme digitali: di ciò viene data evidenza all'utente che a fianco dell'area in cui visualizza il documento vede le informazioni sulle firme ad esso associate: stato di validità (con dettaglio relativo ai vari livelli di controllo della validità); estremi dei certificati di firma; date ed estremi delle eventuali marche temporali presenti nella busta. Peraltro le informazioni sulle firme e sulle marche temporali apposte sul documento vengono mostrate anche in caso di buste crittografiche pdf (PadES) e xml (XAdES) come pure in caso di firma e/o marche detached.

Questa modalità di esibizione è pensata per allargare la fruibilità dei documenti nei casi in cui:

- per il client non vi sia un viewer/reader in grado di restituirgli il documento nel formato originale;
- l'utente che chiede la visualizzazione non voglia o non possa installare sul proprio client il viewer o reader necessario alla restituzione del documento digitale nel formato originale in cui è conservato.

Quando viene utilizzata questa modalità di visualizzazione, se il formato di conservazione del file non è pdf, il sistema dà evidenza del fatto che si tratta di una copia non conforme all'originale conservato e riporta tutte le informazioni del formato originale di conservazione (mimetype, eventuale versione ecc.).

Torna all' [INDICE](#)

7.6.2.3 Esibizione tramite download da web GUI

Questa modalità di esibizione viene attivata dalla stessa interfaccia web da cui che consente l'esibizione on-line del documento (illustrata nel § precedente). In questo caso però il documento digitale non viene visualizzato all'interno di una pagina web, bensì previo scarico – download – del/i file che lo compongono: dopo di che il client che li ha scaricati può visualizzarli off-line.

Torna all' [INDICE](#)

7.6.2.4 Esibizione di singolo documento

Laddove viene reso disponibile il download del/dei file del documento vengono date le seguenti possibilità/opzioni:

- in caso di documento firmato digitalmente che sia una busta crittografica p7m, tsd o m7m, vengono forniti due link, uno per scaricare la busta e uno per scaricarne il contenuto depurato delle firme (il file “sbustato”);
- scelta se scaricare o meno anche il file xml “Indice di Conservazione”, firmato dal Responsabile del servizio di conservazione (o suo delegato) e marcato temporalmente, attestante la conservazione del documento;
- il sistema consente di scaricare la ricevuta di “conformità all'originale conservato” del documento, ovvero un PDF/A che contiene: i riferimenti dell'Ente produttore; gli estremi e i principali dati descrittivi del documento; un timbro digitale – codice a barre bidimensionale - contenente le impronte del/dei componenti digitali del documento.

Torna all' [INDICE](#)

7.6.2.5 Esibizione tramite Stampa

Anche questa modalità di esibizione è messa a disposizione dalle GUI web di DigiDoc: laddove sono rese disponibili l'esibizione online e il download del/dei file del documento (esibizione tramite

download) è data anche una funzione per effettuarne la stampa: selezionandola il sistema attiva la stampa dei file sul client – purché questo sia già dotato dei programmi necessari ad aprire e mandare in stampa quei file – ed eventualmente, se richiesto, la fa seguire dalla stampa della ricevuta di conformità.

L'esibizione tramite stampa, come quella tramite download, può essere effettuata anche contestualmente per più documenti: una volta effettuata la selezione dei documenti di interesse, con un'unica operazione, si può richiedere la stampa su carta di tutti i documenti selezionati (e delle relative ricevute di conformità).

Torna all' [INDICE](#)

7.6.2.6 Esibizione di copia conforme all'originale conservato a norma

Il rilascio di copia conforme di un documento conservato viene realizzata da DigiDoc attraverso la produzione della “ricevuta di conformità all'originale conservato”, ovvero un PDF/A recante, oltre che la dichiarazione di conformità all'originale conservato, anche un timbro digitale contenente la/le impronte dei file che compongono il documento. Tale timbro è realizzato come codice a barre bidimensionale: sono disponibili SW freeware che consentono di interpretare il contenuto di questi codici a barre (anche da un'immagine che è la scansione della ricevuta stampata su carta) e quindi di recuperare le impronte del documento riportate nel timbro al fine di verificare che coincidano con le impronte calcolate sulla copia del documento che è stata rilasciata.

Se la ricevuta viene firmata, digitalmente o su carta (una volta stampata), questo vale a fornire quella garanzia di autenticità della stessa che consente di realizzare un rilascio di copia conforme ai sensi di quanto previsto dalla legge.

La firma sarà apposta da un pubblico ufficiale le cui modalità di coinvolgimento sono descritte nel paragrafo 4.1. Per ogni cliente, nel contratto di affidamento, viene regolamentata l'attività del pubblico ufficiale.

Torna all' [INDICE](#)

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

Dalle web GUI che DigiDoc mette a disposizione è possibile selezionare uno o più documenti e aggregati di documenti al fine di richiedere un pacchetto di distribuzione contenente tutta la

documentazione selezionata. Una volta acquisita la richiesta DigiDoc attiva in modo asincrono l'elaborazione del DIP richiesto e quando questo è pronto rende scaricabile il DIP da apposita GUI in cui il richiedente consulta lo stato delle richieste di esibizione effettuate. Il DIP è un archivio compresso che oltre ai documenti richiesti contiene un file indice conforme allo schema documentato in *Allegato4 - ResponseEsibizione.pdf*.

Nei casi previsti dalla normativa, la firma sarà apposta da un pubblico ufficiale le cui modalità di coinvolgimento sono descritte nel paragrafo 4.1. Per ogni cliente, nel contratto di affidamento, viene regolamentata l'attività del pubblico ufficiale.

Torna all' [INDICE](#)

7.8 Scarto dei pacchetti di archiviazione

Un obiettivo importante per il sistema è quello di dare supporto, oltre che alla conservazione, anche al processo di selezione e scarto di ciò che non deve più essere conservato perché sono trascorsi i tempi di conservazione stabiliti.

Salvo casi particolari in cui il tempo di conservazione è esplicitato sul singolo documento o aggregazione di documenti al momento dell'invio in conservazione, in generale il tempo di conservazione della documentazione non è esplicitato e viene determinato dal sistema sulla base del massimario di selezione e scarto che stabilisce le regole e i tempi di conservazione agganciandoli ad uno o più dei seguenti dati di definizione del contesto:

- tipologie dei documenti e loro aggregati;
- voci del piano di classificazione;
- tipologie dei procedimenti da cui scaturiscono i fascicoli.

Da notare che laddove non specificato e non ricavabile dalle regole configurate il tempo di conservazione della documentazione viene considerato implicitamente "per tempo illimitato".

Così determinato il tempo di conservazione, DigiDoc è in grado di fornire una proposta di scarto che può essere modulata opportunamente istruendo DigiDoc in merito alla "granularità" dello scarto che si vuole effettuare:

- intere unità di aggregazione (fascicoli o serie);
- singoli documenti.

A partire dalla proposta predisposta in automatico da DigiDoc e trasmessa al Soggetto produttore, quest'ultimo redige la proposta di scarto definitiva e la sottomette alla Sovrintendenza competente

per territorio per autorizzazione. La Sovrintendenza verifica la documentazione contenuta nella proposta e seleziona quella di cui autorizzare lo scarto.

Nel caso la documentazione candidata allo scarto sia di particolare interesse culturale, DigiDoc prevede di poter richiedere ed acquisire un'ulteriore autorizzazione allo scarto da parte del Ministro dei Beni e delle attività culturali e del turismo.

Quando viene acquisita l'autorizzazione allo scarto, gli AIP e i documenti digitali corrispondenti alla documentazione scartata vengono rimossi dallo storage; quanto ai metadati della documentazione scartata memorizzati su RDBMS essi vengono spostati in aree logiche – i.e. tabelle – dedicate alla documentazione scartata e

- perdono le informazioni di stabilità e di pacchetto (diventano inutili dal momento che i documenti digitali vengono fisicamente eliminati), e nelle informazioni di pacchetto vengono aggiunte le informazioni relative all'autorizzazione allo scarto;
- perdono le informazioni di rappresentazione (ormai inutili, a fronte dell'eliminazione fisica dei documenti);
- acquisiscono delle nuove informazioni, quelle relative allo scarto (data, autorizzato da chi).

Torna all' [INDICE](#)

7.8.1 Cancellazione di pacchetti di archiviazione inviati per errore

Nel caso in cui il produttore abbia versato dei documenti errati e voglia richiederne la cancellazione, dovrà inviare formale richiesta, trasmessa via PEC, all'indirizzo regionetoscana@postacert.toscana.it indicando nella comunicazione:

- l'elenco degli indici dei pacchetti da eliminare,
- la motivazione della cancellazione.

L'intervento effettuato viene annotato nel sistema e la richiesta di intervento verrà archiviata nel DAX.

Torna all' [INDICE](#)

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

Il sistema DigiDoc rispetta lo standard OAIS e lo standard UNI 11386 - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali; pertanto è in grado di esportare secondo lo schema documentato in *Allegato4 - ResponseEsibizione.pdf* i pacchetti di archiviazione conservati in pacchetti seguendo le regole che permettono la loro importazione in un altro sistema aderente allo standard OAIS.

Allo stesso modo il sistema DigiDoc è in grado di importare e archiviare pacchetti di distribuzione generati da altri sistemi aderente allo standard OAIS.

L'esportazione dei pacchetti di conservazione (pacchetti di archiviazione) può essere effettuata su supporto elettronico in formato ZIP. Il cliente può scaricare i pacchetti utilizzando un'interfaccia WEB messa a disposizione dal sistema DigiDoc.

Torna all' [INDICE](#)

7.10 Riversamento

Il riversamento è la 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 Cfr. Allegato 1 Linee Guida AgiD).

DigiDoc prevede le funzionalità di riversamento necessarie a garantire la conservazione della documentazione anche nel medio e lungo termine e che sono implementate secondo quanto previsto dalle normative in vigore.

Tali procedure possono essere avviate su precisa iniziativa del Responsabile del servizio di conservazione, o su richiesta di un soggetto produttore e la loro realizzazione avverrà in conformità alle indicazioni previste dall'allegato 2 alle Linee Guida AgiD "Formati di file e riversamento", soprattutto per ciò che riguarda la scelta dei formati di arrivo. Nella scelta dei nuovi formati di file, così come nella scelta metodologica circa l'esecuzione del riversamento, saranno prese in considerazione le peculiarità tecniche del formato sorgente e di quello riversato, con particolare riferimento sia alla perdita di dati e metadati, sia alla diversa qualità o rappresentazione tecnica dei medesimi.

Tutte le informazioni relative ai riversamenti che un documento ha subito durante la sua conservazione in DigiDoc vengono man mano ad arricchire il set di metadati contenuti nell'AIP del documento (oltre che essere memorizzate negli audit trail generali del sistema): in particolare, nel caso di sostituzioni con nuovi formati, vengono memorizzati nell'AIP i formati originale e di destinazione e gli eventuali dettagli sul formato originale (versione, rischi connessi, ecc.).

Ogni procedura di riversamento vedrà inoltre il coinvolgimento del pubblico ufficiale per il rilascio dell'attestazione di conformità sottoscritta con firma digitale o altra firma elettronica qualificata, così come stabilito ai sensi dell'art. 23-bis del CAD.

Torna all' [INDICE](#)

8 Il sistema di conservazione

Le componenti del sistema di conservazione di seguito descritte sono intese sia per gli ambienti di collaudo che per quelli di produzione che sono separati e indipendenti.

Torna all' [INDICE](#)

8.1 Componenti Logiche

I processi sopra illustrati corrispondono ad altrettanti gruppi di **servizi applicativi** previsti dalla soluzione DigiDoc:

- DigiDocWePo (versamento): permettono l'invio della documentazione, sia singoli documenti che loro eventuali aggregazioni, al sistema di conservazione nonché l'aggiornamento di quanto già inviato in precedenza;
- DigiDocCtrl: svolgono i controlli sulla documentazione inviata in conservazione, necessari per l'accettazione da parte del sistema di conservazione. Sono controlli sia sui dati di descrizione che sui componenti digitali (file) da conservare, in particolare sui loro formati e su eventuali firme digitali e marche temporali;
- DigiDocConS: comprendono le funzionalità espressamente richieste dalla normativa italiana per la Conservazione dei documenti;
- DigiDocWeCS: consentono le ricerche su tutto il materiale conservato nel sistema, sfruttando tutti i dati di descrizione della documentazione conservata come chiavi di ricerca;
- DigiDocMoEs: permettono di verificare la corretta funzionalità del sistema in tutti i suoi aspetti e componenti, consentendo al Responsabile del servizio di Conservazione ed eventuali autorità di vigilanza di assolvere ai propri compiti di verifica ordinaria e straordinaria;
- DigiDocAdmi: trasversali a tutto il sistema, consentono di aggiornare e storicizzare strumenti e dati di definizione del contesto che sono funzionali alla descrizione degli archivi (es.

organigrammi, piani di classificazione, tipologie documentali, massimari di selezione e scarto)

L'architettura applicativa di DigiDoc, coerentemente con il modello di sviluppo a servizi (SOA), si compone di moduli separati, seppur interdipendenti, che a loro volta composti da servizi e funzionalità applicative, permettono di gestire i processi identificati. Questa separazione consente di installare le varie componenti su sistemi fisici differenti.

Torna all' [INDICE](#)

8.2 Componenti Tecnologiche

Schema e descrizione delle componenti tecnologiche (strumenti informatici a supporto delle funzionalità del sistema di conservazione) che implementano il sistema di conservazione.

Torna all' [INDICE](#)

8.2.1 Software di base

- http Server:
 - CentOS 6.5/7.0;
 - Apache HTTP Server;
 - Java Runtime;
 - JDK e JRE Compatibility level;
- Application Server:
 - CentOS 6.5/7.0;
 - Apache Tomcat;
 - Java Runtime;
 - JDK e JRE Compatibility level;
- Batch Server:
 - CentOS 6.5/7.0;
 - Java Runtime;
 - JDK e JRE Compatibility level;
- DB Server:
 - CentOS 6.5 staging;

- Oracle Linux 6.6;
- Java Runtime.

Torna all' [INDICE](#)

8.2.2 Framework di sviluppo utilizzati

NOME	UTILIZZO
JAX-WS (Java API for XML Web Services)	Per realizzare web-service – SOAP e REST – e client che utilizzano XML per comunicare.
Jersey	Per realizzare web-service REST e i relativi client (è l'implementazione di riferimento della specifica JAX-RS).
Smart GWT	Framework di base per la realizzazione delle web UI: si occupa del rendering del framework ajax GWT appoggiandosi alle librerie Smartclient.
Spring	Per realizzare i componenti come applicazioni java enterprise facilmente configurabili e altamente riusabili.
Hibernate	ORM utilizzato per l'accesso al database.

Torna all' [INDICE](#)

8.3 Componenti Fisiche

Le componenti fisiche del servizio di conservazione sono localizzate in:

- sito primario, situato presso la struttura del TIX, via San Piero a Quaracchi 250, Firenze;
- sito secondario, avente almeno le stesse caratteristiche di sicurezza di quello primario ed utilizzato per erogare il servizio di Disaster Recovery (DR), presso il data centre di Cesano Maderno (MB) di Telecom Italia;
- sito secondario, avente almeno le stesse caratteristiche di sicurezza di quello primario, per la replica dei documenti, presso il data centre di di Engineering Informatica, in Viale Carlo Viola 76, a Pont-Saint-Martin (AO).

Gli impianti tecnologici del TIX sono all'interno del perimetro recintato della sede e sono alloggiati sia all'interno che all'esterno dell'edificio che ospita i CED; ad essi si accede attraverso porte chiuse a chiave e/o sistemi di controllo accessi con badge.

Le sale CED sono comunque separate fisicamente dalle sale dell'edificio che ospitano gli impianti di alimentazione elettrica.

L'accesso agli impianti tecnologici è consentito soltanto alle persone addette alla conduzione e manutenzione degli impianti stessi.

Gli impianti sono presidiati in orario esteso da personale qualificato e con servizio di reperibilità h24.

Il sistema di monitoraggio, controllato H24 dagli operatori del NOC, consente di verificare a distanza lo stato degli apparati e di attivare il personale di manutenzione o la reperibilità. Per garantire il supporto di secondo livello le console del sistema di monitoraggio sono accessibili in occasione dell'attivazione del piano di continuità.

Il sito è dotato di impianti per:

- rilevazione incendi: i locali del DC e alcuni dei locali Impianti sono dotati di un impianto centralizzato di rilevazione incendi, i cui allarmi sono riportati nella cabina di Vigilanza e nel NOC;
- estinzione incendi: i locali del DC e i locali Impianti sono dotati di un sistema automatico di estinzione incendi, compartimentato e pilotato dal sistema di rilevazione; in tutti questi locali l'impianto agisce nello spazio libero dell'ambiente e nel sottopavimento; nelle Sale energia sono presenti anche degli erogatori a scarica automatica (non pilotati dall'impianto di rilevazione) posti all'interno dei quadri elettrici di potenza e degli armadi batterie; in tutti i locali, compresi gli spazi di servizio e di transito, è presente un numero adeguato di estintori della tipologia adatta alle specifiche circostanze,
- impianto elettrico: la continuità dell'alimentazione delle macchine è garantita da un impianto elettrico così composto:
 - cabina di media tensione (15.000 V), situata all'esterno dell'edificio principale, (cabina di consegna) alimentata da una linea fornita da ENEL;
 - due linee di trasformazione di alimentazione indipendenti, alimentate dalla cabina di consegna, ognuna composta da:
 - un trasformatore 15.000/400 V che assicura l'alimentazione in bassa tensione alla linea di appartenenza, installato in una cabina di trasformazione situata all'esterno dell'edificio principale;
 - un gruppo elettrogeno, che garantisce l'alimentazione preferenziale in caso di prolungata interruzione di energia da parte dell'ente erogatore, con inserzione automatica in caso di mancanza rete. L'autonomia è di 24 ore a pieno carico senza rifornimento; il gruppo è posizionato su una struttura metallica sopraelevata di tre metri rispetto al piano stradale, al fine di garantire il funzionamento degli apparati anche a fronte di eventuali

allagamenti dell'area su cui insiste la sede; è un'installazione a cielo aperto, monitorata a distanza e sorvegliata dalle telecamere a circuito chiuso.

- UPS che garantisce la continuità di alimentazione in caso di breve interruzione di energia elettrica (autonomia di circa 10 minuti a pieno carico). L'UPS, insieme agli armadi batterie e ai quadri elettrici della distribuzione primaria, è installato in una Sala energia situata all'interno dell'edificio principale e separata dalle sale CED. Gli UPS hanno ridondanza N+1.
 - doppia alimentazione elettrica indipendente (un'alimentazione da ciascuna linea) su ogni rack ospitante gli apparati IT;
 - Sistema STS di interconnessione tra le sale energia in grado garantire la doppia alimentazione alle sale CED anche con una sola sala energia operativa.
 - impianto di condizionamento: il DC è dotato di un sistema di condizionamento misto differenziato in funzione degli ambienti da climatizzare. In particolare:
 - CDZ ad espansione diretta di tipo under; la ridondanza N+1 è garantita dal dimensionamento di progetto) dal collegamento elettrico alle linee preferenziali di alimentazione, e dalla possibilità di commutare l'alimentazione del CDZ centrale tra le due linee;
 - Il CED AD è un ambiente progettato per l'alta densità e quindi è stato dotato di un raffreddamento di precisione costituito da condizionatori inseriti nelle file di rack; i rack sono a loro volta assemblati in due linee parallele, con il retro contrapposto e chiuso in modo da segregare l'aria calda generata dal raffreddamento degli apparati IT. Il vettore termico è l'acqua refrigerata, prodotta da una coppia di chiller e trasportata da due linee di raffreddamento indipendenti e interscambiabili. I due chiller sono macchine della capacità di 155 KWf ciascuno, collegati ognuno ad una linea di alimentazione diversa. Sono posti all'esterno del primo piano dell'edificio su una piattaforma a cielo aperto non accessibile e sorvegliata con telecamere a circuito chiuso e sono monitorati a distanza. La ridondanza di alimentazione elettrica dei chiller, la duplicazione delle linee di distribuzione acqua (ognuna con una coppia di pompe per la circolazione del refrigerante), il serbatoio di accumulo del refrigerante e la distribuzione a matrice delle alimentazioni elettriche e idrauliche sui CDZ InRow permettono di garantire il condizionamento del CED in qualsiasi condizione tranne quella di un evento disastroso.
- Le due Sale energia e la Sala TLC sono dotate di CDZ ad espansione diretta di tipo under. Il condizionamento di questi ambienti presenta un livello di ridondanza 2N.

Criteri costruttivi: la dislocazione del Data Center e l'infrastruttura che lo compone rappresentano una garanzia rispetto a fenomeni di allagamento per inondazione; la risposta progettuale a questa

tipologia di rischio è la collocazione al di sopra del livello di allagamento dei gruppi elettrogeni e delle Sale energia (UPS e distribuzione elettrica primaria), oltre che ovviamente tutti i locali CED.

Torna all' [INDICE](#)

8.3.1 Componenti HW

L'infrastruttura fisica dei sistemi è costituita da apparati con tecnologia CISCOS UCS che garantisce elevata potenza elaborativa, ridondanza delle connessioni LAN e SAN, capacità di sostituzione di un componente HW guasto attraverso componente spare e configurazione SW.

I sistemi sono server virtuali realizzati su tecnologia VMWARE ESX.

In caso di fault dei sistemi la ripartenza è garantita sfruttando la HA VMWARE.

Tutte le componenti HW utilizzate dal servizio (chassis, lame, storage, SAN, LAN, firewall) sono ridondate ed in configurazione di alta affidabilità.

Torna all' [INDICE](#)

8.4 Procedure di gestione e di evoluzione

- Conduzione e manutenzione applicativa del sistema di conservazione (manutenzione adeguativa e correttiva): si seguirà quanto riportato nell'accordo di servizio siglato tra Regione Toscana e il fornitore della piattaforma Digidoc, nonché quanto previsto dalle procedure del Sistema per la Gestione della Qualità di quest'ultimo;
- monitoraggio delle componenti fisiche e applicative del sistema di conservazione: cfr. capitolo 9;
- conduzione e manutenzione dell'infrastruttura hardware (manutenzione evolutiva e correttiva): vedere paragrafo successivo
- gestione e conservazione dei log (anche in accordo con l'ente Produttore)): vedere paragrafo successivo
- verifica periodica di conformità a normativa e standard di riferimento: sono svolti audit periodici da parte di Regione Toscana, sia per verificare che siano seguite le procedure, sia per verificare che le procedure siano allineate con la normativa e gli standard applicabili e aggiornati (procedure interne "Gestione degli audit" e "Gestione dei riesami del SGSI").

Torna all' [INDICE](#)

8.4.1 Procedure per la conduzione e manutenzione dell'infrastruttura hardware (manutenzione evolutiva e correttiva)

L'esercizio dell'infrastruttura HW e SW utilizzata per l'erogazione dei servizi del TIX si basa sul modello ITIL.

Sono quindi adottate procedure documentate che coprono:

- La gestione degli incident, con particolare attenzione agli aspetti legati alla sicurezza fisica e logica.
- Il Service Desk, come unico punto di contatto per tutti gli aspetti legati all'infrastruttura HW e SW;
- L'event management per il monitoraggio e la gestione delle procedure schedulate;
- Il change management; i change sono valutati in base a diversi parametri, quali ad esempio:
 - l'entità dell'impatto sia sull'operatività del servizio erogato, sia sui componenti HW e SW implicati;
 - la tipologia dell'intervento, espresso in termini di manutenzione correttiva, evolutiva, adeguativa;
 - l'urgenza degli interventi, pianificabili o meno (es. interventi per i quali è necessario un fermo del sistema che può essere programmato o accidentale, a seconda delle cause che lo determinano).

Sulla base dell'analisi dell'impatto si provvede alla pianificazione del change, tenendo in considerazione le modalità operative per un eventuale ritorno all'indietro.

I sistemi HW e SW sono monitorati H24 con strumenti in grado di rilevare dati sulla situazione corrente e per avere un controllo sull'andamento delle risorse, anche ai fini del processo di capacity. La gestione degli incident del TIX è descritta nel documento TIX-ITIL-PRO-001-Incident Management e al paragrafo 9.4.

Il processo di cambiamento dei servizi del TIX è attuato in conformità a quanto definito nel documento TIX-ITIL-PRO-008 Change Management.

Torna all' [INDICE](#)

8.4.2 Procedure per la gestione e conservazione dei log (anche in accordo con il Titolare degli oggetti di conservazione)

I log di sistema sono considerati parte integrante del patrimonio informativo. Per tale motivo sono definite le politiche relative alla gestione dei log sulla base delle prescrizioni di legge e degli impegni contrattuali.

I log applicativi permettono di tracciare le azioni svolte sul sistema, in modo da ricostruirle in caso di necessità.

I log sono raccolti attraverso strumenti centralizzati che garantiscono prestazioni nella raccolta (numero di eventi al secondo) e forniscono adeguati strumenti di analisi e di protezione. La protezione è assicurata dallo strumento di log collection, usato per conservare i log.

I log di sistema sono relativi ad eventi di sistema, di operazioni autorizzative, di anomalie, inviati da apparati di rete e sistemi.

Verifica periodica di conformità a normativa e standard di riferimento: sono svolti audit periodici da parte di Regione Toscana, sia per verificare che siano seguite le procedure, sia per verificare che le procedure siano allineate con la normativa e gli standard applicabili e aggiornati (procedure interne “Gestione degli audit” e “Gestione dei riesami del SGSI”).

I log applicativi sono conservati per almeno un anno e sono oggetto di controllo accessi e backup per assicurarne l'integrità.

Torna all' [INDICE](#)

8.4.2.1 Riesame dei log

I log sono riesaminati in caso di eventi particolari che possono essere stati originati da azioni che necessitano approfondimenti.

Torna all' [INDICE](#)

8.4.2.2 Clock di sistema

L'NTP è erogato da due server presso il TIX, a loro volta sincronizzati con un pool di server riconosciuto come affidabile a livello di comunità Internet. Il controllo di affidabilità è effettuato ad ogni sincronizzazione. I sistemi presso il TIX, per assicurare il livello di sicurezza, non si possono collegare autonomamente a NTP server esterni.

Torna all' [INDICE](#)

9 Monitoraggio e controlli

9.1 Procedure di monitoraggio

Il servizio è strutturato per fornire servizi continuativi con operatività H24 presidiata, garantendo:

- Implementazione dei sistemi di monitoraggio e relativo aggiornamento;
- Rilevazione degli eventi di allarme;
- Tracciamento su Sistema di Ticketing;
- Applicazione dell'opportuna procedura di fixing o innesco della Procedura di Escalation Operativa / Informativa;
- Follow-up del problema in caso di escalation;
- Valutazione dell'utilizzo di risorse rispetto all'andamento passato e futuro del servizio (Capacity planning);
- andamento del servizio, rispetto agli SLA di disponibilità, affidabilità ed esecuzione richieste di servizio.

A supporto delle attività di Monitoring è stato sviluppato un apposito Sistema Informativo ad esclusivo uso del personale tecnico dove sono mantenute e costantemente aggiornate le informazioni riguardanti ogni singolo apparato/sistema monitorato e le procedure da attuare in caso di evento la cui azione correttiva è stata predefinita.

Il monitoraggio dei sistemi viene effettuato con le seguenti modalità:

- monitoraggio istantaneo; vengono utilizzati strumenti per una rapida ed efficace gestione degli eventi; un evento anomalo può essere classificato per l'ambito in cui accade (hardware, software, rete), per il contesto (servizio online, eccezione in un'esecuzione batch, back-up, ecc.) e per la gravità (impatto totale, parziale o nullo sul servizio, ecc.). Una dashboard consente al presidio sistemistico di avere visibilità h24 dell'insorgere di situazioni anomale. Il sistema è realizzato integrando diversi strumenti SW come XYmon, Openms. Il SW di monitoraggio utilizza sia agent (ad es. sui server, sia agentless, ad es. per apparati di rete. Il SW di monitoraggio è configurato anche per controllare il superamento di soglie associate agli indicatori di utilizzo risorse (ad es. CPU, disco, Java VM, etc.).

Oltre ai servizi e sistemi il monitoraggio è in grado di rilevare anomalie sulla Rete Telematica Regione Toscana (RTRT) e sugli impianti tecnologici del CED (alimentazione elettrica, condizionamento, temperatura e umidità relativa attraverso il SW StruXureWare della APC.

Attraverso il monitoraggio istantaneo sono tenute sotto controllo le procedure ricorrenti (ad es. backup).

- monitoraggio andamentale; vengono utilizzati strumenti che permettono una raccolta storica dei dati di monitoraggio, effettuandone delle aggregazioni secondo opportune configurazioni; oltre a permettere una verifica della disponibilità del servizio (SLA),

permettono un'efficace presa visione dell'andamento delle risorse ai fini di un corretto Capacity Planning.

Infatti, il SW conserva la storia di tutti i cambiamenti di stato e l'andamento delle risorse per almeno un anno.

Attraverso i dati del Sistema di monitoraggio e dei Ticket (incident, richieste di servizio) viene predisposta la reportistica sull'andamento del servizio, prodotta trimestralmente ma con aggregato base mensile, per riscontro rispetto agli SLA.

Il servizio di Monitoraggio viene erogato attraverso una Control Room dislocata presso il TIX situata in ambiente protetto (guardiana armata, sistemi autonomi di riscaldamento e condizionamento) e dotata di sistemi di supporto video dedicati (maxi schermi, postazioni audio-video; il presidio TIX opera in modalità H24; gli operatori tengono sotto controllo lo stato dei sistemi e dei servizi; l'obiettivo è il Monitoring Proattivo per rilevare condizioni di criticità e porvi rimedio prima che l'insorgenza del problema generi un disservizio percepibile all'utente.

La procedura prevede che all'insorgere di una anomalia o di un allarme gli operatori, traccino l'evento sul sistema di Ticketing ed utilizzando una "Knowledge Base" mettano in atto le azioni previste (esecuzione di procedure di recovery, dispatching a team sistemistici specializzati on site o remoti ovvero al team responsabile della conduzione del servizio).

A supporto di queste procedure vi sono il sistema di Trouble Ticketing, basato su OTRS, ed il sistema per la documentazione di esercizio, basato su Alfresco.

Tutti gli strumenti utilizzati per monitoraggio e gestione sono oggetto del servizio di Disaster Recovery e quindi operativi anche in caso di switch del servizio sul sito DR.

Torna all' [INDICE](#)

9.2 Procedure di monitoraggio per il cliente

Gli SLA sono forniti ai clienti con report trimestrali che possono essere richiesti a Regione Toscana.

Torna all' [INDICE](#)

9.3 Verifica dell'integrità degli archivi

La verifica dell'integrità dei dati è effettuata mediante l'esecuzione di una procedura schedulabile che può essere configurata per scegliere la profondità di osservazione (file analizzati da oltre un determinato periodo) ed agisce sui pacchetti che rispettano il criterio impostato.

Per ogni file contenuto nell'indice viene verificata la sua presenza e viene controllata la corrispondenza della sua impronta con quella indicata nell'indice. Per ogni elaborazione viene prodotto un report in formato xml, riportante l'esito della verifica per ogni indice e per ogni documento contenuto al suo interno.

La procedura sarà schedata per essere eseguita con frequenza tale da garantire che:

- il tempo di esecuzione sia inferiore alla periodicità di schedulazione;
- sia possibile effettuare il restore dei dati a partire dai backup effettuati con la cadenza prestabilita (ovvero la periodicità della schedulazione deve essere minore del tempo di retention dei backup).
- I backup seguono le seguenti regole:
 - Frequenza almeno ogni 24 ore (con anche alternanza di backup full settimanali e incrementali giornalieri) per macchine virtuali, database, log.
 - conservazione almeno di 15 giorni.

Torna all' [INDICE](#)

9.4 Soluzioni adottate in caso di anomalie

La procedura applicabile è "Gestione degli incidenti del TIX", che specifica le modalità di contatto tra utenti, l'help desk, la conduzione sistemistica e la conduzione applicativa. In particolare, ogni entità (help desk, conduzione sistemistica e conduzione applicativa) contatta le altre attraverso sistemi di ticketing tra loro interfacciati.

Ogni anomalia è risolta dall'entità più adeguata, che predispone anche un rapporto di incidente.

Le anomalie possono essere riscontrate attraverso:

- strumenti di monitoraggio delle funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi, presso la conduzione applicativa;
- strumenti di monitoraggio delle prestazioni dei sistemi e della rete presso la conduzione sistemistica;
- chiamate degli utenti all'help desk (come specificato nella documentazione che descrive il servizio erogato al singolo Ente Produttore).

Torna all' [INDICE](#)