Manuale di Conservazione
Azienda speciale
Servizi alle Imprese
di Trapani

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	23/11/2026		
Verifica			
Approvazione	18/02/2021	Alessandro Carollo	Responsabile conservazione della Azienda speciale Servizi alle Imprese di Trapani. Determina del Direttore n. 2

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
Versione N° 1			

Indice

1 Normativa e standard di riferimento 4
1.1 Normativa di riferimento 4
1.2 Standard di riferimento 5

2 Scopo e ambito del documento 7

3 Terminologia (glossario e acronimi) 8

4 Modello Organizzativo 10
4.1 Affidamento a terzi della conservazione per specifiche aree [da verificare con il fornitore] .....**Errore. Il segnalibro non è definito.**

5 Ruoli e responsabilità 11
5.1 Ruoli 14
5.2 Pubblico Ufficiale 14

6 Organismi di tutela e di vigilanza 15

7 Attivazione del servizio 16
7.1 Affidamento del servizio 16
7.2 Accesso al servizio 16
7.3 Descrizione del servizio 17

8 Oggetti sottoposti a conservazione 18
8.1 Formati 18
8.2 Classe di contenuto 19

9 Il processo di conservazione 20
9.1 Conservazione 20
9.1.1 Formazione e Trasmissione del Pacchetto di versamento (SIP) 20
9.1.2 Presa in carico del Pacchetto di versamento (SIP) da parte del sistema di conservazione 20
9.1.3 Indicizzazione e generazione del pacchetto di archiviazione (AIP) 20
9.2 Esibizione 21
9.3 Produzione di duplicati informatici 21
9.4 Produzione di copie informatiche 22
9.5 Scarto degli oggetti digitali 22
9.6 Verifiche d'integrità 22
9.7 Recesso 23

10 Sicurezza del Sistema di Conservazione 24
10.1 Quadro normativo di riferimento 24
10.2 Principali riferimenti e collegamenti 24
10.3 Organizzazione sicura della Conservazione dei documenti informatici 25
10.4 Obiettivi delle misure di sicurezza 26
10.5 Controllo accessi al sistema di conservazione 26
10.6 Principali impostazioni sicure delle postazioni di lavoro e di comportamento utenti 27
10.7 Indicazioni sulla protezione dei dati personali e conformità al GDPR 27

11 Il Portale della Conservazione e la documentazione del Conservatore 30

Indice delle figure:

Figura 1 - Modello organizzativo.....10
Figura 3 - Ruoli e ambiti considerati per la valutazione dei livelli di sicurezza e privacy.....25

1 Normativa e standard di riferimento

1.1 Normativa di riferimento

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

Normativa Nazionale:

- **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.
- **D.Lgs. 7 marzo 2005, n. 82 e s.m.i.:** Codice dell'amministrazione digitale (CAD).
- **D.Lgs. 22 gennaio 2004, n. 42 e s.m.i.:** Codice dei Beni Culturali e del Paesaggio.
- **D.Lgs. 30 giugno 2003, n. 196 (coordinato con il D.Lgs. 101/2018) e s.m.i.:** Codice in materia di protezione dei dati personali.
- **D.P.R. 28 dicembre 2000, n. 445 e s.m.i.:** Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (TUDA).
- **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.
- **Legge 24 dicembre 2007, n. 244:** Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato.
- **D.M. Economia e Finanze 17 giugno 2014:** Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto (articolo 21, comma 5, del D.Lgs. 82/2005).
- **D.M. Economia e Finanze 3 aprile 2013, n. 55:** Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche.
- **Linee Guida AgID (Maggio 2021):** Sulla formazione, gestione e conservazione dei documenti informatici.
- **Regolamento AgID (Dicembre 2021):** Sui criteri per la fornitura dei servizi di conservazione dei documenti informatici e relativi allegati.
- **Linee Guida AgID:** Contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate.

Normativa Europea:

- **Regolamento (UE) 2016/679 (GDPR):** Relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.
- **Regolamento (UE) 2024/1183 (eIDAS 2.0):** Che modifica il regolamento (UE) n.

910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale.

- **Regolamento di Esecuzione (UE) 2024/482:** Relativo all'adozione del sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC).
- **Regolamento di Esecuzione (UE) 2024/3144:** Che modifica il regolamento di esecuzione (UE) 2024/482 per quanto riguarda le norme internazionali applicabili

Torna al sommario

1.2 Standard di riferimento

L'erogazione del servizio di conservazione e la gestione delle infrastrutture tecnologiche associate si conformano ai seguenti standard internazionali (nell'ultima versione aggiornata) e specifiche tecniche:

Archiviazione e Conservazione Digitale

- **ISO 14721:** *Space data and information transfer systems — Open archival Information system (OAIS) - Reference model*. Modello di riferimento per i sistemi informativi aperti per l'archiviazione.
- **CEN/TS 18170:** *Functional requirements for the electronic archiving service*. Specifica tecnica europea per l'archiviazione elettronica.
- **UNI 11386:** *Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali*.
- **ISO 16363:** *Audit and certification of trustworthy digital repositories*.
- **ISO/TR 18492:** *Long-term preservation of electronic document-based information*.

Metadati e Standard Descrittivi Archivistici

- **ISO 15836:** *Information and documentation - The Dublin Core metadata element set*. Sistema di metadati del Dublin Core.
- **ISO/TS 23081:** *Information and documentation - Records management processes – Metadata for records* (Parti 1, 2 e 3). Quadro di riferimento e guida per l'implementazione e l'autovalutazione sui metadati.
- **ISAD(G):** *General International Standard Archival Description*. Standard generale internazionale per la descrizione archivistica.
- **ISAAR (CPF):** *International Standard Archival Authority Record for Corporate Bodies, Persons and Families*.
- **EAD ed EAC:** *Encoded Archival Description* ed *Encoded Archival Context* (codifiche XML degli standard descrittivi).

Sicurezza, Cibersicurezza e Servizi Fiduciari (Trust Services)

- **ETSI EN 319 401:** *Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers*.

- **ETSI EN 319 421:** *Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps*.
- **ETSI TS 119 511:** *Electronic Signatures and Infrastructures (ESI); 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:** *Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services*.
- **ISO/IEC 15408:2022 (Parti da 1 a 5):** *Information security, cybersecurity and privacy protection - Evaluation criteria for IT security* (Common Criteria).

Sistemi di Gestione Aziendale, Sicurezza e Qualità del Conservatore

- **UNI CEI ISO/IEC 27001:** *Information technology - Security techniques - Information security management systems – Requirements*, unita ai controlli della **ISO/IEC 27002** e alle linee guida per la gestione del rischio **ISO/IEC 27005**.
- **ISO/IEC 27017:** *Code of practice for information security controls based on ISO/IEC 27002 for cloud services*.
- **ISO/IEC 27018:** *Code of practice for protection of personally identifiable information (PII) in public clouds*.
- **UNI EN ISO 22301:** *Sicurezza e resilienza - Sistemi di gestione della continuità operativa*.
- **UNI CEI ISO/IEC 20000-1 e 20000-2:** *Tecnologie informatiche – Gestione del Servizio IT*.
- **UNI EN ISO 9001:** *Sistemi di gestione per la qualità - Requisiti*.
- **UNI ISO 31000:** *Gestione del rischio - Principi e linee guida*.
- **ISO 14001:** *Environmental management systems*.
- **UNI ISO 45001:** *Sistemi di gestione per la salute e sicurezza sul lavoro*

Torna al sommario

2 Scopo e ambito del documento

Il presente manuale descrive il sistema di conservazione dell'Azienda Speciale "Servizi alle Imprese" di Trapani ai sensi dell'art. 44 del CAD e delle "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici".

In particolare, nel presente documento sono definiti:

- i ruoli e responsabilità nel processo di conservazione;
- l'attivazione del servizio;
- gli oggetti sottoposti alla conservazione;
- il processo di conservazione;
- le misure di sicurezza e di protezione dei dati personali.

La parte del processo di conservazione, affidata a InfoCamere Scpa, società in house del sistema camerale, è ulteriormente dettagliata nel manuale della conservazione del Conservatore disponibile all'indirizzo https://conservazione.infocamere.it.

Il presente manuale, predisposto dal Responsabile della conservazione, è condiviso tramite pubblicazione sul sito istituzionale nell'area "Amministrazione trasparente" [dettagliare] con il Conservatore e con tutti i soggetti coinvolti nel processo di conservazione, ai quali sono comunicate tempestivamente le eventuali modifiche.

Torna al sommario

3 Terminologia (glossario e acronimi)

Glossario dei termini e Acronimi	
AgID	Agenzia per l'Italia Digitale
Dublin Core	ISO 15836-1:2017 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.
Codice della privacy	Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali
Produttore del PdV	persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento (SIP) ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale.
GDPR	Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, 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
Linee Guida Agid	Linee Guida sulla formazione, gestione e conservazione dei documenti informatici
OAIS	Open Archival Information System è lo standard ISO 14721:2012 e definisce concetti, modelli e funzionalità inerenti agli archivi digitali e gli aspetti di digital preservation.
Pacchetto di archiviazione (AIP)	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel manuale di conservazione.
Pacchetto di distribuzione (DIP)	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione.
Pacchetto di versamento (SIP)	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione.
Pacchetto di file (file package)	Insieme finito di più file (possibilmente organizzati in una struttura di sottoalbero all'interno di un filesystem) che costituiscono, collettivamente oltre che individualmente, un contenuto informativo unitario e auto-consistente.
Piano della sicurezza	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
Produttore	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 responsabile della gestione documentale.

Regolamento sui criteri per la fornitura dei servizi di conservazione	Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici e relativi allegati, ai sensi dell'art. 34, comma 1bis, lett. B) del CAD
Responsabile della conservazione	soggetto responsabile dell'insieme delle attività elencate al par. 4.5 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici
Servizi Documentali	Applicazioni per la gestione di documenti informatici
Soggetto produttore	Titolare dell'oggetto di conservazione
Unità archivistica (UA)	Unità minima elementare di riferimento di cui è composto un archivio, che può corrispondere a un'aggregazione documentale o a un fascicolo
Unità documentaria (UD)	Termine generico con cui si individua l'unità minima indivisibile di un fondo archivistico, che può aggregare più documenti, logicamente contigui.
UniSincro	UNI 11386 - Supporto all'Interoperabilità nella conservazione e nel Recupero degli oggetti digitali
Utente	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

Torna al sommario

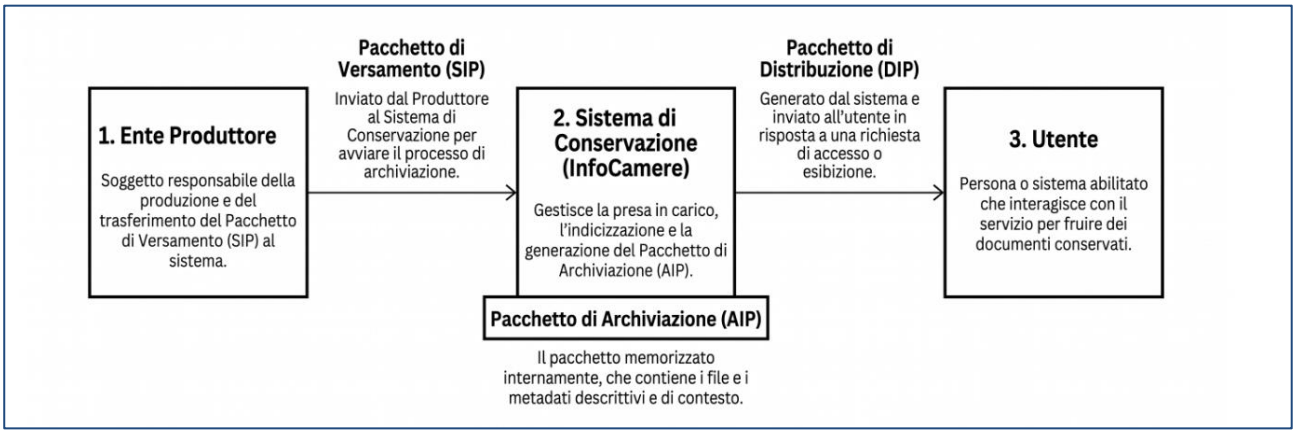
4 Modello Organizzativo

L'Azienda Speciale Servizi alle Imprese di Trapani ha affidato il servizio di conservazione a InfoCamere S.P.c.A, società delle Camere italiane per l'innovazione digitale, iscritta nel Marketplace dei servizi di conservazione e in possesso dei requisiti di qualità, di sicurezza e organizzazione individuati nel rispetto della disciplina europea, delle Linee guida di cui all'art 71 relative alla formazione, gestione e conservazione dei documenti informatici, nonché del regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici emanato da Agid.

La scelta adottata dall'Ente è quella del modello in outsourcing.

Di seguito vengono riportate graficamente le principali caratteristiche del modello organizzativo adottato, in conformità al modello funzionale OAIS:

Figura 1 - Modello organizzativo



5 Ruoli e responsabilità

Titolare dell'oggetto di conservazione

L'Ente è il titolare dei contenuti digitali posti in conservazione e, attraverso il proprio Responsabile della conservazione, definisce e attua le politiche complessive del Sistema di conservazione governandone la gestione con piena responsabilità ed autonomia.

L'Ente, titolare dell'oggetto della conservazione, versa a InfoCamere Scpa gli oggetti digitali da conservare individuati al punto 1 del presente Manuale. Tale versamento avviene in continuità con il processo di gestione documentale iniziato nella fase corrente.

I rapporti tra Produttore e Conservatore, sono formalizzati e regolati per mezzo di alcuni documenti fondamentali:

1. Convenzione per l'affidamento del servizio di conservazione dei documenti informatici
2. Accordo sul trattamento dei dati personali ai sensi dell'art. 28 del Regolamento (UE) 2016/679, nell'ambito del servizio di conservazione dei documenti informatici.
3. Specifiche tecniche pubblicate sul portale https://conservazione.infocamere.it.

I nominativi delle altre figure coinvolte e la descrizione delle principali attività svolte da coloro che hanno ruoli organizzativi all'interno del soggetto produttore sono indicati nel Manuale di gestione documentale.

Sono affidate a InfoCamere Scpa le fasi del processo di conservazione individuate al punto 4.5 delle Linee Guida.

Restano in capo al Responsabile della conservazione dell'Ente i restanti compiti e cioè:

- definire le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;

- assicurare la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite.

L'Ente mantiene la titolarità e la proprietà dei documenti depositati ed è responsabile del contenuto del pacchetto di versamento ed è obbligata a trasmetterlo al servizio di conservazione secondo le modalità operative descritte nel presente Manuale e nel suo allegato.

Produttore dei pacchetti di versamento (SIP)

Le Linee Guida Agid identificano il Produttore dei pacchetti di versamento (SIP) con il Responsabile della gestione documentale. Il Produttore dei pacchetti di versamento è responsabile della generazione e della trasmissione del loro contenuto nel sistema di conservazione. Provvede inoltre a verificare il buon esito della operazione di trasferimento al sistema di conservazione tramite la presa visione del rapporto di versamento prodotto dal sistema di conservazione stesso.

Conservatore / InfoCamere

InfoCamere opera quale Conservatore esterno ai sensi delle Linee Guida Agid e assume il ruolo di responsabile del trattamento dei dati come Previsto dal Codice in materia di protezione dei dati personali, garantendo il rispetto dei requisiti previsti dalle norme in vigore nel tempo per i Sistemi di conservazione, e svolge l'insieme delle attività elencate nel paragrafo 4.7 delle Linee Guida Agid.

Il sistema di conservazione InfoCamere prevede la materiale conservazione dei dati e delle copie di sicurezza sul territorio nazionale e l'accesso dei dati presso le strutture dedicate allo svolgimento del servizio di conservazione o la sede del produttore.

InfoCamere, come Soggetto conservatore e in conformità a quanto previsto dalla normativa vigente:

- Rispetta i requisiti organizzativi, di qualità e sicurezza previsti da AgID ed offre idonee garanzie organizzative e tecnologiche per lo svolgimento delle funzioni affidategli.
- Svolge i suoi compiti avvalendosi di persone che per competenza ed esperienza, garantiscono la corretta esecuzione delle operazioni.
- Prevede la materiale conservazione dei dati e delle copie di sicurezza sul territorio nazionale e l'accesso dei dati presso le strutture dedicate allo svolgimento del servizio di conservazione o la sede del produttore.

Utente abilitato

Le Linee Guida Agid identificano l'utente abilitato come una persona, ente o sistema, che interagisce con i servizi di un sistema per la conservazione di documenti informatici. L'utente può essere interno o esterno all'Ente produttore. Gli utenti abilitati al sistema di conservazione sono interni all'Ente.

L'utente richiede al sistema di conservazione l'accesso ai documenti informatici per acquisire le informazioni di interesse nei limiti previsti dalla legge. Il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, ai documenti informatici conservati e consente la produzione di un pacchetto di distribuzione (DIP) direttamente acquisibile dai soggetti autorizzati.

In termini OAIS la comunità degli utenti può essere definita come comunità di riferimento.

Il Responsabile della conservazione

Nella Pubblica Amministrazione il responsabile della conservazione è un ruolo previsto dall'organigramma del Titolare dell'oggetto di conservazione; viene nominato con atto formale tra i dirigenti e i funzionari interni in possesso di idonee competenze giuridiche, informatiche ed archivistiche e può essere svolto dal responsabile della gestione documentale o dal coordinatore della gestione documentale, ove nominato.

Il Responsabile della conservazione, coadiuvato dal Responsabile del sistema di conservazione:

a) definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il

Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;

b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;

c) genera e sottoscrive il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;

d) genera e sottoscrive il pacchetto di distribuzione (DIP) con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;

e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;

f) effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;

g) 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;

h) provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;

i) predispone le misure necessarie per la sicurezza fisica e logica del sistema di conservazione come previsto dal par. 4.11 delle Linee Guida Agid;

j) 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;

k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;

l) provvede per le amministrazioni statali centrali e periferiche a versare i documenti informatici, le aggregazioni informatiche e gli archivi informatici, nonché gli strumenti che ne garantiscono la consultazione, rispettivamente all'Archivio centrale dello Stato e agli archivi di Stato territorialmente competenti, secondo le tempistiche fissate dall'art. 41, comma 1, del Codice dei beni culturali

m) predispone il manuale di conservazione di cui al par. 4.7 e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

L'Ente ha individuato il Responsabile della conservazione nel Vicedirettore, Alessandro Carollo, nominato con Determina del Direttore n. 2 del 18/02/2021

Il Responsabile della conservazione condivide il Manuale della conservazione con il Conservatore e con tutti i soggetti coinvolti nel processo di conservazione, a cui comunica tempestivamente ogni eventuale modifica.

5.1 Ruoli

Nella tabella successiva vengono indicati i nominativi delle persone fisiche e/o giuridiche che ricoprono i ruoli indicati nel sistema di conservazione.

Ruoli	Nominativo	periodo nel ruolo	eventuali deleghe
Responsabile della conservazione	Alessandro Carollo	Dal 18/02/2021	
Vicario		Dal	
Soggetto Conservatore	InfoCamere	Dal 23/11/2026	

5.2 Pubblico Ufficiale

Il ruolo di pubblico ufficiale che, come previsto dall'art. 23 bis, comma 2 del Decreto Legislativo 7 marzo 2005, n. 82 - Codice dell'Amministrazione Digitale, attesti la conformità all'originale di copie di documenti informatici conservati nel sistema gestito da InfoCamere Scpa, è svolto dal Responsabile della conservazione e dal suo vicario.

Torna al sommario

6 Organismi di tutela e di vigilanza

Gli archivi e i singoli documenti prodotti dall'Ente sono beni culturali e sottoposti, pertanto, alle disposizioni di tutela previste dal Codice dei beni culturali.

Il rispetto delle disposizioni in ordine alla corretta conservazione è in capo al Ministero della Cultura, attraverso la Direzione generale archivi e, in particolare, alla Soprintendenza archivistica e bibliografica della Regione Sicilia. Tale ente, infatti, è investito del potere di vigilanza e ispezione ai sensi degli artt. 18 e 19 del predetto Codice.

Per quanto riguarda il Sistema di conservazione dell'Ente Azienda Speciale Servizi alle Imprese di Trapani la Soprintendenza archivistica e bibliografica territorialmente competente verifica, in particolare, che il processo di conservazione avvenga in modo conforme alla normativa e ai principi di corretta e ininterrotta custodia: autorizza l'affidamento dei documenti e degli archivi a un servizio di conservazione esterno e l'avvio delle operazioni di scarto archivistico.

Il legislatore ha previsto un secondo ente che, in materia di conservazione digitale, lavora a fianco delle Soprintendenza avendo però un ruolo diverso: l'Agenzia per l'Italia digitale

(AgID). AgID ha il compito di svolgere le necessarie attività di verifica circa il rispetto dei requisiti richiesti ai soggetti che intendono erogare il servizio di conservazione per conto delle pubbliche amministrazioni.

I requisiti sono stabiliti dal Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici che segna il superamento del precedente meccanismo di accreditamento dei conservatori.

L'attività di vigilanza dell'AgID riguarda, quindi, il soggetto che eroga il servizio di conservazione e il Sistema di conservazione nel suo complesso, inteso cioè come l'insieme di regole, di procedure e di tecnologie idonee ad assicurare la corretta conservazione dei documenti e dei fascicoli informatici e dei relativi metadati, in ogni fase della vita del documento, dalla presa in carico fino allo scarto.

Torna al sommario

7 Attivazione del servizio

7.1 Affidamento del servizio

Il Responsabile della conservazione ha affidato il processo di conservazione degli oggetti digitali di cui l'Ente è titolare ad InfoCamere, attraverso la sottoscrizione della convenzione per l'affidamento del servizio di conservazione a norma dei documenti informatici avvenuta in data 23/11/2026 e con termine 31/12/2029.

7.2 Accesso al servizio

Nel modello organizzativo adottato dall'Ente, gli utenti abilitati ai Servizi documentali dell'Ente accedono al sistema di conservazione limitatamente ai documenti smistati o prodotti dall'ufficio di appartenenza e, comunque, ai documenti alla cui visibilità siano stati abilitati.I servizi documentali:

- generano i pacchetti di versamento;
- integrano l'applicazione per l'esibizione dei contenuti conservati, in grado di generare i pacchetti di distribuzione.

L'accesso al sistema di conservazione è consentito, agli utenti abilitati, anche tramite il Portale della Conservazione (http://conservazione.infocamere.it).

Sono abilitati al Portale della Conservazione il Responsabile della conservazione e il suo vicario.

7.3 Descrizione del servizio

La descrizione del servizio di conservazione, comprensiva di tutte le componenti tecnologiche, fisiche e logiche, è presente nel Manuale di conservazione del Conservatore.

Torna al sommario

8 Oggetti sottoposti a conservazione

Gli oggetti sottoposti a conservazione ricomprendono tutti i documenti informatici prodotti dall'Ente produttore secondo le indicazioni previste nel manuale di gestione dei documenti dell'ente, per legge o dalla prassi archivistica. La lista delle tipologie degli oggetti conservati e dei tempi di conservazione è presente nell'allegato 1 "Tempi di conservazione, classi di contenuto, formati e visualizzatori".

I documenti informatici devono essere statici, in particolare non devono contenere elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione

Il servizio di conservazione permette la conservazione di file PDF e XML firmati digitalmente e marcati temporalmente, supportando i seguenti standard: P7M (CAdES), PAdES (per i file PDF), M7M, TSD. I Servizi documentali InfoCamere garantiscono la validità dei documenti sottoscritti digitalmente e la marcatura temporale, la cui validità pertanto non viene verificata dal sistema di conservazione.

L'Ente, in qualità di Titolare dell'oggetto della conservazione, determina la relazione di appartenenza tra i documenti che costituiscono l'unità documentaria e l'unità archivistica, mentre InfoCamere Scpa, nella sua qualità di Conservatore, in un secondo momento, si fa carico di mantenere stabili, consultabili e contestualizzate nel tempo tali informazioni, secondo i parametri definiti nel suo Manuale di conservazione e nella Convenzione di servizio.

8.1 Formati

Secondo quanto previsto nella convenzione di servizio, l'Ente trasferisce gli oggetti digitali da sottoporre a conservazione, nei modi e nelle forme definite da InfoCamere Scpa, tramite il sistema di gestione documentale GeDoc. L'Ente garantisce l'autenticità e l'integrità della documentazione nelle fasi di produzione e di archiviazione corrente, effettuata nel rispetto delle Linee Guida. In particolare garantisce che il trasferimento dei documenti informatici sia realizzato utilizzando formati compatibili con la funzione di conservazione e rispondenti a quanto previsto dalla normativa vigente.

D'accordo con il Conservatore, è prevista la conservazione di formati non standard, la cui conservazione a lungo termine non è tuttavia garantita. L'elenco di tali formati è indicata nell'allegato al presente Manuale.

Le tipologie di formato adottate e gestite dall'Ente produttore ed inviate in conservazione sono dettagliate nell'allegato 1 "Tempi di conservazione, classi di contenuto, formati e visualizzatori".

Il Servizio di conservazione InfoCamere garantisce la conservazione a norma solo dei formati ritenuti idonei alla conservazione, secondo quanto previsto nell'allegato 2 delle Linee Guida

L'Ente ha adottato i formati idonei alla conservazione presenti nell'allegato 2 delle Linee Guida in quanto questi forniscono le caratteristiche di apertura, sicurezza, portabilità, funzionalità, diffusione, leggibilità nel tempo e supporto allo sviluppo.

In casi eccezionali, l'Ente utilizza formati non presenti in tale lista in virtù di considerazioni sui:

- vincoli tecnici;
- specificità del formato;
- durata della conservazione richiesta dalla tipologia documentale.

Per questi formati, l'Ente fornirà ad InfoCamere indicazioni del relativo visualizzatore, nel rispetto dei diritti di proprietà intellettuale ed eventuali restrizioni nell'utilizzo del software.

8.2 Classe di contenuto

Vengono approvate le modalità di conservazione dei documenti descritte nel manuale di conservazione InfoCamere secondo la logica archivistica di 'unità documentarie' e 'unità archivistiche'.

Con classe di contenuto si intende l'insiemi di dati (metadati) da associare alla 'unità documentarie' e alla 'unità archivistiche' per identificarle e descriverne il contesto, il contenuto, la struttura. Tali informazioni sono presenti nei pacchetti di versamento, archiviazione e distribuzione del sistema di conservazione.

La lista delle tipologie degli oggetti conservati e dei tempi di conservazione è presente nell'allegato 1 "Tempi di conservazione, classi di contenuto, formati e visualizzatori".

Le tipologie sono aggiornate in funzione delle classi di contenuto utilizzate dai Servizi documentali in uso presso l'Ente.

Torna al sommario

9 Il processo di conservazione

I principali processi del servizio di conservazione sono:

- conservazione;
- esibizione;
- produzione di duplicati e copie informatiche;
- procedura di scarto.

9.1 Conservazione

Il processo di conservazione opera secondo le seguenti fasi:

- Formazione e trasmissione del pacchetto di versamento (SIP) da parte dell'Ente produttore;
- Presa in carico del pacchetto di versamento (SIP) da parte del sistema di conservazione;
- Indicizzazione e generazione del pacchetto di archiviazione (AIP).

Di seguito, si riportano i dettagli delle suddette fasi.

9.1.1 Formazione e Trasmissione del Pacchetto di versamento (SIP)

Il Responsabile della gestione documentale dell'Ente produce i pacchetti di versamento attraverso i Servizi documentali InfoCamere e li invia al sistema di conservazione.

I pacchetti di versamento contengono un'unità archivistica (UA) o un'unità documentaria (UD) secondo quanto previsto nel Manuale della conservazione di InfoCamere.

I tempi di versamento in conservazione delle unità archivistiche e delle unità documentarie variano in funzione della tipologia di contenuto e del sistema versante utilizzato.

Al fine di garantirne il costante aggiornamento in caso di variazioni tecniche o normative, il dettaglio dei tempi esatti entro i quali le diverse tipologie di oggetti digitali gestite dall'Ente vengono trasferite al sistema di conservazione è definito e mantenuto aggiornato all'interno dell'**Allegato 1 "Tempi di conservazione, classi di contenuto, formati e visualizzatori".**

9.1.2 Presa in carico del Pacchetto di versamento (SIP) da parte del sistema di conservazione

Il sistema di conservazione effettua il controllo del pacchetto di versamento (SIP) ricevuto. La lista dei controlli automatici effettuati sul pacchetto di versamento (SIP) è riportata nel manuale di conservazione di InfoCamere e nelle specifiche tecniche allegate alla convenzione per l'affidamento del servizio.

Nel caso in cui l'insieme dei controlli abbia avuto esito negativo, il sistema di conservazione comunica al Servizio documentale InfoCamere l'errore riscontrato.

Nel caso in cui l'insieme dei controlli abbia avuto esito positivo, il sistema di conservazione genera un rapporto di versamento verso il Servizio documentale InfoCamere e il pacchetto è preso in carico dal sistema.

9.1.3 Indicizzazione e generazione del pacchetto di archiviazione (AIP)

L’indicizzazione dei contenuti e la generazione del pacchetto di archiviazione (AIP) viene descritta nel Manuale della conservazione di InfoCamere.

9.2 Esibizione

L’esibizione dei documenti conservati dal sistema di conservazione avviene tramite l’apposita applicazione web di esibizione dei documenti conservati, integrata con i Servizi documentali utilizzati dall’Ente. L’esibizione di un documento tramite tale funzione è permesso agli operatori del Titolare dell’oggetto di conservazione abilitati nel Servizio documentale alla gestione/trattamento del documento.

In caso di richiesta di esibizione a norma di documenti conservati da parte di un utente esterno al Soggetto produttore, o interno ma non abilitato alla generazione di pacchetti di distribuzione, è in carico al Responsabile della conservazione:

- valutare la richiesta e generare i pacchetti di distribuzione in base a quanto richiesto, accedendo direttamente al sistema o delegando la generazione dei pacchetti ad utenti dell’Ente produttore abilitati;
- mettere a disposizione il contenuto dei pacchetti di distribuzione al richiedente.

9.3 Produzione di duplicati informatici

Ai sensi della normativa vigente e delle Linee Guida AgID, per "duplicato informatico" si intende un documento ottenuto mediante la memorizzazione della medesima sequenza di bit (evidenza informatica) dell'originale. Avendo struttura informatica e contenuto identici, il duplicato mantiene il medesimo e assoluto valore giuridico e probatorio del documento informatico da cui è tratto, senza necessità di ulteriori attestazioni di conformità.

La produzione e l'estrazione dei duplicati informatici avvengono tramite l’apposita applicazione web di esibizione, integrata nel Servizi di gestione documentale in uso o tramite portale della conservazione.

A garanzia dell'inalterabilità del dato e del mantenimento del contesto archivistico, il sistema di conservazione non restituisce all'utente il singolo file isolato, ma elabora la richiesta generando in tempo reale un Pacchetto di Distribuzione (DIP). Tale pacchetto informativo, scaricabile dall'utente abilitato, racchiude al suo interno non solo l'oggetto digitale richiesto (il duplicato), ma anche:

- L'insieme delle informazioni di conservazione, inclusi i metadati associati al documento;
- L'Indice di conservazione, firmato digitalmente e marcato temporalmente dal Conservatore;
- Il rapporto di versamento.

In questo modo, la consegna del Pacchetto di Distribuzione fornisce all'Ente o agli organi ispettivi tutte le evidenze informatiche e crittografiche necessarie per dimostrare la perfetta corrispondenza tra il duplicato estratto e il documento originariamente versato in conservazione.

È in carico al Soggetto Produttore:

- valutare i casi in cui sia richiesto produrre copie conformi;
- produrre le copie e richiedere, quando necessario, la presenza di un pubblico

ufficiale. L'attestazione di conformità, anche nel caso sia necessario un cambio di formato, rimarrà a carico dell'Ente Produttore.

Il sistema di conservazione prevede appositi metadati per il tracciamento delle operazioni di riversamento e versamento di copie informatiche (in particolare attraverso l'attributo di relazione isFormatOf) che permettono di memorizzare e mantenere stabile il legame tra le diverse versioni delle unità documentarie.

9.4 Produzione di copie informatiche

È in carico al Soggetto Produttore:

- valutare i casi in cui sia richiesto produrre copie conformi;
- produrre le copie e richiedere, quando necessario, la presenza di un pubblico ufficiale. L'attestazione di conformità, anche nel caso sia necessario un cambio di formato, rimarrà a carico dell'Ente Produttore.

Il sistema di conservazione prevede appositi metadati per il tracciamento delle operazioni di versamento di copie informatiche che permettono di memorizzare il legame tra le diverse versioni delle unità documentarie.

9.5 Scarto degli oggetti digitali

Il "Piano di fascicolazione e conservazione" allegato al Manuale di gestione documentale dell'Ente stabilisce i tempi trascorsi i quali le diverse tipologie di oggetti digitali possono essere scartate. Il responsabile della conservazione genera l'elenco dei pacchetti di archiviazione contenenti i documenti destinati allo scarto e, dopo aver verificato il rispetto dei termini temporali stabiliti dal piano di conservazione, lo comunica al responsabile della gestione documentale.

Nel rispetto del Decreto 42/2004, è in carico al Responsabile della gestione documentale fornire alla Soprintendenza archivistica competente la lista dei contenuti da scartare. Il Responsabile della gestione documentale, una volta ricevuto il nulla-osta della Soprintendenza archivistica provvede ad adeguare, se necessario, l'elenco di scarto e le sue modalità alle decisioni dell'autorità.

Il Responsabile della gestione documentale trasmette al Conservatore la lista degli identificativi dei contenuti da scartare, alla quale dovrà allegare anche l'autorizzazione allo scarto rilasciata dalla Soprintendenza archivistica in maniera tale da consentire il tracciamento dell'operazione di scarto sul sistema.

Al termine delle operazioni di eliminazione dal sistema di conservazione dei pacchetti di archiviazione scartati, l'Ente notifica l'esito della procedura di scarto agli organi preposti alla tutela come già indicato in precedenza.

Lo scarto avrà efficacia solo al momento del completo aggiornamento delle copie di sicurezza del sistema.

I documenti e le aggregazioni documentali informatiche sottoposti a scarto nel sistema di conservazione saranno eliminati anche da tutti i sistemi gestiti dall'Ente.

9.6 Verifiche d'integrità

L'Ente affida al Soggetto Conservatore il compito di verificare periodicamente l'integrità

degli archivi. Il Responsabile della conservazione può richiedere al Conservatore l'evidenza dei controlli eseguiti.

9.7 Recesso

Nel caso in cui l'Ente intenda recedere dalla convenzione per l'affidamento del servizio di conservazione, le modalità operative, le tempistiche e le specifiche tecniche di trasferimento dell'archivio sono integralmente demandate all'apposito documento "Piano di Esportazione" (o "Exit Plan"), parte integrante e sostanziale della Convenzione/Condizioni di servizio di conservazione sottoscritta con il Soggetto conservatore al quale si rimanda per ulteriori dettagli.

Le modalità di esportazione e di trasferimento dell'archivio sono stabilite nel documento "Exit Plan/Piano di esportazione", parte integrante e sostanziale della Convenzione/Condizioni di servizio di conservazione al quale si rimanda per ulteriori dettagli.

In fase di recesso e transizione, le responsabilità e le attività in capo all'Ente e al suo Responsabile della Conservazione prevedono i seguenti adempimenti:

1. Individuazione del conservatore subentrante e blocco dei versamenti: l'Ente, in qualità di Titolare dell'oggetto di conservazione, individua un nuovo conservatore subentrante, designandolo formalmente quale Responsabile del Trattamento ai sensi dell'art. 28 del GDPR. Per consentire l'avvio delle attività di trasferimento, l'Ente interromperà l'invio di nuovi pacchetti di versamento verso il Sistema di conservazione.

2. Trasferibilità dei dati e download degli archivi: Il Responsabile della Conservazione comunica al conservatore uscente il referente autorizzato al recupero dei dati ed effettua le necessarie operazioni di verifica e controllo sui pacchetti scaricati.

3. Passaggio di responsabilità: Il Responsabile della Conservazione concorre alla redazione del formale rapporto di consegna per attestare il passaggio di responsabilità giuridica dell'archivio. A verifiche concluse, autorizza il conservatore uscente alla cancellazione definitiva dei dati dai propri sistemi.

4. Comunicazione agli Organi di Tutela: l'Ente comunicherà formalmente alla Soprintendenza Archivistica e Bibliografica competente per territorio il trasferimento del proprio archivio ad altro Soggetto conservatore.

Torna al sommario

10 Sicurezza del Sistema di Conservazione

Questa sezione costituisce un quadro generale dell'Ente rispetto alle politiche di sicurezza delle informazioni e protezione dei dati personali, implementate per assicurare una corretta gestione della sicurezza del sistema di conservazione dei documenti informatici.

In gran parte integra e fa riferimento alle misure di sicurezza tecniche ed organizzative descritte nel Manuale di Conservazione e nel Piano della Sicurezza predisposti e mantenuti aggiornati da InfoCamere, in qualità di Soggetto Conservatore al quale l'Ente rinvia per quanto non di competenza.

10.1 Quadro normativo di riferimento

Come indicato nella determinazione n. 407/2020 con cui AgID ha adottato le "Linee guida per la formazione, gestione e conservazione dei documenti informatici", il Responsabile della Conservazione di concerto il Responsabile della sicurezza e con il Responsabile della transizione digitale, acquisito il parere del Responsabile della protezione dei dati personali, provvede a predisporre, nell'ambito del piano generale della sicurezza, il piano della sicurezza del sistema di conservazione, mettendo in atto opportune misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali, ai sensi dell'art. 32 del Regolamento (UE) 2016/679 e con riferimento alle misure di sicurezza in materia di cybersicurezza per la Pubblica Amministrazione.

Fatta questa premessa, nell'ambito dell'inquadramento normativo della "Conservazione dei documenti informatici", l'Ente ha stipulato una convenzione con un soggetto esterno che offre le garanzie organizzative e tecnologiche prescritte dalla legge (articolo 44. Requisiti per la gestione e conservazione dei documenti informatici del D.Lgs. 07/03/2005, n. 82), attribuendo il ruolo di Conservatore (quindi la qualifica di responsabile del servizio di conservazione), con la finalità di affidare la conservazione dei propri documenti informatici, ad InfoCamere S.C.p.A., società consortile di informatica delle Camere di commercio Italiane.

10.2 Principali riferimenti e collegamenti

Alla data di revisione, l'elenco dei principali riferimenti in materia di sicurezza delle informazioni (a cui si rimanda per approfondimenti a seconda delle varie aree coinvolte) è costituito da:

- **Piano della Sicurezza del Sistema di Conservazione**
  Documento predisposto, mantenuto ed aggiornato dal Soggetto Conservatore (in osservanza alle linee guida AgID) che, nell'ambito del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il Sistema di Conservazione dei documenti informatici da possibili rischi cui sono soggetti (la perdita o non adeguatezza delle caratteristiche di riservatezza, integrità e disponibilità) ossia, nello specifico, in grado di mantenere nel tempo i documenti correttamente conservati preservando le specifiche proprietà di: reperibilità, autenticità, integrità, affidabilità e leggibilità.

- **Piano Generale della Sicurezza dell'Ente**
  Documento che pianifica le attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione, in osservanza delle Linee Guida dell'Agenzia per la Cybersicurezza Nazionale (ACN) in materia di cyber risk management e security by design."

- **Piano della Sicurezza del Sistema di Gestione Informatica dei Documenti**
  Documento predisposto, mantenuto ed aggiornato dall'Ente (in osservanza alle linee guida AgID) che, nell'ambito del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere i dati elaborati ed ospitati, le infrastrutture, le applicazioni e i servizi del Sistema di Gestione Informatica dei Documenti da possibili rischi cui sono soggetti (la perdita o non adeguatezza delle caratteristiche di riservatezza, integrità e disponibilità).

10.3 Organizzazione sicura della Conservazione dei documenti informatici

Nell'erogazione del servizio di conservazione, InfoCamere tiene conto del modello OAIS (Open Archival Information System), ovvero come descritto AgiD "una struttura organizzata di persone e sistemi che accetti la responsabilità di conservare l'informazione e di renderla disponibile per una comunità di riferimento".

A titolo esemplificativo, di seguito si rappresenta un quadro di riferimento riassuntivo dei ruoli e ambiti considerati per la valutazione dei livelli di sicurezza e privacy del servizio digitale.

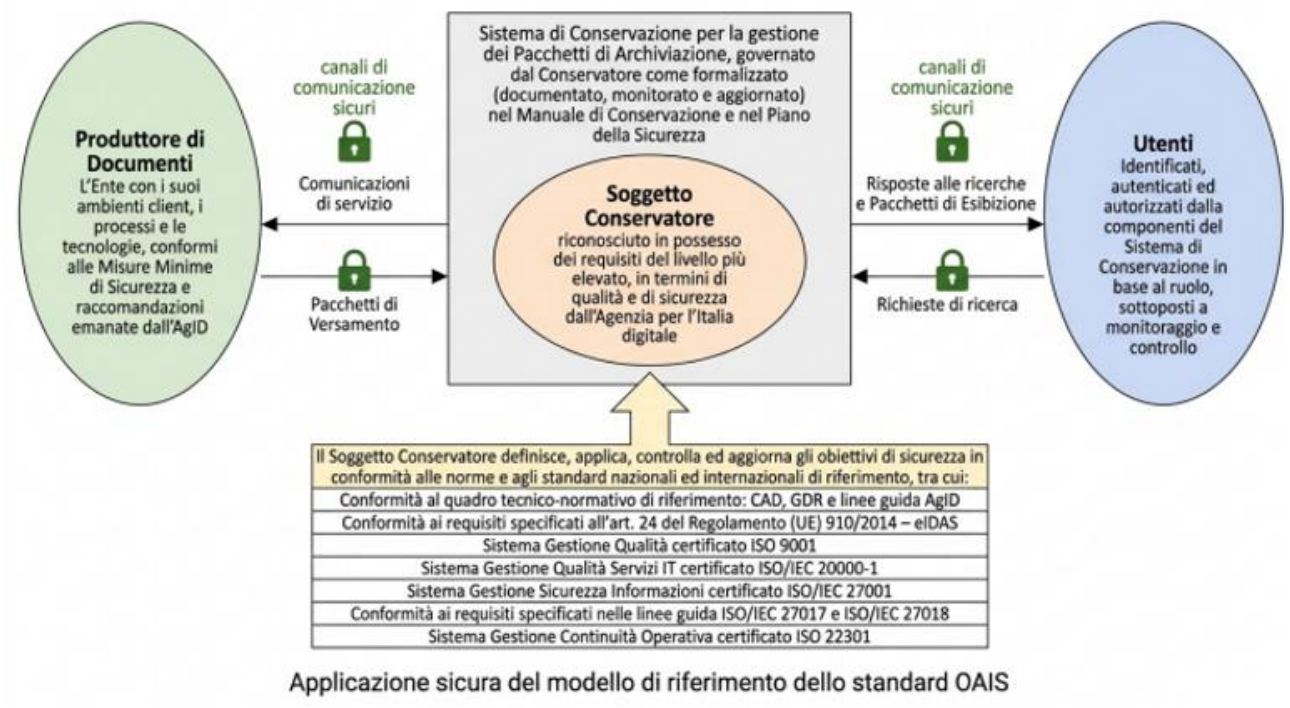


Figura 2 - Ruoli e ambiti considerati per la valutazione dei livelli di sicurezza e privacy

10.4 Obiettivi delle misure di sicurezza

Come riferimento per le indicazioni relative all'adeguatezza delle misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento sicuro, nel tempo, del Sistema di Conservazione amministrato dal Soggetto Conservatore si tiene conto:

- del contesto e delle finalità del processo di conservazione digitale che assicura di conservare a norma i documenti informatici, ossia garantire autenticità, integrità, affidabilità, leggibilità e reperibilità dei documenti conservati;
- dell'adeguatezza e competenze, del Soggetto Conservatore, in relazione alle certificazioni acquisite e all'aderenza al quadro normativo di riferimento e agli schemi e linee guida AgID, richiesti e utili ad un sistema per essere qualificato come sistema di gestione di governo della sicurezza informazioni e protezione dati personali, affidabile e garantito;
- dell'adeguatezza del livello di sicurezza delle informazioni e protezione dei dati personali, realizzato con idonee misure tecniche ed organizzative, per mitigare i rischi che derivano dalla distruzione, dalla perdita, dall'alterazione, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, dalla indisponibilità a dati e informazioni trasmessi, conservati o comunque trattati da sistemi e infrastrutture;
- di un'adeguata e formalizzata procedura di notifica di violazione dei dati personali all'autorità di controllo e quella di comunicazione di una violazione dei dati personali all'interessato;
- della formazione e consapevolezza del personale autorizzato in materia di sicurezza delle informazioni e protezione dei dati personali trattati;
- del monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza tecniche ed organizzative applicate.

10.5 Controllo accessi al sistema di conservazione

Sono stabilite le regole finalizzate a proteggere dall'accesso non autorizzato in modo da salvaguardare la riservatezza e prevenire trattamenti non autorizzati di utenti che non possiedono i necessari diritti.

InfoCamere pone attenzione nella gestione delle utenze e dei profili di accesso definendo policy e procedure di riferimento; garantisce che il sistema sia sicuro ed affidabile e che i dati e le applicazioni ospitate siano protette ed accessibili solo agli utenti autorizzati.

L'Ente, ha messo in atto controlli per limitare in modo efficace l'accesso al sistema solo al personale in possesso di un legittimo requisito nel rispetto del principio per cui l'accesso ai dati e ai sistemi per mezzo di applicazioni informatiche deve essere limitato a quanto strettamente necessario per la prestazione delle attività richieste.

Le identità e le credenziali di accesso per gli utenti autorizzati sono gestite, periodicamente verificate e revocate. I diritti di accesso e le autorizzazioni sono gestite secondo il principio del privilegio minimo e separazione delle funzioni.

10.6 Principali impostazioni sicure delle postazioni di lavoro e di comportamento utenti

L'uso delle postazioni di lavoro configurato secondo le migliori pratiche sicurezza (es. anti-malware, disattivazione di servizi non necessari, etc.) del software installato e certificato, aggiunto alla gestione dei permessi sulle singole utenze, consente un controllo effettivo sull'uso improprio degli strumenti di lavoro e sul divieto di installare software pericoloso e non ritenuto affidabile dall'Ente.

- L'Ente promuove al personale autorizzato l'assunzione di responsabilità del corretto utilizzo delle dotazioni informatiche assegnate, evidenziando come ogni impiego inopportuno rispetto ai compiti ed alle attività lavorative assegnate può contribuire a provocare disservizi e malfunzionamenti e minacce alla sicurezza ed alla protezione dei dati trattati.
- Rimandando alla consultazione dei riferimenti indicati nella sezione "8.2 Riferimenti e collegamenti", di seguito si riportano alcune regole e precauzioni di base:
- Consapevolezza del proprio ruolo e delle responsabilità e contribuire al corretto e sicuro utilizzo delle risorse assegnate, segnalando qualsiasi evento non conosciuto che potrebbe compromettere sistemi, applicazioni e dati trattati;
- Impegno a tenere comportamenti tali da ridurre il rischio di attacco al sistema mediante software malevoli (sono tipici esempi di comportamento consapevole; non aprire mail o relativi allegati sospetti, non navigare su siti non riconosciuti come affidabili, non condividere credenziali di accesso, e così via);
- Aggiornamento periodico delle componenti applicative e del sistema anti-malware adottato;
- Limitazione della connettività a dispositivi sconosciuti/non identificati;
- Configurazione sicura delle postazioni di lavoro (sia fisica che virtuale);
- Servizi di auditing attivabili all'occorrenza sulle postazioni di lavoro;
- Non condividere codici di autenticazione e rispettare le policy di riferimento;
- Non condividere in modo incontrollato dati personali e informazioni che possano compromettere la sicurezza e la riservatezza di individui o dell'Ente.

10.7 Indicazioni sulla protezione dei dati personali e conformità al GDPR

Il servizio di Conservazione dei documenti informatici implica il trattamento di dati di varia natura e sensibilità tra cui quelli personali ossia le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica etc. Queste operazioni richiedono l'osservanza del quadro normativo in materia di protezione dati personali e la valutazione delle potenziali minacce (violazione e perdita del controllo dei dati), considerando che tali dati sono classificabili in varie tipologie che, a seconda della loro sensibilità, devono essere trattati con cautele e regole diverse, tenendo conto della valutazione preventiva, realizzata dal Titolare del trattamento e delle conseguenze del trattamento dei dati sulle libertà e i diritti degli interessati.

Il Soggetto Conservatore InfoCamere, ha stabilito un modello organizzativo per protezione dei dati personali e svolge operazioni di trattamento sui dati di titolarità dei Soggetti Produttori solo sulla base di una nomina formale a Responsabile del Trattamento, ai sensi dell'art. 28 del Regolamento UE 2016/679, adottando adeguate misure tecniche ed organizzative per garantire la riservatezza, l'integrità e la disponibilità dei dati personali per tutta la durata contrattuale, in osservanza degli aspetti legali, del quadro normativo nazionale ed europeo di riferimento e coerentemente con i provvedimenti dell'autorità che esercita il controllo sul rispetto della disciplina in materia di protezione dei dati personali .
Di seguito si riportano le principali strategie e interventi adottati:

- L'architettura del Sistema di Conservazione è costituita da risorse informatiche ospitate, presso Data Center localizzati in Europa. Sono attuate misure di sicurezza fisica per proteggere dall'accesso non autorizzato e da rischi ambientali i locali, data center e aree sensibili.
- Definiti ruoli e responsabilità (interni ed esterni), inclusa la gestione delle responsabilità ed il controllo di eventuali Fornitori esterni / Sub fornitori di cui il Conservatore si riserva la possibilità di avvalersi per l'esecuzione di operazioni, singole attività, servizi relativi a funzioni o fasi del processo di conservazione che per conoscenza, esperienza, capacità e affidabilità forniscano idonee garanzie certificate.
- Nominata la figura del DPO che riporta alla Direzione, svolgendo compiti indicati nel Regolamento UE 679/2016.
- Stabilito un Piano formativo periodico specifico su aspetti di sicurezza durante il trattamento di dati personali.
- Definita una procedura finalizzata a descrivere i trattamenti, valutarne l'adeguatezza e contribuire alla gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dai trattamenti.
- Individuate ed applicate le misure tecniche ed organizzative adeguate e proporzionate al trattamento dei dati personali, in modo sistematico, ricorrendo ad un approccio basato sui rischi.
- Predisposte informative privacy e cookie policy, chiare ed adeguate, la raccolta e gestione dei consensi qualora necessario, le modalità di divulgazione e trasferimento dati, i diritti di proprietà intellettuale.
- Procedura di monitoraggio e controllo di conformità delle misure di sicurezza a quanto stabilito nelle policy aziendali, in particolare dedicando molta attenzione agli aspetti di gestione accessi e della trasmissione dei dati con l'utilizzo di meccanismi (applicazione di criteri password complesse) e protocolli affidabili e sicuri alle risorse ICT utilizzate (Infrastrutture, Dati, Applicazioni e Servizi), garantendo che siano protette e accessibili solo alle utenze autorizzate e certificate con criteri basati sui ruoli e necessità di accesso, monitorate e controllate per identificare eventuali segnali di violazione e permettere di intervenire tempestivamente in caso di eventi anomali.
- Definito il processo e le politica per la segnalazione e gestione degli incidenti di sicurezza e l'individuazione delle vulnerabilità nei sistemi che trattano dati personali.
- Formalizzata la procedura con cui vengono gestite e comunicate le eventuali

violazioni di sicurezza tali da mettere in pericolo i diritti e le libertà degli individui, informando le Autorità competenti e i Titolari, secondo le tempistiche e le modalità indicate dalla normativa di riferimento.

- Definito il piano di continuità operativa e le procedure di backup e ripristino, valutate e collaudate regolarmente. In particolare, a tutela dall'eventuale compromissione dei dati derivante da attacchi informatici o ransomware, ci si avvale delle misure di sicurezza erogate dal Conservatore InfoCamere, il quale adotta rigorose politiche di salvataggio, proteggendo i dati in un repository di backup in cloud isolato e immutabile con una retention predefinita, all'interno del quale il dato viene criptato e reso accessibile esclusivamente agli amministratori dello strumento di backup; tali misure sono inoltre rafforzate da una validazione automatica e continua dei blocchi di storage per intercettare corruzioni o anomalie logiche, e da una replica asincrona e continua verso un sito di Disaster Recovery geograficamente separato.

Si rimanda ad approfondimenti e disposizioni contenute in politiche e procedure aziendali, regolamenti e standard a cui il Soggetto Conservatore InfoCamere aderisce, oltre a riferimenti individuati dall'Ente.

Torna al sommario

11 Il Portale della Conservazione e la documentazione del Conservatore

Tutti i dettagli relativi alle componenti tecnologiche, fisiche e logiche della quota parte del processo affidata in outsourcing sono integralmente descritti nel Manuale di conservazione del Conservatore redatto da InfoCamere.
Tale documento, unitamente a tutti gli strumenti fondamentali che regolano il servizio, è reso disponibile, consultabile e costantemente aggiornato all'interno del Portale della Conservazione, una piattaforma web sicura messa a disposizione da InfoCamere e raggiungibile all'indirizzo *https://conservazione.infocamere.it.*
All'interno di tale Portale, a cui sono abilitati ad accedere il Responsabile della Conservazione dell'Ente e i suoi delegati autorizzati, sono formalmente pubblicati e mantenuti:

- Il Manuale di conservazione del Conservatore (InfoCamere), che descrive l'infrastruttura, il modello di funzionamento e le misure di sicurezza.
- Le Specifiche Tecniche del servizio, che includono la lista aggiornata dei formati di file ammessi al versamento, l'elenco delle classi documentali gestite dal sistema e la definizione tecnica dei relativi metadati previsti.
- L'Area Comunicazioni, attraverso la quale il Conservatore pubblica tutte le comunicazioni rilevanti inviate al Soggetto produttore nelle modalità previste dalla convenzione, le integrazioni e le evoluzioni inerenti al servizio.
- Il Manuale utente del Portale (e dell'applicazione web di esibizione integrata), che illustra in dettaglio agli operatori dell'Ente le funzionalità operative, le modalità di navigazione, di ricerca e di utilizzo della piattaforma.