



PROVINCIA DI TREVISO

PROVINCIA DI TREVISO

Manuale di conservazione

INFORMAZIONI SUL DOCUMENTO

TITOLO	Manuale di Conservazione della Provincia di Treviso
VERSIONE	1.0
NOME FILE	Manuale_conservazione_conAllegati_v.1.pdf
REDAZIONE	Ing. Antonio Cianfrone - Dirigente Settore Innovazione Digitale e Servizi di Supporto, Responsabile della gestione documentale e della conservazione
VERIFICA	Segretario Generale dott. Giampietro Cescon Ing. Antonio Cianfrone - Dirigente Settore Innovazione Digitale e Servizi di Supporto, Responsabile della gestione documentale e della conservazione
APPROVAZIONE	Approvato con Decreto del Presidente n. 124 del 19/06/2026
DISTRIBUZIONE	Amministrazione Trasparente

STORIA DELLE MODIFICHE APPORTATE AL DOCUMENTO

VERSIONE	VARIAZIONI	DATA DI APPROVAZIONE
1.0	Prima emissione: Decreto Presidente n. 124 del 19/06/2026	19/06/2026

Indice generale

1. Principi generali.....	4
1.1 Premessa.....	4
1.2 Scopo e ambito di applicazione.....	4
1.3 Documento informatico.....	6
1.4 Documento amministrativo informatico.....	8
1.5 Il Sistema di conservazione.....	9
1.6 Definizioni e norme di riferimento.....	10
2. Modello organizzativo, ruoli e responsabilità.....	10
2.1 Modello organizzativo.....	10
2.2 Ruoli e responsabilità.....	11
2.2 a) Titolare dell'oggetto della Conservazione.....	11
2.2. b) Produttore di PdV.....	11
2.2 c) Utente abilitato.....	13
2.2 d) Responsabile della conservazione.....	13
2.2 e) Conservatore.....	15
2.3 Organismi di tutela e vigilanza.....	16
3. Struttura organizzativa per il servizio di conservazione.....	16
4. Oggetti sottoposti a conservazione.....	16
4.1 Oggetti sottoposti a conservazione presso Infocert Tinexta S.p.A.....	16
4.2 Oggetti sottoposti a conservazione presso Argentea S.r.L.....	20
5. Processo di conservazione.....	20
6. Il Sistema di conservazione.....	21
7. Monitoraggio e controlli.....	21
8. Selezione dei documenti e Piano di conservazione.....	21
9. Trattamento dei dati personali.....	22
10. Approvazione e aggiornamento del manuale, norme transitorie e finali.....	24
11. Elenco degli allegati.....	25

1. Principi generali

1.1 Premessa

Il presente Manuale di conservazione ha l'obiettivo di descrivere le modalità di funzionamento del Sistema di conservazione digitale dei documenti prodotti dalla Provincia di Treviso, come previsto dalle nuove *Linee guida sulla formazione, gestione e conservazione dei documenti informatici*, emanate dall'Agenzia per l'Italia Digitale (AgID), pubblicate in G.U. Serie generale n. 259 del 19/10/2020 (da ora in poi Linee guida AgID - GU 259/2020) e le seguenti integrazioni emanate con Determinazione n. 371 del 17 maggio 2021.

La Provincia di Treviso, in quanto soggetto produttore, come previsto dall'art. 44 del CAD, ha affidato il servizio di conservazione principalmente a Infocert S.p.A. ora Tinexta Infocert S.p.A., con apposito atto sottoscritto il 10/09/2014 dal Segretario generale dell'Amministrazione; attivando lo stesso con Determinazione n. 1453 del 27/06/2024 (PG 67425/2014), inizialmente per i contratti firmati digitalmente, poi ad altre tipologie documentarie, ed annualmente prorogato sino ad oggi.

Per la parte relativa alla tipologia mandati di pagamento e ordinativi informatici il servizio è invece attualmente affidato ad Argentea S.r.L. attraverso Determinazione n. 1777 del 02/12/2024; in continuità con quanto già svolto da UNI.IT S.r.L., fusasi ed incorporatasi all'attuale fornitore, così come dalla presa d'atto con Determinazione n. 1495 del 13/12/2019 (PG 76516/2019).

1.2 Scopo e ambito di applicazione

Il Manuale di conservazione è un documento informatico che illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.

Il presente Manuale è composto da una parte introduttiva che descrive l'ambito del Manuale, i soggetti coinvolti e i loro ruoli, il rapporto tra soggetto produttore ed enti conservatori, rimandando gli aspetti

tecnici al Manuale di conservazione predisposto dai Conservatori stessi (*Allegati 1 e 3*) e alle rispettive Condizioni generali di contratto - Allegato tecnico e Accordo di versamento (*Allegati 2, 2-A e 4*).

Il presente Manuale di conservazione risulta composto come segue:

- Manuale di conservazione della Provincia di Treviso
- Allegato 1 – Manuale di conservazione di Tinexta Infocert S.p.A.
- Allegato 2 – Condizioni generali di contratto Tinexta Infocert S.p.A.
- Allegato 2-A – Allegato tecnico Tinexta Infocert S.p.A.
- Allegato 3 – Manuale di conservazione di Argentea S.r.L.
- Allegato 4 – Accordo di versamento con Argentea S.r.L.

Nello specifico, il Manuale di conservazione, riporta:

- a) i dati dei soggetti che nel tempo hanno assunto la responsabilità del sistema di conservazione, descrivendo in modo puntuale, in caso di delega, i soggetti, le funzioni e gli ambiti oggetto della delega stessa;
- b) la struttura organizzativa comprensiva delle funzioni, delle responsabilità e degli obblighi dei diversi soggetti che intervengono nel processo di conservazione;
- c) la descrizione delle tipologie degli oggetti digitali sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di oggetti e delle eventuali eccezioni;
- d) la descrizione delle modalità di presa in carico di uno o più pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento;
- e) la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione;
- f) la modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;
- g) la descrizione del sistema di conservazione, comprensivo di tutte le componenti tecnologiche, fisiche e logiche, opportunamente documentate e delle procedure di gestione e di evoluzione delle medesime;
- h) la descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie;

- i) la descrizione delle procedure per la produzione di duplicati o copie;
- j) i tempi entro i quali le diverse tipologie di oggetti digitali devono essere trasferite in conservazione ed eventualmente scartate, qualora, nel caso delle Pubbliche Amministrazioni, non siano già indicati nel piano di conservazione allegato al manuale di gestione documentale;
- k) le modalità con cui viene richiesta la presenza di un pubblico ufficiale, indicando anche quali sono i casi per i quali è previsto il suo intervento;
- l) le normative in vigore nei luoghi dove sono conservati gli oggetti digitali.

1.3 Documento informatico

Il documento informatico è la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti ed è redatto mediante una delle seguenti modalità:

- a) creazione tramite l'utilizzo di strumenti software o servizi cloud qualificati che assicurino la produzione di documenti nei formati e nel rispetto delle regole di interoperabilità di cui all'allegato 2 delle Linee guida AgID - GU 259/2020;
- b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;
- c) memorizzazione su supporto informatico, in formato digitale, delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;
- d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

Il documento informatico deve essere identificato in modo univoco e persistente.

Nel caso della Provincia di Treviso, l'identificazione dei documenti oggetto di registrazione di protocollo è rappresentata dalla segnatura di protocollo univocamente associata al documento. L'identificazione dei documenti non protocollati è affidata alle funzioni del sistema di gestione informatica dei documenti. In alternativa l'identificazione univoca può essere realizzata mediante associazione al documento di una sua impronta crittografica basata su funzioni di *hash* che siano ritenute crittograficamente sicure, e conformi alle tipologie di algoritmi previsti nell'allegato 6 delle Linee guida AgID - GU 259/2020 nella tabella 1 del paragrafo 2.2 "Regole di processamento".

Il documento informatico è imm modificabile se la sua memorizzazione su supporto informatico in formato digitale non può essere alterata nel suo accesso, gestione e conservazione.

Nel caso di documento informatico formato secondo la sopracitata lettera a), l'immodificabilità e l'integrità sono garantite da una o più delle seguenti operazioni:

1. apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
2. memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza in accordo con quanto riportato al paragrafo 3.9 delle Linee guida AgID - GU 259/2020;
3. il trasferimento a soggetti terzi attraverso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal regolamento (UE) 23 luglio 2014 n. 910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (regolamento eIDAS), valido ai fini delle comunicazioni elettroniche aventi valore legale;
4. versamento ad un sistema di conservazione.

Nel caso di documento informatico formato secondo la sopracitata lettera b) l'immodificabilità ed integrità sono garantite da una o più delle seguenti operazioni mediante:

1. apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;

2. memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza in accordo con quanto riportato al paragrafo 3.9 delle Linee guida AgID - GU 259/2020;
3. versamento ad un sistema di conservazione.

Nel caso di documento informatico formato secondo le sopracitate lettere c) e d) le caratteristiche di immodificabilità e di integrità sono garantite da una o più delle seguenti operazioni:

1. apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
2. registrazione nei log di sistema dell'esito dell'operazione di formazione del documento informatico, compresa l'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema;
3. produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.

La certezza dell'autore è la capacità di poter associare in maniera certa e permanente il soggetto che ha sottoscritto al documento stesso.

Al momento della formazione del documento informatico immodificabile, devono essere generati e associati permanentemente ad esso i relativi metadati.

La disponibilità e la riservatezza delle informazioni contenute nel documento informatico sono garantite attraverso l'adozione di specifiche politiche e procedure predeterminate dall'ente, in conformità con le disposizioni vigenti in materia di accesso e protezione dei dati personali.

In tutti i casi di documento informatico, l'originale è informatico.

1.4 Documento amministrativo informatico

Il documento amministrativo informatico è la rappresentazione grafica, fotografica, informatica o di qualsiasi altra specie del contenuto di atti o fatti giuridicamente rilevanti, anche interni, prodotti ed acquisiti ai fini dell'attività amministrativa, così come previsto dall'art. 1 del DPR 28 dicembre 2000, n. 445.

La Provincia di Treviso forma gli originali dei propri documenti attraverso gli strumenti informatici riportati nel Manuale di gestione documentale oppure acquisendo le istanze, le dichiarazioni e le comunicazioni di cui agli articoli 5-bis, 40-bis e 65 del CAD. Pertanto, come stabilito dal CAD e dalle Linee guida AgID - GU 259/2020, il documento amministrativo è informatico.

1.5 Il Sistema di conservazione

Il Sistema di gestione informatica dei documenti della Provincia di Treviso trasferisce al sistema di conservazione, ai sensi dell'art. 44, comma 1-bis, del CAD:

- a) i fascicoli informatici chiusi e le serie informatiche chiuse, trasferendoli dall'archivio corrente o dall'archivio di deposito;
- b) i fascicoli informatici e le serie informatiche non ancora chiuse, trasferendo i documenti in essi contenuti sulla base di specifiche esigenze dell'Ente e con particolare attenzione per i rischi di obsolescenza tecnologica.

Il Sistema di conservazione assicura, dalla presa in carico fino all'eventuale scarto, la conservazione dei seguenti oggetti digitali in esso conservati, tramite l'adozione di regole, procedure e tecnologie, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità:

- a) i documenti informatici e i documenti amministrativi informatici con i metadati ad essi associati;
- b) le aggregazioni documentali informatiche (fascicoli e serie) con i metadati ad esse associati contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che costituiscono le aggregazioni medesime, nel rispetto di quanto indicato per le Pubbliche Amministrazioni nell'articolo 67, comma 2, del DPR 445/2000 e art. 44, comma 1-bis, CAD;
- c) gli archivi informatici con i metadati associati.

Il Sistema di conservazione garantisce l'accesso all'oggetto conservato per il periodo previsto dal piano di conservazione della Provincia di Treviso (in via di redazione e futura adozione) e dalla normativa vigente, o per un tempo superiore eventualmente concordato tra le parti, indipendentemente dall'evoluzione del contesto tecnologico.

Il Sistema di conservazione è logicamente distinto dal Sistema di gestione informatica dei documenti.

1.6 Definizioni e norme di riferimento

Le definizioni di riferimento del presente Manuale sono riportate alle pp. 7 - 12 del Manuale di conservazione di Tinexta Infocert S.p.A e alla sezione 2 del Manuale di conservazione di Argentea S.r.L.

La normativa e gli standard di riferimento sono riportati alle pp. 13 - 15 del Manuale di conservazione di Tinexta Infocert S.p.A. e alla sezione 3 del Manuale di conservazione di Argentea S.r.L.

Di seguito gli acronimi utilizzati nella parte redatta dalla Provincia di Treviso.

AOO	Area Organizzativa Omogenea
AgID	Agenzia per l'Italia Digitale
CAD	Codice dell'Amministrazione Digitale, D. lgs 82/2005
d.lgs	Decreto legislativo
DPCM	Decreto del Presidente del Consiglio dei Ministri
DPR	Decreto del Presidente della Repubblica
GDPR	General Data Protection Regulation, Regolamento Europeo n. 679/2016
IPA	Indice delle Pubbliche Amministrazioni
PEC	Posta Elettronica Certificata
PdA	Pacchetto di Archiviazione
PdV	Pacchetto di Versamento
RUP	Responsabile Unico del Procedimento
SUAP	Sportello unico Attività Produttive
SUE	Sportello unico Edilizia privata
TUDA	Testo Unico sulla Documentazione Amministrativa, DPR 445/2000
UOR	Unità Organizzativa Responsabile

2. Modello organizzativo, ruoli e responsabilità

2.1 Modello organizzativo

La Provincia di Treviso ha individuato un'unica Area Organizzativa Omogenea (AOO) in quanto insieme definito di Unità Organizzative

Responsabili (UOR) che usufruiscono, in modo omogeneo e coordinato, di comuni servizi per la gestione dei flussi documentali. L'Area Organizzativo Omogenea della Provincia di Treviso è identificata dal codice AOO "AC2E4D5".

Le UOR sono individuate nell'organigramma della Provincia di Treviso, approvato con Decreto del Presidente n. 71 del 27/03/2026.

La Provincia di Treviso, nell'ambito degli adempimenti previsti, si è accreditato presso l'Indice delle Pubbliche Amministrazioni (IPA), il codice identificativo IPA dell'Amministrazione associato alla propria AOO è "P_TV".

2.2 Ruoli e responsabilità

I ruoli individuati nel processo di conservazione sono dalle Linee guida AgID - GU 259/2020:

- a) titolare dell'oggetto della conservazione;
- b) produttore dei PdV;
- c) utente abilitato;
- d) responsabile della conservazione;
- e) conservatore.

2.2 a) Titolare dell'oggetto della Conservazione

Il Titolare dell'oggetto della Conservazione (o Produttore) è il soggetto produttore dei documenti informatici, che, attraverso il proprio Responsabile della conservazione, definisce ed attua le politiche complessive del Sistema di conservazione.

In base all'art. 44 del CAD il Soggetto produttore può affidare la conservazione dei documenti informatici ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative, e tecnologiche e di protezione dei dati personali.

Nel presente Manuale, il Titolare dell'oggetto della Conservazione è la Provincia di Treviso.

2.2. b) Produttore di PdV

Il produttore dei Pacchetti di Versamento (PdV) è la Provincia di Treviso. Presso l'Ente, la responsabilità della produzione dei PdV è assegnata al Responsabile della gestione documentale.

I dirigenti, di concerto con il Responsabile della gestione documentale, individuano presso le proprie UOR, i responsabili incaricati alla produzione di PdV di tipologie documentarie specifiche.

Attualmente, oltre al Responsabile della gestione documentale, l'Ente ha individuato responsabili per la produzione di PdV per le seguenti UOR e tipologie:

UOR	Tipologie
Segreteria generale	Provvedimenti degli organi collegiali e monocratici (testo degli atti e proposte), Pareri, Visti, Certificati di pubblicazione
Stazione Unica Appaltante, Contratti e Trasporti; Edilizia e patrimonio; Viabilità	Contratti
Finanza e contabilità - ufficio entrate	Fatture attive

Oltre alle UOR, possono essere individuati come produttori dei PdV anche i sistemi informatici, diversi dal Sistema di gestione documentale, che producono documentazione destinata a confluire nel sistema di conservazione, a cadenza periodica o *una tantum*.

Attualmente i sistemi abilitati a creare PdV sono:

Sistema	Tipologie
SmartCons	Atti, contratti, fatture, registro giornaliero di protocollo e documenti amministrativi soggetti a registrazione di protocollo
UniTesoWeb	Mandati e ordinativi (ordini di pagamento e riscossione, quietanze e bollette rilasciate dal Tesoriere,

	ricevute di servizio rilasciate dal Tesoriere, sospesi di entrata e uscita rilasciati dal Tesoriere)
--	---

2.2 c) Utente abilitato

L'Utente è una persona, ente o sistema che interagisce con i servizi di un Sistema di conservazione al fine di fruire delle informazioni di interesse nei limiti previsti dalle norme vigenti.

Nel ruolo dell'Utente vengono definiti i soggetti abilitati secondo le indicazioni del Produttore: nei documenti Condizioni generali di contratto - Allegato tecnico e Accordo di versamento (*Allegati 2, 2-A e 4*) sono riportati gli utenti che possono accedere esclusivamente ai documenti conservati, previa autorizzazione del Responsabile della Conservazione e secondo le politiche di accesso concordate con i Conservatori.

2.2 d) Responsabile della conservazione

Ai sensi dell'art. 44, comma 1-quater, del CAD e del paragrafo 4.5 "Responsabile della conservazione" delle Linee guida AgID - GU 259/2020, il Responsabile della conservazione è un dirigente o un funzionario interno formalmente designato e in possesso di idonee competenze giuridiche, informatiche ed archivistiche ed è un ruolo che può essere svolto dal responsabile della gestione documentale. Il Responsabile della conservazione opera di intesa con il Responsabile del trattamento dei dati personali, con il Responsabile della sicurezza e con il Responsabile dei sistemi informativi.

Al Responsabile della conservazione è assegnato il compito di:

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

- conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;
- b) gestire il processo di conservazione e garantirne nel tempo la conformità alla normativa vigente;
 - c) generare e sottoscrivere il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
 - d) generare e sottoscrivere il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
 - e) effettuare il monitoraggio della corretta funzionalità del sistema di conservazione;
 - f) effettuare la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;
 - g) adottare misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adottare analoghe misure con riguardo all'obsolescenza dei formati;
 - h) provvedere alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
 - i) predisporre le misure necessarie per la sicurezza fisica e logica del sistema di conservazione;
 - j) 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;
 - k) assicurare agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
 - l) predisporre il manuale di conservazione e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

La Provincia di Treviso, con Decreto del Presidente n. 229 del 31/12/2025, ha nominato Responsabile della gestione documentale l'ing. Antonio Cianfrone, e con Decreto del Presidente n. 121 del 12/06/2026 il medesimo è stato investito anche del ruolo di Responsabile della conservazione.

2.2 e) Conservatore

Il Conservatore è il soggetto affidatario del processo di conservazione per conto del Titolare dell'oggetto della conservazione. La sua attività consiste nell'erogazione del Servizio di conservazione dei documenti attraverso una struttura organizzativa, processi operativi e sistemi informatici di supporto da lui gestiti.

Il Conservatori per la Provincia di Treviso sono:

- Tinexta Infocert S.p.A, Ditta già vincitrice della gara indetta dalla Regione Veneto con DGRV n. 1006 del 23/03/2010, "Fornitura dei servizi di firma digitale, marcatura temporale e conservazione sostitutiva a norma dei documenti informatici, nonché di posta elettronica certificata ed *help desk* a favore della Regione Veneto e degli Enti Locali veneti". Il servizio è stato attivato in seno all'Ente medesimo con la Determina n. 1453 del 27/06/2014 (PG 67425/2014), ed annualmente prorogato sino ad oggi, ed affidato con apposito atto sottoscritto il 10/09/2014 dal Segretario Generale dell'Amministrazione, avente per oggetto la conservazione sostitutiva dei contratti firmati digitalmente, servizio poi successivamente esteso ad altre tipologie documentarie.
- Argentea S.r.L. a cui è stato affidato il servizio di conservazione dei mandati e ordinativi elettronici attraverso Determinazione n. 1777 del 02/12/2024; in continuità con quanto già svolto da UNI.IT S.r.L., fusasi ed incorporatasi all'attuale fornitore, così come dalla presa d'atto con Determinazione n. 1495 del 13/12/2019 (PG 76516/2019).

La missione dei conservatori è quella di costituire l'archivio informatico per la conservazione e l'accesso dei documenti informatici e in generale degli oggetti digitali di competenza a supporto dei processi di innovazione e semplificazione amministrativa, con gli obiettivi di:

- garantire la conservazione, archiviazione e gestione dei documenti informatici e degli altri oggetti digitali;
- erogare servizi di accesso basati sui contenuti digitali conservati;
- fornire supporto, formazione e consulenza ai Produttori per i processi di dematerializzazione.

2.3 Organismi di tutela e vigilanza

Il Ministero della Cultura (MiC) esercita funzioni di tutela e vigilanza dei sistemi di conservazione degli archivi di enti pubblici o di enti privati dichiarati di interesse storico particolarmente importante e autorizza le operazioni di scarto e trasferimento della documentazione conservata ai sensi del D.Lgs 42/2004.

Per le modalità di tutela e vigilanza si rimanda rispettivamente alla p. 30 del Manuale di conservazione di Tinexta Infocert S.p.A. e alla sezione 7.8 del Manuale di conservazione di Argentea S.r.L. nonché ai rimandi interni ivi citati.

3. Struttura organizzativa per il servizio di conservazione

Per quanto in oggetto si rimanda rispettivamente alle pp. 16 - 20 del Manuale di conservazione di Tinexta Infocert S.p.A. e alla sezione 5 del Manuale di conservazione di Argentea S.r.L.

4. Oggetti sottoposti a conservazione

4.1 Oggetti sottoposti a conservazione presso Infocert Tinexta S.p.A.

- Contratti (dal 10/10/2014)
Oggetto dell'invio in conservazione sono gli atti amministrativi in forma pubblica (rogati dal Segretario provinciale o da altro soggetto autorizzato) e le scritture private in cui l'Ente è parte, i quali afferiscono rispettivamente a due distinti repertori.

Di seguito, l'elenco dei metadati che sono inviati contestualmente ai contratti:

- Data documento
- Numero
- Oggetto
- Tipo registro
- Importo
- Anno
- Date ("stipula" e "registrazione")
- Forma contratto

- Firmatario Ente (con anche indicazione del “ruolo”)
- Contraenti (cognome nome / ragione sociale, partita IVA, sede legale)
- Natura atto
- Luogo stipula
- CIG (codice identificativo gara)
- Note
- Ufficiale rogante (cognome nome, codice fiscale e ruolo)
- Identificativi dell’oggetto digitale (tipo allegato, nome file, impronta, algoritmo, identificativo documento, segnatura, formato, ecc.)
- Formazione e afferenza dell’oggetto (id documento, modalità di formazione, tipologia documentale, tipologia flusso, tipo registro, data registrazione, numero documento, codice registro, tipo aggregazione, id aggregazione, versione, ecc.)
- Soggetti e ruoli (ruolo, tipo, denominazione)
- Consultabilità, con valore “riservato” per gli oggetti valorizzati come tali
- Verifiche (firma digitale, sigillo, marca temporale, conformità copie)
- Tempo di conservazione

I contratti, indipendentemente dall’afferenza tipologica, vengono inviati in conservazione manualmente.

- Registro giornaliero di protocollo (dal 12/10/2015)
 Il sistema di gestione del protocollo informatico in uso presso l’Ente è dotato di una specifica funzionalità di produzione e invio in conservazione dal Registro giornaliero di protocollo, prodotto automaticamente in formato .PDF e predisposto per il contestuale riversamento al sistema di conservazione. Tale elaborazione, realizzata con le caratteristiche, in termini di metadati esposti, che si ritengono idonee a garantire la totale aderenza alla normativa vigente (DPCM 03/12/2013 e modalità operative descritte da AgID), prevede la produzione sia della stampa del Registro che della stampa delle eventuali modifiche, gestite come allegato allo stesso. Il documento così creato riporta su un unico file il riepilogo di tutte le registrazioni di protocollo eseguite nell’ambito della stessa giornata e, a seguire, gli eventuali annullamenti (parziali o totali) occorsi ai protocolli acquisiti nel corso dei giorni precedenti.

La produzione del documento avviene dopo la chiusura del Registro di protocollo e prima della riapertura nel giorno successivo in modo che nessun altro documento possa essere protocollato nel registro della giornata precedente né tramite operatore né in modalità automatica.

I metadati da inviare in conservazione, unitamente alla copia del registro di cui sopra, sono stati suddivisi in tre sottogruppi:

- Metadati di identificazione (informazioni memorizzate tra le proprietà di sistema relative all'Ente versante e quelle del protocollo che identificano univocamente il documento);
- Metadati di profilo generali (oggetto, data e altre informazioni generali sul documento memorizzati sulla relativa registrazione di protocollo);
- Metadati di profilo specifici (numero protocolli giornalieri, iniziale, finale e altre informazioni specifiche del tipo di documento memorizzati sulla registrazione di protocollo e tra le proprietà dell'AOO).

Il processo automatico si occupa di fatto di creare il pacchetto di versamento, inviarlo al sistema di conservazione e registrare lo stato del versamento stesso, comprese le eventuali anomalie dell'iter che vengono notificate al Responsabile della conservazione. L'uso integrato dei diversi meccanismi permette in ogni caso di conferire validità e integrità ai contenuti del file del Registro di protocollo giornaliero.

- Documenti soggetti a registrazione di protocollo (dal 01/01/2026)
Documenti oggetto dell'invio in conservazione sono tutte le registrazioni di protocollo con associato un documento informatico, con la chiave univoca della registrazione identificata da numero, anno e codice del registro.
I file oggetto dell'invio al sistema di conservazione sono il documento principale, gli allegati ed i messaggi prodotti dal sistema di interoperabilità (segnatura .xml, ecc.). Il formato dei file non è predeterminabile in quanto, in particolare per i documenti in arrivo, vengono registrati nel sistema i documenti prodotti ed inviati all'Ente dal mittente, indipendentemente dall'apposizione della firma digitale. La data di riferimento temporale per la verifica della firma digitale del file principale e dei file associati agli allegati è la data di protocollo. Di seguito, l'elenco dei metadati che sono inviati contestualmente al documento:
 - Anno

- Tipo registro
- Numero
- Data registrazione
- Movimento (Arrivo, Partenza, Interno)
- Oggetto
- Estremi del documento esterno ("numero_documento", "data_documento")
- Mittente/destinatario (opzionale) con valore "cognome nome o ragione sociale o descrizione dell'Amministrazione/AOO" e "codice fiscale o partita IVA". Per mittente/destinatario si intendono tutti i mittenti / destinatari associati alla registrazione di protocollo.
- Classificazione (opzionale)
- Fascicolo ("fascicolo_anno" / "fascicolo_numero")
- Annullato (si/no)
- Dati di annullamento (data, motivo, provvedimento ed esecutore)
- Documento precedente ("descrizione del registro", "anno" / "numero" e "data protocollo precedente")
- Operatore ("descrizione unità protocollante" e "cognome nome dell'utente protocollante")
- Descrizione tipo Documento
- Consultabilità, con valore "riservato" per i documenti valorizzati come tali
- Modalità trasmissione

Le registrazioni di protocollo vengono inviate in conservazione tramite automatismo di sistema decorso un periodo prestabilito di tempo dalla data di registrazione delle stesse.

- Atti degli organi monocratici e collegiali dell'Ente (dal 01/10/2015)

I documenti oggetto dell'invio in conservazione sono le deliberazioni, determinazioni dirigenziali e in generale tutti gli atti amministrativi, firmati digitalmente, prodotti dalla Provincia tramite i processi di dematerializzazione di adozione dei provvedimenti. La chiave univoca della registrazione è identificata da numero, anno e codice del registro. Tutti i documenti prodotti dal sistema e firmati digitalmente (cioè testo degli atti e delle proposte, pareri, visti e certificati di pubblicazione) sono nel formato PDF/A e pertanto sono inviati al

sistema di conservazione con estensione PDF.P7M.
Le tipologie di atti in questione vengono inviati in conservazione manualmente.

- Fatture elettroniche (dal 2015)
Le fatture passive inviate dai fornitori esterni vengono acquisite automaticamente dal sistema e inviate come tipologia “fattura elettronica passiva” in conservazione. Gli elementi eventualmente allegati alla fattura, contenuti negli appositi spazi previsti dalle specifiche tecniche, sono inclusi nello schema XML. La conservazione avviene tramite automatismo.
Le fatture attive prodotte dall’Amministrazione vengono caricate sul sistema di conservazione come tipologia “fattura elettronica attiva”. La conservazione avviene manualmente.

Per tutto quanto non espressamente citato si rimanda alle pp. 22 - 26 del Manuale di conservazione di Tinexta Infocert S.p.A.

4.2 Oggetti sottoposti a conservazione presso Argentea S.r.L. (già UNI IT)

- Mandati di pagamento e ordinativi informatici (dal 2015)
Si tratta di ordini di pagamento e riscossione, quietanze e bollette rilasciate dal Tesoriere, ricevute di servizio rilasciate dal Tesoriere, sospesi di entrata e uscita rilasciati dal Tesoriere.

Il Servizio provinciale produttore dispone in merito alla conservazione, in relazione a quanto assicurato dall’Istituto incaricato del servizio di tesoreria.

Per quanto non espressamente citato si rimanda alla sezione 6 del Manuale di conservazione di Argentea S.r.L.

5. Processo di conservazione

Per quanto in oggetto si rimanda rispettivamente alle pp. 27 - 31 del Manuale di conservazione di Tinexta Infocert S.p.A. e alla sezione 7 del Manuale di conservazione di Argentea S.r.L.

6. Il Sistema di conservazione

Per quanto in oggetto si rimanda rispettivamente alle pp. 32 - 39 del Manuale di conservazione di Tinexta Infocert S.p.A. e alla sezione 8 del Manuale di conservazione di Argentea S.r.L.

7. Monitoraggio e controlli

Il Responsabile della conservazione effettua verifiche periodiche, con cadenza non superiore ai cinque anni, del corretto versamento dei documenti al Sistema di conservazione, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentali degli archivi e adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità.

Per il monitoraggio e i controlli eseguiti dai Conservatori si vedano le pp. 38 - 39 del Manuale di conservazione Tinexta Infocert S.p.A. e la sezione 9 del Manuale di conservazione di Argentea S.r.L., nonché i rimandi interni ivi citati.

8. Selezione dei documenti e Piano di conservazione

L'art. 68 del DPR 445/2000 prevede che ogni amministrazione debba dotarsi di un «piano di conservazione degli archivi, integrato con il sistema di classificazione, per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione dei documenti». Per quanto attiene all'argomento si rimanda al paragrafo 8 del Manuale di gestione documentale in uso presso l'ente Provincia di Treviso.

Ai sensi dell'art. 21, comma 1, lettera d) del Codice dei beni culturali e del paesaggio (D. lgs. 22 gennaio 2004, n. 42) e dell'art. 43, comma 4 del CAD (D.lgs. 82/2005), la selezione archivistica, o scarto, deve avvenire previa autorizzazione del Ministero per i beni e le attività culturali e con provvedimento formale dell'Amministrazione (deliberazione dell'organo collegiale o atto monocratico).

Ne consegue che anche lo scarto di documenti digitali della Provincia di Treviso debba avvenire previa autorizzazione della Soprintendenza archivistica e bibliografica del Veneto e del Trentino Alto Adige. Il Responsabile della conservazione effettua periodicamente l'analisi dei documenti presenti nel Sistema di conservazione da sottoporre a scarto, redige l'elenco di selezione e lo invia alla Soprintendenza archivistica e bibliografica del Veneto e del Trentino Alto Adige per ottenere l'autorizzazione. Una volta ottenuta l'autorizzazione, il Responsabile della conservazione trasmette al Conservatore l'autorizzazione e il provvedimento di scarto, in seguito al quale il Conservatore procede con lo scarto della documentazione.

All'attivazione di ogni nuovo flusso documentale inviato al Sistema di conservazione, è in capo al Responsabile della conservazione la verifica sulla presenza del metadato 'tempo di conservazione' associato alla nuova tipologia documentaria inviata al Conservatore, in analogia al Piano di conservazione in uso presso l'Ente, nonché l'inserimento dello stesso all'interno del Disciplinare tecnico/accordo di versamento in essere con il singolo Conservatore, in corrispondenza della scheda dedicata alla tipologia attivata.

9. Trattamento dei dati personali

La titolarità del trattamento di dati personali contenuti nei documenti oggetto di conservazione è in capo al Produttore, mentre Tinexta Infocert S.p.A. e Argentea S.r.L. sono nominate quali Responsabili del trattamento dei dati personali necessari allo svolgimento del processo di conservazione come stabilito, per Argentea S.r.L., dalla nota PG 5581/2020 e relativi allegati.

Di conseguenza, Tinexta Infocert S.p.A. ed Argentea S.r.L. si impegnano, nel trattamento dei dati, ad attenersi alle istruzioni e a svolgere i compiti indicati dall'Ente Produttore, così come meglio definiti alle pp. 34 - 35 del Manuale di conservazione di Tinexta Infocert S.p.A. e nell'atto di nomina sopracitato per Argentea S.r.L., nonché ai rimandi interni ivi citati.

Coerentemente a quanto espresso, i rispettivi Responsabili dei conservatori individuati dalla Provincia di Treviso, Titolare del trattamento, sulla base di Accordi ex art. 28 del GDPR quale

Responsabile del trattamento, assumono la responsabilità sulla garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali e sulla garanzia che il trattamento dei dati affidati dalla Provincia di Treviso avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.

La Provincia di Treviso, recependo le prescrizioni e i principi espressi dalla normativa in materia, adotta e aggiorna appositi regolamenti. Nello specifico, sono adottati i seguenti regolamenti:

1. *“Regolamento protezione dati personali (GDPR)”*, approvato con deliberazione del Consiglio Provinciale n. 16/63246 del 25 luglio 2018, in vigore dal 25 luglio 2018.

Per quanto riguarda le politiche sul trattamento dei dati del Conservatore si vedano le pp. 34 - 35 del Manuale di conservazione di Tinexta Infocert S.p.A. e nell'atto di nomina sopracitato per Argentea S.r.L., nonché ai rimandi interni ivi citati.

10. Approvazione e aggiornamento del manuale, norme transitorie e finali

Il presente Manuale è approvato dal Presidente della Provincia con proprio Decreto ed è aggiornato, su proposta del Responsabile della conservazione, con le medesime modalità.

Gli aggiornamenti potranno rendersi necessari a seguito di:

- a) adeguamenti normativi o tecnologici che rendano superate le prassi definite nel Manuale;
- b) introduzione di nuove pratiche tendenti a migliorare l'azione amministrativa in termini di efficacia, efficienza e trasparenza;
- c) inadeguatezza delle procedure rilevate nello svolgimento delle attività correnti;
- d) rinnovo della Convenzione con il Conservatore o cambio Conservatore;

Gli allegati al presente Manuale, che contengono indicazioni di dettaglio sulle procedure operative e sulle modalità di funzionamento dei sistemi gestionali, sono modificati con Determinazione dirigenziale o con provvedimento del Responsabile della gestione documentale.

Entra in vigore alla data di esecutività del provvedimento che lo approva.

In ottemperanza alla normativa vigente, il Manuale di conservazione e i suoi allegati sono pubblicati sul sito istituzionale della Provincia di Treviso, nell'area "Amministrazione trasparente", come previsto dall'art. 9 del D.lgs. 33/2013 e dalle *Linee guida AgID - GU 259/2020*.

11. Elenco degli allegati

- Allegato 1 – Manuale di conservazione di Tinexta Infocert S.p.A.
- Allegato 2 – Condizioni generali di contratto Tinexta Infocert S.p.A.
- Allegato 2-A – Allegato tecnico Tinexta Infocert S.p.A.
- Allegato 3 – Manuale di conservazione di Argentea S.r.L.
- Allegato 4 – Accordo di versamento con Argentea S.r.L.

tinexta
infocert

Manuale della Conservazione

Sommario

MANUALE DELLA CONSERVAZIONE.....	1
REGISTRO DELLE VERSIONI.....	4
SCOPO E AMBITO DEL DOCUMENTO	6
TERMINOLOGIA.....	7
NORMATIVA E STANDARD DI RIFERIMENTO	13
RUOLI E RESPONSABILITÀ	16
PROFILO DI TINEXTA INFOCERT	16
RESPONSABILI TINEXTA INFOCERT	19
OGGETTI SOTTOPOSTI A CONSERVAZIONE	22
FORMATI.....	23
METADATI	23
IL PROCESSO DI CONSERVAZIONE	27
CONTROLLI DI VERSAMENTO	28
PRODUZIONE DI COPIE O DUPLICATI	29
VERIFICHE DI INTEGRITÀ E LEGGIBILITÀ.....	29
SCARTO DEI PACCHETTI DI ARCHIVIAZIONE	30
HANDOVER E INTEROPERABILITÀ	31
RICERCA ED ESIBIZIONE DEI DOCUMENTI CONSERVATI.....	31
I SISTEMI DI CONSERVAZIONE	32
SIGILLO DEI PACCHETTI DI ARCHIVIAZIONE	33
MARCA TEMPORALE DEI PACCHETTI DI ARCHIVIAZIONE	33



STORAGE34

SICUREZZA E PROTEZIONE DEI DATI34

PROCEDURE DI GESTIONE E MONITORAGGIO35

CONTROLLI PERIODICI E AUDIT38

SPECIFICITÀ DEL CONTRATTO 40

Registro delle versioni

N° versione	Data emissione	Modifiche apportate
01	Luglio 2014	Prima versione
02	Novembre 2015	Utilizzo dello schema proposto da AgID
03	Febbraio 2016	Correzioni formali e di layout
04	Marzo 2016	Correzioni formali e di layout
05	Settembre 2017	Glossario, Normativa, Mission, Comunità di riferimento, Riferimenti a policy aziendali interne
05.1	Novembre 2017	Specificità del contratto
06	Luglio 2018	Normativa GDPR, semplificazione glossario e nuovi Responsabili
07	Gennaio 2019	Nuovo logo aziendale
08	Maggio 2019	Nuovo Responsabile sistemi
09	Ottobre 2020	Glossario, nuovi Responsabili, aggiornamento procedure di monitoraggio, semplificazione delle Specificità del contratto
10	Novembre 2020	Ampliamento servizi di storage e introduzione Linee Guida AgID
11	Aprile 2022	Semplificazione nella descrizione dei processi Introduzione del servizio SAFE LTA Aggiornamento procedure di monitoraggio
12	Maggio 2023	Nuovo logo Aggiornamento TSS per la marca temporale
13	Agosto 2024	Semplificazione e aggiornamento Responsabili, Profilo Tinexta Infocert (indirizzi e qualificazione ACN), Sistema SAFE LTA e Specificità del contratto
14	Aprile 2025	Nuovo logo Cambio Responsabile del servizio
15	Dicembre 2025	Cambio ragione sociale

tinexta
infocert

SCOPO E AMBITO DEL DOCUMENTO

Il presente documento è il **manuale della conservazione di Tinexta Infocert**, ai sensi delle **Linee Guida AgID**, Agenzia per l'Italia Digitale, su formazione, gestione e conservazione dei documenti informatici di maggio 2021, richiamate dal **Codice dell'Amministrazione Digitale** - decreto legislativo n. 82 del 2005.

Il manuale della conservazione illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.

In caso di ispezione da parte delle autorità di vigilanza preposte, il manuale della conservazione permette un agevole svolgimento di tutte le attività di controllo.

Ogni soggetto produttore, cliente dei servizi di conservazione di Tinexta Infocert e titolare dei documenti conservati, può liberamente far riferimento al presente documento nel proprio manuale della conservazione.

Il presente manuale è firmato digitalmente a riprova del fatto che il management aziendale ha approvato i contenuti.

TERMINOLOGIA

TERMINE	DEFINIZIONE
ACCESSO	Operazione che consente di prendere visione dei documenti informatici.
AFFIDABILITÀ	Caratteristica che, con riferimento a un sistema di gestione documentale o conservazione, esprime il livello di fiducia che l'utente ripone nel sistema stesso, mentre con riferimento al documento informatico esprime la credibilità e l'accuratezza della rappresentazione di atti e fatti in esso contenuta.
AGGREGAZIONE DOCUMENTALE INFORMATICA	Insieme di documenti informatici o insieme di fascicoli informatici riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente.
ARCHIVIO	Complesso dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività.
ARCHIVIO INFORMATICO	Archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche.
ATTESTAZIONE DI CONFORMITÀ DELLE COPIE PER IMMAGINE SU SUPPORTO INFORMATICO DI UN DOCUMENTO ANALOGICO	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.
AUTENTICITÀ	Caratteristica in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto un oggetto è autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze.
CERTIFICAZIONE	Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi.
CLASSIFICAZIONE	Attività di organizzazione di tutti i documenti secondo uno schema costituito da un insieme di voci articolate in modo gerarchico e che individuano, in astratto, le funzioni, competenze, attività e/o materie del soggetto produttore.
CONSERVATORE	Soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici.
CONSERVAZIONE	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti

DESTINATARIO	Soggetto o sistema al quale il documento informatico è indirizzato.
DIGEST	Vedi Impronta crittografica.
DOCUMENTO AMMINISTRATIVO INFORMATICO	Ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa
DOCUMENTO ELETTRONICO	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva
DOCUMENTO INFORMATICO	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
DUPLICATO INFORMATICO	Vedi art. 1, comma 1, lett) i quinquies del CAD.
ESEAL	Vedi sigillo elettronico.
ESIBIZIONE	operazione che consente di visualizzare un documento conservato
ESIGNATURE	Vedi firma elettronica.
ESTRAZIONE STATICA DEI DATI	Estrazione di informazioni utili da grandi quantità di dati (es. database, datawarehouse ecc..), attraverso metodi automatici o semi-automatici
EVIDENZA INFORMATICA	Sequenza finita di <i>bit</i> che può essere elaborata da una procedura informatica.
FASCICOLO INFORMATICO	Aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento.
FILE	Insieme di informazioni, dati o comandi logicamente correlati, raccolti sotto un unico nome e registrati, per mezzo di un programma di elaborazione o di scrittura, nella memoria di un computer.
FIRMA ELETTRONICA	Vedi articolo 3 del Regolamento eIDAS.
FIRMA ELETTRONICA AVANZATA	Vedi articoli 3 e 26 del Regolamento eIDAS.
FIRMA ELETTRONICA QUALIFICATA	Vedi articolo 3 del Regolamento eIDAS.
FLUSSO (BINARIO)	Sequenza di bit prodotta in un intervallo temporale finito e continuativo che ha un'origine precisa ma di cui potrebbe non essere predeterminato il suo istante di interruzione.
FORMATO CONTENITORE	Formato di file progettato per consentire l'inclusione ("imbustamento" o <i>wrapping</i>), in uno stesso file, di una o più evidenze informatiche soggette a differenti tipi di codifica e al quale possono essere associati specifici metadati.
FORMATO DEL DOCUMENTO INFORMATICO	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.

FUNZIONE DI HASH CRITTOGRAFICA	Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o <i>digest</i> (vedi) in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
GESTIONE DOCUMENTALE	Processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta, uso, selezione e conservazione dei documenti.
HASH	Termine inglese usato, impropriamente, come sinonimo d'uso di "impronta crittografica" o " <i>digest</i> " (vedi).
IDENTIFICATIVO UNIVOCO	Sequenza di numeri o caratteri alfanumerici associata in modo univoco e persistente ad un'entità all'interno di uno specifico ambito di applicazione.
IMPRONTA CRITTOGRAFICA	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di <i>hash</i> crittografica a un'evidenza informatica.
INTEGRITÀ	Caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità.
INTEROPERABILITÀ	Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi.
LEGGIBILITÀ	Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica.
MANUALE DI CONSERVAZIONE	Documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture.
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 DIGITALE	Oggetto informativo digitale, che può assumere varie forme tra le quali quelle di documento informatico, fascicolo informatico, aggregazione documentale informatica o archivio informatico.

PACCHETTO DI ARCHIVIAZIONE	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel manuale di conservazione.
PACCHETTO DI DISTRIBUZIONE	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione.
PACCHETTO DI FILE (<i>FILE PACKAGE</i>)	Insieme finito di più file (possibilmente organizzati in una struttura di sottoalbero all'interno di un filesystem) che costituiscono, collettivamente oltre che individualmente, un contenuto informativo unitario e auto-consistente.
PACCHETTO DI VERSAMENTO	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione.
PACCHETTO INFORMATIVO	Contenitore logico che racchiude uno o più oggetti di conservazione con i relativi metadati, oppure anche i soli metadati riferiti agli oggetti di conservazione.
<i>PATH</i>	Percorso (<i>vedi</i>).
<i>PATHNAME</i>	Concatenazione ordinata del percorso di un file e del suo nome.
<i>PERCORSO</i>	Informazioni relative alla localizzazione virtuale del file all'interno del filesystem espressa come concatenazione ordinata del nome dei nodi del percorso.
PIANO DI CONSERVAZIONE	Documento, allegato al manuale di gestione e integrato con il sistema di classificazione, in cui sono definiti i criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445.
PIANO DI ORGANIZZAZIONE DELLE AGGREGAZIONI DOCUMENTALI	Strumento integrato con il sistema di classificazione a partire dai livelli gerarchici inferiori di quest'ultimo e finalizzato a individuare le tipologie di aggregazioni documentali (tipologie di serie e tipologie di fascicoli) che devono essere prodotte e gestite in rapporto ai procedimenti e attività in cui si declinano le funzioni svolte dall'ente
PIANO GENERALE DELLA SICUREZZA	Documento che pianifica le attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza.
PRESA IN CARICO	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione e, in caso di affidamento del servizio all'esterno, dagli accordi stipulati tra il titolare dell'oggetto di conservazione e il responsabile del servizio di conservazione.
PROCESSO	Insieme di attività correlate o interagenti che trasformano elementi in ingresso in elementi in uscita.

PRODUTTORE DEI PDV	Persona fisica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con il responsabile della gestione documentale.
QSEAL	Sigillo elettronico qualificato, come da art. 35 del Regolamento eIDAS.
QSIGNATURE	Firma elettronica qualificata, come da art. 25 del Regolamento eIDAS.
RAPPORTO DI VERSAMENTO	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.
RESPONSABILE DEL SERVIZIO DI CONSERVAZIONE	soggetto che coordina il processo di conservazione all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
RESPONSABILE DELLA CONSERVAZIONE	Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.
RESPONSABILE DELLA FUNZIONE ARCHIVISTICA DI CONSERVAZIONE	soggetto che coordina il processo di conservazione dal punto di vista archivistico all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
RIFERIMENTO TEMPORALE	Insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC).
RIVERSAMENTO	Procedura mediante la quale uno o più documenti informatici sono convertiti da un formato di file (ovvero di busta, ovvero di pacchetto di file) ad un altro, lasciandone invariato il contenuto per quanto possibilmente permesso dalle caratteristiche tecniche del formato (ovvero dei formati) dei file e delle codifiche di destinazione.
SCARTO	Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico-culturale.
SIGILLO ELETTRONICO	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi.
SISTEMA DI CONSERVAZIONE	Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, comma 1, del CAD.
SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI	Insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle organizzazioni per la gestione dei documenti. Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445

<i>TIMELINE</i>	Linea temporale virtuale su cui sono disposti degli eventi relativi ad un sistema informativo o a un documento informatico. Costituiscono esempi molto diversi di <i>timeline</i> un file di log di sistema, un flusso multimediale contenente essenze audio\video sincronizzate.
TITOLARE DELL'OGGETTO DI CONSERVAZIONE	Soggetto produttore degli oggetti di conservazione.
TRASFERIMENTO	Passaggio di custodia dei documenti da una persona o un ente ad un'altra persona o un altro ente.
UTENTE ABILITATO	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.
VERSAMENTO	Passaggio di custodia, di proprietà e/o di responsabilità dei documenti. Nel caso di un organo giudiziario e amministrativo dello Stato operazione con la quale il responsabile della conservazione trasferisce agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali.

NORMATIVA E STANDARD DI RIFERIMENTO

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

- eIDAS (electronic IDentification Authentication and Signature) Reg. 910/2014 of the European Parliament and of the Council, of 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market, così come modificato dal Reg. (UE) 2024/1183 of the European Parliament and of the Council of April 2024.
- GDPR (General Data Protection Regulation) EU Regulation 679/2016 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
- Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- Legge 7 agosto 1990, n. 241 e ss.mm.ii. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e ss.mm.ii – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e ss.mm.ii. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e ss.mm.ii. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e ss.mm.ii. (D. Lgs. 26 agosto 2016, n.179) – Codice dell'amministrazione digitale (CAD) e ss.mm.ii.;
- 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;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche per il protocollo informatico ai sensi degli articoli 40 -bis, 41, 47, 57 -bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 [parzialmente abrogate dalle Linee Guida AgID a partire da gennaio 2022];
- Decreto del Ministero dell'Economia e delle Finanze 17 giugno 2014 - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82 del 2005;
- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.
- Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici pubblicate a settembre 2020, aggiornate nel maggio 2021 e pienamente applicabili dal gennaio 2022.

- Regolamento AgID sui criteri per la fornitura dei servizi di conservazione dei documenti informatici di dicembre 2021 (marketplace).

Si riportano di seguito gli standard di riferimento:

- UNI 11386 - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 14721 - OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ISO 15836 - Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core;
- ISO/TR 18492 - Long-term preservation of electronic document-based information;
- ISO 20652 - Space data and information transfer systems - Producer-Archive interface - Methodology abstract standard;
- ISO 20104 - Space data and information transfer systems — Producer-Archive Interface Specification (PAIS);
- ISO/CD TR 26102 - Requirements for long-term preservation of electronic records;
- SIARD Software Independent Archiving of Relational Databases 2.0;
- 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;
- Ministère de la culture et de la communication, Service interministériel des Archives de France, Standard d'échange de données pour l'archivage. Transfert – Communication – Élimination – Restitution - Modification, ver. 2.1, 2018;
- METS - Metadata Encoding and Transmission Standard;
- PREMIS – PREservation Metadata: Implementation Strategies;
- EAD (3)/ISAD (G);
- EAC (CPF)/ISAAR (CPF)/NIERA (CPF);
- SCONS2/EAG/ISDIAH;
- ISO 16363 - Space data and information transfer systems -- Audit and certification of trustworthy digital repositories;
- ISO/IEC 27001 - Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ISO/IEC 27017 - Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services;
- ISO/IEC 27018 - Information technology -- Security techniques -- Code of practice for

protection of personally identifiable information (PII) in public clouds acting as PII processors;

- ETSI TS 101 533-1 V1.2.1 - Technical Specification, Electronic Signatures and Infrastructures;
- (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- ETSI TR 101 533-2 V1.2.1 - 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.

Inoltre, si segnalano due procedure aziendali interne connesse al servizio:

- **Procedura di handover e scarto**, che descrive le modalità di richiesta ed esecuzione delle attività di versamento da/a un altro Conservatore e delle attività di cancellazione fisica e logica dei documenti, nel rispetto delle Linee Guida AgID e del GDPR.
- **Piano di cessazione**, che descrive le attività di Tinexta Infocert in caso di cessazione dei servizi di conservazione, in modo da fornire a utenti e clienti il supporto necessario alla migrazione verso altri Conservatori.

RUOLI E RESPONSABILITÀ

Nel processo di conservazione digitale intervengono numerosi soggetti, a differenti livelli e con diverse responsabilità.

I ruoli individuati dalle Linee Guida AgID sono:

- a) **TITOLARE DELL'OGGETTO DELLA CONSERVAZIONE** (soggetto produttore degli oggetti di conservazione);
- b) **PRODUTTORE DEI PACCHETTI DI VERSAMENTO** (persona fisica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione, anche attraverso l'utilizzo di piattaforme o sistemi Tinexta Infocert);
- c) **UTENTE ABILITATO** (persona, ente o sistema che interagisce con i servizi di conservazione, al fine di fruire delle informazioni di interesse, cioè per le attività di ricerca ed esibizione a norma);
- d) **RESPONSABILE DELLA CONSERVAZIONE** (interno al cliente/produttore, che sceglie di affidare il servizio a Tinexta InfoCert);
- e) **CONSERVATORE** (Tinexta Infocert).

I primi quattro ruoli sono tipicamente individuati all'interno dell'organigramma di quello che per Tinexta Infocert è il cliente/produttore.

Quest'ultimo affida in *full outsourcing* il servizio di conservazione a Tinexta Infocert S.p.A., in accordo con quanto previsto dai documenti contrattuali descritti al capitolo 'Specificità del Contratto' e dalle Linee Guida AgID. In particolar modo, nell'Atto di affidamento sono elencate funzioni e ambiti oggetto della delega.

All'interno dell'organigramma di Tinexta Infocert, sono, invece, individuati un **Responsabile del servizio di conservazione**, un **Responsabile della funzione archivistica** (come previsto dal Regolamento AgID) e gli altri ruoli qui di seguito riportati.

PROFILO DI TINEXTA INFOCERT

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

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

La mission aziendale si declina anche nel servizio di Conservazione digitale: innovazione, sicurezza, affidabilità e conformità normativa, con lo scopo di assicurare la corretta gestione, archiviazione e

conservazione dei documenti informatici di diversi soggetti produttori, assicurando l'esibizione a norma dei documenti conservati e la consulenza specialistica su progetti di paperless design.

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

Da febbraio 2022, è iscritta al Marketplace dei servizi di conservazione di AgID come conservatore qualificato - <https://conservatoriqualeficati.agid.gov.it/>

Inoltre, Tinexta Infocert è tra i fornitori presenti nel Catalogo delle Infrastrutture digitali e dei Servizi Cloud di ACN (Agenzia per la Cybersicurezza Nazionale), requisito normativo necessario per offrire alla Pubblica Amministrazione, le proprie soluzioni di conservazione digitale a norma: SAFE LTA (SaaS - ID Scheda in ACN: SA-3452) e LegalDoc (SaaS - ID Scheda: SA-779),

<https://www.acn.gov.it/portale/catalogo-delle-infrastrutture-digitali-e-dei-servizi-cloud>

denominazione sociale	Tinexta Infocert S.p.A.
sede legale:	Piazzale Flaminio 1/b, 00196 Roma
sedi operative:	Piazza da Porto, 3, 35131 - Padova Via Fernanda Wittgens, 6, 20123 – Milano Via Gian Domenico Romagnosi 4, 00196 Roma
telefono:	049.7849350
sito web	www.infocert.it
e-mail	info@infocert.it
PEC	infocert@legalmail.it
codice fiscale / partita IVA	07945211006
numero REA	RM – 1064345

Oggi il servizio di conservazione di Tinexta Infocert si declina in due prodotti:

- **LegalDoc**, storico servizio, sviluppato sulla base delle Regole Tecniche del 2013, pensato per il mercato italiano e accreditato AgID dal 2014.
- **SAFE LTA (Long-Term-Archiving)**, sviluppato nel 2021, sulla base delle specifiche *eArchiving building block* del *Connecting Europe Facility* (CEF), in ottica internazionale.

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



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

Tinexta Infocert è costantemente impegnata nel monitoraggio della propria comunità designata, al fine di acquisire nuove informazioni o esigenze o standard tecnologici, anche con lo scopo di combattere l'obsolescenza tecnologica.

Tinexta Infocert, inoltre, nello svolgimento delle proprie attività, ha conseguito le seguenti certificazioni: <https://www.infocert.it/certificazioni>

RESPONSABILI TINEXTA INFOCERT

Si riportano di seguito i profili professionali di responsabilità legate al servizio di conservazione e le rispettive attività di competenza.

Tutti i Responsabili sono assunti a tempo indeterminato.

RUOLI	NOMINATIVI	ATTIVITA'	PERIODI
Responsabile del servizio di Conservazione	Lucia Bortoletto	- 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 (in collaborazione con Ufficio Legale e Product Marketing Manager), 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.	da marzo 2025
Responsabile funzione archivistica di conservazione	Marta Gaia Castellan	- 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	da settembre 2015

RUOLI	NOMINATIVI	ATTIVITA'	PERIODI
		Ministero dei beni e delle attività culturali per quanto di competenza; controlli periodici a campione sulla leggibilità dei documenti conservati.	

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

RUOLI	NOMINATIVI PRECEDENTI	PERIODI
Responsabile del servizio	Nicola Maccà	Da luglio 2018 a marzo 2025
Responsabile sviluppo e manutenzione del sistema di conservazione	Lucia Bortoletto	da luglio 2018 a gennaio 2022 (data in cui il Regolamento AgID ha ristretto le figure di responsabilità alle due nella precedente tabella)
Responsabile trattamento dati personali	Ilenia Gentilezza	da marzo 2020 a luglio 2023
Responsabile Sicurezza dei sistemi per la conservazione	Giovanni Belluzzo	da luglio 2018 a gennaio 2022
Responsabile sistemi informativi per la conservazione	Stefano Mameli	da maggio 2019 a ottobre 2020
Responsabile trattamento dati personali	Valentina Zoppo	da luglio 2018 a marzo 2020
Responsabile sistemi informativi per la conservazione	Nicolò Poniz	da luglio 2018 a maggio 2019
Responsabile sviluppo e manutenzione del sistema di conservazione	Nicola Maccà	da gennaio 2013 a luglio 2018
Responsabile sistemi informativi per la conservazione	Massimo Biagi	da marzo 2014 a luglio 2018
Responsabile funzione archivistica di conservazione precedente	Silvia Loffi	da dicembre 2014 ad agosto 2015

RUOLI	NOMINATIVI PRECEDENTI	PERIODI
Responsabile trattamento dati personali	Alfredo Esposito	da gennaio 2011 a luglio 2018
Responsabile Sicurezza dei sistemi per la conservazione	Alfredo Esposito	da gennaio 2011 a luglio 2018
Responsabile del servizio di Conservazione	Antonio Dal Borgo	da luglio 2008 a luglio 2018
Responsabile del servizio di Conservazione	Pio Barban	da luglio 2007 a luglio 2008

OGGETTI SOTTOPOSTI A CONSERVAZIONE

In generale si definisce '**pacchetto**' un contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche).

I pacchetti sono contrattualizzati con il soggetto produttore e si basano sui documenti che fanno parte delle 'Specificità del Contratto'.

Per "**PACCHETTO DI VERSAMENTO**" si intende l'insieme di documenti che il soggetto produttore invia al sistema di conservazione in un'unica sessione o in una singola chiamata. Le modalità di versamento sono diverse: dal caricamento manuale attraverso portale web, all'utilizzo di chiamate applicative. Il sistema ritorna una Ricevuta di versamento.

Per "**PACCHETTO DI ARCHIVIAZIONE**" si intende un pacchetto informativo composto dalla trasformazione di pacchetti di versamento, depositato nei data center Tinexta Infocert e associato a un file XML, detto Indice del Pacchetto di Archiviazione (IPdA o indice di conservazione UNI SInCRO) sigillato e marcato temporalmente dal Responsabile del servizio di Tinexta Infocert. In LegalDoc coincide con il Rapporto di versamento.

Questo indice di conservazione, secondo lo standard **UNI 11386 SInCRO 2020**, contiene: una sezione di SelfDescription (con i riferimenti dell'applicativo e del Conservatore), una sezione di PVolume (con lo schema xsd), una sezione MoreInfo per LegalDoc (con token, bucket, policy, operation, target), una sezione FileGroup (con token, hash e SHA dei vari file del pacchetto), una sezione Process (con i riferimenti al manuale, al Responsabile del servizio e al riferimento temporale).

Ogni documento da conservare viene identificato in modo univoco attraverso un token (es. per LegalDoc TB853E72B7552EBB8D0AF3FE9EE1EAB3D97519959346B83DD5E539).

Per "**PACCHETTO DI DISTRIBUZIONE**" si intende un pacchetto informativo inviato dal sistema di conservazione all'utente, in risposta a una sua ricerca e richiesta di esibizione. Il suo contenuto coincide con il "pacchetto di archiviazione".

Eventuali specificità sono concordate con il Soggetto produttore e descritte nelle 'Specificità del Contratto' - Specifiche tecniche per l'integrazione – Allegato Tecnico al Contratto LegalDoc o SAFE LTA. Un pacchetto di archiviazione in LegalDoc è composto da:

- L'Indice di Conservazione UNI SInCRO, altrimenti detto Indice del Pacchetto di Archiviazione o Indice di Conservazione (sigillato e marcato dal Responsabile del servizio di Tinexta Infocert)
- File di parametri (contenente le informazioni per la leggibilità nel tempo)
- File di indici (contenente i metadati del documento conservato)
- File di dati (documento conservato)

Un pacchetto di archiviazione in SAFE LTA è composto da:

- L'Indice di Conservazione UNI SInCRO, altrimenti detto Indice del Pacchetto di Archiviazione o Indice di Conservazione (sigillato e marcato da Tinexta Infocert)
- Metadata Descriptive (file XML di metadattazione)
- Metadata Preservation (file XML di metadattazione secondo lo standard PREMIS)
- Schemas (file XSD di metadattazione)

- Representation (documento conservato)

FORMATI

Tipologie documentali e formati sono sempre concordati con il soggetto produttore, e vengono elencati nelle 'Specificità del Contratto' - 'Scheda Dati Tecnici di attivazione'.

In LegalDoc i visualizzatori di alcuni formati (definiti in Tinexta Infocert come 'standard' perché maggiormente richiesti) sono automaticamente assegnati all'atto dell'attivazione del proprio ambiente di conservazione e sono forniti da Tinexta Infocert al soggetto produttore all'atto di attivazione del servizio.

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

Tutti i documenti inviati in conservazione sono associati al visualizzatore configurato per il particolare formato.

Conservare documenti in altri formati (jpeg, Open Document Format, eml, DICOM, ecc..), in conformità con l'**Allegato 2 delle Linee Guida AgID**, è sempre possibile. Qualora un soggetto produttore necessiti di formati aggiuntivi rispetto a quelli standard, può segnalarlo nei 'Dati Tecnici di attivazione' per LegalDoc o *Submission Agreement* per SAFE LTA (compresi nelle 'Specificità del Contratto') o configurarli autonomamente utilizzando l'apposita funzionalità ed eventualmente conservare gli appositi visualizzatori all'interno del sistema. Un'apposita sezione dell'ambiente di conservazione, infatti, è dedicata alla conservazione dei visualizzatori dei formati (*viewer*), che può essere arricchita a seconda delle esigenze.

METADATI

I metadati sono dati associati ai documenti da conservare in fase di formazione, per identificarli, descrivendone il contesto, il contenuto e la struttura, così da permetterne la gestione del tempo. Nei sistemi di conservazione sono anche utilizzati come chiavi di ricerca.

Le Linee Guida di AgID su formazione gestione e conservazione dei documenti informatici, all'**Allegato 5**, prevedono un set di metadati obbligatori per il documento informatico (maggiormente diffuso), il documento amministrativo informatico (pensato per le pubbliche amministrazioni) e per le aggregazioni documentali (come per esempio i fascicoli).

In breve:

Identificativo del Documento

Un set di metadati serve a identificare il documento da conservare. Si indica il numero utilizzato nel sistema di gestione documentale dove il documento viene formato e gestito, per es. documentID, o identificativo Sdl per le fatture o ID SAP o DossierID. Si indica anche l'impronta di hash e l'algoritmo utilizzato (si suggerisce SHA-256).

Modalità di Formazione

Questo metadato serve a dichiarare come il documento da conservare è stato formato. Le possibilità sono:

- per 'creazione tramite l'utilizzo di strumenti software' (es. documenti scritti al pc)
- per 'acquisizione per via telematica o della copia per immagine' (es. documenti scansionati)
- per 'transazioni o processi informatici o moduli o formulari resi disponibili all'utente' (es. documenti compilati come form online)
- per 'generazione da registrazioni o banca dati' (es. estrazioni da database).

Tipologia Documentale

Metadato che può essere compilato con un valore fisso (default) per determinati processi e che indica per es. contratti, libri sociali, libri e registri contabili, fatture, determine, nota spese, ecc.

Dati di Registrazione

Questo set di metadati descrive un'eventuale registrazione del documento su un registro o repertorio prima del suo versamento in conservazione.

Il flusso può essere:

- in uscita se il documento viene spedito all'esterno dell'azienda/amministrazione
- in entrata se il documento è stato ricevuto dall'esterno
- interno se il documento resta all'interno dell'azienda/amministrazione che lo ha formato.

Il tipo di registro può essere:

- Nessuno
- Protocollo Ordinario/ Protocollo Emergenza
- Repertorio/Registro.

È necessario anche indicare la data e ora di registrazione e il numero attribuito al documento (es. numero del contratto, numero della nota spese, o nel caso dei libri sociali potrebbe coincidere con il progressivo del verbale di assemblea o nel caso di libri fiscali il numero potrebbe essere un progressivo formato da mese e anno).

Oggetto

In questo campo si indica l'oggetto del documento, con particolare attenzione alle parole chiave con cui verrà ricercato in futuro.

Soggetti e Ruoli

Questo set di metadati indica i soggetti vari che sono coinvolti nella formazione e gestione del documento prima del suo versamento in conservazione.

I valori ammessi da AgID sono:

- assegnatario
- autore
- mittente
- destinatario
- operatore
- produttore
- RGD= Responsabile della Gestione Documentale
- RSP= Responsabile del Servizio di Protocollo
- Soggetto che effettua la registrazione
- Altro
- Amministrazione che effettua la registrazione
- RUP= Responsabile Unico del Procedimento

Almeno un soggetto che effettua la registrazione del documento (tipicamente l'Organizzazione che protocolla) e un autore o un mittente vanno indicati obbligatoriamente.

Questi set di metadati possono essere ripetibili.

Per es. possiamo indicare il mittente e il destinatario di una fattura, l'autore e il soggetto che effettua la registrazione di un libro sociale o fiscale, o di una nota spese, l'autore di un contratto.

Per ciascun ruolo è necessario poi specificare anche il tipo di soggetto, tra:

- AS per Assegnatario
- PF per persona fisica
- PG per organizzazione
- PAI per amministrazione pubblica italiana
- PAE per le Amministrazioni Pubbliche estere
- SW per i documenti prodotti automaticamente (Se Ruolo = Produttore)
- RUP per Responsabile Unico del Procedimento.

E per ciascuno si specificano poi rispettivamente nome, cognome (se PF) o denominazione (se PG), ed eventualmente anche il codice fiscale e gli indirizzi mail.

Allegati

Questo set di metadati serve a indicare se il documento da conservare ha allegati, quanti sono (valori ammessi: 0, 1, 2, 3...) e quali sono, legando il documento padre e i suoi allegati con un reciproco rimando, basato sul numero identificativo di ciascun documento.

Classificazione e Fascicolazione

Questo set di metadati, tipicamente utilizzato dalle pubbliche amministrazioni, indica il riferimento al titolo e alla classe del titolare/piano di classificazione, con la possibilità di inserirne la codifica, la descrizione e l'URI per un rimando puntuale.

È possibile indicare anche l'identificativo dell'aggregazione documentale (es. del fascicolo o della serie) a cui il documento da conservare fa riferimento.

Booleani

Alcuni metadati, definiti come 'booleani' vengono popolati solo con 'vero' o 'falso', indicando se il documento conservato è o non è riservato, è o non è firmato digitalmente, è o non è marcato temporalmente, è o non è sigillato, è o non è accompagnato da una certificazione di processo (se scansionato).

Formato

Un set di metadati indica il formato del documento da conservare (es. PDF, XML, ecc.), specificando opzionalmente anche il prodotto software, la versione e il produttore.

Nome File e Versione

Tra i metadati si indicano anche il nome file del documento da conservare e la sua versione (es. 1, 2, 3).

Se la versione è maggiore di 1, cioè si sta versando in conservazione un documento che è una rettifica o un'annotazione o integrazione di un documento già conservato, questa modifica va tracciata con un set di metadati che indica il tipo di modifica, l'identificativo della versione precedente, chi l'ha fatta e quando.

Tempo di Conservazione

Opzionalmente è possibile inserire tra i metadati anche il riferimento alle tempistiche di conservazione, per facilitare le attività di selezione e scarto.

Nei servizi erogati in ambito internazionale, i metadati sono concordati con il produttore, in base alla normativa locale e specifica.

Tipologie documentali e metadati sono sempre concordati con il soggetto produttore, e vengono elencati nelle 'Specificità del Contratto' - 'Scheda Dati Tecnici di attivazione' per LegalDoc o *Submission Agreement* per SAFE LTA, che contengono anche delle note operative per una corretta metadattazione, secondo le Linee Guida AgID e nel 'file di configurazione', che descrive nel dettaglio l'ambiente di conservazione (bucket o Company).

Tuttavia, il produttore può in autonomia aggiungere ulteriori metadati ad ogni versamento.

IL PROCESSO DI CONSERVAZIONE

I sistemi di conservazione sono erogati in modalità **SaaS** (*Software as a Service*) secondo uno schema di *Business Process Outsourcing* (BPO).

I servizi hanno l'obiettivo di mantenere e garantire nel tempo l'integrità, la leggibilità e la validità legale di tutti i documenti informatici conservati, nel rispetto della normativa vigente.

Il processo può essere così schematizzato:

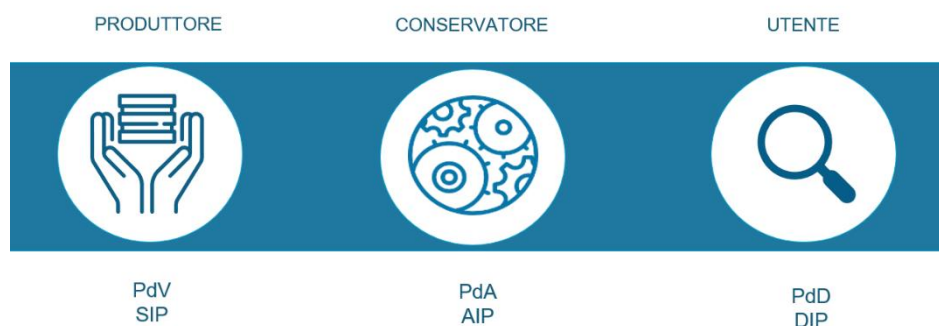


Figura 1 disegno di processo

1. *il produttore invia i documenti in conservazione con un pacchetto di versamento, contenente anche i metadati necessari;*
2. *il pacchetto viene preso in carico dal sistema se rispetta la configurazione concordata (formati, metadati, parametri, policy...) e se l'impronta di hash calcolata coincide con quella contenuta nel pacchetto;*

in SAFE LTA, il sistema restituisce al produttore il link per potere reperire il rapporto di versamento;

3. *il sistema crea i pacchetti di archiviazione; il Responsabile del servizio sigilla e marca temporalmente l'indice di conservazione UNI SInCRO di ogni singolo pacchetto di archiviazione, a garanzia di integrità, immutabilità e autenticità;*

in LegalDoc, il sistema restituisce al produttore l'indice di conservazione come ricevuta (rapporto di versamento);

4. *il database del sistema viene aggiornato, il pacchetto di archiviazione viene indicizzato, memorizzato e ridondato più volte;*
5. *il documento conservato può essere ricercato attraverso i metadati, su richiesta dell'utente in possesso delle apposite credenziali, in qualsiasi momento, ed esibito mediante un pacchetto di distribuzione, che contiene tutte le evidenze del processo.*

I sistemi consentono, quindi, le funzionalità di:

- **accettazione del pacchetto di versamento**, formato dal documento da conservare e dai metadati ad esso associati dal produttore;
- **conservazione del pacchetto di archiviazione**, a norma di legge e per tutta la durata prevista dal contratto;
- **rettifica del pacchetto di archiviazione**, modifica logica, nel pieno rispetto del principio di tracciabilità;
- **ricerca** tra i documenti conservati, utilizzando uno o più metadati popolati in fase di versamento;
- **esibizione del pacchetto di distribuzione**, contenente sia il documento conservato che gli altri documenti a corredo della corretta conservazione, che possono essere scaricati in autonomia, in qualsiasi momento;
- **scarto**, su richiesta formale del Responsabile della conservazione del produttore, cioè cancellazione fisica e logica dei pacchetti di archiviazione e di ogni loro duplicato.

I sistemi di conservazione, quindi, integrano il sistema di gestione documentale del soggetto produttore, sia esso un'azienda o un ente, e ne estendono i servizi con funzionalità di archivio di deposito.

Le fasi di formazione e gestione dei documenti sono organizzate liberamente dal cliente/produttore all'interno del proprio sistema di gestione documentale, in quanto i servizi qui descritti intervengono solamente nella fase di conservazione e solamente per i documenti che il soggetto produttore sceglie di conservare.

CONTROLLI DI VERSAMENTO

In fase di versamento vengono automaticamente eseguiti dei controlli sui pacchetti:

- formato dichiarato del documento da conservare (mime type),
- correttezza della struttura dei pacchetti di versamento,
- controlli formali di coerenza rispetto alla configurazione,
- validazione dei tracciati dei file di indice (metadati),
- abilitazione utenza all'attività di versamento,
- validità sessione in uso.

secondo regole e policy concordate in fase di attivazione 'Specificità del Contratto – Scheda Dati Tecnici per LegalDoc o *Submission Agreement* per SAFE LTA di attivazione e File di configurazione'.

All'interno delle 'Specificità del Contratto' SPT/NDOCERR – Descrizione dei codici di errore di LegalDoc è presente la griglia riassuntiva dei codici errore che il servizio LegalDoc restituisce in seguito a situazioni che impediscono la corretta e completa esecuzione del servizio richiesto. I campi codice e descrizione vengono inseriti nel corpo della risposta HTTP.

La documentazione tecnica per integrare SAFE LTA con altri sistemi via API è disponibile su <https://developers.infocert.digital/>

Al terzo rifiuto del pacchetto, sarà necessario contattare il servizio di assistenza tecnica di Tinexta Infocert per tentare una soluzione del problema.

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

PRODUZIONE DI COPIE O DUPLICATI

All'attivazione del servizio vengono concordate con il soggetto produttore le modalità di ricerca ed esibizione dei documenti conservati ('Specificità del Contratto' - 'Scheda Dati Tecnici di attivazione' per LegalDoc o *Submission Agreement* per SAFE LTA) e vengono create apposite credenziali (user/password).

Gli utenti abilitati possono in qualsiasi momento ricercare e scaricare pacchetti di distribuzione, attraverso interfaccia web o chiamate applicative.

Ogni documento informatico così scaricato in locale è da considerarsi un duplicato, ovvero il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario (CAD art. 1 - i quinquies).

Laddove richiesto dalla natura delle attività, il Responsabile della Conservazione può in autonomia formare copie su diversi supporti dei documenti ottenuti dai pacchetti di distribuzione, anche con l'intervento di un pubblico ufficiale, a garanzia della loro conformità all'originale.

Anche il Responsabile del servizio può valutare il coinvolgimento di un pubblico ufficiale, in relazione all'evolversi dei formati e del contesto tecnologico dei sistemi.

VERIFICHE DI INTEGRITÀ E LEGGIBILITÀ

I sistemi di memorizzazione utilizzati, grazie alle caratteristiche intrinseche dei supporti, alla configurazione architettuale e alle procedure di memorizzazione permanente dei dati, garantiscono l'immodificabilità, l'integrità, la leggibilità e la reperibilità nel sistema di quanto conservato, ai fini della corretta esibizione.

I sistemi mantengono traccia di tutte le operazioni effettuate sui documenti in appositi file di log.

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

In aggiunta, Tinexta Infocert ha attivato sottosistemi di controllo automatico dedicati alla simulazione della navigazione nel sistema e delle operazioni che effettua l'utente, svolgendo controlli di coerenza dei dati e attività di ripristino da situazioni di errore.

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

I servizi assicurano la **verifica periodica**, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi con procedure automatiche e manuali.

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

Vengono eseguiti i seguenti passi operativi:

- calcolo dell'impronta del documento;
- confronto con quella contenuta all'interno del file IPdA;

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

In caso di anomalie, viene inviato un *alert* al Responsabile del servizio della conservazione, che tenterà il ripristino manuale partendo da un'altra sorgente (per esempio le copie di backup). Se nessuna sorgente è disponibile viene redatto un verbale di incidente, sottoscritto e conservato dal Responsabile del servizio per attestare la situazione rilevata. Analoga procedura viene applicata in caso di perdita di tutte le copie del dato.

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

Anche in questo caso viene poi redatto automaticamente un verbale con gli identificativi dei documenti visualizzati, successivamente sottoscritto e conservato dal Responsabile del servizio.

SCARTO DEI PACCHETTI DI ARCHIVIAZIONE

I servizi di conservazione di Tinexta Infocert consentono lo scarto archivistico, cioè la **cancellazione di un pacchetto di archiviazione** e di qualsiasi suo duplicato prodotto durante le attività di conservazione, sia dal punto di vista logico che dal punto di vista fisico, su richiesta formale del Responsabile della conservazione interno al soggetto produttore/titolare del documento.

La procedura può essere attivata per varie ragioni, sia alla chiusura del contratto, sia in continuità di servizio (in itinere), per il venir meno della rilevanza amministrativa, legale o storica dei documenti conservati per il suo produttore, anche in relazione alla *retention period policy* configurata in fase di attivazione del servizio.

Il così detto **scarto in itinere** si può, quindi, richiedere al Customer Care di Tinexta Infocert tramite apposito **modulo**, oppure può essere attivato tramite **chiamate applicative**. In entrambi i casi è richiesta una lista di token firmata digitalmente dal Responsabile della Conservazione interno al produttore/titolare.

Per gli enti pubblici e per gli archivi privati dichiarati di notevole interesse storico, le richieste di scarto sono sottoposte a nulla osta delle soprintendenze archivistiche o delle commissioni di sorveglianza di competenza., verifica che deve essere effettuata dal Responsabile della Conservazione dell'ente.

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

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

Per ulteriori dettagli si rimanda all'apposito documento interno 'Procedura di handover tra conservatori e scarto'.

HANDOVER E INTEROPERABILITÀ

Gli archivi di conservazione generati dai sistemi Tinexta Infocert sono conformi allo standard di interoperabilità **UNI SInCRO**. L'adozione di tale standard permette l'interoperabilità e la trasferibilità dei dati in modo semplificato.

Nel caso il soggetto produttore decida di rescindere, chiudere o interrompere il contratto di affidamento del servizio di conservazione, in qualsiasi momento può effettuare il **download** dei propri **pacchetti di distribuzione** in autonomia, attraverso la procedura di esibizione, o, in alternativa, richiedendo il **servizio di restituzione** (su supporto da concordare in base a volume ed esigenze) tramite apposito **modulo**.

Al termine della procedura di handover verso il nuovo Conservatore, i pacchetti verranno cancellati. Seguendo i dettami dello standard OAIS, il versamento in Tinexta Infocert di pacchetti di distribuzione (PdD) provenienti da un altro Conservatore dovrà riguardare sempre **interi pacchetti**, qualsiasi sia il 'modo' con cui vengono formati e le tipologie di metadati o indici che hanno, e non dovrà mai riguardare il singolo documento. È fondamentale in questa procedura di versamento conservare in Tinexta Infocert quante più informazioni possibili sul processo di conservazione precedente e sul Conservatore di provenienza.

Per ulteriori dettagli si rimanda all'apposito documento interno 'Procedura di handover e scarto'.

RICERCA ED ESIBIZIONE DEI DOCUMENTI CONSERVATI

La ricerca e l'esibizione a norma dei documenti conservati può avvenire tramite chiamate applicative o tramite portale WEB.

Le chiavi di ricerca sono i metadati popolati in fase di versamento.

I sistemi restituiscono un pacchetto di distribuzione, contenente sia il documento conservato che tutti i report e le evidenze di conservazione.

La guida al portale LegalDoc WEB è disponibile qui:

<https://knowledgecenter.infocert.digital/Home/Guida/manuale-utente-legaldoc-web?lang=it>

La guida al portale SAFE LTA WEB è disponibile qui:

<https://knowledgecenter.infocert.digital/Home/Guida/manuale-utente-safe-lta>

I SISTEMI DI CONSERVAZIONE

I sistemi sono organizzati su più siti nel territorio italiano (Region AWS Milano), con applicazioni software in architettura distribuita, utilizzano servizi AWS in modalità SaaS, e una serie di servizi di interesse generalizzato condivisi con altre applicazioni (marca temporale, firme digitali e sigilli, supporti di conservazione).

Per ragioni di sicurezza, i sistemi sono protetti da firewall configurati in alta affidabilità e costantemente aggiornati per assicurare i massimi livelli di protezione possibile. Gli interi sistemi sono interessati periodicamente da processi di back-up completi dei documenti, delle evidenze qualificanti il processo, dei database di gestione del sistema e di ogni altra informazione necessaria.

I servizi di conservazione sono accessibili online, tramite portale o chiamate applicative e sono erogati anch'essi in modalità SaaS.

Dal punto di vista architetturale **LegalDoc** è realizzato utilizzando la tecnologia dei Web Services, secondo architettura REST su protocollo HTTPS. Solo per un ristretto numero di Clienti viene utilizzato uno storage presente nel DataCenter di Milano. Ha quindi un'architettura HYBRID Cloud.

Dal punto di vista architetturale **SAFE LTA** si basa su architettura a microservizi, espone api REST-ful e aderisce allo standard OAuth2 / OIDC per quanto riguarda gli scenari di autenticazione / autorizzazione. L'autenticazione utilizza Kong e Keycloak.

Rispetta lo standard ISO 14721 recante il reference model OAIS (*Open Archival Information System*) utilizzato a livello internazionale per la conservazione di risorse digitali e lo standard PREMIS per la metadattazione.

SAFE LTA è interamente erogato su cloud AWS, ha quindi un'architettura PUBLIC Cloud.

I servizi generalizzati usati da servizi di conservazione sono:

- Identity Provider Tinexta Infocert, in quanto Provider ed erogatore di servizi riferiti alla identità digitale,
- SignAPI Tinexta Infocert, in quanto Provider ed erogatore di servizi legati alla Certification Authority.

Sia le applicazioni WEB di interfaccia sia le API REST sono adoperabili solo previa autenticazione: per LegalDoc

- In entrambi i casi l'autenticazione è una basic authentication

per SAFE LTA

- l'autenticazione da interfaccia web è governata attraverso flusso di *authorization-code-flow*, così come previsto da standard,
- l'autenticazione da agenti software che integrano le API REST è governata da flusso di *client-credential-flow*, così come previsto da standard.

Le funzionalità fruibili sono:

- Invio in conservazione dei pacchetti di versamento
- Attività di ricerca avanzata
- Recupero di documenti e metadati
- Download di pacchetti di distribuzione.

Inoltre, per SAFE LTA sono previste le seguenti funzionalità

- Provisioning
- Gestione utenti, gruppi e autorizzazioni

I servizi di conservazione non solo effettuano la validazione di pacchetti di versamento, ma si occupano anche di effettuare una verifica formale dei formati.

Tutte le interazioni tra gli utenti e l'archivio sono registrate in appositi log per ragioni di sicurezza e trasparenza.

La configurazione degli ambienti di conservazione di Legaldoc prevede le seguenti definizioni:

- **Bucket:** è l'area di conservazione dei documenti
- **Policy;** descrive le regole che devono essere seguite durante il processo di conservazione (mime type si possono usare, durata del retention period, etc)
- **Classe documentale:** identifica una tipologia documentale con i suoi metadati. Ad esempio: fatture attive, contratti, libri e registri contabili, ecc.

La configurazione degli ambienti di conservazione di SAFE LTA prevede le seguenti definizioni:

- **Company Group:** identifica un contenitore logico dal quale possono dipendere una o più Company, cioè aree di conservazione. Ogni Company Group è ad uso esclusivo di un solo cliente/titolare.
- **Company:** area di conservazione dei documenti, che può essere usata, ad esempio, per raggruppare i documenti delle diverse società/aziende di un gruppo (Company Group), denominando ogni Company con il nome della singola azienda facente parte del Gruppo.
- **Country:** identifica gli standard normativi adottati dal sistema per la conservazione rispetto alle varie geografie, ed è configurabile a livello di Company.
- **Document Class:** identifica una tipologia documentale con i suoi metadati. Ad esempio: fatture attive, contratti, libri e registri contabili, ecc.

La documentazione tecnica di dettaglio è disponibile su <https://developers.infocert.digital/>

SIGILLO DEI PACCHETTI DI ARCHIVIAZIONE

Al buon esito del processo di conservazione, su ogni pacchetto di archiviazione il Responsabile del servizio della conservazione di Tinexta Infocert appone:

- **in Legaldoc una firma digitale qualificata con certificato intestato al Responsabile del servizio di conservazione di Tinexta Infocert**
- **in SafeLTA un sigillo qualificato a nome di Tinexta Infocert.**

Il servizio utilizza un sistema automatico erogato dalla CA - Certification Authority – Tinexta Infocert.

MARCA TEMPORALE DEI PACCHETTI DI ARCHIVIAZIONE

Al buon esito del processo di conservazione, viene apposta anche una marca temporale su ogni pacchetto di archiviazione. La marca temporale viene richiesta al TSS - *Time Stamping Service* - Tinexta Infocert, che la restituisce firmata con un certificato emesso dalla TSA - *Time Stamping Authority* - Tinexta Infocert. Il TSS è sincronizzato tramite i segnali forniti dai sistemi satellitari GPS, Galileo e

GLONASS ed è protetto contro la manomissione della sincronizzazione mediante misure fisiche e logiche, nel pieno rispetto delle norme di legge.

STORAGE

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

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

Per garantire la riservatezza vengono applicate appropriate politiche sulle autorizzazioni che prevedano la cifratura di tutti i documenti.

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

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

Per entrambi i servizi cloud è stata scelta AWS Europe (*Region Milan*), quindi, tutti i dati risiedono in **territorio italiano**.

SICUREZZA E PROTEZIONE DEI DATI

Tinexta Infocert si impegna a mantenere i più alti livelli di qualità e sicurezza, assegna un'importanza strategica alla gestione sicura delle informazioni e riconosce la necessità di sviluppare, mantenere, controllare e migliorare costantemente un **sistema di gestione della sicurezza delle informazioni (ISMS)** in conformità alla **norma UNI CEI EN ISO/IEC 27001: 2017**. Nella policy di sicurezza di Tinexta Infocert per ciascun capitolo della norma ISO vengono fornite le indicazioni da seguire nello svolgimento di tutte le attività. In particolar modo:

- *Management direction for information security,*
- *Organization of information security,*
- *Human resource security,*
- *Asset management,*
- *Access control, Cryptography,*
- *Physical and environmental security,*
- *Operations security,*
- *Communications security,*
- *System acquisition, development, and maintenance,*
- *Supplier relationships,*
- *Information security incident management,*
- *Information security aspects of business continuity management,*
- *Compliance with legal and contractual requirements.*

Tinexta Infocert ha anche ottenuto il **Report SOC 2 Tipo II**, su sicurezza, disponibilità, integrità del trattamento, riservatezza e privacy dei servizi, in conformità all'International **Standard on Assurance Engagements (ISAE) 3000**.

I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio. L'azienda ha mappato tutti i flussi di dati interni e di quelli da e per l'esterno. Sono implementati controlli automatici per evitare l'interconnessione con server esterni non autorizzati. L'accesso alla rete e ai sistemi è consentito esclusivamente agli utenti autorizzati, seguendo quanto prescritto dalla policy aziendale relativa agli Amministratori di Sistema e alla gestione degli accessi logici. Le risorse (es: hardware, dispositivi, dati, allocazione temporale, personale e software) sono priorizzate in base alla loro classificazione (e.g. confidenzialità, integrità, disponibilità), criticità e valore per il business dell'organizzazione. Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity e al trattamento e la protezione dei dati personali per tutto il personale e per eventuali terze parti rilevanti.

A supporto di tali censimenti è stato implementato un CMDB (*Configuration Management Data Base*). Viene effettuata una valutazione di impatto sulla protezione dei dati personali. Il ciclo di vita dei dati è definito e documentato.

Tutti gli accessi (fisici e logici) sono regolati da policy apposite. I diritti di accesso sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni.

L'integrità di rete è protetta. Le reti di comunicazione e controllo sono protette.

I processi di risk management sono stabiliti, gestiti e concordati tra i responsabili.

Sono attivi ed amministrati piani di *Incident Response* e di *Business Continuity, Incident Recovery, Disaster Recovery e Vulnerability Management*.

I sistemi informativi, il personale e gli asset sono costantemente monitorati per identificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione. Sono implementati meccanismi che permettono di soddisfare requisiti di resilienza sia durante il normale esercizio che in situazioni avverse. È attiva una policy di gestione dei log, inclusiva della conservazione dei log di sicurezza dei sistemi.

L'organizzazione ha implementato un processo formalizzato di *Incident Management* che include i criteri per documentare l'incidente ai fini del *problem management*, delle comunicazioni istituzionali e delle comunicazioni verso gli stakeholder.

Tutti gli utenti sono informati e addestrati.

Ai sensi del Regolamento UE n. 679/2016 GDPR, Tinexta Infocert assume il ruolo di Responsabile del trattamento dei dati personali. La nomina è inserita all'interno delle "Specificità del Contratto – Atto di Affidamento".

Il trattamento dei dati è effettuato:

- ai soli fini dell'erogazione del servizio,
- con l'adozione delle misure di sicurezza ex art. 32 del Regolamento,
- nel rispetto degli obblighi posti in carico al Responsabile del trattamento dall'art. 28 del Regolamento.

PROCEDURE DI GESTIONE E MONITORAGGIO

I sistemi di conservazione di Tinexta Infocert e i processi da questi implementati rispondono interamente alle norme di legge che regolano la materia. La loro progettazione e il loro continuo miglioramento sono il frutto di una intensa opera di confronto tra le professionalità e le competenze delle diverse funzioni aziendali, al fine di giungere all'erogazione di servizi architetturealmente stabili, affidabili, e che

garantiscano elevati livelli di servizio all'utente, in condizioni di assoluta sicurezza, certezza degli accessi e tracciabilità delle operazioni.

Punto fondante del processo di progettazione è l'attenta disamina delle norme e degli standard, al fine di definire puntualmente i requisiti di *compliance*. Oltre a questi sono definiti ulteriori requisiti funzionali, di architettura e di connettività e interoperabilità, anche in relazione con le evoluzioni tecnologiche, sfruttando le economie di scala e di conoscenza. I Responsabili Tinexta Infocert, infatti, sono costantemente impegnati nell'attività di *technology watch* attraverso la partecipazione a gruppi di lavoro nazionali e internazionali, forum e associazioni di settore, con lo scopo di monitorare e prevenire l'obsolescenza tecnologica sia logica che fisica.

Inoltre, Tinexta Infocert ha deciso di adottare un sistema di gestione dei servizi IT (SMS) conforme a **ISO IEC 20000** (standard internazionale di gestione dei servizi IT) al fine di mantenere e migliorare la qualità dei servizi aziendali che fornisce. Questi hanno un'attenzione particolare alle esigenze dei clienti, sostenuti da un ciclo continuo di monitoraggio, reporting e revisione degli SLA concordati.

Inoltre, Tinexta Infocert ha adottato un sistema di gestione dei servizi IT (SMS) certificato per la norma **ISO/IEC 20000-1:2018** (standard internazionale di gestione dei servizi IT) al fine di mantenere e migliorare la qualità dei servizi aziendali che fornisce. Questi hanno un'attenzione particolare alle esigenze dei clienti, sostenuti da un ciclo continuo di monitoraggio, reporting e revisione degli **SLA concordati**.

Tale modello di *Service Management System* ha permesso di:

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

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

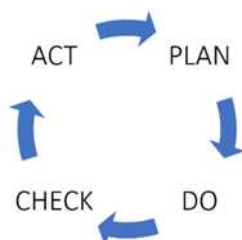


Figura 2 Rappresentazione del modello PDCA SMS

- istituzione del sistema - SMS (Plan) in cui si definiscono e si pianificano le politiche e i requisiti per la gestione dei servizi inerenti il campo di applicazione; si stabiliscono gli obiettivi di gestione del servizio a tutti i livelli pertinenti;

- implementazione ed attuazione del sistema-SMS (Do) e dei processi di design, transition, delivery e improvement continuo dei servizi sulla base di quanto definito nel service management plan, con particolare attenzione al controllo delle modifiche al SMS valutando e limitando i rischi;
- azioni di monitoraggio e revisione del sistema-SMS (Check);
- attuazione di misure a miglioramento del sistema-SMS (Act) ove sono pianificate e attuate idonee azioni correttive sulla base dei risultati della fase precedente.

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

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

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

- orario di servizio
- disponibilità di servizio.

Inoltre, Tinexta Infocert si è dotata di una soluzione di monitoraggio open source denominata Grafana LGTM (Loki Grafana Tempo Mimir), un'architettura autogestita in-house nella Region "Milano" del fornitore AWS, che permette la completa gestione dei dati di osservabilità ai Team DEVOPS.

Questa piattaforma di osservabilità abilita i Team DEVOPS di identificare e analizzare problemi di tipo infrastrutturale e applicativo.

Utilizzando un evoluto sistema di gestione e raccolta dati effettua un monitoring full-stack, fornisce gli strumenti per l'ottimizzazione dei servizi, oltre ad un'efficiente gestione di segnalazione degli incident.

Inoltre, è stata abilitata l'integrazione con le piattaforme di controllo Cloudwatch, tool nativi di AWS, che consente di avere il pieno controllo e la gestione delle metriche e log di tutte le "componenti gestite" presenti in cloud.

Il tool è composto dai seguenti elementi fondamentali:

- AGENT: risiedono sui server e collezionano i segnali di telemetria inviando (con connessione unidirezionale) i dati alla piattaforma centrale posta in cloud attraverso protocollo TLS. Gli agent effettuano un controllo sia di tipo infrastrutturale che di performance, consentendo anche la costruzione di schemi architetturali tra i servizi;
- GRAFANA SERVER: è il cuore dello strumento, dove i segnali sono accessibili tramite linguaggi di query dedicati consentendo di gestire, aggregare ed elaborare i dati, definendo la modalità di visualizzazione e gestione di eventuali alert;
- SONDE: possono essere di tipo "black box" oppure script di navigazione complessi, eseguiti da location privata o pubblica; grazie a questa diversa collocazione è possibile verificare il corretto funzionamento di un servizio sia della rete interna che da rete Internet.

Con le metriche raccolte si popola una base di dati in ottica di business intelligence, che risulta di fondamentale importanza per la redazione della reportistica riguardante gli SLA dei vari servizi ma anche, e soprattutto, per supportare i processi di decisione aziendale.

La soluzione di monitoraggio fin qui descritta risulta indispensabile per individuare e prevenire tempestivamente anomalie sui servizi erogati da Tinexta Infocert, segnalando in modo puntuale le componenti impattate.

Il monitoring della disponibilità del servizio viene svolto coerentemente con le procedure generali di Tinexta Infocert. In particolare, tutte le componenti costituenti il sistema di conservazione, ovvero i servizi applicativi, i processi di elaborazione batch e le interfacce per l'utente finale, sono monitorate con i tool definiti nella piattaforma precedentemente descritta.

A fronte di anomalie rilevate, lo strumento, grazie all'integrazione nativa, invia delle segnalazioni ad OPSGENIE, tool di gestione delle notifiche in conformità ai processi di Incident Management aziendali. Tali processi sono descritti nelle procedure che definiscono il Sistema di gestione integrato Tinexta Infocert.

CONTROLLI PERIODICI E AUDIT

In Tinexta Infocert è attiva una struttura appositamente preposta alla supervisione e controllo della gestione dei problemi e del rispetto dei livelli del sistema per tutte le applicazioni. La struttura si avvale di un gruppo di lavoro trasversale, ed effettua la raccolta dei dati relativi al funzionamento dei servizi. Il gruppo si riunisce periodicamente, al fine di individuare le cause dei malfunzionamenti registrati nel periodo, analizzare le soluzioni contingenti adottate per il superamento del problema e sviluppare eventuali proposte per rimedi strutturali.

Ad ogni semestre il Responsabile del servizio della conservazione effettua un riesame generale del sistema insieme ai soggetti incaricati, al fine di accertare la conformità del sistema al livello atteso, analizzare le cause di eventuali incidenti o disservizi e promuovere attività di prevenzione o miglioramento. Qualora necessario, una riunione di riesame può essere indetta a fronte di particolari eventi (ad esempio, a titolo non esaustivo, cambi tecnologici, normativi o di requisiti funzionali, stagionalità di carico elaborativo, arrivo consistente e non pianificato di nuova clientela, ecc.).

Inoltre, il programma di audit aziendale è attuato secondo le procedure del Sistema Integrato di Gestione, con il fine di determinare se i processi aziendali sono:

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

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

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

- strutture organizzative
- risorse utilizzate

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

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

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

SPECIFICITÀ DEL CONTRATTO

Le **Condizioni Generali di Contratto** o **Accordo Quadro** regolano la vendita in generale di tutti i servizi Tinexta Infocert.

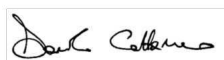
A questi tipicamente si aggiungono i seguenti allegati:

- Allegato A – Offerta Commerciale,**
- Allegato B – DPA - Data Processing Agreement,**
- Allegato C – Allegato Tecnico,**
- Allegato D – Misure di Sicurezza,**
- Allegato E – Manuale Operativo**, cioè il presente manuale.

Nell'**Allegato C – Allegato Tecnico** sono descritte le condizioni particolari di LegalDoc e SAFE LTA ed è inserito l'**Atto di Affidamento**, che rappresenta la formalizzazione della delega ad Tinexta Infocert del servizio di conservazione e stabilisce espressamente quali attività di fatto vengano assunte da Tinexta Infocert e quali, al contrario, rimangano a carico dell'affidatario, soggetto produttore, come stabilito dalle Linee Guida AgID.

Qui è maggiormente dettagliata anche l'infrastruttura tecnica e l'architettura di ciascun servizio.

Sono richiamati anche la **Scheda dati tecnici d'attivazione** per LegalDoc e il **Submission Agreement** per SAFE LTA, con cui il soggetto produttore/cliente/titolare fornisce tutte le informazioni necessarie su tipologie documentali, metadati, formati e utenze di accesso, per la configurazione degli ambienti di conservazione.



Firmato
digitalmente da:
Danilo Cattaneo

tinexta
infocert

think next,
trust now



CONDIZIONI GENERALI DI CONTRATTO DEI SERVIZI INFOCERT **("Accordo")**

1. OGGETTO

1.1 Con il presente Accordo, InfoCert concede al Cliente:

- a) la fornitura di servizi sottoposti a regolamentazione normativa specifica per i servizi *Trust* (di seguito i "**Servizi**"), alle condizioni economiche di cui all'**Allegato A - Offerta Commerciale** e osservando le modalità previste per ciascuno di essi, nel rispetto della disciplina afferente ai dati personali disciplinata nell'**Allegato B - DPA** e nell'**Allegato C – Allegato Tecnico** e nel **Manuale Operativo**, come di volta in volta aggiornato, che il Cliente ha letto e compreso e i cui riferimenti sono inseriti all'interno di ciascun **Allegato C**, ove è applicabile. I Servizi, ove possibile, potranno essere impiegati anche da parte di soggetti terzi utilizzatori (di seguito "**Utente/i**"), il cui numero è indicato nella relativa Offerta Commerciale, e l'Utente potrà accedervi unicamente tramite accesso remoto dai propri terminali; e/o
- b) se previsto, la licenza d'uso ("**Licenza**") di una piattaforma ("**Software**") come meglio definita anch'essa nell'**Allegato A – Offerta Commerciale** e nell'**Allegato C - Allegato Tecnico**;

1.2 InfoCert si impegna, ove previsto, a fornire al Cliente il supporto tecnico secondo i livelli di servizio specificati nell'**Allegato C - Allegato Tecnico**; e, sempre ove previsti, eventuali servizi di formazione, di consulenza e assistenza disciplinati nell'**Allegato A – Offerta Commerciale**.

1.3 In caso di contrasto tra le previsioni contenute nell'Accordo e negli Allegati, queste ultime prevarranno.

2. OBBLIGHI E GARANZIE DEL CLIENTE

2.1 Il Cliente, si impegna a:

- a) utilizzare i Servizi e/o il Software nel rispetto delle leggi, dei regolamenti vigenti e per le finalità d'uso ai sensi del presente Accordo;
- b) non depositare, inviare, pubblicare, trasmettere e/o condividere applicazioni o documenti informatici che:
 - (i) siano in contrasto o violino diritti di proprietà intellettuale, segreti commerciali, marchi, brevetti o altri diritti di proprietà di terzi;
 - (ii) veicolino contenuti diffamatori, calunniosi o minacciosi;
 - (iii) contengano materiale pornografico, osceno o comunque contrario alla pubblica morale;
 - (iv) contengano virus, *worm*, *trojan* o altre caratteristiche di contaminazione o distruttive;
 - (v) danneggino, violino o tentino di violare il segreto della corrispondenza e il diritto alla riservatezza;
 - (vi) siano in contrasto alle disposizioni normative e/o regolamentari applicabili;
 - (vii) possano causare malfunzionamenti o danni ai sistemi di InfoCert;
- c) non trasferire, cedere, copiare, modificare, decompilare, disassemblare, distribuire anche *online*, concedere in uso a terzi (ad eccezione degli Utenti), rivendere, noleggiare e/o riallocare il Servizio e/o il Software;
- d) non porre in essere alcun comportamento che possa costituire violazione dei Diritti IP sulla Licenza e/o sui Servizi oggetto del presente Accordo;
- e) rendere edotto l'Utente delle previsioni del presente Accordo e, in particolare, degli obblighi ed oneri specificamente richiesti ai fini dell'utilizzo dei Servizi e/o del Software. Il Cliente, anche per conto dell'Utente, si impegna a fornire tutte le informazioni necessarie all'attivazione dei Servizi e/o Software e a dotarsi di tutti i requisiti necessari per l'accesso agli stessi come meglio specificati nei relativi Allegati;
- f) assumere, anche per conto degli Utenti, ogni responsabilità sull'utilizzo dei Servizi e/o del Software sulle azioni e sulle attività poste in essere dagli stessi;
- g) attenersi ai principi di buona fede e correttezza nell'uso e nella fruizione del Software e/o dei Servizi;



h) fornire in modo chiaro tutte le informazioni e i dati utili o necessari a consentire la corretta esecuzione del contratto.

- 2.2** Il Cliente si impegna per tutta la Durata dell'Accordo a garantire che eventuali servizi di informatica, prestati in suo favore da terze parti, non interferiscano con la corretta erogazione dei Servizi e/o del Software e non ostacolino o rendano l'esecuzione più onerosa per InfoCert, rispetto a quanto previsto nel presente Accordo. Nel caso in cui rilevi problemi nella fruizione del Software e/o dei Servizi, il Cliente si impegna a dare tempestiva comunicazione scritta a InfoCert, ai sensi dell'art. 21.1, identificando in dettaglio le disfunzioni riscontrate, così da consentire ad InfoCert l'adozione di tutte le misure eventualmente necessarie.
- 2.3** Qualora, nella fornitura di Licenza, sia previsto lo sviluppo del *front-end* da parte del Cliente, quest'ultimo si impegna a rispettare tutte le misure, garanzie e specifiche, come definite nell'Allegato Tecnico sub C.
- 2.4** Il Cliente si impegna a rispettare e/o implementare le misure di sicurezza come previste negli Allegati sub B e D.
- 2.5** Il Cliente si impegna a verificare, prima dell'acquisto del Servizio e/o della Licenza (e così del Software) che, rispetto a quelli richiesti per l'utilizzo e per le finalità degli stessi, i propri sistemi *hardware* e software siano idonei ed aggiornati all'ultima versione disponibile e/o, comunque, compatibile con quella eventualmente indicata da InfoCert. Il Cliente, pertanto, provvederà personalmente a configurare correttamente il proprio *hardware* e a installare il Software idoneo propedeutico all'utilizzo del Servizio. Il Cliente usufruirà dei Servizi e/o del Software tramite il collegamento internet di cui si dovrà dotare autonomamente per il tramite di un operatore di telecomunicazioni, rispondente ai requisiti indicati nell'Allegato sub C e nel Manuale Operativo.
- 2.6** InfoCert informa il Cliente che la conoscenza, da parte di soggetti terzi, degli strumenti di autenticazione necessari per usufruire dei Servizi e/o della Licenza, potrebbe consentire anche a soggetti estranei e quindi diversi dall'Utente/utilizzatore l'accesso agli stessi (o, a titolo esemplificativo, alla casella di posta elettronica certificata assegnata al medesimo) e ai dati in essa contenuti. Al fine di evitare qualunque tipo di accesso indebito, il Cliente e/o l'Utente sono/saranno tenuti a conservare detti strumenti di autenticazione con la massima riservatezza e diligenza, in modo da impedirne la conoscenza a terzi.

3. OBBLIGHI E GARANZIE DI INFOCERT

3.1 InfoCert dichiara e garantisce:

- (a) di rispettare le misure di sicurezza indicate dalla normativa in materia di protezione dei dati personali nonché dai provvedimenti delle autorità competenti laddove applicabili;
- (b) con riguardo alla tutela dei dati, di proteggere gli stessi in caso di sottrazione o distruzione intenzionale o accidentale, perdita accidentale, alterazioni, uso non autorizzato, modifiche, divulgazione, diffusione, accessi non previsti e ogni altra forma di trattamento illecito;
- (c) di utilizzare i sistemi di accesso dotati di funzionalità di *data security* atti a monitorare e controllare il flusso di dati personali attraverso gli *endpoint* (a titolo esemplificativo, analisi e correlazione *real-time* dei *log* mediante servizio SOC/SIEM ai fini dell'identificazione di eventi anomali) o verso le reti esterne (a titolo esemplificativo, limitazione dell'accesso di rete ai soli servizi web funzionali alla richiesta dei certificati);

3.2 InfoCert non fornisce alcuna garanzia espressa o implicita relativamente ai Servizi e/o Software forniti per: assenza di vizi; originalità o idoneità del Software e/o dei Servizi per un uso specifico o per il raggiungimento di un particolare scopo.

3.3 È escluso ogni obbligo di vigilanza e/o sorveglianza, da parte di InfoCert, sui contenuti dei documenti formati, trasmessi o conservati nell'ambito dell'esecuzione del presente Accordo, essendo tali attività svolte sotto l'esclusivo controllo, e quindi di esclusiva responsabilità, del Cliente.

InfoCert SpA

Piazzale Flaminio 1/B, 00196 – Roma (RM), Italia
T +39 06 836691 F +39 06 833669634
info@infocert.it
infocert.it infocert.digital

Società soggetta alla direzione e coordinamento di Tinexta SpA
P.IVA 07945211006 REA n. 1064345
Cap. Soc. Sottoscritto e versato € 21.099.232,00



- 3.4 Fatto salvo quanto previsto dal precedente paragrafo, InfoCert potrà a modificare, a costi e spese del Cliente stesso – come concordati tra le Parti - e su richiesta scritta di quest'ultimo, le modalità di erogazione del Software e/o Servizi che si dovessero rendere necessarie a causa di:
- (a) informazioni errate fornite dal Cliente;
 - (b) informazioni derivanti da errori di programmazione o di elaborazione di dati imputabili al Cliente.
- 3.5 InfoCert potrà, a sua discrezione, avvalersi e incaricare subfornitori nell'erogazione del Software e/o dei Servizi. In ogni caso, InfoCert rimarrà sempre l'unico soggetto responsabile nei confronti del Cliente ai sensi del presente Accordo. In tale ipotesi, InfoCert dichiara sin da ora di aver regolato il rapporto con tali società terze con apposito contratto, nel rispetto della normativa applicabile, anche in materia di trattamento dei dati personali.
- 3.6 InfoCert provvederà: (i) all'adeguamento di carattere tecnico e normativo dei Servizi e/o del Software, dandone comunicazione tramite posta elettronica certificata al Cliente i quali si impegnano ad adeguare le caratteristiche dei propri sistemi e la propria strumentazione alle modifiche indicate, entro il termine assegnato da InfoCert; (ii) alla manutenzione correttiva ed all'aggiornamento dei Servizi e/o del Software per esigenze di rettifica degli eventuali errori presenti sul Software e/o sui Servizi. L'aggiornamento consiste nell'attività necessaria ad adeguare i Servizi e/o il Software ad eventuali evoluzioni normative. In caso di particolari mutamenti della normativa od obsolescenza della tecnologia utilizzata che rendano eccessivamente onerosa l'attività di aggiornamento (i.e., modifiche del Software superiori al 25%), InfoCert si riserva la facoltà di non adeguare i Servizi e/o il Software provvedendo al rilascio, secondo le condizioni tecniche ed economiche che saranno previamente comunicate al Cliente, di nuovi applicativi Software.
- 3.7 InfoCert, su richiesta del Cliente, potrà mettere a disposizione le relative misure di sicurezza, contenute in apposito **Allegato D**, che elenca le misure di sicurezza tecniche ed organizzative implementate da InfoCert che saranno poste in essere per permettere, a titolo esemplificativo ma non esaustivo, l'esecuzione di pratiche di sicurezza nel cloud, la continuità di servizio, le procedure di *disaster recovery* e la gestione degli *incident*. Tale Allegato è parte integrante e sostanziale del presente Accordo.

4. QUALITÀ DEI SERVIZI

- 4.1 Fermo quanto previsto ai precedenti articoli, i Servizi verranno da InfoCert realizzati secondo modalità, caratteristiche e contenuti indicati nel relativo Allegato Tecnico. InfoCert risponderà, nei confronti del Cliente, solo ed esclusivamente di quei difetti di conformità e/o completezza del Servizio rispetto a tali modalità, caratteristiche e contenuti, che rendano il Servizio inidoneo all'uso cui è destinato (c.d. difetti sostanziali).
- 4.2 L'eventuale presenza, nel Servizio reso, di difetti sostanziali dovrà essere dal Cliente denunciata, a pena di decadenza, entro 8 (otto) giorni dalla scoperta e, in ogni caso, entro e non oltre 90 (novanta) giorni dall'evasione del Servizio contestato. Una volta ricevuta la denuncia di cui al precedente punto, InfoCert procederà, ove necessario, all'immediato integrale rifacimento del Servizio contestato. Il relativo costo sarà addebitato al Cliente, qualora venisse dimostrato che il Servizio originariamente reso non presentava difetti sostanziali; diversamente resterà a carico di InfoCert.
- 4.3 Relativamente ai Servizi per i quali è previsto un corrispettivo unitario, qualora, per causa imputabile ad InfoCert, il singolo Servizio reso dovesse presentare difetti sostanziali, la stessa InfoCert corrisponderà al Cliente, a titolo di penale, un importo pari al doppio del corrispettivo dal Cliente stesso dovuto per il Servizio risultato inficiato da difetti sostanziali. In ogni caso, nessuna penale e nessun risarcimento saranno dovuti se, nel corso del mese, risulterà evaso senza difetti sostanziali almeno il 95% (novantacinque per cento) dei Servizi a corrispettivo unitario resi al Cliente in quello stesso mese.
- 4.4 Relativamente ai Servizi per i quali è previsto un corrispettivo a canone forfettario, qualora in un determinato mese dovessero essere messi a disposizione del Cliente Servizi che – per causa imputabile a InfoCert a

InfoCert SpA

Piazzale Flaminio 1/B, 00196 – Roma (RM), Italia
T +39 06 836691 F +39 06 833669634
info@infocert.it
infocert.it infocert.digital

Società soggetta alla direzione e coordinamento di Tinexta SpA
P.IVA 07945211006 REA n. 1064345
Cap. Soc. Sottoscritto e versato € 21.099.232,00



titolo di dolo o colpa grave – presentassero difetti sostanziali in percentuale superiore al 5% (cinque per cento) rispetto al complesso dei Servizi messi a disposizione del Cliente stesso nel mese, InfoCert corrisponderà a quest'ultimo, a titolo di penale, un importo pari al 6% (sei per cento) del canone mensile contrattualmente previsto per il Servizio risultato inficiato da difetti sostanziali.

4.5 In ogni caso, per ogni anno di vigenza del rapporto contrattuale, non potranno esser corrisposte da InfoCert penali per un importo che superi l'ammontare dei corrispettivi annui dovuti dal Cliente a InfoCert per la fornitura dei Servizi.

4.6 InfoCert dichiara – ed il Cliente ne prende atto – che attualmente la stessa ha in essere e che manterrà in essere anche in futuro una polizza assicurativa a copertura dei rischi derivanti dalla violazione delle previsioni di cui al presente articolo.

5. SUPPORTO E ASSISTENZA

5.1 I Per qualsiasi informazione relativa a modalità, caratteristiche e contenuti dei Servizi fruiti in forza del presente Accordo, il Cliente potrà mettersi in contatto con la funzione Customer Care, operativa dalle ore 8.30 alle ore 19.00 dal lunedì al venerdì, escluse le giornate festive infrasettimanali, i cui riferimenti sono rinvenibili al seguente link: help.infocert.it/contatti. E' parimenti possibile fruire per il Cliente di una apposita piattaforma di ticketing, attraverso cui aprire le segnalazioni.

6. ADEMPIMENTI IN MATERIA DI SICUREZZA E SALUTE SUL LAVORO

6.1 Con esclusivo riferimento alla richiesta di fornitura di Servizi da parte del Cliente, InfoCert si impegna a rispettare ed a far rispettare, dalle persone delle quali si avvale per l'esecuzione delle proprie attività, tutte le norme di legge per la prevenzione degli infortuni e sull'igiene sul lavoro. A tal fine, ai sensi dell'art. 26, c. 1 lett. b), D.Lgs. 81/2008, ove applicabile, il Cliente invierà ad InfoCert ogni informazione relativa ai rischi specifici esistenti nei luoghi in cui InfoCert opererà nonché alle misure di prevenzione e di emergenza adottate in relazione alla propria attività e a tali luoghi, sia nel caso in cui i dipendenti di InfoCert prestino la propria attività lavorativa presso i locali del Cliente sia che prestino tale attività altrove.

6.2 InfoCert si impegna a corrispondere ai propri lavoratori i trattamenti retributivi, contributivi, assicurativi e fiscali dovuti. InfoCert, su richiesta scritta del Cliente, inoltrerà a quest'ultimo copia del Documento Unico di Regolarità Contributiva (DURC) in corso di validità. I costi relativi alla sicurezza sono specificatamente indicati negli Ordini.

6.3 Con esclusivo riferimento alla fornitura di Servizi, ai sensi e per gli effetti di cui all'art. 26, comma 3, del D.Lgs. 81/2008 e successive modifiche e integrazioni, qualora le Parti, all'esito della valutazione dei rischi di eventuali interferenze, non escludano la sussistenza di rischi da interferenza, in particolare in relazione con le attività dei lavoratori del Cliente, quest'ultimo predisporrà un Documento Unico di Valutazione dei Rischi di eventuali Interferenze (DUVRI), recante descrizione delle misure adottate per eliminare possibili interferenze, che verrà allegato all'Accordo e che costituirà parte integrante e sostanziale di quest'ultimo.

7. PROPRIETA' INTELLETTUALE

7.1 Tutti i diritti di utilizzazione e di sfruttamento, anche economico, del Servizio e/o della Licenza in essi presenti, sono riservati a InfoCert. Al Cliente e/o all'Utente è concesso l'uso dei Servizi e/o della Licenza nei limiti e alle condizioni stabilite nel presente Accordo.

7.2 Tutti i dati, documenti e/o materiali forniti da InfoCert relativi ai Servizi, nonché il Software acquisito in Licenza d'uso da InfoCert (“**Diritti IP**”), rimarranno di esclusiva proprietà di InfoCert.

7.3 I Diritti IP relativi al Software ed ai Servizi e qualsivoglia ulteriore modifica, incremento, revisione o cambi effettuati da InfoCert rimarranno di proprietà di InfoCert.

InfoCert SpA

Piazzale Flaminio 1/B, 00196 – Roma (RM), Italia
T +39 06 836691 F +39 06 833669634
info@infocert.it
infocert.it infocert.digital

Società soggetta alla direzione e coordinamento di Tinexta SpA
P.IVA 07945211006 REA n. 1064345
Cap. Soc. Sottoscritto e versato € 21.099.232,00



- 7.4 Se applicabile, la Licenza è personale, non esclusiva, non trasferibile a terzi ad alcun titolo e limitata nel tempo fino alla data di scadenza e/o cessazione del presente Accordo.
- 7.5 Ciascuna Parte si impegna a non rendere dichiarazioni o tenere comportamenti che possano ledere in qualsiasi modo l'immagine e/o il nome dell'altra o che possano comunque arrecare pregiudizio commerciale all'altra.
- 7.6 Resta inteso che il marchio, il dominio e tutti i segni distintivi del Cliente, come pure tutti i diritti di utilizzazione e di sfruttamento dell'immagine, del nome e dell'identità economica della stessa sono liberamente impiegabili da parte di InfoCert (a titolo esemplificativo e non esaustivo sul sito istituzionale, sui social media e per presentazioni della forza vendita). Viceversa, il marchio, il dominio e tutti i segni distintivi di InfoCert, come pure tutti i diritti di utilizzazione e di sfruttamento dell'immagine, del nome e dell'identità economica della stessa, non potranno essere liberamente utilizzati dal Cliente per qualsiasi finalità, salvo previa autorizzazione scritta di InfoCert.

8. LIMITAZIONI E RESPONSABILITA'

- 8.1 InfoCert s'impegna a fornire i Servizi e/o la Licenza (e così il Software) richiesti dal Cliente, in osservanza di quanto stabilito dal presente Accordo, dai relativi Allegati e dalla rispettiva normativa di settore tempo per tempo applicabile, non assumendo alcuna responsabilità al di fuori di quanto in essi espressamente stabilito.
- 8.2 Salvi i casi di dolo o colpa grave, InfoCert non sarà in alcun caso responsabile di qualsiasi danno, diretto e/o indiretto, derivante in via anche alternativa: i) per danni costituiti da lucro cessante, perdita di opportunità commerciali o di risparmi, perdita di dati, perdita di interesse, danni all'immagine o perdita di reputazione commerciale, né per multe, ammende, soprattasse o altre sanzioni, derivanti, direttamente o indirettamente, da atti od omissioni di InfoCert ai sensi del presente Accordo; ii) dall'uso non conforme dei Servizi e/o del Software a quanto previsto dal presente Accordo, ed eventuali successive modifiche; iii) per manomissioni o interventi sui Servizi e/o sul Software effettuati dal Cliente e/o dall'Utente stesso e/o da parte di terzi non autorizzati da InfoCert, anche qualora non cagionino espressamente un danno alle Parti o a terzi; iv) da un improprio utilizzo delle credenziali e/o dei Servizi e/o della Licenza e/o del Software da parte del Cliente e/o dell'Utente; v) dalla mancata fruizione del Servizio e/o Software dovuta a malfunzionamenti o blocchi della rete internet o a fronte di ritardi o interruzioni o per errori e/o malfunzionamenti rientranti nell'ambito dei parametri di indisponibilità indicati nell'Allegato Tecnico.
- 8.3 Il Cliente, salvo le ipotesi di intervento per manutenzione ordinaria e/o straordinaria, in caso di superamento dei parametri di indisponibilità stabiliti, ove applicabile, nei livelli di servizio indicati nell'Allegato Tecnico avrà diritto ad ottenere, a titolo di risarcimento di tutti i danni eventualmente subiti, il rimborso del prezzo pagato per il Servizio/Software correlato al periodo di mancata fruizione dello stesso. Il rimborso non potrà essere richiesto qualora la mancata fruizione sia imputabile al gestore della connettività ovvero sia derivante da caso fortuito, Forza Maggiore o cause, comunque, non imputabili ad InfoCert.
- 8.4 InfoCert, in ipotesi di dolo o colpa grave del Cliente e/o dell'Utente, si riserva, oltre al diritto al risarcimento del danno e/o al recupero dei crediti spettanti, la facoltà di trattenere il Corrispettivo a compensazione parziale o totale degli eventuali danni, pregiudizi o spese sostenute per l'erogazione o gestione della singola fattispecie.
- 8.5 Fermo quanto previsto e/o pattuito in altre clausole del presente Accordo, resta inteso che, in ogni caso, qualora InfoCert risultasse responsabile per eventuali danni, sarà tenuta a corrispondere al Cliente, a titolo di risarcimento del danno da questo subito, un importo non superiore al 10% (dieci per cento) del Corrispettivo complessivo annuo ("**Indennizzo Massimo**"). L'Indennizzo Massimo sarà riconosciuto solo previo accertamento degli eventuali inadempimenti verificatisi nel relativo anno solare di vigenza del

InfoCert SpA

Piazzale Flaminio 1/B, 00196 – Roma (RM), Italia
T +39 06 836691 F +39 06 833669634
info@infocert.it
infocert.it infocert.digital

Società soggetta alla direzione e coordinamento di Tinexta SpA
P.IVA 07945211006 REA n. 1064345
Cap. Soc. Sottoscritto e versato € 21.099.232,00



presente Accordo e comprenderà tutti i danni derivanti da violazione di legge o di contratto e qualsiasi penale, restituzione di prezzo e costo che InfoCert sia tenuta a corrispondere al Cliente.

8.6 Nessuna azione potrà essere iniziata dal Cliente, a pena di decadenza, decorsi 9 (nove) mesi dalla data in cui il presente Accordo si è risolto o è cessato.

8.7 Nel caso in cui il Cliente (e/o l'Utente) compia atti che costituiscano violazione di Diritti IP di un terzo, il Cliente (all'occorrenza, anche per conto dell'Utente) manleverà e/o terrà indenne InfoCert da qualsiasi danno o spesa, compresi onorari e spese legali, che quest'ultima sopporti, in conseguenza delle rivendicazioni del terzo.

8.8 Il Cliente si obbliga, anche per conto dell'Utente, a garantire e tenere indenne InfoCert da qualsiasi perdita, danno, spesa, costo o altro onere che questa possa sopportare in conseguenza delle sue azioni o pretese (e/o dell'Utente) comunque avanzate da terzi in relazione all'esecuzione del presente Accordo, per fatti imputabili al Cliente medesimo (e/o all'Utente).

9. AUDIT

9.1 InfoCert ha la facoltà di effettuare, anche attraverso soggetti da essa incaricati, Audit presso il Cliente, in modalità self-assessment e/o audit on-site, allo scopo di accertare il rispetto delle misure di sicurezza e di trattamento dei dati personali, nonché verificare il puntuale rispetto delle previsioni del presente Accordo e dei relativi Allegati ("Audit").

9.2 In caso di Audit, il Cliente si impegna sin da ora a collaborare con InfoCert e con i soggetti da questa incaricati, fornendo senza ritardo tutte le informazioni richieste e illustrando i processi della propria organizzazione. InfoCert, a fronte di criticità emerse in fase di Audit, si riserva di esercitare, a propria discrezione, il diritto di richiedere ulteriori approfondimenti, eseguiti anche eventualmente da parte di società terze specializzate, per le finalità del presente Accordo.

9.3 Nel caso in cui InfoCert rilevi, all'esito degli accertamenti a proprio insindacabile giudizio, che il Cliente non si sia attenuto a quanto stabilito nel presente Accordo, il Cliente si impegna ad uniformarsi alle indicazioni ed alle istruzioni comunicate da InfoCert con diffida ad adempiere ex art. 1454 c.c., entro i tempi indicati dalla stessa. Decorso inutilmente il congruo termine imposto da InfoCert, il presente Accordo si intenderà senz'altro risolto, ai sensi del successivo art. 14.

10. DURATA

10.1 Il presente Accordo avrà la durata di 12 mesi ("**Durata**") a decorrere dalla data di sottoscrizione.

10.2 Alla scadenza, il presente Accordo si rinnova in automatico per periodi di 1 (un) anno ciascuno, salvo che una delle Parti dia disdetta, con comunicazione da inviarsi entro e non oltre 90 (novanta) giorni prima della scadenza dell'Accordo.

11. CORRISPETTIVI

11.1 Il Cliente si impegna a pagare i corrispettivi a InfoCert secondo quanto previsto nell'Offerta Commerciale ("**Corrispettivo/i**").

11.2 I Corrispettivi saranno dovuti dal Cliente entro 60 (sessanta) giorni dalla data di invio della fattura da parte di InfoCert. Resta inteso tra le Parti che, in caso di mancato pagamento entro tale termine, saranno dovuti gli interessi di cui al D.lgs. 231/2002, in via automatica e senza necessità di previa costituzione in mora del Cliente.

11.3 In caso di mancato pagamento dei Corrispettivi, InfoCert si riserva il diritto di risolvere il presente Accordo ai sensi del successivo art. 11, nonché il diritto di sospendere l'erogazione del Servizio e/o il relativo accesso al medesimo e/o l'utilizzo del Software fino al pagamento dei Corrispettivi dovuti.

InfoCert SpA

Piazzale Flaminio 1/B, 00196 – Roma (RM), Italia
T +39 06 836691 F +39 06 833669634
info@infocert.it
infocert.it infocert.digital

Società soggetta alla direzione e coordinamento di Tinexta SpA
P.IVA 07945211006 REA n. 1064345
Cap. Soc. Sottoscritto e versato € 21.099.232,00



11.4 Le Parti convengono che i Corrispettivi sono soggetti a variazione annuale in funzione dell'indice ISTAT dei prezzi al consumo per le famiglie di operai ed impiegati applicata a decorrere dal 31 gennaio di ogni anno successivo a quello di rilevazione.

12.PRIVACY

12.1 Con la sottoscrizione del presente Accordo le Parti si impegnano, informandosi reciprocamente, a far sì che tutti i dati personali forniti direttamente dalle Parti o dei quali le stesse vengano in possesso durante la vigenza del presente Accordo e comunque connessi con l'Accordo stesso, relativi al proprio personale o ai propri collaboratori o a terzi, saranno oggetto di trattamento, automatizzato e non, esclusivamente per le finalità gestionali e amministrative inerenti l'adempimento degli obblighi contrattuali e legislativi. A tal fine, InfoCert, in qualità di titolare del trattamento dei dati forniti dal Cliente, informa lo stesso che, i relativi dati personali saranno trattati, per le finalità e nelle modalità illustrate nell'informativa presente sul sito www.infocert.it, di cui il Cliente dichiara di aver preso visione.

12.1.1 Il conferimento dei dati, come previsto al paragrafo precedente, è necessario per l'assolvimento delle predette finalità e in difetto non sarà possibile realizzarle in tutto o in parte. I dati saranno utilizzati dalle Parti solo con modalità e procedure necessarie al perseguimento delle finalità indicate. Le Parti dichiarano e si danno reciprocamente atto che, in relazione al trattamento dei dati personali di cui al presente articolo, gli interessati potranno esercitare i diritti di cui agli articoli 15-22 del Regolamento (UE) 2016/679.

12.1.2 Per le finalità del presente Accordo e sulla base delle modalità di erogazione/utilizzo del Servizio e/o del Software, le Parti sottoscriveranno un separato accordo sul trattamento dei dati ai sensi **dell'Allegato B – DPA**.

12.2 Presso il Data Center di InfoCert, sono messi a disposizione appositi macchinari hardware per la gestione dei dati dei Clienti, necessari all'erogazione/utilizzo dei Servizi e/o Software.

12.2.1 Il Data Center è organizzato e amministrato nel rispetto delle norme legislative applicabili sulle misure di sicurezza, e fornito di appositi sistemi di protezione logica e fisica, al fine di impedire accessi non autorizzati. Le regole di sicurezza sono autonomamente stabilite e implementate da InfoCert; in particolare, le stesse potranno essere modificate, per essere rese conformi ad eventuali mutamenti della disciplina di cui al Regolamento UE 679/2016, ed alle successive disposizioni legislative e regolamentari in materia di sicurezza dei dati personali.

12.2.2 Il Cliente riconosce e accetta che InfoCert si avvale di terze parti, debitamente nominate come responsabili del trattamento dei dati personali, per lo svolgimento di talune attività quali, a titolo esemplificativo e non esaustivo, la fornitura di servizi di storage dei dati in cloud, i quali operano su server situati all'interno dell'UE e nel pieno rispetto della normativa in materia di trattamento dei Dati Personali. Maggiori informazioni circa i terzi tempo per tempo responsabili del trattamento sopra citati saranno richiedibili ad InfoCert all'indirizzo richieste.privacy@legalmail.it.

13.RISERVATEZZA

13.1 Ai fini del presente Accordo, con **"Informazioni Confidenziali"** si intende qualsiasi informazione riguardante, ma non limitata a contenuti base, contenuti, marchio, programmi informatici, codici, algoritmi, nomi e capacità di lavoratori dipendenti ed autonomi, *know-how*, formule, procedimenti, idee, invenzioni (brevettabili o meno), schemi ed altri piani tecnici, commerciali, finanziari e di sviluppo, previsioni, strategie, prezzi, profitti, utili, margini, elenco o dettagli di clienti, sia individualmente, sia collettivamente, ed altre informazioni non pubbliche. Ciascuna delle Parti si impegna a mantenere riservate le Informazioni Confidenziali relative all'altra Parte, nella stessa misura in cui protegge le proprie Informazioni Confidenziali

InfoCert SpA

Piazzale Flaminio 1/B, 00196 – Roma (RM), Italia
T +39 06 836691 F +39 06 833669634
info@infocert.it
infocert.it infocert.digital

Società soggetta alla direzione e coordinamento di Tinexta SpA
P.IVA 07945211006 REA n. 1064345
Cap. Soc. Sottoscritto e versato € 21.099.232,00



e di utilizzare tali Informazioni Confidenziali soltanto nella misura strettamente necessaria per l'adempimento delle obbligazioni derivanti dal presente Accordo.

13.2 Tali restrizioni sulla comunicazione e sull'utilizzo delle informazioni resteranno in vigore per 5 (cinque) anni successivi alla risoluzione o cessazione del presente Accordo.

13.3 Resta salva la possibilità di una Parte di comunicare a terzi tali informazioni, a seguito di ordine del Giudice o della Pubblica Autorità e previa comunicazione, ove possibile, all'altra Parte.

13.4 InfoCert si riserva il diritto, in caso di diffusione non autorizzata delle Informazioni Riservate, di tutelare i propri diritti in ogni più opportuna sede.

14. SOSPENSIONE. RISOLUZIONE. RECESSO

14.1 InfoCert ha il diritto di sospendere e/o cessare l'erogazione del Software e/o Servizio e/o bloccare l'accesso del Cliente (e/o dell'Utente) allo stesso, quando:

- (a) abbia fondato motivo di ritenere che si sia verificato, anche per ragioni non imputabili al Cliente stesso, un evento che possa mettere a rischio la sicurezza delle informazioni e dei dati contenuti nel Software e/o Servizi. La sospensione può durare, senza che il Cliente possa avanzare alcuna pretesa al riguardo, finché InfoCert non riterrà fondatamente superato il rischio di cui sopra;
- (b) in caso di utilizzo improprio del Software e/o dei Servizi ovvero di impedire l'accesso ai documenti e/o ai dati ivi contenuti da parte del Cliente e/o dell'Utente, dando, se del caso, idonea comunicazione dell'illecito alle autorità competenti;
- (c) venga a conoscenza della violazione di uno o più divieti di cui il presente Accordo o come previsti sul Manuale Operativo di riferimento o venga avanzata espressa richiesta in tal senso da un organo giurisdizionale o amministrativo competente in materia in base alle norme vigenti;
- (d) vengano superati i limiti di utilizzo indicati nel presente Accordo o qualora si verifichino situazioni che possano compromettere la sicurezza del Servizio e/o del Software.

Nelle ipotesi di cui sopra, InfoCert, salvo cause di Forza Maggiore e/o per ordine di un'autorità pubblica, provvederà a comunicare al Cliente a mezzo e-mail - all'indirizzo indicato ai sensi dell'art. 21.1 - le motivazioni dell'adozione dei provvedimenti ivi stabiliti e avrà facoltà di risolvere il presente Accordo, senza alcun preavviso e senza per questo essere tenuta ad alcun risarcimento, e fatta salva ogni altra azione di rivalsa nei confronti del responsabile delle violazioni.

14.2 Salvo quanto specificato nei paragrafi successivi, qualora il Cliente si rendesse inadempiente ad un obbligo previsto nell'Accordo e non ponesse rimedio a tale inadempimento entro 30 (trenta) giorni dal ricevimento di una diffida ad adempiere ex art. 1454, c.c., inviata da InfoCert e contenente la descrizione dell'inadempimento e l'invito ad eseguire correttamente la prestazione entro il suddetto termine, il presente Accordo si intenderà risolto di diritto.

14.3 Sarà facoltà di InfoCert risolvere di diritto il presente Accordo ex art. 1456 c.c. mediante comunicazione scritta al Cliente, qualora quest'ultimo violi i seguenti articoli: art.1 (Oggetto); art.2 (Obblighi e garanzie del Cliente); art.7 (Proprietà Intellettuale); art.12 (Privacy); art.13 (Riservatezza); art.18 (Normativa antimafia e anticorruzione); art. 19 (D.Lgs. 231/2001 e Codice Etico).

14.4 Ciascuna Parte potrà recedere con effetto immediato, nel caso in cui l'altra Parte (i) sia dichiarata fallita o sottoposta a procedure concorsuali, o presenti essa stessa istanza per il proprio fallimento o per l'ammissione a procedure concorsuali (ii) abbia deliberato lo scioglimento e/o la messa in liquidazione.

15. MODIFICHE CONTRATTUALI

15.1 Ogni modifica sarà valida ed efficace solo se concordata per iscritto tra le Parti. Ogni variazione dovrà essere comunicata da InfoCert per iscritto e acquisterà efficacia a partire dal trentesimo giorno successivo

InfoCert SpA

Piazzale Flaminio 1/B, 00196 – Roma (RM), Italia
T +39 06 836691 F +39 06 833669634
info@infocert.it
infocert.it infocert.digital

Società soggetta alla direzione e coordinamento di Tinexta SpA
P.IVA 07945211006 REA n. 1064345
Cap. Soc. Sottoscritto e versato € 21.099.232,00



alla data di ricezione della comunicazione da parte del Cliente, salvo quest'ultimo decida di non voler accettare tale variazione e, pertanto, intenda recedere, dandone comunicazione ad InfoCert medesima.

16. OBBLIGHI POST CONTRATTUALI

- 16.1** Ove applicabile, in caso di cessazione del presente Accordo, le Parti si impegnano, previo accordo scritto circa le modalità e le condizioni economiche, a collaborare in buona fede al fine di assicurare il passaggio ordinato al Cliente, o ad altro fornitore da questi designato, dei dati e dei documenti oggetto del presente Accordo e/o di quanto necessario a garantire la continuità del Servizio al nuovo fornitore.
- 16.2** In caso di mancato accordo di cui sopra, InfoCert depositerà tali dati e documenti nell'area riservata del Cliente per un periodo di 60 (sessanta) giorni successivi alla cessazione del presente Accordo, affinché il Cliente stesso possa scaricarli nel formato definito da InfoCert.
- 16.3** In nessun caso, InfoCert sarà tenuta, senza la previsione di apposito corrispettivo, a trasferire i dati al Cliente o a terzi, in un formato diverso da quello definito da InfoCert, o ad interfacciarsi con i sistemi informatici di terzi soggetti indicati dal Cliente.

17. FORO COMPETENTE

- 17.1** Il presente Accordo è regolato dalla legge italiana.
- 17.2** In caso di controversia derivante o inerente al presente Accordo, la sua interpretazione, efficacia, esecuzione o risoluzione le Parti avranno la facoltà di raggiungere tra di loro una eventuale soluzione bonaria, entro 30 (trenta) giorni dal sorgere della controversia.
- 17.3** Rimasto infruttuoso il tentativo di conciliazione di cui al precedente 17.2, ciascuna Parte avrà il diritto di agire a propria tutela. In tal caso le Parti, di comune accordo, riconoscono e stabiliscono che per qualsiasi controversia dovesse insorgere in ordine al presente Accordo e/o relativi contratti/ordini attuativi, comprese quelle relative alla sua validità, interpretazione, esecuzione e risoluzione, sarà competente in via esclusiva il Foro di Roma.

18. NORMATIVA ANTIMAFIA E ANTICORRUZIONE

- 18.1** Nell'esecuzione del presente Accordo, il Cliente si obbliga a rispettare per sé e per i propri incaricati e/o dipendenti e/o collaboratori la normativa Antimafia e Anticorruzione, secondo quanto disposto rispettivamente dal D. Lgs. n. 159/2011 e dalla Legge n. 190/2012, e successive modificazioni e integrazioni ("Normativa Antimafia e Anticorruzione").
- 18.2** Il Cliente dichiara inoltre che nei propri confronti o dei propri incaricati e/o dipendenti e/o collaboratori non sussistono le cause di divieto, di sospensione o di decadenza previste dall'articolo 67 del D. Lgs. n. 159/2011.

19. D. LGS. 231/2001 E CODICE ETICO

- 19.1** Nell'esecuzione del presente Accordo, il Cliente si obbliga a rispettare per sé e per i propri incaricati e/o dipendenti e/o collaboratori, in maniera integrale e rigorosa, il D. Lgs. 231/2001 e ss.mm.ii., nonché il "Modello 231" e il Codice Etico adottati da InfoCert, presenti sul sito internet istituzionale, da considerarsi parte integrante e sostanziale del presente Accordo.
- 19.2** Resta espressamente inteso che, in caso di inadempimento del Cliente ad una qualsiasi delle obbligazioni di cui al presente articolo, InfoCert avrà facoltà di risolvere il presente Accordo ex art. 1456, c.c., mediante semplice comunicazione scritta.

20. CESSIONE

InfoCert SpA

Piazzale Flaminio 1/B, 00196 – Roma (RM), Italia
T +39 06 836691 F +39 06 833669634
info@infocert.it
infocert.it infocert.digital

Società soggetta alla direzione e coordinamento di Tinexta SpA
P.IVA 07945211006 REA n. 1064345
Cap. Soc. Sottoscritto e versato € 21.099.232,00



- 20.1** Il presente Accordo non potrà essere ceduto dal Cliente se non previo consenso scritto di InfoCert.
- 20.2** Resta salvo tra le Parti, che le società controllate come definite ai sensi dell'art.2359 c.c. del Cliente e/o società di cui il Cliente sia una controllata possono accedere al presente Accordo previa autorizzazione scritta da parte di InfoCert.

21. VARIE

21.1 Le Parti comunicheranno mediante gli indirizzi che seguono:

- Se dirette a InfoCert: InfoCert S.p.A., Piazzale Flaminio 1/B, Roma; PEC: infocert@legalmail.it
- Se dirette al Cliente: agli indirizzi indicati nell' intestazione dell' Offerta Commerciale.

Qualora una delle Parti cambiasse il suo indirizzo, questa darà comunicazione scritta all'altra Parte del nuovo indirizzo e della data dalla quale diventerà effettivo. In mancanza, qualsiasi comunicazione inviata ai precedenti recapiti si considererà consegnata, anche in caso di tentativo di recapito andato a vuoto.

- 21.2** Ciascuna Parte sarà sollevata da responsabilità ed esentata dall'obbligo di fornire la prestazione per tutto il tempo e fino a quando la stessa sia nell'impossibilità di adempiere, in tutto o in parte, per l'insorgenza di una causa di Forza Maggiore (a titolo meramente esemplificativo, guerra, moti popolari, scioperi o provvedimenti di autorità giudiziarie, disservizi dei gestori della rete elettrica, azioni di terzi o altre cause al di fuori del ragionevole controllo della/e Parte/i che impediscono in tutto o in parte l'esecuzione). In tali ipotesi, la mancata erogazione dei Servizi e/o del Software non costituirà inadempimento o motivo di sospensione dei pagamenti o di risoluzione del presente Accordo. La Parte che abbia avuto notizia di un evento causato da Forza Maggiore, ne darà immediata comunicazione scritta all'altra Parte e le Parti si incontreranno immediatamente, al fine di concordare gli eventuali rimedi preordinati al tempestivo ripristino della normale funzionalità dei Servizi e/o adempimento delle prestazioni previste dal presente Accordo, a seconda del caso.
- 21.3** In ogni caso, qualora un evento causato da Forza Maggiore impedisca la regolare esecuzione del presente Accordo per un periodo superiore a 60 (sessanta) giorni, ciascuna delle Parti avrà la facoltà di recedere dal presente Accordo dandone comunicazione all'altra Parte ai sensi dell'art. 21.1. e senza che nulla sia dovuto a quest'ultima a titolo di risarcimento o mancato guadagno, salvo il diritto di InfoCert al Corrispettivo per le attività già svolte e per quelle ulteriormente necessarie.
- 21.4** Qualora una clausola del presente Accordo fosse dichiarata nulla, entrambe le Parti saranno sollevate da tutti gli obblighi derivanti da detta clausola, senza che tale nullità affligga le altre clausole del presente Accordo. Per quanto possibile, le clausole dichiarate nulle saranno automaticamente sostituite con nuove clausole di contenuto equivalente che perseguano le medesime finalità delle clausole dichiarate nulle.
- 21.5** Ai sensi dell'art. 1469 bis e ss., c.c., qualora qualche previsione contenuta del Contratto non sia applicabile al Cliente in quanto consumatore, le restanti parti del Contratto rimarranno comunque efficaci. Il Cliente, se consumatore, avrà facoltà di recedere dal Contratto, entro 14 giorni dalla data di conclusione dello stesso, tramite comunicazione da inviarsi a tramite il seguente form: <https://contatta.infocert.it/rimborsi/> oppure a mezzo PEC all'indirizzo: richieste.rimborso@legalmail.it o a mezzo raccomandata a.r. indirizzata a InfoCert S.p.A., - Direzione Generale e Amministrativa – Piazzale Flaminio 1/B 00196 Roma. A tal fine è possibile utilizzare il modulo tipo di recesso reperibile al seguente link: <https://www.infocert.it/pdf/Modulo-di-recesso-tipo.pdf>.

22. CAMBIO DI CONTROLLO

- 22.1** Nel caso in cui il Cliente sia soggetto al cambio di controllo, il Cliente si obbliga ad informare preventivamente InfoCert, la quale può riservarsi di recedere dal presente Accordo a seguito della comunicazione.

InfoCert SpA

Piazzale Flaminio 1/B, 00196 – Roma (RM), Italia
T +39 06 836691 F +39 06 833669634
info@infocert.it
infocert.it infocert.digital

Società soggetta alla direzione e coordinamento di Tinexta SpA
P.IVA 07945211006 REA n. 1064345
Cap. Soc. Sottoscritto e versato € 21.099.232,00



Lista Allegati:

Allegato A – Offerta Commerciale

Allegato B – DPA

Allegato C – Allegato Tecnico

Allegato D – Misure di Sicurezza

InfoCert SpA

Piazzale Flaminio 1/B, 00196 – Roma (RM), Italia

T +39 06 836691 F +39 06 833669634

info@infocert.it

infocert.it infocert.digital

Società soggetta alla direzione e coordinamento di Tinexta SpA

P.IVA 07945211006 REA n. 1064345

Cap. Soc. Sottoscritto e versato € 21.099.232,00

ALLEGATO A – ALLEGATO TECNICO
LegalDoc

Sommario

1. RIFERIMENTI ESTERNI.....	1
2. Descrizione del servizio	1
3. Specifiche tecnico-normative.....	2
4. Specifiche tecniche d'uso.....	7
5. SLA e KPI.....	10
Affidamento del servizio di conservazione a norma.....	12

1. RIFERIMENTI ESTERNI

Documentazione	Link di dettaglio
Manuale Operativo: Manuale della conservazione di Tinexta InfoCert	https://www.infocert.it/pdf/conservazione/manuale-conservazione-infocert.pdf
Manuale Utente	https://knowledgecenter.infocert.digital/Home/Guida/manuale-utente-legaldoc-web?lang=it
Link di supporto (FAQ, Video, Guide)	https://help.infocert.it/cerca?searchText=LegalDoc&idProdotto=51
Scheda dati tecnici di attivazione	https://www.infocert.it/documentazione

2. Descrizione del servizio

LegalDoc è un servizio di conservazione di dati e documenti informatici a norma.
In particolare, il Servizio comprende:

- la licenza d'uso dei software che compongono i Servizi erogati da Tinexta InfoCert, in uso non esclusivo e non trasferibile;
- la messa a disposizione dello spazio necessario a conservare presso il Data Center i dati e documenti inviati;
- l'adeguamento, la manutenzione e l'aggiornamento dei Servizi;
- l'attività di supporto;
- l'affidamento del servizio di conservazione

Inoltre, il sistema di conservazione assicura, dalla presa in carico fino all'eventuale scarto, la conservazione degli oggetti digitali in esso conservati, tramite l'adozione di regole, procedure e tecnologie che garantiscano le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità, ai sensi delle Linee Guida AgID su



formazione, gestione e conservazione dei documenti informatici di maggio 2021 e ss.mm.ii e del D.M.E.F 17.06.2014. Il sistema di conservazione garantisce l'accesso all'oggetto conservato per il periodo previsto dal piano di conservazione del titolare dell'oggetto della conservazione e dalla normativa vigente, o per un tempo superiore eventualmente concordato tra le parti, indipendentemente dall'evoluzione del contesto tecnologico. Il sistema garantisce, altresì, la possibilità di esibizione di un documento già conservato ("Pacchetto di Distribuzione" - "PdD"), di eventuale cancellazione e scarto.

Tinexta InfoCert dal 2014 è stata tra le prime aziende italiane accreditate dall'Agenzia per l'Italia Digitale (AgID) come Conservatore, quando era requisito normativo necessario per erogare servizi di Conservazione Digitale a norma per la Pubblica Amministrazione Italiana secondo il DPCM allora in vigore.

Tinexta InfoCert ha ottenuto dal 2019 la qualifica AgID Cloud Marketplace (CSP Tipo B Infrastruttura e SaaS per il servizio LegalDoc). Dal gennaio 2023 la competenza del suddetto Marketplace è passata a Agenzia per la Cybersicurezza Nazionale (ACN): l'infrastruttura e il servizio SaaS di conservazione LegalDoc sono qualificati all'interno dell'ACN Cloud Marketplace (che sostituisce l'ex AgID Cloud Marketplace).

Dal 2022 Tinexta InfoCert è tra le prime aziende italiane iscritte al Marketplace dei servizi di conservazione di AgID, secondo le più recenti Linee Guida pienamente applicabili dal primo gennaio di quello stesso anno. La presenza di Tinexta InfoCert nell'Elenco dei conservatori iscritti libera l'Amministrazione che le affida il servizio di conservazione dall'obbligo di trasmettere ad AgID i relativi contratti entro trenta giorni dalla stipula affinché l'Agenzia possa svolgere le attività di verifica dei requisiti generali nonché dei requisiti di qualità, di sicurezza e organizzazione di cui all'allegato A del Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici.

3. Specifiche tecnico-normative

Il Cliente è inteso come colui che accetta i presenti termini, unitamente a quelli previsti dall'Accordo e può identificarsi come il legale rappresentante del Titolare ossia all'incaricato autorizzato all'acquisto del presente prodotto o può averlo acquistato in proprio, versando il corrispettivo del Servizio a Tinexta InfoCert. Il titolare degli oggetti da conservare (il "Titolare"), o soggetto produttore, è colui che ha formato o che comunque è titolare del documento che sarà oggetto di conservazione (può coincidere col Cliente e/o con il Responsabile della Conservazione -*soggetto riconducibile sia all'organizzazione del Titolare, sia esterno a tale organizzazione, che definisce e attua le politiche complessive del sistema di conservazione di questi e ne governa la gestione con piena responsabilità ed autonomia e che sottoscrive l'Atto di Affidamento, in rappresentanza del Titolare, nei confronti del Conservatore Tinexta InfoCert*- e/o può coincidere con il Produttore dei PdV - soggetto produttore dei pacchetti di versamento degli oggetti da conservare (può coincidere con il Titolare e/o con il Cliente)- quando forma altresì il pacchetto di versamento degli oggetti della conservazione. I dati e documenti del Titolare si intendono definitivamente acquisiti nel momento in cui ne viene data evidenza all'utente tramite la ricevuta dell'"Indice Pacchetto di Archiviazione (IPdA)", che funge da rapporto di versamento. Prima di tale ricevuta, Tinexta InfoCert non assume alcuna responsabilità, salvo i casi di dolo o colpa grave, per l'eventuale sottrazione, perdita, distruzione o smarrimento dei dati e documenti del Cliente, il quale, ai fini della sua conservazione dovrà provvedere ad inviarli nuovamente.

Affidamento del servizio di conservazione

Ai fini dello svolgimento delle attività di cui al punto 2. da parte di Tinexta InfoCert, il Titolare, per tutta la durata dell'Accordo, affida a Tinexta InfoCert il Servizio di conservazione dei Dati del Titolare, previa sottoscrizione dell'Atto di Affidamento da parte del Responsabile della conservazione (sia esso interno o esterno all'organizzazione del Titolare) e dell'Offerta da parte del Cliente.

Tinexta InfoCert assume pertanto il ruolo di "Conservatore" ai sensi del punto 4.4, par. 1, lett. e) delle Linee Guida.

Nomina del Responsabile (o sub-Responsabile) del trattamento dei dati personali, ai sensi del Regolamento UE n. 679/2016.



Ai sensi del punto 4.10 delle Linee Guida, Tinexta InfoCert, quale soggetto esterno cui il Responsabile della conservazione, in nome e per conto del Titolare, affida il servizio di conservazione, assume il ruolo di responsabile del trattamento dei dati personali di cui il Responsabile della Conservazione è “titolare del trattamento” ai sensi dell’art. 4, n. 7), del Regolamento, ovvero assume il ruolo di sub-responsabile, nel caso in cui il Responsabile della conservazione sia a sua volta “responsabile del trattamento” ai sensi dell’art. 4, n. 8, del Regolamento. In particolare, il Responsabile della Conservazione affida a Tinexta InfoCert l’esecuzione delle seguenti operazioni di trattamento, da effettuarsi con l’ausilio di strumenti elettronici e negli specifici limiti previsti dalle Linee Guida e dall’Accordo: raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, selezione, estrazione, interconnessione, comunicazione, cancellazione e (eventuale) distruzione di dati. Il Responsabile della conservazione, pertanto, garantisce di fondare il trattamento dei suddetti dati personali (e la relativa delega in favore di Tinexta InfoCert) su idonea base giuridica, ai sensi dell’art. 6 del Regolamento, presentandosi quali autonomo titolare del trattamento o quale responsabile a sua volta legittimamente incaricato. Il Responsabile della conservazione, pertanto, nomina Tinexta InfoCert quale responsabile o sub-responsabile del trattamento dei dati (il “Responsabile” – si precisa che, per semplicità, viene utilizzata questa locuzione tanto nel caso in cui Tinexta InfoCert sia Responsabile del trattamento, quanto nel caso in cui sia sub-Responsabile), assumendo tutti gli obblighi e le responsabilità connesse e manlevando Tinexta InfoCert da ogni pretesa eventualmente proveniente da terzi in riferimento alle operazioni di trattamento messe in atto da Tinexta InfoCert in virtù dell’incarico conferitole con il presente atto. La natura stessa del Servizio implica che le uniche istruzioni che il Responsabile riceverà saranno quelle previste dall’Accordo, dai suoi Allegati e dalla normativa in materia di conservazione dei documenti informatici.

Alla luce di quanto sopra, Tinexta InfoCert si impegna a:

- adottare le misure di sicurezza previste dalla normativa applicabile, ivi comprese quelle di cui all’art. 32 del Regolamento (UE) 679/2016;
- rispettare gli obblighi posti in capo al Responsabile (o sub-Responsabile) del trattamento dall’art. 28 del Regolamento (UE) 679/2016;
- assistere il Responsabile della conservazione (o, ove necessario o richiesto, il Titolare) nell’adempimento degli obblighi derivanti dal Regolamento (UE) 679/2016, nei limiti degli impegni assunti ai sensi dell’Accordo, al fine di garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del Regolamento (UE) 2016/679, tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile;
- con particolare riferimento agli obblighi in materia di notificazione dei dati personali ex artt. 33 e 34 del Regolamento, informare il Responsabile della conservazione (o, ove necessario o richiesto, il Titolare) della eventuale violazione di dati personali senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione stessa;
- delegare singole operazioni di trattamento a eventuali società terze, debitamente designate per iscritto quali sub-responsabili del trattamento e istruite in modo da assumere i medesimi obblighi assunti da Tinexta InfoCert in virtù della presente nomina rispetto alla tutela dei dati personali;
- incaricare per iscritto le persone che tratteranno dati personali per conto del Responsabile della conservazione, autorizzando le stesse allo svolgimento delle sole operazioni di trattamento strettamente necessarie alla corretta erogazione del Servizio, con impegno alla riservatezza e indicazione di ogni istruzione necessaria all’esecuzione di un trattamento conforme al D.L.vo 196/2003 e al Regolamento (EU) 679/2016;
- dar seguito a richieste o provvedimenti del Garante per la protezione dei dati personali o altra autorità competente in relazione al trattamento dei dati cui Tinexta InfoCert è preposta;
- effettuare le operazioni di cancellazione dei dati, quando richieste dal Responsabile della conservazione o direttamente dal Titolare nel corso dell’efficacia dell’Accordo e nei termini stabiliti nel medesimo;
- cancellare e/o restituire - a scelta del Responsabile della conservazione, o direttamente del Titolare - i dati oggetto di trattamento alla cessazione del Servizio, salvi gli obblighi di conservazione dei dati personali eventualmente derivanti dal diritto dell’Unione o degli Stati membri;
- non comunicare a terzi i dati personali oggetto di trattamento.

Nel caso in cui il Responsabile della conservazione (o direttamente il Titolare) manifesti per iscritto necessità tali da richiedere un trattamento diverso rispetto a quello di cui all’Accordo, previa valutazione relativa alla



compliance normativa della richiesta del Responsabile della conservazione/Titolare, Tinexta InfoCert informerà per iscritto il Responsabile della conservazione/Titolare/Cliente circa la percorribilità della soluzione richiesta e i relativi costi, mediante specifica offerta, eventualmente rivalutando altresì l'inquadramento da conferire al rapporto, anche ai sensi del Regolamento (UE) 2016/679. Il Responsabile della conservazione, in qualità di titolare o Responsabile del trattamento, prende atto e accetta che Tinexta InfoCert è autorizzata ad avvalersi di Amazon Web Services, Inc. E WIIT S.p.A. quale sub-Responsabile del trattamento per l'espletamento dei Servizi di storage dei dati in cloud. Il Responsabile informa il Responsabile della conservazione che lo storage dei dati in cloud presso Amazon Web Services, Inc. E WIIT S.p.a. si svolge su server localizzati in Italia.

Conservazione dei dati

I dati e documenti del Titolare si intendono definitivamente acquisiti nel momento in cui effettuata la verifica descritta nella successiva sezione "Obblighi di Tinexta InfoCert", ne viene data evidenza al produttore del pacchetto di versamento (in seguito del "PdV") e/o all'Utente tramite la ricevuta dell'"Indice Pacchetto di Archiviazione (IPdA)" (rapporto di versamento).

Prima di tale ricevuta, Tinexta InfoCert non assume alcuna responsabilità, salvo i casi di dolo o colpa grave, per l'eventuale sottrazione, perdita, distruzione o smarrimento dei dati e documenti del Titolare, il quale, ai fini della sua conservazione dovrà provvedere ad inviarli nuovamente.

Obblighi di Tinexta InfoCert

Tinexta InfoCert si impegna a conservare i documenti inviati dal Cliente/Titolare e/o dal Produttore del PdV, subordinatamente all'esito positivo della verifica di conformità dei documenti inviati alle caratteristiche previste negli Allegati e alla verifica del formato e delle altre specifiche concordate in fase progettuale del sistema di conservazione, secondo quanto previsto nell'Atto di Affidamento ed in base alle procedure specifiche per ciascun servizio meglio evidenziate negli Allegati all'Accordo. In particolare, il Cliente/Produttore/Titolare prende atto che, in virtù di quanto previsto nel punto 4.7, par. 2, lett. b), delle Linee Guida, tale verifica di conformità viene effettuata avendo riguardo esclusivamente a quanto stabilito nel Manuale della Conservazione di Tinexta InfoCert ed a quanto indicato, in tema di formati file, nell'All. 2 alle Linee Guida, nonché, per ciò che concerne le verifiche sui metadati, a quanto riportato nelle Linee Guida. La conservazione dei documenti è limitata ad un periodo di 10 anni a partire dalla data di marcatura temporale apposta sui pacchetti di archiviazione, salvo diverso specifico accordo regolato nell'Offerta o nell'Accordo sottoscritto e/o accettato.

Allo scadere di tale retention period e tramite apposito portale messo a disposizione da Tinexta InfoCert, il Cliente e il proprio Responsabile della Conservazione, possono scegliere se rinnovare il servizio, oppure procedere con lo scarto dei documenti conservati. Per 'scarto' si intende l'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.

Resta fermo che il periodo effettivo di conservazione è collegato all'efficacia dell'Accordo, dovendosi intendere che, in caso di mancato rinnovo o comunque di risoluzione anticipata dell'Accordo per qualsiasi ragione, salvo quanto descritto nella sezione "Obblighi del Cliente", Tinexta InfoCert non sarà più tenuta alla conservazione dei documenti.

Limitazione del Servizio in mera consultazione

Il Cliente può chiedere che il Servizio sia usufruito in modalità ridotta, ossia con la mera consultazione dei documenti già archiviati, ma senza la possibilità di trasmetterne in conservazione di nuovi.

La richiesta di limitazione può essere formulata a Tinexta InfoCert in occasione della scadenza del servizio o di uno dei successivi rinnovi, mediante PEC o raccomandata A/R, almeno 30 giorni prima del termine di scadenza.

In caso di tempestiva richiesta, Tinexta InfoCert formulerà apposita offerta economica per il Servizio di mera consultazione. Se le Parti non raggiungono l'accordo sul corrispettivo del nuovo Servizio, l'Accordo si intende risolto alla scadenza in vista della quale il Cliente ha avanzato la richiesta di limitazione.

Responsabilità di Tinexta InfoCert

Tinexta InfoCert SpA

Piazzale Flaminio 1/B, 00196 – Roma (RM), Italia

T +39 06 836691

info@infocert.it

infocert.it infocert.digital

Società soggetta alla direzione e coordinamento di Tinexta SpA

P.IVA 07945211006 REA n. 1064345

Cap. Soc. Sottoscritto e versato € 21.099.232,00



Tinexta InfoCert si impegna a fornire i Servizi richiesti dal Cliente in osservanza di quanto stabilito dall'Accordo, dagli Allegati ad esso relativi, dalle Linee Guida AgID, dal D.M. Economia e Finanze del 17.06.2014 ed eventuali successive modifiche o integrazione degli stessi, non assumendo alcuna responsabilità al di fuori di quanto in essi espressamente stabilito.

Ai fini di quanto indicato al punto precedente, non rientra nell'oggetto del presente Accordo l'attività interpretativa delle norme sopra richiamate e, più in generale, della normativa fiscale, in relazione alle singole fattispecie concrete, trattandosi di competenze più propriamente attribuibili ad appartenenti alle rispettive categorie professionali regolamentate.

Tinexta InfoCert, salvo il caso di dolo o colpa grave, non incorrerà in responsabilità per danni diretti o indiretti di qualsiasi natura ed entità che dovessero verificarsi al Produttore del PdV, al Cliente, al Titolare, all'Utente e/o a terzi in conseguenza dell'uso non conforme a quanto prescritto negli Allegati e nelle normative richiamate al primo comma del presente articolo, ed eventuali successive modifiche, e/o del mancato uso dei Servizi, anche a fronte di ritardi o interruzioni o per errori e/o malfunzionamenti dello stesso, qualora rientranti nell'ambito dei parametri di indisponibilità.

Il solo Cliente e/o Titolare, in caso di superamento dei parametri di indisponibilità stabiliti nei livelli di servizio, salvo le ipotesi di intervento per manutenzione ordinaria e/o straordinaria, avrà diritto ad ottenere, a titolo di risarcimento di tutti i danni eventualmente subiti, il rimborso del prezzo pagato per il servizio correlato al periodo di mancata fruizione dello stesso.

Salve le ipotesi di dolo e colpa grave, Tinexta InfoCert sarà tenuta a tenere indenne il Cliente e/o il Titolare e/o l'Utente, in caso di mancata osservanza ad essa imputabile delle tempistiche e delle modalità procedurali per la conservazione dei documenti trasmessi stabilite dalla normativa e dagli Allegati, unicamente in caso di accertamento e comminazione da parte dell'amministrazione finanziaria di sanzioni amministrative nei confronti dei medesimi e nel limite della sanzione applicata.

Il rimborso non potrà essere richiesto qualora la mancata fruizione sia imputabile al gestore della Connettività ovvero derivante da caso fortuito, forza maggiore o cause comunque non imputabili a Tinexta InfoCert, quali, a titolo esemplificativo, scioperi, sommosse, terremoti, atti di terrorismo, tumulti popolari, sabotaggio organizzato, eventi chimici e/o batteriologici, guerra, alluvioni, provvedimenti delle competenti autorità in materia o inadeguatezza delle strutture, dei macchinari *hardware* e/o dei *software* utilizzati dal Cliente e/o Titolare e/o dall'Utente.

Tinexta InfoCert, inoltre, salvo il caso di dolo o colpa grave non sarà gravata da oneri o responsabilità per danni diretti o indiretti di qualsiasi natura ed entità che dovessero verificarsi al Cliente e/o Produttore e/o all'Utente causati da manomissioni o interventi sul servizio o sulle apparecchiature effettuati dal Cliente e/o dal Produttore e/o dall'Utente stesso e/o da parte di terzi non autorizzati da Tinexta InfoCert.

Obblighi del Cliente

Il Cliente dichiara, sotto la propria esclusiva responsabilità, di essere dotato dei poteri necessari per la sottoscrizione del presente atto ovvero di aver ricevuto formale incarico da parte del Titolare, ai sensi degli artt. 1387 ss., c.c., e, se del caso, 1704, c.c., per la sottoscrizione dell'Accordo. Il Cliente si obbliga a rendere edotto l'Utente delle previsioni del presente Accordo e, in particolare, degli obblighi ed oneri specificamente richiesti ai fini dell'utilizzo dei Servizi. Il Cliente, il Titolare, il Responsabile della Conservazione e l'Utente si impegnano a fornire tutte le informazioni necessarie all'attivazione dei Servizi ed a dotarsi di tutti i requisiti necessari per l'accesso agli stessi come meglio specificati nei relativi Allegati.

Il Responsabile della Conservazione, il Produttore, il Cliente, il Titolare e l'Utente si impegnano, altresì, ad inviare tutti i documenti che devono essere conservati in forma elettronica con le modalità e nei formati previsti negli Allegati e nel rispetto delle modalità e dei termini stabiliti dalla normativa di riferimento. Qualora siano trasmessi per la conservazione documenti nei formati "*standard*" indicati nell'Allegato Tecnico, la leggibilità di detti documenti sarà garantita da Tinexta InfoCert mediante i programmi indicati nel medesimo Allegato Tecnico. In tali casi il Titolare e/o l'Utente potrà non inviare i programmi per la visualizzazione dei documenti medesimi, ferma restando a suo carico la necessaria verifica di compatibilità tra i formati utilizzati ed i programmi di visualizzazione proposti da Tinexta InfoCert.

Il Cliente e/o Titolare e/o il Responsabile della Conservazione si impegnano ad indicare, nell'apposita sezione della scheda dati tecnici, l'invio di documenti in modalità cifrata, impegnandosi in tali casi a conservare gli strumenti necessari per la decifrazione e visualizzazione dei medesimi documenti. In tali ipotesi l'obbligo di esibizione dovrà essere assolto direttamente dal Titolare/Utente.



Il Titolare e/o l'Utente sono tenuti ad inviare all'Amministrazione Finanziaria tutte le comunicazioni e ad effettuare, in proprio, tutti gli adempimenti prescritti dalla normativa fiscale in materia di conservazione dei documenti.

Ciascun soggetto avrà comunque, oltre quanto previsto nell'Accordo, gli obblighi e le responsabilità derivanti dal proprio ruolo, come definito dalle Linee Guida.

Responsabilità del Cliente

La responsabilità dei Dati del Titolare, ivi compresi quelli di cui lo stesso esegua dei trattamenti anche non in qualità di Titolare ai sensi del Regolamento EU 679/2016, è esclusivamente a carico del Titolare e/o dell'Utente e/o del Responsabile della conservazione.

L'accesso ai Servizi è consentito unicamente secondo le modalità indicate nella Scheda Dati Tecnici di Attivazione ed il Cliente, il Titolare, l'Utente e il Responsabile della conservazione si obbligano a non utilizzare ed a non far utilizzare applicazioni diverse e/o processi manuali o applicazioni automatiche per accedere, visualizzare, copiare o utilizzare i Servizi.

È fatto divieto di utilizzare i Servizi al fine di depositare, conservare, inviare, pubblicare, trasmettere e/o condividere dati, applicazioni o documenti informatici che:

- siano in contrasto o violino diritti di proprietà intellettuale, segreti commerciali, marchi, brevetti o altri diritti di proprietà di terzi;
- abbiano contenuti diffamatori, calunniosi o minacciosi;
- contengano materiale pornografico, osceno o comunque contrario alla pubblica morale; contengano *virus*, *worm*, *trojan horse* o, comunque, altre caratteristiche di contaminazione o distruttive;
- in ogni caso siano in contrasto alle disposizioni normative e/o regolamentari applicabili.

Il Titolare/Responsabile della conservazione prende atto che Tinexta InfoCert, anche ai sensi di quanto previsto dall'art. 14, 15, 16 del D.Lgs. 9.4.2003, n. 70, non ha alcun obbligo di sorveglianza sui contenuti dei documenti e sui dati che sono memorizzati, visualizzati o condivisi a mezzo dei Servizi e, pertanto, non avrà alcun obbligo di monitoraggio o di esame degli stessi.

Tinexta InfoCert, ai sensi di quanto previsto nell'art. 17 del sopra citato decreto legislativo, è sottoposta agli obblighi di informazione ivi previsti e si riserva altresì di sospendere i Servizi, ovvero di impedire l'accesso ai documenti e/o ai dati ivi contenuti, qualora venga a conoscenza di una violazione di quanto sopra previsto e/o venga avanzata espressa richiesta in tal senso da un organo giurisdizionale o amministrativo competente in materia in base alle norme vigenti.

Nelle ipotesi di cui al comma precedente, Tinexta InfoCert provvederà a comunicare a mezzo posta elettronica certificata al Titolare/Responsabile della conservazione le motivazioni dell'adozione dei provvedimenti ivi stabiliti, con facoltà della stessa di risolvere di risolvere il rapporto ai sensi dell'Accordo.

Obblighi e responsabilità in tema di generazione ed associazione dei metadati

Il Cliente, il Titolare, il Produttore e il Responsabile della conservazione, ciascuno per quanto di propria competenza, prendono atto che, ai sensi del punto 2.1.1 delle Linee Guida, "Al momento della formazione del documento informatico immutabile, devono essere generati e associati permanentemente ad esso i relativi metadati", così come definiti nell'All. 5 alle Linee Guida stesse (i "Metadati").

L'obbligo della corretta e completa attività di associazione dei Metadati al documento informatico oggetto di conservazione è in capo esclusivamente al Titolare, che si assume pertanto, anche nei confronti di Tinexta InfoCert, ogni responsabilità al riguardo. Il Produttore, comunque, quale soggetto che predispone il Pacchetto di Versamento, risponde in solido col Titolare dell'attività di associazione dei Metadati. Tinexta InfoCert, in qualità di Conservatore, non ha alcun onere di verifica in ordine al contenuto dei Metadati. Tinexta InfoCert inoltre non svolge, nell'ambito del presente Servizio, alcuna attività di consulenza finalizzata alla regolarizzazione dei documenti informatici rispetto a quanto previsto dalla normativa applicabile e dalle Linee Guida. Nel caso in cui il documento informatico trasmesso in conservazione non sia conforme a quanto indicato nel documento "Scheda dati tecnici per l'attivazione di un ambiente di conservazione", che indica le informazioni tecniche necessarie a consentire l'integrazione con il sistema di conservazione, Tinexta InfoCert

trasmetterà al Titolare e/o al Responsabile della conservazione una comunicazione di errore e di rifiuto con la segnalazione del problema.

Dopo che, in base a quanto sopra indicato, il rifiuto sia stato reiterato tre volte, è onere del Titolare e/o del Responsabile della conservazione contattare il servizio di assistenza tecnica di Tinexta InfoCert per tentare una soluzione del problema. Il Titolare/Responsabile della conservazione prende atto che Tinexta InfoCert, anche ai sensi di quanto previsto dall'art. 14, 15, 16 del D.Lgs. 9.4.2003, n. 70, non ha alcun obbligo di sorveglianza sui documenti e sui dati che sono memorizzati, visualizzati o condivisi a mezzo dei Servizi e, pertanto, non avrà alcun obbligo di monitoraggio o di esame degli stessi.

Tinexta InfoCert, ai sensi di quanto previsto nell'art. 17 del sopra citato decreto legislativo, è sottoposta agli obblighi di informazione ivi previsti e si riserva altresì di sospendere i Servizi, ovvero di impedire l'accesso ai documenti e/o ai dati ivi contenuti, qualora venga a conoscenza di una violazione di quanto sopra previsto e/o venga avanzata espressa richiesta in tal senso da un organo giurisdizionale o amministrativo competente in materia in base alle norme vigenti. Nelle ipotesi di cui al comma precedente, Tinexta InfoCert provvederà a comunicare a mezzo posta elettronica certificata al Titolare/Responsabile della conservazione le motivazioni dell'adozione dei provvedimenti ivi stabiliti, con facoltà della stessa di risolvere il Servizio ai sensi delle previsioni di cui all'Accordo.

Restituzione

In ogni caso di cessazione del Servizio, Tinexta InfoCert restituisce al Cliente/Titolare i pacchetti di distribuzione (PdD) consentendo allo stesso, a titolo gratuito, di effettuare un download dei dati e documenti del Titolare. Il download va effettuato entro 30 (trenta) giorni dalla cessazione di efficacia del Servizio.

In alternativa a quanto previsto nel primo capoverso, su richiesta del Titolare i Dati verranno forniti da Tinexta InfoCert, a fronte del pagamento di appositi corrispettivi da definirsi, su supporti fisici all'uopo predisposti da Tinexta InfoCert stessa. Decorsi 30 (trenta) giorni dalla data di cessazione del Servizio, Tinexta InfoCert non avrà più alcuna responsabilità in merito alla conservazione dei Dati del Titolare o dell'Utente.

Attivazione

Tinexta InfoCert, verificati i requisiti di accesso, provvede entro 10 giorni dall'attivazione del Servizio ad assegnare al Titolare/Utente un profilo di abilitazione per l'accesso ai Servizi richiesti.

4. Specifiche tecniche d'uso

Il processo di conservazione



Il processo di conservazione proposto, secondo lo standard ISO 14721 OAIS, gestisce la conservazione dei documenti attraverso la creazione di "Information Packages" (IP). Questi pacchetti contengono il documento e tutte le relative informazioni (metadati), che permettono di arricchirlo e di metterlo a disposizione del Cliente nel tempo.

Il processo può essere così schematizzato:

1. il produttore invia i documenti in conservazione con un pacchetto di versamento, contenente anche i metadati necessari;
2. il pacchetto viene preso in carico dal sistema se rispetta la configurazione concordata (formati, metadati, parametri, policy...) e se l'impronta di hash calcolata coincide con quella contenuta nel pacchetto;
3. il sistema crea i pacchetti di archiviazione; il Responsabile del servizio firma o sigilla e marca temporalmente l'indice di conservazione UNI SInCRO di ogni singolo pacchetto di archiviazione, a garanzia di integrità, immutabilità e autenticità;
4. il sistema restituisce al produttore l'indice di conservazione come ricevuta (rapporto di versamento);
5. il database del sistema viene aggiornato, il pacchetto di archiviazione viene indicizzato, memorizzato e ridondato più volte (ogni pacchetto è soggetto a controlli periodici di integrità e leggibilità a distanza di tempo);
6. il documento conservato può essere ricercato attraverso i metadati, su richiesta dell'utente in possesso delle apposite credenziali, in qualsiasi momento, ed esibito mediante un pacchetto di distribuzione, che contiene tutte le evidenze del processo.

Funzionalità principali:

- accettazione del pacchetto di versamento, formato dal documento da conservare e dai metadati ad esso associati dal produttore;
- conservazione del pacchetto di archiviazione, a norma di legge e per tutta la durata prevista dall' Accordo;
- rettifica del pacchetto di archiviazione, modifica logica, nel pieno rispetto del principio di tracciabilità;
- ricerca tra i documenti conservati, utilizzando uno o più metadati popolati in fase di versamento;
- esibizione del pacchetto di distribuzione, contenente sia il documento conservato che gli altri documenti a corredo della corretta conservazione, che possono essere scaricati in autonomia, in qualsiasi momento;
- scarto, su richiesta formale del Responsabile della conservazione del produttore, cioè cancellazione fisica e logica dei pacchetti di archiviazione e di ogni loro duplicato.

Esiste una versione LEGALDOC accessibile esclusivamente tramite interfaccia web e disponibile nell'e-commerce Tinexta Infocert che mantiene tutte le funzionalità principali di LEGALDOC ma è limitato alla conservazione delle seguenti classi documentali predefinite, e senza possibilità di customizzazioni:

- FATTURE (Il_Ig_fattu)
- DDT (Il_Ig_ddt)
- LIBRI e REGISTRI CONTABILI (Il_Ig_lib)
- ORDINI D'ACQUISTO NSO (Il_Ig_oda)
- OIL, MANDATI e REVERSALI (Il_Ig_oil)
- CONTRATTI (Il_Ig_contratto)
- REGISTRO CARICO E SCARICO RIFIUTI (caso d'uso RENTRI)
- FORMULARIO IDENTIFICAZIONE RIFIUTI (caso d'uso RENTRI)

Una versione specifica destinata alle Pubbliche Amministrazioni dispone invece delle seguenti classi documentali predefinite e senza possibilità di customizzazione:

- FATTURE (Il_Ig_fattu)
- DDT (Il_Ig_ddt)
- LIBRI e REGISTRI CONTABILI (Il_Ig_lib)
- ORDINI D'ACQUISTO NSO (Il_Ig_oda)
- OIL, MANDATI e REVERSALI (Il_Ig_oil)
- CONTRATTI (Il_Ig_contratto)
- DELIBERAZIONI di Giunta, di Consiglio, CdA... (Il_Ig_delib)
- DETERMINAZIONI dirigenziali (Il_Ig_deter)
- REGISTRO GIORNALIERO DI PROTOCOLLO (Il_Ig_regprot)
- DOCUMENTO PROTOCOLLATO (Il_Ig_docprot)
- LIBRO UNICO DEL LAVORO (Il_Ig_lul)
- AGGREGAZIONI DOCUMENTALI (Il_Ig_aggr)

Modalità di erogazione del servizio

Il servizio LEGALDOC può essere erogato nelle seguenti modalità:

- In modalità SaaS
- On-premise

Il cliente potrà accedere al servizio e alle sue funzionalità tramite interfaccia web dedicata, oppure tramite API in caso di offering enterprise.

Requisiti di sistema

Il prodotto non specifica requisiti di sistema perché non è prevista alcuna installazione in loco su datacenter parti terze. Il prodotto è erogato esclusivamente come servizio SaaS.

Nel contesto LegalDoc si fa riferimento a requisiti di integrazione che sono i seguenti:

- linguaggio di interoperabilità del dato: XML
- catalogo Web Services: Api RestFull
- protocollo di comunicazione: HTTPS

Formati supportati

L'ambiente di conservazione è configurato per accettare solo formati concordati, associati ad appositi visualizzatori, al fine di preservare la leggibilità futura dei documenti.

I visualizzatori dei formati standard sono:

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

I visualizzatori dei formati standard sono automaticamente assegnati all'atto dell'attivazione del proprio ambiente di conservazione e sono forniti da Tinexta InfoCert al Soggetto Produttore.

Conservare documenti in altri formati (jpeg, Open Document Format, EML, DICOM, ecc..) è sempre possibile, indicandoli nella Scheda Dati Tecnici - documento referenziato "NDOC – Scheda dati tecnici per l'attivazione di un ambiente di conservazione".

I visualizzatori di formati aggiuntivi ai predefiniti devono essere inviati dal Produttore prima di iniziare la conservazione dei documenti (il sistema accetta i documenti in conservazione anche se il visualizzatore non è caricato, ma finché non viene caricato non è possibile effettuare l'esibizione dei documenti).

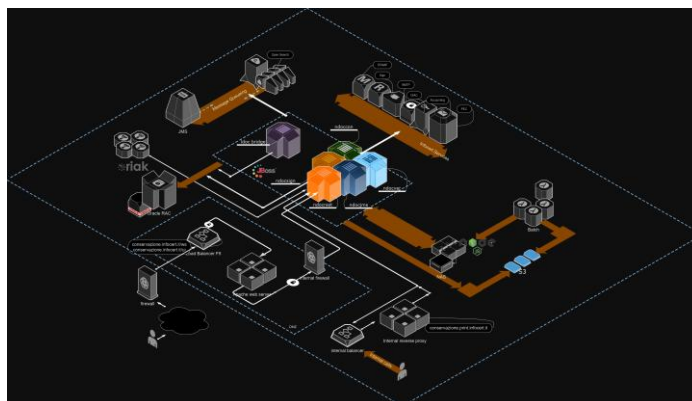
Nel caso si abbia necessità di versare in conservazione un file di tipo "archivio compresso" (come ad esempio zip, tar, rar) il Produttore/Utente si impegna a mantenere gli strumenti necessari per la visualizzazione dei

documenti contenuti all'interno dei file di tipo 'archivio compresso' (e di quelli eventualmente a questi allegati). In tali ipotesi il Produttore/Utente dovrà infatti assicurare quanto previsto dalle citate Linee Guida AgID, in particolare l'Allegato 2, e e ss.mm.ii., relativamente ai programmi per la visualizzazione dei documenti medesimi e l'obbligo di esibizione.

Per i formati MSG e EML il Produttore si impegna a conservare il software necessario alla lettura dei file allegati. Nel caso di invio in conservazione di file cifrati, essi andranno distinti valorizzando l'apposito tag nel file dei parametri che accompagna la conservazione. Per i documenti di questo tipo, il Produttore si impegna a conservare il software necessario alla loro decrittazione, sollevando Tinexta InfoCert dalla responsabilità sulla loro visualizzazione.

Architettura di alto livello

Il disegno architetturale di Ndoc rispecchia il paradigma SOA ed è composto da aree che svolgono compiti specifici, sono connesse tra loro in quanto comunicano via TCP/IP ovvero specificatamente via HTTP(S), NFS, AJP, JMS ecc basandosi su il servizio svolto da ciascun componente.



Identificativi e accessi al sistema

Il Titolare e/o Cliente e/o l'Utente può utilizzare i Servizi previa verifica dei requisiti di accesso al sistema, mediante gli strumenti di identificazione previsti negli appositi Allegati.

Il Titolare e/o Cliente e/o l'Utente sono informati del fatto che la conoscenza degli strumenti di identificazione da parte di soggetti terzi consentirebbe a questi ultimi l'accesso ai Servizi ed ai Dati del Titolare. Il Titolare e/o Cliente e/o l'Utente è pertanto tenuto a conservare ed a far conservare al proprio personale che utilizza i Servizi tali strumenti di identificazione con la massima riservatezza e con la massima diligenza, obbligandosi a non cederli o consentirne l'uso a terzi. Tinexta InfoCert non potrà in alcun caso essere ritenuta responsabile di qualsiasi danno diretto e/o indiretto derivante dalla mancata osservanza da parte del Titolare e/o Cliente e/o dell'Utente di quanto sopra.

5. SLA e KPI

SLA di Servizio

In termini di erogazione, si prevedono i seguenti valori di disponibilità mensile del servizio:

KPI	Servizio	Orario	Disponibilità
D01	LegalDoc	24x7	99,00%



Di seguito sono descritte le modalità di calcolo dei KPI di disponibilità:

KPI	Ambito	Descrizione
D01, D02, ...	Disponibilità dei Servizi	Il metodo di calcolo per gli indicatori di disponibilità si basa sui seguenti valori: periodo osservato = durata in secondi del periodo di osservazione, al netto delle manutenzioni programmate tempo indisponibilità = somma delle durate in secondi dei tempi di indisponibilità del servizio, nel periodo di osservazione Il valore di disponibilità è calcolato, per ogni servizio, tramite la seguente formula: $D = \frac{\text{Periodo osservato} - \text{Tempo indisponibilità}}{\text{Periodo osservato}} * 100$ Il periodo di osservazione è mensile. La violazione si individua quando D < disponibilità concordata

Tinexta InfoCert limita la propria responsabilità all'erogazione dei propri servizi, non è quindi responsabile per eventuali anomalie di performance dovuti a indisponibilità o lentezza nella rete che connette il Cliente all'IDC. Tinexta InfoCert non è inoltre responsabile di anomalie derivanti da:

- incorretta configurazione o dimensionamento dell'infrastruttura del Cliente;
- incorretta installazione o configurazione di software che utilizzano servizi Tinexta InfoCert sull'infrastruttura del Cliente.

KPI di performance

P1 -Tempo medio conservazione -> 1 sec
P2 -Tempo medio indicizzazione -> 1 sec
P3 - Tempo medio esibizione -> 1 sec

Affidamento del servizio di conservazione a norma

Il sottoscritto **Responsabile della conservazione** (il “**Responsabile della Conservazione**”), a tal fine ed in questo ruolo nominato dal seguente soggetto, in nome e per conto del quale agisce:

[RAGIONE SOCIALE] _____ - C.F. _____;
(il “**Titolare degli oggetti della conservazione**”)

Cognome e Nome _____

Data di Nascita ____/____/____ Cod. Fisc. _____ Cittadinanza _____

Indirizzo **PEC** per comunicazioni _____@_____

nell’ambito del proprio ruolo di **Responsabile della conservazione**, così come previsto dal par. 4.5 delle “Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici” adottate da AgID nel maggio 2021 e dall’art. 34 comma 1-bis del Codice dell’Amministrazione Digitale (decreto legislativo 7 marzo 2005, n. 82 e successive modifiche), e comunque dichiarando, ad ogni effetto di legge, di essere legittimato a sottoscrivere il presente documento, in nome e per conto del/i Titolare/i degli oggetti della conservazione,

AFFIDA

a Tinexta InfoCert S.p.a., con sede legale in Roma, Piazzale Flaminio 1/B, P. IVA 07945211006, il servizio di conservazione dei documenti informatici del Titolare/i degli oggetti della conservazione, secondo quanto previsto nell’Allegato Tecnico.

Data _____

Firma del Responsabile della Conservazione _____

In particolare:

- 1) Sono escluse dall’affidamento le attività di riversamento dei documenti conservati da un supporto di memorizzazione ad un altro, che costituiscono un servizio a sé stante, effettuato dietro eventuale, espressa e separata richiesta, le attività che precedono l’invio dei documenti (ad es., la digitalizzazione dei documenti analogici, il rispetto dei tempi prescritti per l’invio in conservazione, l’idoneità del software adottato dal Titolare) e la correttezza e coerenza dei contenuti dei medesimi.
- 2) Ai fini della conservazione dei documenti analogici originali, il Titolare dell’oggetto della conservazione o altro soggetto da questi debitamente delegato dovrà provvedere autonomamente ad apporre la firma digitale ai documenti e, ove previsto, per particolari tipologie di documenti analogici originali unici, a far intervenire un pubblico ufficiale, che attesti la conformità tra il documento conservato e l’originale, ai sensi dell’art. 22, c. 4 e 5 del D. Lgs 7.03.2005, n. 82 CAD e dell’art. 4 del D.M.E.F 17.06.2014 per i documenti rilevanti ai fini fiscali e tributari.
- 3) In base al presente atto di affidamento Tinexta InfoCert S.p.a. opererà quale Conservatore dei documenti informatici del Titolare/i dell’oggetto della conservazione, provvedendo all’esecuzione dei compiti definiti



dalle Linee Guida AgID, secondo quanto previsto nell'Accordo e nell'Allegato Tecnico ivi definito.

In particolare, nell'ambito della propria organizzazione, Tinexta InfoCert S.p.A. ha nominato un Responsabile del servizio di conservazione, il quale:

- definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;
- gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
- genera e sottoscrive il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
- genera e sottoscrive il pacchetto di distribuzione con firma digitale, nei casi previsti dal manuale di conservazione;
- effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
- effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;
- al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;
- provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
- predispone le misure necessarie per la sicurezza fisica e logica del sistema di conservazione;
- 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.

(Firma Responsabile della conservazione)

Manuale di Conservazione

Il contenuto del presente documento è di proprietà di Argentea s.r.l. Tutti i diritti riservati.



EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	30/04/2019	Roberto Conci	<i>Resp. della sicurezza dei sistemi per la conservazione</i>
Verifica	30/04/2019	Di Domenico Marco	<i>Resp. dello sviluppo e della manutenzione del sistema di conservazione e dei sistemi informativi per la conservazione</i>
Verifica	30/04/2019	Benvenuti Carlo	<i>Resp. del servizio di conservazione</i>
Verifica	19/03/2021	Anghinolfi Andrea	<i>Resp. del servizio di conservazione</i>
Verifica	10/03/2022	Anghinolfi Andrea	<i>Resp. del servizio di conservazione</i>
Verifica	19/05/2022	Anghinolfi Andrea	<i>Resp. del servizio di conservazione</i>
Verifica	18/09/2025	Anghinolfi Andrea	<i>Resp. del servizio di conservazione</i>

REGISTRO DELLE VERSIONI

N°Ver	Data emissione	Modifiche apportate	Redatto da	Approvato da
1.0	30/04/2019	Prima stesura	Roberto Conci	Benvenuti Carlo
1.1	05/11/2019	Aggiornamento Organigramma e Ruoli (Responsabile del servizio di conservazione)	Cherotti Francesco	Anghinolfi Andrea
1.2	19/03/2021	Revisione generale del documento per cambio dell'infrastruttura di intermediazione	Cherotti Francesco	Anghinolfi Andrea
1.3	10/03/2022	Aggiornamento ruoli e revisione	Cherotti Francesco	Anghinolfi Andrea
1.4	19/05/2022	Aggiunto paragrafo 6.4.1	Bertè Maria	Anghinolfi Andrea
1.5	18/09/2025	Aggiornamento paragrafi 8.5 e 8.6 Aggiornamento riferimenti normativi standard tecnici; revisioni. Aggiornamento ruoli.	Antonio Placanica	Anghinolfi Andrea



SOMMARIO

1. SCOPO E AMBITO DEL DOCUMENTO.....	5
2. TERMINOLOGIA (GLOSSARIO E ACRONIMI).....	6
2.1. Glossario dei termini e acronimi	6
2.2. Abbreviazioni e termini tecnici.....	16
3. NORMATIVA E STANDARD DI RIFERIMENTO	19
3.1. Normativa di riferimento	19
3.2. Standard di riferimento	19
4. RUOLI E RESPONSABILITÀ	21
4.1. Profili professionali.....	22
5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE	25
5.1. Organigramma	25
5.2. Strutture organizzative e Ruoli.....	25
5.3. Responsabilità e funzioni nel processo di conservazione	26
6. OGGETTI SOTTOPOSTI A CONSERVAZIONE.....	27
6.1. Descrizione delle tipologie dei documenti sottoposti a conservazione	27
6.2. Copie informatiche di documenti analogici originali unici	28
6.3. Formati gestiti	28
6.3.1. Caratteristiche generali dei formati.....	29
6.3.2. Formati consigliati per la conservazione.....	29
6.3.3. Identificazione.....	32
6.3.4. Migrazione dei formati	32
6.4. Metadati da associare alle diverse tipologie di documenti.....	32
6.4.1. Metadati obbligatori AGID.....	33
6.5. Pacchetto di versamento	33
6.5.1. Specifiche Pacchetto di Versamento	34
6.6. Pacchetto di archiviazione	34
6.6.1. Specifiche Pacchetto di Archiviazione.....	34
6.7. Pacchetto di distribuzione.....	34
7. IL PROCESSO DI CONSERVAZIONE	35
7.1. Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico	35
7.1.1. Ricezione dell'indice del pacchetto di versamento.....	36
7.2. Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti	37
7.3. Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico	39
7.3.1. Specifiche rapporto di versamento.....	39
7.4. Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie	40
7.5. Preparazione e gestione del pacchetto di archiviazione	40
7.5.1. Chiusura anticipata (in corso d'anno) del Pacchetto di Archiviazione.	40

7.6.	Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione	40
7.6.1.	Funzioni svolte alla conclusione del contratto.....	41
7.7.	Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti	42
7.7.1.	Produzione di duplicati	42
7.7.2.	Produzione di copie	42
7.7.3.	Produzione copie o duplicati su supporti rimovibili.....	42
7.7.4.	Intervento del Pubblico Ufficiale	43
7.8.	Scarto dei pacchetti di archiviazione.....	43
7.8.1.	Trasferimento dei documenti informatici in conservazione	43
7.8.2.	Scarto dei documenti informatici conservati.....	43
7.9.	Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori.....	44
7.10.	Cessazione del Servizio di Conservazione	44
7.11.	Tabella riepilogativa delle fasi del processo di conservazione	44
7.12.	Audit Log	48
8.	IL SISTEMA DI CONSERVAZIONE	49
8.1.	Infrastruttura informatica datacenter	49
8.2.	Caratteristiche generali della soluzione di conservazione	49
8.3.	Componenti Logiche	50
8.4.	Componenti tecnologiche	51
8.5.	Componenti fisiche	51
8.5.1.	Ambiente di Produzione	52
8.5.2.	Sito Secondario (DR)	52
8.6.	Politica di gestione degli accessi applicativi	53
8.7.	Procedure di gestione e di evoluzione	54
8.7.1.	Change management.....	54
8.7.2.	Verifica periodica di conformità a normativa e standard di riferimento	55
9.	MONITORAGGIO E CONTROLLI.....	56
9.1.	Conduzione e manutenzione del sistema di conservazione, gestione log, monitoraggio Infrastruttura.....	56
9.2.	Procedure di monitoraggio (applicativo)	56
9.3.	Verifiche sull'integrità degli archivi	57
9.3.1.	Pianificazione delle verifiche periodiche da effettuare	57
9.3.2.	Mantenimento della firma per il periodo di conservazione	57
9.4.	Soluzioni adottate in caso di anomalie	57
9.4.1.	Procedura di ripristino in caso di corruzione o perdita dei dati:.....	58
9.4.2.	Gestione dei log	58

1. SCOPO E AMBITO DEL DOCUMENTO

Il presente documento è il Manuale del sistema di conservazione erogato da Argentea S.r.l. (di seguito per brevità chiamato anche “Manuale”) ed è reperibile collegandosi alla pagina del sito di AgID dei conservatori accreditati (<https://conservatoriqualeificati.agid.gov.it/>). Illustra dettagliatamente l’organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, i processi inerenti al servizio, in particolare le modalità di versamento, archiviazione e distribuzione, le architetture e le infrastrutture utilizzate, le misure di sicurezza adottate ed ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione digitale di documenti informatici.

Il servizio, pur essendo predisposto in maniera nativa per la conservazione di ogni documento che rispetti i formati previsti, è rivolto principalmente agli Enti della Pubblica Amministrazione che utilizzano l’Ordinativo Informatico.

Il Manuale è costituito dalla versione corrente del presente documento.

In particolare, nel presente Manuale sono riportati:

- a) i dati dei soggetti che nel tempo hanno assunto la responsabilità del servizio di conservazione, descrivendo in modo puntuale i soggetti, le funzioni e gli ambiti oggetto dell’affidamento stesso;
- b) la struttura organizzativa comprensiva delle funzioni, delle responsabilità e degli obblighi dei diversi soggetti che intervengono nel processo di conservazione;
- c) la descrizione delle tipologie dei documenti informatici sottoponibili a conservazione, comprensiva dell’indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di documenti e delle eventuali eccezioni;
- d) la descrizione delle modalità di presa in carico di uno o più pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento e della descrizione dei controlli effettuati su ciascuno specifico formato adottato;
- e) la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione;
- f) la modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;
- g) la descrizione del sistema di conservazione, comprensivo di tutte le componenti tecnologiche, fisiche e logiche, opportunamente documentate e delle procedure di gestione e di evoluzione delle medesime;
- h) la descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull’integrità degli archivi con l’evidenza delle soluzioni adottate in caso di anomalie;
- i) la descrizione delle procedure per la produzione di duplicati o copie;
- j) i tempi entro i quali le diverse tipologie di documenti informatici devono essere oggetto di scarto/cancellazione;
- k) le modalità con cui viene richiesta la presenza di un pubblico ufficiale, indicando anche quali sono i casi per i quali è previsto il suo intervento;
- l) le normative in vigore nei luoghi dove sono conservati i documenti.

Il Manuale recepisce le disposizioni di cui al D.Lgs. 7 marzo 2005, n. 82, e s.m.i. (Codice dell’Amministrazione Digitale), di seguito per brevità chiamato anche “Codice” o “CAD”, oltre alle indicazioni riportate nei provvedimenti di legge o di prassi richiamati nel capitolo “Riferimenti normativi e di prassi” nonché i provvedimenti di natura tecnica richiamati nel capitolo “Riferimenti tecnici”.

Il Cliente è tenuto a leggere con la massima attenzione il presente Manuale predisposto da Argentea S.r.l. ed in qualità di unico Responsabile della Conservazione, ne approva e ne fa propri i contenuti.

Si precisa che il Manuale illustra il solo procedimento di conservazione di documenti nativamente informatici o resi tali da un processo di scannerizzazione e indicizzazione (anch’esso esterno al contesto qui trattato) mentre non tratta alcun aspetto in merito alla gestione dei documenti analogici e/o della loro trasformazione in digitale.

2. TERMINOLOGIA (GLOSSARIO E ACRONIMI)

Secondo la normativa vigente e ai fini dell'interpretazione del presente Manuale, i termini e le espressioni sotto elencate avranno il significato descritto nelle definizioni in esso riportate. Qualora le definizioni adottate dalla normativa di riferimento non fossero riportate nell'elenco che segue, si rimanda ai testi in vigore per la loro consultazione.

I termini e le espressioni non definiti avranno il significato loro attribuito all'interno del paragrafo o sezione che li contiene.

Ai fini della fruizione del Servizio di conservazione digitale dei documenti informatici descritto nel presente Manuale, valgono ad ogni effetto anche le definizioni contenute nel contratto, da intendersi, pertanto, qui interamente riportate e trascritte, nonché le seguenti.

2.1. Glossario dei termini e acronimi

Glossario dei termini e Acronimi	
AgID	Agenzia per l'Italia Digitale
Accesso	Operazione che consente a chi ne ha diritto di prendere visione dei documenti informatici conservati.
Accordo di versamento	Accordo di versamento è la traduzione di "Submission Agreement", termine definito nello standard OAIS – ISO 14721. Il produttore (Producer) deposita le risorse informative all'interno di un OAIS affinché siano conservate a lungo termine. Concordate le modalità di versamento nell'archivio mediante un accordo formale (Submission Agreement) che stabilisca il tipo di informazioni e i relativi metadati oggetto di conservazione, nonché i formati da adottare e le modalità operative di trasferimento, il produttore invia il materiale all'OAIS che, attraverso un processo di acquisizione (Ingestion), accetta le risorse e le predispone per l'inclusione nell'archivio.
Accreditamento	Riconoscimento, da parte dell'Agenzia per l'Italia Digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza, ad un soggetto pubblico o privato che svolge attività di conservazione o di certificazione del processo di conservazione.
Agente di alterazione	Qualsiasi codice contenuto in un documento informatico potenzialmente idoneo a modificare la rappresentazione dell'informazione senza alterarne il contenuto binario (in via meramente esplicativa e non esaustiva: macro, codici eseguibili nascosti, formule di foglio di lavoro occulte in tutto o in parte, sequenze di caratteri occultate all'interno dei documenti informatici).
Aggregazione documentale informatica	Raccolta di documenti informatici o 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 organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività.
Archivio informatico	Archivio logico abbinato ad un codice fiscale/partita IVA, corrispondente ad una organizzazione pubblica o privata aderente al servizio, costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico.
Area organizzativa omogenea	Un insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445 e s.m.i
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 di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico.
Base di dati	Collezione di dati registrati e correlati tra loro.
Certificatore accreditato	Soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, dell'Agenzia per l'Italia Digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza.
Certificati elettronici	Gli attestati elettronici che collegano all'identità del titolare i dati utilizzati per verificare le firme elettroniche.
Chiave privata	L'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico.
Chiave pubblica	L'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche.
Chiusura del pacchetto di archiviazione	Operazione consistente nella sottoscrizione del pacchetto di archiviazione con firma digitale apposta da un Firmatario Delegato di Argentea S.r.l. e apposizione di una validazione temporale con marca temporale alla relativa impronta.

Ciclo di gestione	Arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo.
Classificazione	Attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati.
Codice o CAD	Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni.
Codice eseguibile	Insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici.
Conservatore accreditato	Soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia Digitale o da un certificatore accreditato, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza.
Conservazione	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel Manuale di conservazione.
Contrassegno a stampa	Contrassegno generato elettronicamente, apposto a stampa sulla copia analogica di un documento amministrativo informatico per verificarne provenienza e conformità all'originale.
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 DPR 445/2000 e s.m.i. nei casi di amministrazioni che abbiano istituito più Aree Organizzative Omogenee.
Copia analogica di documento informatico	Documento analogico avente contenuto identico a quello del documento informatico da cui è tratto.
Copia informatica di documento analogico	Il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto.
Copia per immagine su supporto informatico di documento analogico	Il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto.
Copia informatica di documento informatico	Il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari.
Copia di sicurezza	Copia di backup degli archivi del sistema di conservazione.
Descrittore evidenze	Vedi pacchetto informativo.

Destinatario	Identifica il soggetto/sistema al quale il documento informatico è indirizzato.
DIRT	Documenti informatici rilevanti ai fini delle disposizioni tributarie.
Documento analogico	La rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.
Documento analogico originale	Documento analogico che può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi.
Documento originale unico	E' quel documento analogico il cui contenuto non può essere desunto da altre scritture o documenti di cui sia obbligatoria la tenuta, anche presso terzi e che non soddisfa, dunque, alcuna delle condizioni elencate nella definizione di "Documento analogico originale".
Documento informatico	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
Duplicato informatico	Il documento informatico ottenuto mediante la memorizzazione, sullo stesso supporto o su supporti diversi, della medesima sequenza di valori binari del documento originario.
Duplicazione dei documenti informatici	Produzione di duplicati informatici.
Esibizione	Operazione che consente di visualizzare un documento conservato e di ottenerne copia.
Estratto per riassunto	Documento nel quale si attestano in maniera sintetica ma esaustiva fatti, stati o qualità desunti da dati o documenti in possesso di soggetti pubblici.
Evidenza informatica	Una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.
Fascicolo informatico	Raccolta, individuata con identificativo univoco, di atti, documenti e dati informatici, da chiunque formati, del procedimento amministrativo, nell'ambito della pubblica amministrazione, secondo le disposizioni stabilite dall'articolo 41 del Codice. Per i soggetti privati è da considerarsi fascicolo informatico ogni aggregazione documentale, comunque formata, funzionale all'erogazione di uno specifico servizio o prestazione.
Firma digitale	Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità

	di un documento informatico o di un insieme di documenti informatici.
Firma elettronica	L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.
Firma elettronica avanzata	Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.
Firma elettronica qualificata	Un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma.
Firmatario delegato	Responsabile del servizio di conservazione o Persona formalmente delegata ad apporre la propria firma digitale sui Pacchetti di Archiviazione per conto di Argentea S.r.l.; questa persona può essere interna o esterna ad Argentea S.r.l., laddove è giuridicamente possibile.
Fruibilità di un dato	La possibilità di utilizzare il dato anche trasferendolo nei sistemi informativi automatizzati di un'altra amministrazione.
Formato	Modalità di rappresentazione del documento informatico mediante codifica binaria; comunemente è identificato attraverso l'estensione del file e/o il tipo MIME.
Fornitore esterno	Organizzazione che fornisce ad Argentea S.r.l. servizi relativi al suo sistema di conservazione dei documenti.
Funzionalità aggiuntive	Le ulteriori componenti del sistema di protocollo informatico necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni.
Funzionalità interoperative	Le componenti del sistema di protocollo informatico finalizzate a rispondere almeno ai requisiti di interconnessione di cui all'articolo 60 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.
Funzionalità minime	La componente del sistema di protocollo informatico che rispetta i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.
Funzione di Hash	Una funzione matematica che genera, a partire da una evidenza informatica, una sequenza di bit (impronta) in modo tale che risulti di fatto impossibile, a partire da questa,

	ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
Generazione automatica di documento informatico	Formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni.
Gestione informatica dei documenti	L'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato, effettuate mediante sistemi informatici.
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
idPdA	Indice del Pacchetto di Archiviazione Evidenza informatica associata ad ogni volume di conservazione (VdC), contenente un insieme di informazioni articolate come descritto dallo Schema XML fornito nel seguito. L'IdC deve essere corredato da: riferimento temporale, firma digitale dei soggetti titolari a effettuare il processo di conservazione sostitutiva, coerentemente con le disposizioni della normativa vigente. Nota: L'IdC coincide con lo Schema XML descritto nel presente documento, istanziato secondo le specifiche esigenze di contesto e provvisto di riferimento temporale e firma digitale. (Standard UNI 11386, 2020 – "Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali – SInCRO")
idPdV	Indice del Pacchetto di Versamento.
Immodificabilità	Caratteristica che rende la rappresentazione 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	La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash (Standard UNI 11386, 2020 - "Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali – SInCRO").
Insieme minimo di metadati del documento informatico	Complesso dei metadati da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta.

<i>Integrità</i>	Insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato.
<i>Interoperabilità</i>	Capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi.
<i>Leggibilità</i>	Insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti.
<i>Log di sistema</i>	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.
<i>Manuale di gestione</i>	Strumento che descrive il sistema di gestione informatica dei documenti di cui all'articolo 5 delle regole tecniche del protocollo informatico ai sensi delle regole tecniche per il protocollo informatico D.P.C.M. 31 ottobre 2000 e successive modificazioni e integrazioni.
<i>Memorizzazione</i>	Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici.
<i>Marca temporale</i>	Evidenza informatica che consente di rendere opponibile a terzi un riferimento temporale; la marca temporale prova l'esistenza in un certo momento di una determinata informazione, sotto forma di struttura dati firmata da una Time Stamping Authority.
<i>Metadati</i>	Insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 delle Linee guida sulla formazione, gestione e conservazione dei documenti informatici.
<i>Normativa regolante la conservazione digitale di documenti informatici</i>	Si intende: il D.lgs. 7 marzo 2005, n. 82 e s.m.i. (Codice dell'amministrazione Digitale "CAD") e i relativi decreti attuativi, le regole tecniche, le linee guida e aggiungendo, per il documento informatico a rilevanza tributaria, le disposizioni di cui al DMEF 17 giugno 2014 e s.m.i., il DPR 26 ottobre 1972 n. 633 e s.m.i., il DPR 29 settembre 1973 n. 600 e s.m.i., i provvedimenti interpretativi emessi dagli organi competenti.
<i>Originali non unici</i>	I documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi.

<i>Pacchetto di archiviazione</i>	Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento.
<i>Pacchetto di distribuzione</i>	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta.
<i>Pacchetto di invio documenti</i>	Pacchetto informativo utilizzato per inviare i documenti fisici al sistema di conservazione a seguito dell'avvenuta accettazione di un pacchetto di versamento.
<i>Pacchetto di versamento</i>	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel Manuale di conservazione.
<i>Pacchetto informativo</i>	Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, documenti amministrativi informatici, documenti informatici rilevanti ai fini tributari, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare.
<i>Piano della sicurezza del sistema di conservazione</i>	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.
<i>Piano della sicurezza del sistema di gestione informatica dei documenti</i>	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.
<i>Piano di conservazione</i>	Strumento, integrato con il sistema di classificazione per la definizione dei 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 e s.m.i.
<i>Piano generale della sicurezza</i>	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.
<i>Presa in carico</i>	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal Manuale di conservazione.
<i>Processo di conservazione</i>	Insieme delle attività finalizzate alla conservazione dei documenti informatici.
<i>Processo/servizio di marcatura temporale</i>	E' il processo/servizio che associa in modo affidabile un'informazione a un particolare momento, al fine di stabilire prove attendibili che indicano il momento in cui l'informazione esisteva.
<i>Produttore</i>	Persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce – in proprio o

	attraverso specifico delegato - il <i>PdV (pacchetto di Versamento)</i> ed è responsabile del trasferimento del suo contenuto nel Sistema di Conservazione.
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 specializzato per tipologia o per oggetto; nell'ambito della pubblica amministrazione è previsto ai sensi dell'articolo 53, comma 5 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.
Registro di protocollo	Registro informatico della corrispondenza 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.
Referente/i del Cliente	E'/sono le persone fisiche che il Cliente indica ad Argentea S.r.l. quali punti di riferimento tecnico ed organizzativo per gli aspetti che riguardano le comunicazioni relative all'erogazione del servizio di conservazione.
Repertorio informatico	Registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche che trattano il procedimento, ordinati secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica.
Responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi	Dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al 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, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione.
Responsabile della Conservazione	E' il soggetto responsabile dell'insieme delle attività di conservazione.
Responsabile del Servizio di Conservazione	E' la persona designata da Argentea S.r.l. a gestire il <i>SdC</i> affidato in outsourcing alla stessa dal <i>Titolare dei documenti informatici</i> . L'attività del <i>RSC</i> consiste nel gestire ed erogare il servizio di conservazione come definito nel <i>contratto</i> e nel presente <i>Manuale di Conservazione</i> utilizzando strumenti e metodi conformi alla normativa vigente.
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 di dati personali.
Responsabile della sicurezza	Soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza.
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, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse culturale.
Sistema di classificazione	Strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata.
Sistema di conservazione (SdC)	Insieme di hardware, software, politiche, procedure, linee guida, regolamenti interni, infrastrutture fisiche e organizzative, volto ad assicurare la conservazione elettronica dei documenti del Cliente per il periodo di tempo specificato nel contratto. Detto sistema tratta i documenti informatici in conservazione in pacchetti informativi che si distinguono in pacchetti di versamento, pacchetti di archiviazione e pacchetti di distribuzione.
Sistema di gestione informatica dei documenti	Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.; per i privati è il sistema che consente la tenuta di un documento informatico.
Staticità	Caratteristica che indica 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.
Transazione informatica	Particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche della base di dati.
Testo unico	Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni.
Titolare/i	La persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica.
Titolare dei Documenti Informatici	E' il soggetto che, sottoscrivendo apposito contratto, affida ad Argentea S.r.l. le attività di conservazione dei propri documenti informatici (autoprodotti o acquisiti da terzi), che per legge o regolamento o per propria volontà è tenuto o comunque intenzionato a conservare. Tale figura

	generalmente va anche a ricoprire (direttamente o tramite proprio personale interno) il ruolo di <i>Produttore</i> previsto dalle <i>Regole tecniche</i> .
Titolare del trattamento	La/e persona/e fisica/che o giuridica/che o altro tipo di società o ente che è/sono giuridicamente responsabili/e, anche unitamente ad altro titolare, delle decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
Ufficio utente	Riferito ad un area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico.
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.
Validazione temporale	Il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi.
Versamento agli archivi di stato	Operazione con cui il responsabile della conservazione di un'amministrazione statale effettua l'invio 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.

2.2. Abbreviazioni e termini tecnici

Abbreviazioni e termini tecnici	
Agenzia per L'Italia Digitale (già DigitPA)	Ente pubblico non economico, con competenza nel settore delle tecnologie dell'informazione e della comunicazione nell'ambito della pubblica amministrazione. L'Ente, che ha ereditato le funzioni di DigitPA che, a sua volta, ha ereditato le funzioni del CNIPA, opera secondo le direttive per l'attuazione delle politiche e sotto la vigilanza del Ministro per la pubblica amministrazione e l'innovazione, con autonomia tecnica e funzionale, amministrativa, contabile, finanziaria e patrimoniale.
ASP - Application Service Provider	Fornitore di Servizi Applicativi
CAD	Decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni - "Codice dell'amministrazione digitale".
CA - Certificatore Accreditato	Soggetto autorizzato dall'Agenzia per l'Italia Digitale che garantisce l'identità dei soggetti che utilizzano la firma digitale.
CC - Common Criteria	Criteri per la valutazione della sicurezza nei sistemi informatici, con riconoscimento internazionale in quanto evoluzione dei criteri europei (ITSEC), statunitensi (Federal Criteria), e canadesi (Canadian Criteria).

C.M.	Circolare Ministeriale
CNIPA – Centro Nazionale per l'Informatica nella Pubblica Amministrazione	Creato con l'articolo 176 del DL 196/03, il CNIPA ha incorporato le strutture e le funzioni dell'AIPA e del Centro Tecnico della RUPA ed è stato quindi sostituito da DigitPA e quindi dall'AgID - Agenzia per l'Italia Digitale.
CSCD - contratto di servizio di conservazione dei documenti	Contratto di servizio di conservazione dei documenti, ove sono esplicitate chiaramente l'ambito della delega conferita, le specifiche funzioni, le attività e le responsabilità affidate dal Cliente ad Argentea S.r.l.
D.LGS.	Decreto Legislativo
D.M.	Decreto Ministeriale
DNS – Domain Name System	Sistema di gestione dei nomi simbolici associati ad indirizzi di siti e domini Internet. Quando un messaggio di posta elettronica (e-mail), o un applicativo di consultazione di siti internet (browser) punta ad un dominio, il DNS traduce il nome inserito sotto forma di URL (es. http://www.....it) / in un indirizzo costituito da una sequenza numerica convenzionale (es. 123.123.23.3)
D.P.C.M.	Decreto del Presidente del Consiglio dei Ministri
D.P.R.	Decreto Presidente della Repubblica
DPS	Documento Programmatico per la Sicurezza
ETSI	European Telecommunications Standards Institute
HSM - Hardware Security Module	Dispositivi hardware dedicati per la sicurezza crittografica e la gestione delle chiavi in grado di garantire un elevato livello di protezione.
HTTP (Hypertext Transfer Protocol)	Protocollo di trasmissione, che permette lo scambio di file (testi, immagini grafiche, suoni, video e altri documenti multimediali) su World Wide Web.
HTTPS (Secure Hypertext Transfer Protocol)	Protocollo di trasmissione, sviluppato da Netscape Communications Corporation, per la cifratura e decifratura dei dati trasmessi durante la consultazione di siti e pagine Internet. Corrisponde ad un'estensione del protocollo Internet standard HTTP (Hypertext Transfer Protocol), attraverso il protocollo SSL.
ICT - Information and Communication Technology	Tecnologia dell'Informazione e delle Telecomunicazioni. Il dipartimento che gestisce i sistemi informatici e telematici.
INTERNET	Un sistema globale di reti informatiche nel quale gli utenti di singoli computer possono ottenere informazioni da luoghi diversi. Lo sua grande diffusione è stata determinata principalmente dall'introduzione dei protocolli di trasmissione di documenti con riferimenti ipertestuali (HTTP) e dallo sviluppo del World Wide Web (WWW).
ISO – International Organization for Standardization	Organizzazione internazionale per la standardizzazione, costituita da organismi nazionali provenienti da più di 75 paesi. Ha stabilito numerosi standard nell'area dei sistemi informativi. L'ANSI (American National Standards Institute) è uno dei principali organismi appartenenti all'ISO.

ITSEC – Information Technology Security Evaluation Criteria	Criteri europei per la valutazione della sicurezza nei sistemi informatici.
MEF	Ministero dell'Economia e delle Finanze
NTP – Network Time Protocol	Protocollo per la sincronizzazione del tempo
OID – Object Identifier	Sequenza numerica univoca che identifica un oggetto (struttura, algoritmo, parametro, sistema) nell'ambito di una gerarchia generale definita dall'ISO.
PdV	Pacchetto di Versamento
PdA	Pacchetto di Archiviazione
PdD	Pacchetto di Distribuzione
PU	Pubblico Ufficiale
PIN – Personal Identification Number	Codice di sicurezza riservato che permette l'identificazione del soggetto abbinato ad un dispositivo fisico. Permette ad esempio l'attivazione delle funzioni del dispositivo di firma.
POP – Point of Presence	Punto di accesso alla rete internet
PSCD - Prestatore di Servizi di Conservazione dei Dati	Nella fattispecie, Argentea S.r.l.
SSL – Secure Socket Layer	Protocollo standard per la gestione di transazioni sicure su Internet, basato sull'utilizzo di algoritmi crittografici a chiave pubblica.
TSA	Time Stamping Authority
TSS	Time Stamping Service
TUDA - DPR 28 dicembre 2000, n. 445, e successive modificazioni - “Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa”;	DPR 28 dicembre 2000, n. 445, e successive modificazioni - “Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa”.
URL – Uniform Resource Locator	Sistema standard di nomenclatura specificante un sito, dominio o altro oggetto (file, gruppo di discussione, ecc.) su Internet. La prima parte dell'URL (http, ftp, file, telnet, news) specifica il protocollo di accesso all'oggetto.
XML	È l'acronimo di Extensible Markup Language. Viene utilizzato per definire le strutture dei dati utilizzando dei marcatori (markup tags). È lo standard utilizzato, ad esempio, per l'emissione delle Fatture Elettroniche verso la Pubblica Amministrazione.
WWW – World Wide Web	Insieme di risorse interconnesse da hyperlink accessibili tramite Internet.

3. NORMATIVA E STANDARD DI RIFERIMENTO

3.1. *Normativa di riferimento*

Il sistema di conservazione digitale di Argentea S.r.l. è stato realizzato in conformità alla normativa vigente in materia di conservazione dei documenti informatici. Alla data l'elenco dei principali riferimenti normativi italiani in materia, ordinati secondo il criterio della gerarchia delle fonti, è costituito da:

- **Codice Civile** [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- **Legge 7 agosto 1990**, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- **Decreto del Presidente della Repubblica 28 dicembre 2000**, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- **Decreto Legislativo 30 giugno 2003**, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- **Decreto Legislativo 22 gennaio 2004**, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- **Decreto Legislativo 7 marzo 2005** n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
- **Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013** – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;
- **D.M. 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;
- **Il DPR nr. 1409 del 30 settembre 1963** - (Legge archivistica) all'art. 30 prevede che le cartelle cliniche siano conservate illimitatamente. Secondo le norme vigenti, inoltre, gli originali cartacei delle cartelle cliniche in quanto originali unici, non possono essere distrutti;
- **Circolare Ministero della Sanità 19 dicembre 1986**, n. 61 - Circolare avente per oggetto il periodo di conservazione della documentazione sanitaria presso le istituzioni sanitarie pubbliche e private di ricovero e cura
- **DM 14.2.1997** - Norma di attuazione del D.lgs n.230/95, "Determinazione delle modalità affinché i documenti radiologici e di medicina nucleare e i resoconti esistenti siano resi tempestivamente disponibili per successive esigenze mediche, ai sensi dell'art. 111, comma 10, del decreto legislativo 17 marzo 1995, n. 230"
- **D.lgs 26 maggio 2000**, n. 187 - Attuazione della direttiva 97/43/Euratom in materia di protezione sanitaria delle persone contro i pericoli delle radiazioni ionizzanti connesse ad esposizioni mediche
- **Prontuario di selezione per gli archivi delle aziende sanitarie locali e delle aziende ospedaliere, 2005**
Atto di indirizzo che reca indicazioni sui tempi di conservazione dei documenti generati e/o custoditi Aziende Sanitarie pubbliche ed accreditate, redatto dal Ministero per i Beni e la Attività Culturali
- **Consiglio dei Ministri – Conferenza Stato Regioni 02 Marzo 2012** - Linee Guida per la dematerializzazione della documentazione clinica in diagnostica per immagini. Normativa e prassi.
- **Linee guida sulla formazione, gestione e conservazione del documento informatico settembre 2020.**

3.2. *Standard di riferimento*

Dove non sono indicate una versione e/o una data specifica, si intende fare riferimento alla più recente versione disponibile del documento citato:

- **ISO 14721:2025 OAIS** (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- **ISO/IEC 27001:2022**, 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 11386:2020 Standard SInCRO** – Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- **ISO 15836:2009** Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.
- **Dicom 3.0** (Digital Imaging and COmmunications in Medicine, immagini e comunicazione digitali in medicina)
- **Health Level 7 (HL7)** versione 2.3.1 e 2.5
- **Integrating the Healthcare Enterprise (IHE)**
- **CEN/TS 181/70:2025** - Functional requirements for the electronic archiving service

4. RUOLI E RESPONSABILITÀ

Nell'ambito di un processo di Conservazione dei documenti informatici si identificano 3 soggetti fondamentali, ben distinti: il Produttore, l'Utente, e il Responsabile della Conservazione.

Soggetto	Organizzazione di appartenenza
Produttore	Cliente
Conservatore	Argentea S.r.l.
Utente	Cliente/Terzi autorizzati

Il **Produttore** è il soggetto che affida al Conservatore i propri documenti informatici, intesi come documenti singoli e/o documenti aggregati, allo scopo di conservarli a norma per la durata e secondo le modalità indicate nel Contratto di affidamento del Servizio di Conservazione. Il Produttore versa gli oggetti digitali e le relative informazioni sulla sua rappresentazione, ovvero i metadati, da conservare a norma, secondo quanto indicato nelle specifiche tecniche allegate al Contratto di affidamento (si parla in questo caso di "**Pacchetti di Versamento**"). Il Produttore, in quanto titolare del documento informatico, è responsabile del contenuto del pacchetto di versamento; per tale ragione incarica un Responsabile interno del processo di Conservazione, normalmente il Responsabile della gestione documentale.

Il **Conservatore** è il soggetto che svolge le attività di Conservazione dei documenti informatici tramite il Servizio di Conservazione (si parla in questo caso di "**Pacchetti di Archiviazione**") ed in ottemperanza a quanto stabilito nel Contratto di affidamento. Il Conservatore, nella persona del proprio Responsabile del Servizio di Conservazione incaricato, che opera d'intesa con le altre figure della struttura organizzativa, garantisce le attività di Conservazione in aderenza con quanto specificato nel modello organizzativo.

Argentea S.r.l., quale Conservatore dei documenti informatici del Cliente, agisce nei limiti della delega ad essa conferita e nell'osservanza degli obblighi ivi previsti nonché nel rispetto della normativa regolante la conservazione digitale di documenti informatici e delle presenti prescrizioni; in particolare, essa agirà attraverso persone fisiche dalla stessa formalmente incaricate. L'attività di Argentea S.r.l. riguarda la sola conservazione digitale dei documenti informatici del Cliente, senza alcuna responsabilità e/o possibilità di intervento sul contenuto degli stessi.

A carico del Conservatore non è posto alcun obbligo/dovere di elaborare i documenti informatici versati in conservazione al fine di estrarre i relativi metadati che, pertanto, dovranno essere forniti e associati ai rispettivi documenti a cura e carico del Cliente; il Conservatore opera altresì nell'osservanza di quanto stabilito nel presente *Manuale*, al quale, se necessario, è sin da ora autorizzato ad apportare le modifiche, le integrazioni e gli aggiornamenti ritenuti necessari e/o conseguenti al mutato contesto tecnico-giuridico della normativa in materia.

L'**utente** è il soggetto che richiede al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge. Tali informazioni vengono fornite dal sistema di conservazione secondo le modalità previste nel presente *Manuale*.

Come già anticipato, il processo di conservazione impone al Cliente l'istituzione di una struttura ed una organizzazione interna, coerente con le proprie politiche di efficienza gestionale, che garantisca la piena osservanza alle disposizioni normative di riferimento e di quanto previsto dal presente *Manuale*, dal contratto e dai rispettivi allegati.

A tale scopo, in base alle specifiche necessità, il Cliente deve, sia dal punto di vista dell'impostazione operativa delle attività propedeutiche alla conservazione digitale dei propri documenti informatici sia dal punto di vista della scelta delle risorse coinvolte nel processo, organizzare il lavoro all'interno della propria organizzazione affinché esso venga svolto secondo i principi stabiliti dalla normativa in materia nonché dalle specifiche regole tecniche.

Il Sistema di Conservazione permette ai soggetti autorizzati l'accesso ai documenti informatici conservati, estraendo, su richiesta esplicita da parte dell'Utente, i documenti ricercati (si parla in questo caso di "**Pacchetti di Distribuzione**").

4.1. *Profili professionali*

Nell'ambito della fornitura del Servizio di Conservazione dei documenti informatici risulta essenziale definire ed implementare una struttura organizzativa in grado di garantire, come minimo, i livelli e le esperienze richieste dalla normativa in essere in termini di qualità, professionalità, sicurezza e aderenza alla normativa stessa.

Lo svolgimento delle attività di Conservazione prevede la presenza di più ruoli Responsabili, ognuno dei quali ha appunto responsabilità specifiche:

1. *Responsabile del servizio di conservazione (RSC);*
2. *Responsabile della funzione archivistica di conservazione (RFA);*
3. *Responsabile esterno del trattamento dei dati personali (RTD);*
4. *Responsabile della sicurezza dei sistemi per la conservazione (RSS);*
5. *Responsabile dei sistemi informativi per la conservazione (RSI);*
6. *Responsabile dello sviluppo e della manutenzione del sistema di conservazione (RSM).*

Di seguito le **responsabilità associate a ciascuna delle figure sopra elencate:**

1. **Responsabile del servizio di conservazione (RSC)**

- 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;
- ogni altra attività affidata, con Atto di affidamento, dal Responsabile della Conservazione del Cliente

2. **Responsabile della funzione archivistica di conservazione (RFA)**

- definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte del Cliente, 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 col Cliente 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.

3. **Responsabile del trattamento dei dati personali (RTD)**

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

4. **Responsabile della sicurezza dei sistemi per la conservazione (RSS)**

- 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.

5. Responsabile dei sistemi informativi per la conservazione (RSI)

- gestione dell'esercizio delle componenti hardware e software del sistema di conservazione; monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con il fornitore e 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.

6. Responsabile dello sviluppo e della manutenzione del sistema di conservazione (RSM)

- 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 col Cliente 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.

Nello schema seguente sono riportati i dati dei soggetti che rivestono o hanno rivestito le responsabilità sopra indicate con riferimento al sistema di conservazione. Ciascun responsabile possiede gli specifici requisiti di onorabilità e di esperienza minima nel ruolo e può eventualmente avvalersi, per lo svolgimento delle attività al medesimo attribuite, di addetti ed operatori formalmente incaricati.

Ruolo	Cognome	Nome	Data nomina	Data cessazione
Responsabile del Servizio di Conservazione (RSC)	Anghinolfi	Andrea	Dicembre 2019	
	Benvenuti	Carlo	Maggio 2019	Dicembre 2019
Responsabile della Funzione Archivistica di Conservazione (RFA)	Placanica	Antonio	Gennaio 2025	
	Bertè	Maria	Gennaio 2021	Gennaio 2025
	Piazza	Nadia	Aprile 2019	Gennaio 2021
Responsabile del Trattamento dei Dati Personali (RTP)	Torresani	Marco	Aprile 2019	
Responsabile della Sicurezza dei Sistemi per la Conservazione (RSS)	Ruocco	Paolo	Aprile 2022	
	Conci	Roberto	Aprile 2019	Aprile 2022



Responsabile dei Sistemi Informativi per la Conservazione (RSI)	Anghinolfi	Andrea	Gennaio 2021	
	Di Domenico	Marco	Aprile 2019	Gennaio 2021
Responsabile dello Sviluppo e della Manutenzione del Sistema di Conservazione (RSM)	Benedetti	Giulia	Giugno 2021	
	Dalfovo	Alessandro	Gennaio 2021	Giugno 2021
	Di Domenico	Marco	Aprile 2019	Gennaio 2021

5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

In questo capitolo sono indicate le strutture organizzative coinvolte nel servizio di conservazione, comprese le responsabilità, che intervengono nelle principali funzioni riguardanti il servizio di conservazione

5.1. Organigramma

La figura riporta l'organigramma di Argentea e la sua struttura organizzativa, compresa la parte coinvolta nel servizio di conservazione

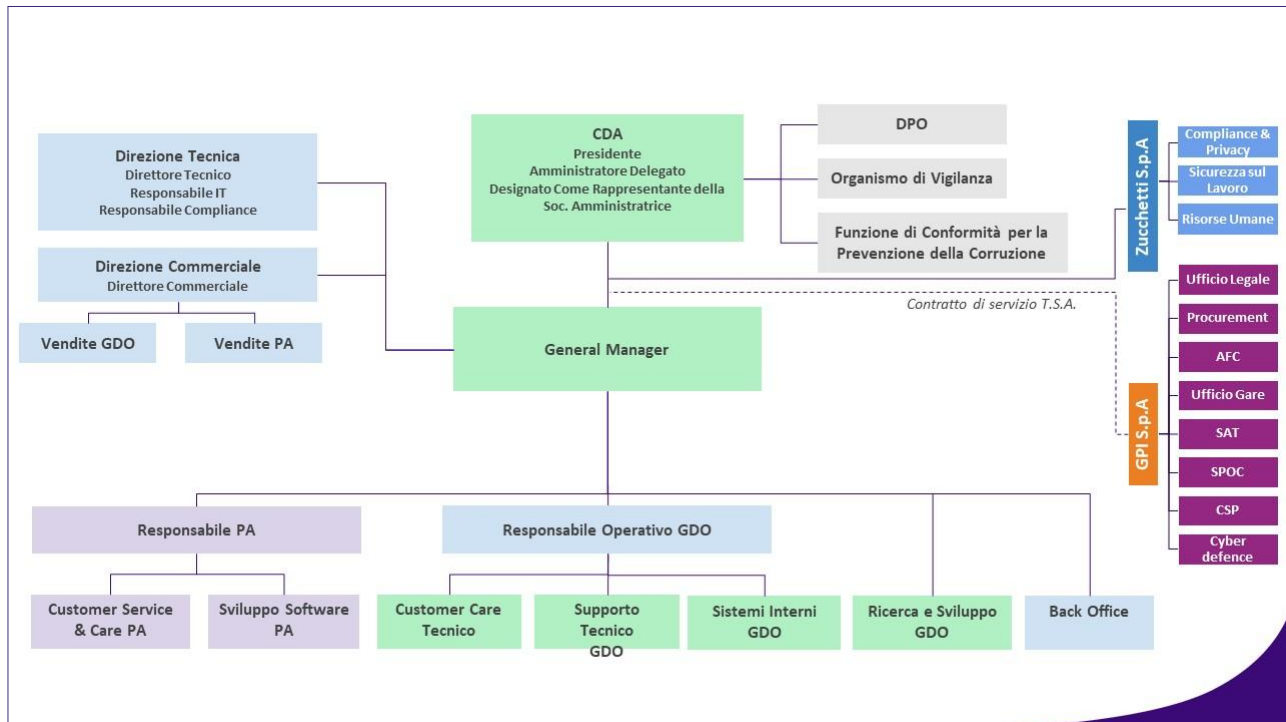


Figura 1: Organigramma della Società

5.2. Strutture organizzative e Ruoli

Le attività relative al servizio di conservazione coinvolgono vari settori dell'organizzazione di Argentea S.r.l. che interagiscono tra loro al fine di garantire la gestione di tutte le esigenze del produttore dei documenti. Specificamente, le attività impattano sulle seguenti strutture organizzative/ruoli:

- **Amministratore Delegato:** per la formalizzazione delle procedure interne per la gestione dei rischi dell'organizzazione. A valle della fase di analisi dei rischi approva il piano di mitigazione e sicurezza presentato dal Responsabile della Sicurezza. L'Amministratore Delegato definisce i parametri contrattuali relativi al servizio di conservazione;
- **Area Direzione commerciale:** per la fase di definizione e predisposizione della contrattualistica, nonché per il perseguimento amministrativo/contabile del servizio stesso;
- **Area Supporto Tecnico PA:** per il mantenimento e monitoraggio del sistema, servizio help desk e, coadiuvata dal *Responsabile della Funzione Archivistica di Conservazione*, per le fasi di setup dell'integrazione tra i sistemi del produttore ed il sistema di conservazione;



- *Area Sviluppo Software PA*: per lo sviluppo e la manutenzione della soluzione tecnologica del front-end e back-end del sistema di conservazione sviluppato da Argentea;
- *Responsabile dei Sistemi Informativi per la Conservazione e SGSI*: per la definizione e attuazione delle politiche complessive del sistema di conservazione, nonché per la gestione e la sicurezza del sistema di conservazione.
- *Responsabile della Funzione Archivistica di Conservazione*, per la 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.

5.3. Responsabilità e funzioni nel processo di conservazione

Di seguito sono indicati i compiti, le responsabilità e le funzioni di firma in relazione alle diverse fasi del processo di conservazione digitale.

- RSC = Responsabile del Servizio di Conservazione
- RFA = Responsabile della Funzione Archivistica
- RTD = Responsabile del Trattamento dei Dati Personali
- RSS = Responsabile della Sicurezza dei Sistemi per la Conservazione
- RSI = Responsabile dei Sistemi Informativi per la Conservazione
- SP = Soggetto Produttore
- RE = Responsabile Esterno, fornitore esterno per i servizi di Data Center

	RSC	RFA	RTD	RSS	RSI	SP	RE
Condizioni Generali di Contratto	R					A	
Atto di affidamento	A					R	
Specifiche tecniche di integrazione	V			A	R	V	V
Impegno alla riservatezza	V		R	A			
Acquisizione del documento da conservare	R						
Metadattazione e archiviazione	A	R					
Validazione del pacchetto di versamento	R						
Generazione del pacchetto di archiviazione	R						
Scarto dei pacchetti di archiviazione	R	V					
Chiusura del servizio di conservazione al termine di un contratto	R	V					
Monitoraggio del sistema di conservazione	A	V			R		
Change Management	R	V		V	A		
Verifica periodica di conformità a normativa e standard di riferimento	A	R\E	V	V	A		

R-responsabile; E-esegue; V- verifica; A-approva

Il processo di conservazione è normalmente effettuato da procedure totalmente automatizzate, che non necessitano dell'intervento di altri soggetti o delegati. Argentea S.r.l. si riserva la possibilità eventualmente di avvalersi di partner tecnologici per l'esecuzione di operazioni, singole attività, servizi relativi a funzioni o fasi del processo di conservazione, a terzi soggetti, fornitori esterni, che per conoscenza, esperienza, capacità e affidabilità forniscano idonee garanzie.

6. OGGETTI SOTTOPOSTI A CONSERVAZIONE

6.1. *Descrizione delle tipologie dei documenti sottoposti a conservazione*

Il servizio di conservazione a norma dei documenti informatici riguarda la conservazione di documenti digitali, il sistema di conservazione può accettare sia documenti firmati digitalmente che non.

Prima dell'attivazione del servizio il Cliente esplicita la tipologia di documenti che intende sottoporre a conservazione mediante il servizio offerto da Argentea S.r.l., evidenziandone le caratteristiche nell'apposito documento "Accordo di versamento", tra le caratteristiche da esplicitare va indicato se il Cliente intende o meno inviare documenti privi di firma digitale.

Argentea S.r.l. configura sul servizio un profilo di conservazione per ogni tipologia/classe di documenti su indicazione del Cliente, classificato come omogeneo in base ai dati da utilizzare per l'indicizzazione ed i termini di conservazione (informazioni indicate nell'Accordo di versamento).

Ogni variazione di formato di documento o dei dati utilizzati per l'indicizzazione deve essere preventivamente concordato con Argentea S.r.l. e configurato sul servizio.

Il sistema di conservazione digitale dei documenti informatici è impostato per accettare le seguenti tipologie di documenti:

- Documenti amministrativi;
- Documenti contabili;
- Documenti clinici;
- Immagini diagnostiche;
- Altri documenti in genere.

Le diverse tipologie di documenti sono prodotte/formate/emesse a cura e sotto l'esclusiva responsabilità del Cliente mediante una delle seguenti principali modalità:

- a) redazione tramite l'utilizzo di appositi strumenti software;
- b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;
- c) registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari;
- d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

6.2. Copie informatiche di documenti analogici originali unici

Come noto, l'art. 22 del CAD stabilisce che:

- a) (comma 2) Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico hanno la stessa efficacia probatoria degli originali da cui sono estratte, se la loro conformità è attestata da un notaio o da altro pubblico ufficiale a ciò autorizzato, secondo le Linee guida.
- b) (comma 3) Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico nel rispetto delle Linee guida hanno la stessa efficacia probatoria degli originali da cui sono tratte se la loro conformità all'originale non è espressamente disconosciuta.

Pertanto, alla luce di quanto sopra, il Cliente qualora intendesse depositare in conservazione copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico è tenuto, a propria cura e spese, a predisporre quanto necessario per ottemperare a quanto previsto dalle richiamate disposizioni.

In particolare, sarà cura e carico del Cliente:

1. produrre la copia per immagine su supporto informatico del documento analogico mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto;

successivamente, in alternativa:

2. dovrà sottoscrivere con firma digitale la copia per immagine del documento analogico (ai fini di quanto stabilito dall'articolo 22, co. 4-bis, del CAD);
3. laddove richiesto dalla natura dell'attività, (art. 22, comma 4-bis, del CAD), dovrà inserire nel documento informatico contenente la copia per immagine, l'attestazione di conformità all'originale analogico. Il documento informatico così formato dovrà poi essere sottoscritto con firma digitale del notaio o con firma digitale o firma elettronica qualificata di pubblico ufficiale a ciò autorizzato.

Si tenga presente che l'attestazione di conformità delle copie per immagine su supporto informatico di uno o più documenti analogici, effettuata per raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia, può essere prodotta, sempre a cura e carico del Cliente, come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. Tale documento informatico separato dovrà essere sottoscritto con firma digitale del notaio o con firma digitale o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato.

In sostanza, in questi casi il Cliente dovrà alternativamente depositare in conservazione:

- la copia per immagine su supporto informatico dell'originale analogico contenente l'attestazione di conformità all'originale analogico debitamente sottoscritto come sopra riportato;

oppure

- le copie per immagine su supporto informatico unitamente all'attestazione di conformità prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni singola copia per immagine, debitamente sottoscritto come sopra riportato.

6.3. Formati gestiti

Come noto, la leggibilità di un documento informatico dipende dalla possibilità e dalla capacità di interpretare ed elaborare correttamente i dati binari che costituiscono il documento, secondo le regole stabilite dal formato con cui esso è stato rappresentato. Il formato di un documento informatico è la convenzione usata per rappresentare il contenuto informativo mediante una sequenza di byte.

Il sistema di conservazione di Argentea S.r.l. garantisce la conservazione dei documenti prodotti nei formati previsti dalle Linee guida sulla formazione, gestione e conservazione del documento informatico (Allegato 2 -  Formati di file e

riversamento).

I formati ammessi alla conservazione, devono essere specificati dal Cliente prima del versamento in conservazione e per tale ragione vengono esplicitati all'interno dell'Accordo di versamento stipulato con Argentea S.r.l.

6.3.1. Caratteristiche generali dei formati

I formati scelti devono essere, puntualmente richiamati nel Contratto. Argentea S.r.l., comunque raccomanda un insieme di formati che sono stati dalla stessa valutati in funzione di alcune caratteristiche quali:

	Caratteristica	Descrizione della caratteristica
1	APERTURA	Un formato si dice "aperto" quando è conforme a specifiche pubbliche, cioè disponibili a chiunque abbia interesse ad utilizzare quel formato. La disponibilità delle specifiche del formato rende sempre possibile la decodifica dei documenti rappresentati in conformità con dette specifiche, anche in assenza di prodotti che effettuino tale operazione automaticamente. Questa condizione si verifica sia quando il formato è documentato e pubblicato da un produttore o da un consorzio al fine di promuoverne l'adozione, sia quando il documento è conforme a formati definiti da organismi di standardizzazione riconosciuti. In quest'ultimo caso tuttavia si confida che quest'ultimi garantiscono l'adequatezza e la completezza delle specifiche stesse. In relazione a questo aspetto, Argentea S.r.l. ha privilegiato formati già approvati dagli Organismi di standardizzazione internazionali quali ISO e OASIS.
2	SICUREZZA	La sicurezza di un formato dipende da due elementi: - grado di modificabilità del contenuto del file; - capacità di essere immune dall'inserimento di codice maligno.
3	PORTABILITÀ	Per portabilità si intende la facilità con cui i formati possano essere usati su piattaforme diverse, sia dal punto di vista dell'hardware che del software, inteso come sistema operativo. Di fatto si ottiene mediante l'impiego fedele di standard documentati e accessibili e dalla loro diffusione sul mercato.
4	FUNZIONALITÀ	Per funzionalità si intende la possibilità da parte di un formato di essere gestito da prodotti informatici, che prevedono una varietà di funzioni messe a disposizione del Cliente per la formazione e gestione del documento informatico.
5	SUPPORTO ALLO SVILUPPO	Il supporto allo sviluppo è la modalità con cui si mettono a disposizione le risorse necessarie alla manutenzione e sviluppo del formato e i prodotti informatici che lo gestiscono (organismi preposti alla definizione di specifiche tecniche e standard, società, comunità di sviluppatori, ecc.).
6	DIFFUSIONE	La diffusione è l'estensione dell'impiego di uno specifico formato per la formazione e la gestione dei documenti informatici. Questo elemento influisce sulla probabilità che esso venga supportato nel tempo, attraverso la disponibilità di più prodotti informatici idonei alla sua gestione e visualizzazione.

6.3.2. Formati consigliati per la conservazione

Oltre al soddisfacimento delle caratteristiche suddette, nella scelta dei formati idonei alla conservazione, Argentea S.r.l.



è stata estremamente attenta affinché i formati stessi fossero in grado di far assumere al documento le fondamentali caratteristiche di immutabilità e staticità.

Pertanto, alla luce delle suddette considerazioni, **i formati consigliati da Argentea S.R.L.** per la conservazione delle diverse tipologie di documenti informatici sono i seguenti:

Formato	Descrizione
XML	Extensible Markup Language (XML) è un formato di testo flessibile derivato da SGML (ISO 8879). Su XML si basano numerosi linguaggi standard utilizzati nei più diversi ambiti applicativi. Ad esempio: SVG usato nella descrizione di immagini vettoriali, XBRL usato nella comunicazione di dati finanziari, ebXML usato nel commercio elettronico, SOAP utilizzato nello scambio dei messaggi tra Web Service
	Caratteristiche e dati informativi
	Informazioni gestibili
	Contenuto di evidenze informatiche, dei pacchetti di versamento, archiviazione e distribuzione, ecc.
	Sviluppato da
	W3C - http://www.w3.org/
	Estensione
	.xml
	Tipo MIME
	Application/xml Text/xml
	Formato aperto
	SI
	Specifiche tecniche
	Pubblicate da W3C – http://www.w3.org/XML/
	Altre caratteristiche
	E' un formato di testo flessibile derivato da SGML (ISO 8879).
	Software necessario alla visualizzazione
	Qualsiasi editor di testo.

Formato	Descrizione
PDF/A	Il PDF (Portable Document Format) è un formato creato da Adobe nel 1993 che attualmente si basa sullo standard ISO 32000. Questo formato è stato concepito per rappresentare documenti complessi in modo indipendente dalle caratteristiche dell'ambiente di elaborazione del documento. Il formato è stato ampliato in una serie di sotto-formati tra cui il PDF/A.
	Caratteristiche e dati informativi
	Informazioni gestibili
	Testo formattato, immagini, grafica vettoriale 2D e 3D, filmati.
	Sviluppato da
	Adobe Systems - http://www.adobe.com/
	Estensione
	.pdf

	Tipo MIME	Application/pdf
	Formato aperto	SI
	Specifiche tecniche	Pubbliche
	Standard	ISO 19005-1:2005 (ver. PDF 1.4)
	Altre caratteristiche	Assenza di collegamenti esterni
		Assenza di codici eseguibili
		Assenza di contenuti crittografati
		Il file risulta indipendente da codici e collegamenti esterni che ne possono alterare l'integrità e l'uniformità nel lungo periodo
		Le più diffuse suite d'ufficio permettono di salvare direttamente i file nel formato PDF/A
		Sono disponibili prodotti per la verifica della conformità di un documento PDF al formato PDF/A.
	Software necessario alla visualizzazione	Adobe Reader

Formato	Descrizione	
EML	Electronic Mail Message (EML) è un formato di testo che definisce la sintassi di messaggi di posta elettronica scambiati tra utenti	
	Caratteristiche e dati informativi	
	Informazioni gestibili	Messaggi di posta elettronica e PEC
	Sviluppato da	Internet Engineering Task Force (IETF) - http://www.ietf.org/
	Estensione	.eml
	Tipo MIME	Message/rfc2822
	Formato aperto	SI
	Specifiche tecniche	Pubblicate da IETF - http://www.ietf.org/rfc/rfc2822.txt
	Altre caratteristiche	E' un formato di testo flessibile derivato da SGML (ISO 8879).
	Software necessario alla visualizzazione	La maggior parte dei client di posta elettronica supportano la visualizzazione di file eml

Per quanto concerne il formato degli allegati al messaggio di posta elettronica, valgono le indicazioni di cui sopra.

6.3.3. Identificazione

L'associazione del documento informatico al suo formato può avvenire, attraverso varie modalità, tra cui le più impiegate sono:

1. l'estensione: una serie di lettere, unita al nome del file attraverso un punto, ad esempio [nome del file].doc identifica un formato sviluppato dalla Microsoft;
2. il magic number: i primi byte presenti nella sequenza binaria del file, ad esempio 0xffd8 identifica i file immagine di tipo .jpeg;
3. verifica della corrispondenza tra il tipo MIME ricavato dall'estensione del file ed il tipo MIME ricavato dal magic number;
4. l'utilizzo di tool automatici specifici come Apache TIKA

Per identificare il formato dei files posti in conservazione occorre procedere all'analisi di ogni singolo documento informatico contenuto all'interno dei pacchetti di versamento. Argentea S.r.l. procede come segue, garantendo così la leggibilità utilizzando gli adeguati visualizzatori:

1	Fase di IDENTIFICAZIONE	Ogni documento che viene inviato al sistema di conservazione deve essere stato precedentemente ed espressamente indicato dal sistema versante. In questo modo tutti i documenti non noti vengono automaticamente non riconosciuti e quindi rifiutati.
2	Fase di RICEZIONE	Il sistema Argentea S.r.l., una volta noti i documenti che il Cliente vuole mettere in conservazione si mette in attesa, secondo i canali concordati, della loro ricezione.
3	Fase di VALIDAZIONE	Una volta che i documenti vengono recepiti dal sistema di conservazione la prima elaborazione effettuata sugli stessi è quella del rilevamento della tipologia corretta del documento. Solo se questo esame restituisce esito positivo vengono realizzate ulteriori validazioni atte a garantire la correttezza formale del documento, secondo gli standard qui esposti e gli accordi convenuti col Cliente.

6.3.4. Migrazione dei formati

Particolarmente delicata è l'operazione di migrazione dei formati, operazione, questa, che potrà essere necessaria nei casi di obsolescenza dei formati.

Il problema che si pone è quello di capire se il contenuto del file di partenza e di arrivo è rimasto inalterato. In altre parole è necessario capire se le *significant properties* si sono conservate.

E' necessario quindi impostare dei test di controllo che, inevitabilmente dovranno essere automatici. Sulla base dello specifico formato divenuto obsoleto e sulla base del nuovo formato di destinazione scelto per l'operazione di migrazione verranno designati quanti e quali controlli sul buon esito della conversione inserire.

Le specifiche dei formati di partenza e di destinazione saranno decisive e determinanti per l'individuazione dei controlli da attuare.

6.4. Metadati da associare alle diverse tipologie di documenti

Con il termine "metadati" si indicano tutte le informazioni significative associate al documento informatico, escluse quelle che costituiscono il contenuto del documento stesso. I metadati riguardano principalmente, ma non esclusivamente, i modi, i tempi ed i soggetti coinvolti nel processo della formazione del documento informatico, della sua gestione e della sua conservazione.



Metadati sono anche le informazioni riguardanti gli autori, gli eventuali sottoscrittori e le modalità di sottoscrizione e la classificazione del documento. I metadati che seguono devono essere associati al documento dal Cliente prima del versamento in conservazione.

I metadati forniti dal Cliente restano di proprietà del Cliente medesimo.

I metadati, seppur chiaramente associati al documento informatico, possono essere gestiti indipendentemente dallo stesso. In relazione ai diversi tipi di documenti informatici posti in conservazione, sono previsti i metadati obbligatori previsti dalle Linee guida sulla formazione, gestione e conservazione del documento informatico (Allegato 5 – Metadati).

Oltre ai metadati obbligatori, il Cliente potrà decidere di associare al documento informatico eventuali ulteriori metadati che dovranno essere puntualmente individuati nell'Accordo di versamento e verranno opportunamente gestiti da Argentea S.r.l. come indicato.

6.4.1. Metadati obbligatori AGID

Nelle Linee Guida AGID sulla formazione, gestione e conservazione dei documenti informatici sono definiti, all'allegato 5, i metadati da associare alle varie tipologie documentali.

Metadato "Modalità di formazione"

Tra i metadati obbligatori è presente il metadato "Modalità di formazione" (element xsd: ModalitaDiFormazione), indica la modalità di generazione del documento informatico e può essere così valorizzato:

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

Agid ammette sia la valorizzazione dell'intera stringa, sia la valorizzazione di A, B, C o D. Quest'ultima modalità può essere utilizzata purché il Produttore e il Conservatore annotino il suo utilizzo sul Manuale di Conservazione.

Tenendo conto che – come descrivono le Linee guida - i metadati sono associati al documento prima della fase di Conservazione, Argentea S.r.l. può gestire sul proprio Sistema di Conservazione entrambe le valorizzazioni.

6.5. Pacchetto di versamento

In questo paragrafo sono fornite le tipologie di Pacchetto di Versamento (PdV) gestite e per ciascuna di esse descritta la struttura dati.

Il nostro standard prevede l'indice di un Pacchetto di Versamento che si caratterizza per le seguenti parti:

- area di identificazione del PdV;
- area di identificazione dei documenti costituenti il pacchetto e composta dai seguenti elementi:
 - metadati obbligatori;
 - eventuali altri metadati definiti sull'Accordo di versamento.

Nella prima parte il dato importante e obbligatorio è l'idPacchettoVersamento ovvero l'identificativo del PdV. Esso deve

essere unico all'interno dello spazio gestito dal produttore.

La seconda parte prevede una lista di elementi, uno per ogni documento da versare. Ogni singolo file deve essere per prima cosa identificato. A questo scopo sono necessari i seguenti dati:

- nome file;
- algoritmo di hashing per la generazione dell'impronta;
- impronta del documento.

Per rimanere poi aderenti alla norma vigente deve essere presente anche un id unico dei singoli documenti del pacchetto.

6.5.1. Specifiche Pacchetto di Versamento

Le specifiche del Pacchetto di Versamento secondo lo standard definito da Argentea S.r.l., sono disponibili all'interno dell'Accordo di versamento inviato al Cliente in fase di attivazione del servizio.

[Torna al sommario](#)

6.6. *Pacchetto di archiviazione*

In questo paragrafo viene presentata la struttura del Pacchetto di Archiviazione (PdA) nonché il trattamento dei pacchetti di archiviazione.

6.6.1. Specifiche Pacchetto di Archiviazione

Il Pacchetto di Archiviazione è composto da varie parti:

- insieme degli elementi che compongono il pacchetto;
- IPdA ovvero l'Indice del Pacchetto di Archiviazione che elenca tutti gli elementi del pacchetto.

Il formato dell'IPdA è aderente allo standard UNISInCRO ed è marcato temporalmente e firmato elettronicamente con certificato del Responsabile del servizio di conservazione.

6.7. *Pacchetto di distribuzione*

Il Pacchetto di Distribuzione (PdD) contiene l'insieme degli elementi (documenti e/o PdA) precedentemente ricercati e selezionati dall'utente.

Il Pacchetto di Distribuzione risultante dalla richiesta di esibizione contiene:

- i documenti da esibire;
- gli indici dei PdA, marcati temporalmente e firmati elettronicamente così come al momento della conservazione, del flusso di conservazione relativo ai documenti scelti;
- I file dei metadati dei soli documenti da esibire.

7. IL PROCESSO DI CONSERVAZIONE

In questo capitolo sono riportate tutte le fasi inerenti il processo di conservazione dei documenti informatici.

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

Come già anticipato in altre parti del presente *Manuale*, unico responsabile del contenuto del pacchetto di versamento è il Cliente (Produttore), che deve formarlo e trasmetterlo al sistema di conservazione secondo le modalità operative di versamento definite nel presente *Manuale*, nel *Contratto* e nei rispettivi allegati.

L'operazione di versamento consiste nella trasmissione di un file .zip contenente l'indice del Pacchetto di Versamento e i documenti da conservare.

Questo può essere trasmesso al sistema di conservazione attraverso canali diversi. Alternativamente essi possono essere:

- interfaccia web;
- invocazione di metodi tramite web service REST;
- trasferimento via protocollo WebDav;

Ogni canale messo a disposizione è provvisto di opportuni accorgimenti per la trasmissione dei dati in modalità sicura e cifrata:

- interfaccia web che viaggia HTTPS con protocollo TLS 1.2;
- web service REST contattabile tramite HTTPS con protocollo TLS 1.2;
- WebDav HTTPS con protocollo TLS 1.2;

Il sistema di conservazione una volta ricevuto un PdV effettua le seguenti verifiche:

- identificazione certa del Soggetto produttore verificando l'utente che effettua il versamento con le informazioni riportate nell'indice;
 - validazione del file indice;
 - congruenza tra i dati dichiarati nell'indice e la numerosità dei documenti inviati;
 - verifica hash tra quanto dichiarato nell'indice e quello calcolato dal sistema;
 - verifica antivirus e malware;
 - verifica di eventuali firme digitale e marcature temporali;
 - verifica che i formati degli oggetti da conservare siano conformi con quanto dichiarato nel modulo "Accordo di Versamento";
 - verifica che i metadati siano conformi con quanto dichiarato nel modulo "Accordo di Versamento".

L'esito positivo delle verifiche effettuate sui Pacchetti di Versamento (PdV) viene ufficialmente sancita dalla produzione del cosiddetto Rapporto di Versamento (RdV) che viene reso disponibile al cliente.

Poiché la produzione del Rapporto di versamento (RdV) rappresenta formalmente la presa in carico del PdV da parte del sistema di conservazione, il RdV viene marcato temporalmente e firmato digitalmente direttamente dal Responsabile del servizio di conservazione.

7.1.1. Ricezione dell'indice del pacchetto di versamento

Come detto precedentemente il PdV è costituito dall'indice del Pacchetto di Versamento e dai documenti in esso contenuti.

L'indice del Pacchetto di Versamento (IPdV) è un'evidenza informatica, ovvero un file, che descrive il versamento stesso e i documenti che ne fanno parte attraverso l'uso di metadati. Questi sono di carattere diverso a seconda che descrivano proprietà e qualità del pacchetto in genere o dei singoli documenti.

E' bene sottolineare che ogni PdV può contenere esclusivamente documenti della stessa tipologia, ovvero della stessa Classe Documentale. In questo senso l'elenco dei metadati dei singoli documenti è in qualche modo omogeneo.

Per consentire l'elaborazione automatica dei metadati il sistema di conservazione di Argentea S.r.l. richiede l'incapsulamento degli stessi in un determinato formato XML, che di fatto costituisce l'IPdV.

Xsd dell'indice

In tale file sono contenute sezioni diverse che identificano la qualità dei metadati. Essi infatti possono essere caratteristici del PdV e del soggetto versante, rappresentare direttive speciali di elaborazione per la conservazione e, infine, essere descrittivi dei singoli documenti che si vogliono conservare.

La struttura dell'indice del Pacchetto di Versamento, come indicato al paragrafo 6.6.1 è descritta nel manuale tecnico inviato al Cliente in fase di attivazione del servizio.

La funzione di ricezione degli indici dei pacchetti di versamento nel sistema di conservazione effettua, per ogni indice, i seguenti controlli:

- abilitazione alla conservazione da parte del sistema di gestione documentale versante e in particolare dell'utente che effettua il versamento. In caso di esito negativo il sistema rifiuta il tentativo di versamento;
- controllo formale dell'indice versato. In particolare viene verificato che sia un formato XML valido per una delle Classi Documentali registrate a sistema. In caso di esito negativo il sistema rifiuta il tentativo di versamento;
- verifica, tramite l'id univoco contenuto nell'indice, dell'eventuale presenza del PdV già nel sistema. In caso di esito positivo il sistema rifiuta il tentativo di versamento;
- controllo sulla completezza e correttezza formale dei metadati, in relazione alla Classe Documentale rilevata. In caso di esito negativo il sistema rifiuta il tentativo di versamento;
- controllo sulla tipologia di documenti che si vuole versare. Ogni documento deve appartenere ad almeno uno dei formati ammessi dalla tipologia di Classe Documentale. In caso di esito negativo il sistema rifiuta il tentativo di versamento;
- eventuali controlli supplementari definiti insieme al Cliente;
- verifica della congruenza dei documenti dichiarati con quelli presenti nel PdV;
- verifica degli hash dei documenti presenti nel PdV con quello dichiarato nel IPdV;
- verifica della unicità dei documenti versati.

Relativamente al singolo documento tra i metadati indicati nell'IPdV sono di particolare importanza quelli utili all'identificazione dello stesso. Essi sono principalmente due: un identificativo univoco utile all'identificazione del documento e un hash del file stesso, ovvero una stringa di caratteri che normalizza con un particolare algoritmo in maniera univoca il documento stesso.

Come detto precedentemente con l'identificativo andiamo a verificare che nel sistema di conservazione non esista già un documento appartenente alla stessa struttura con lo stesso identificativo, in tal caso il PdV verrà rifiutato.

Con l'hash, che per il sistema di conservazione Argentea S.r.l. deve essere in formato SHA256 o SHA512 entrambi con Encoding Base64, viene verificata l'integrità del documento inviato al sistema di conservazione.

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

Le funzionalità attivate nel processo di versamento/acquisizione del pacchetto di versamento prevedono dei controlli sia sull'indice del PdV che sui singoli documenti inviati. La tabella riportata in basso elenca le diverse tipologie di controlli effettuati e per ognuna di esse indica l'azione prevista dal sistema. Quest'ultima può tradursi in una operazione di scarto o notifica di un warning.

Controlli dell'indice del Pacchetto di Versamento

Un Pacchetto di Versamento può contenere unicamente documenti informatici omogenei (ossia aventi la stessa classe documentale). Pertanto, a classi documentali diverse corrispondono diversi PdV e versamenti, uno per ogni classe.

Controlli nella fase di ricezione del PdV	
Oggetto del controllo	Azione in caso di check negativo
Verifica Autorizzazioni	
Viene verificato che l'utente che effettua il versamento sia abilitato all'invio dei PdV	Il sistema scarta l'intero pacchetto
Verifica formale indice del PdV	
Viene verificato che l'oggetto ricevuto sia formalmente un indice xml in linea con lo standard convenuto	Il sistema scarta l'intero pacchetto

Viene verificato che i dati riportati nell'indice di organizzazione e struttura siano quelle per il quale l'utente è autorizzato	Il sistema scarta l'intero pacchetto
Viene verificato che l'identificativo del pacchetto di versamento non sia già presente sul sistema di conservazione	Il sistema scarta l'intero pacchetto
Verifica sui documenti e metadati	
Viene verificato che il numero di documenti/allegati dichiarati nell'indice e congruo con quelli presenti nel versamento	Il sistema scarta l'intero pacchetto
Viene verificato che l'hash del documento informatico inviato sia corrispondente all'hash dichiarato all'interno del medesimo indice del pacchetto, al fine di avere garanzia che la trasmissione del pacchetto sia avvenuta correttamente e che l'integrità del documento informatico ricevuto sia assicurata	Il sistema scarta l'intero pacchetto
Viene controllato che per ciascun documento e allegato dichiarato e descritto all'interno dell'indice del PdV che: a) tutti i metadati minimi obbligatori siano presenti e nel formato corretto; b) il formato del documento è un formato ammesso; c) l'estensione del documento sia tra quelle ammesse per il tipo documento; d) il formato dichiarato sia corrispondente all'estensione del nome file; e) l'identificativo del documento non sia già presente all'interno della struttura.	Il sistema scarta l'intero pacchetto
Vengono verificate le eventuali firme e marche temporali apposte sui documenti/allegati	Il sistema non scarta il pacchetto viene segnalato un warning

Vengono eseguite le scansioni antivirus e malware

Il sistema non scarta il pacchetto viene segnalato un warning

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

Il sistema di conservazione predispone, per uno o più pacchetto di versamento, un **Rapporto di Versamento (RdV)** che viene firmato dal Responsabile del servizio di conservazione e marcato temporalmente. Lo schema del rapporto di versamento è illustrato nel paragrafo successivo (par. 7.3.1).

7.3.1. Specifiche rapporto di versamento

Il Rapporto di Versamento è basilare nel processo di conservazione, in quanto è il documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore. Esso viene prodotto nell'arco della giornata di versamento, secondo le specifiche configurazioni impostate.

In esso sono presenti sempre i seguenti dati:

- id del Rapporto di Versamento;
- data di generazione;
- organizzazione;
- struttura.

per ogni Pacchetto di Versamento contenuto

- id dei Pacchetti di Versamento;
- hash indice del Pacchetto di Versamento;
- data di versamento;
- stato.

per ogni documento contenuto nel Pacchetto di Versamento

- identificativo del documento;
- hash del documento;
- nome del documento principale.

per ogni allegato al documento

- hash dell'allegato documento;
- nome del file allegato.

Il Rapporto di Versamento viene sempre firmato digitalmente con certificato del Responsabile del servizio di conservazione e marcato temporalmente: in questo modo viene reso non modificabile.

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

Nel caso il Pacchetto di Versamento venga scartato viene generato un Rapporto di Versamento con esito negativo e vengono dettagliati tutti gli errori presenti nel Pacchetto di Versamento.

7.5. Preparazione e gestione del pacchetto di archiviazione

Il Pacchetto di Archiviazione è quello conservato dal sistema di conservazione e possiede un insieme completo di metadati utili alla conservazione a lungo termine.

Il Pacchetto di Archiviazione viene realizzato secondo lo standard di riferimento SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2020), che rappresenta lo standard nazionale riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione.

Uno o più Pacchetti di Versamento vengono trasformati in un Pacchetto di Archiviazione (PdA) in base a regole configurate e condivise nel documento Accordo di versamento. L'apposizione della marca temporale, per stabilirne l'istante di creazione, e di firma digitale del Responsabile del Servizio di Conservazione o di un suo delegato, garantisce l'immodificabilità del PdA.

Con la sottoscrizione dei pacchetti di archiviazione Argentea S.r.l. non sottoscrive il contenuto e la semantica dei documenti conservati ma asserisce solamente che il processo di conservazione è stato eseguito correttamente, nel rispetto della normativa regolante la conservazione digitale di documenti informatici.

7.5.1. Chiusura anticipata (in corso d'anno) del Pacchetto di Archiviazione.

In caso di accessi, verifiche ed ispezioni in corso d'anno, il sistema consente, dietro specifica richiesta del Cliente, l'anticipata chiusura del pacchetto di archiviazione rispetto ai tempi programmati.

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

Nel modello OAIS e in linea con la normativa vigente, il Pacchetto di Distribuzione (PdD) è strutturato nel modello dati come il pacchetto di archiviazione. La differenza sta nella sua destinazione in quanto esso viene concepito per essere fruito ed utilizzato dall'utente finale (esibizione).

In questo caso, un PdD può anche non coincidere con il pacchetto di archiviazione originale conservato. Molto spesso però, ragioni di opportunità inducono a distribuire pacchetti informativi che sono un'estrazione del contenuto informativo di un PdA, ma può anche verificarsi il caso di PdD contenenti documenti provenienti da più PdA che vengono "spacchettati" e reimpacchettati per un più fruibile utilizzo da parte dell'utente.

Un utente autorizzato da un soggetto produttore, quindi, è in grado di interrogare il sistema per ricevere in uscita uno specifico pacchetto di distribuzione. L'utente utilizzerà le funzionalità di richiesta di esibizione di un documento o di un insieme di documenti, per ottenerne una replica esatta secondo i fini previsti dalla norma.

In risposta alla richiesta iniziale di esibizione, da parte dell'utente, il sistema di conservazione risponderà restituendo un PdD che nel caso più completo conterrà:

- i file/documenti richiesti così come sono stati archiviati dal sistema al momento della messa in conservazione;
- gli Indici dei Pacchetti di Archiviazione, marcati temporalmente e firmati come all'origine, con cui sono stati conservati i documenti richiesti. I file dei metadati dei soli file/documenti compresi nel PdD.

A fronte di una richiesta di produzione del Pacchetto di Distribuzione, il sistema effettua delle verifiche di coerenza e correttezza del pacchetto e dei documenti in esso contenuti. A tal proposito, il sistema di conservazione verifica che le impronte dei documenti restituiti nel PdD corrispondano a quelle presenti nel relativo indice del Pacchetto di Archiviazione; in modo da garantire che i documenti stessi non abbiano subito alterazioni o modifiche nei contenuti.

La richiesta di esibizione può avvenire da due tra i canali messi a disposizione: interfaccia web e web service.

In entrambi i casi il flusso di selezione dei documenti da esibire è il medesimo:

1. ricerca dei documenti attraverso opportuni filtri;
2. selezione e spostamento dei riferimenti dei documenti individuati all'interno di un'area di lavoro;
3. richiesta di esibizione a partire dai documenti nell'area di lavoro;
4. produzione del link di download da cui scaricare il Pacchetto di Distribuzione.

La ricerca dei documenti avviene tramite la selezione di filtri sui metadati. Una volta individuata la classe documentale di interesse, l'utente può effettuare le ricerche inserendo i valori su cui filtrare per uno o più metadati di riferimento.

La ricerca contemporanea su più metadati implica un filtro più forte, ovvero una restrizione del numero dei documenti risultanti.

Tutti i documenti devono appartenere ad una specifica classe documentale.

Il Pacchetto di Distribuzione risultante dalla richiesta di esibizione contiene:

- i documenti da esibire;
- gli indici dei PdA, marcati temporalmente e firmati elettronicamente così come al momento della conservazione, del flusso di conservazione relativo ai documenti scelti;
- i file dei metadati dei soli documenti da esibire.

Nel caso in cui tra i documenti figurino interi PdA, il Pacchetto di Distribuzione contiene tutti i documenti che lo compongono.

7.6.1. Funzioni svolte alla conclusione del contratto

In tutti i casi di cessazione del Contratto Argentea S.r.l. consentirà al Cliente di recuperare i propri documenti, entro e non oltre 60 (sessanta) giorni dalla data in cui detta cessazione è divenuta efficace e previo pagamento ad Argentea S.r.l. di tutti gli importi contrattualmente dovuti.

I documenti informatici dovranno essere prelevati dal Cliente – quindi non incombe su Argentea S.r.l. alcun obbligo di provvedere alla materiale restituzione dei documenti informatici conservati – secondo le modalità stabilite di seguito:

1. viene fatta formale richiesta da parte del Cliente per la restituzione dei documenti;
2. Argentea estrae dal sistema di conservazione tutti i Pacchetti di Archiviazione conservati e genera i relativi Pacchetti di Distribuzione;
3. il Cliente riceve comunicazione via mail PEC o altro canale previsto dal contratto del buon esito della procedura;
4. entro i termini stabiliti da contratto o dalla documentazione collegata, il sistema rende disponibile il Pacchetto di Distribuzione che potrà essere scaricato dal cliente.

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

Nei successivi paragrafi vengono descritte le procedure adottate per la produzione di duplicati o copie.

7.7.1. Produzione di duplicati

La produzione di duplicati informatici dei documenti conservati può avvenire a seguito di una richiesta proveniente dal settore tecnico a supporto del servizio di conservazione oppure da una richiesta effettuata direttamente all'interno del sistema di conservazione.

In entrambe le situazioni, il passo iniziale consiste nella ricerca del documento informatico di interesse sfruttando le funzionalità messe a disposizione dal sistema di conservazione. Individuato il documento informatico di interesse, un'apposita funzione consente di effettuare il download del documento stesso, producendo quindi un duplicato.

Il documento informatico richiesto viene infatti estratto dal sistema in formato binario controllando che l'estrazione sia eseguita senza errori e quindi inviata all'utente che ne ha fatto richiesta.

7.7.2. Produzione di copie

La produzione di copie si rende necessaria solamente a seguito di obsolescenza tecnologica di un formato accettato in conservazione e determina, quale diretta conseguenza, l'avvio di una procedura di riversamento sostitutivo. Argentea S.r.l. verifica periodicamente l'eventuale obsolescenza dei formati di file conservati.

In tale contesto Argentea S.r.l., previo perfezionamento di specifico accordo scritto (dove saranno concordati ruoli, modalità, tempi e corrispettivi), si renderà disponibile a collaborare col Cliente nell'effettuare le copie informatiche dei documenti informatici depositati in conservazione secondo quanto stabilito dalle regole tecniche vigenti.

7.7.3. Produzione copie o duplicati su supporti rimovibili

Argentea non rilascia copie o duplicati su supporto rimovibile. Eventuali richieste di fornitura dati sono assolute andando a depositare i pacchetti su un'area cloud accessibile tramite canale sicuro, che verrà messa a disposizione del cliente per il tempo necessario allo scarico dei dati, come previsto dal Piano di Cessazione.

7.7.4. Intervento del Pubblico Ufficiale

Argentea S.r.l. richiede la presenza di un Pubblico Ufficiale nei casi in cui sia previsto il suo intervento assicurando allo stesso l'assistenza tecnica necessaria per l'espletamento delle attività al medesimo attribuite.

Ogni risorsa, comprese quelle di natura economica, necessaria per l'espletamento delle attività attribuite al pubblico ufficiale dovranno essere garantite e sostenute dal Cliente; pertanto, qualora il Cliente non se ne sia fatto carico direttamente, Argentea S.r.l. è sin da ora autorizzata ad addebitare al Cliente tutti i costi e le spese, compresi gli onorari inerenti le attività prestate dal Pubblico Ufficiale, qualora la normativa ne richieda obbligatoriamente la presenza.

7.8. *Scarto dei pacchetti di archiviazione*

7.8.1. Trasferimento dei documenti informatici in conservazione

Nell'Accordo di versamento o nella documentazione collegata, sono indicati i tempi entro i quali le diverse tipologie di documenti vanno trasferite in conservazione.

7.8.2. Scarto dei documenti informatici conservati

Relativamente alla possibilità di scarto, ossia di eliminare legalmente i documenti informatici conservati digitalmente a norma di legge, occorre distinguere preliminarmente la tipologia dei soggetti (Clienti) produttori, pubblici o privati.

Va preliminarmente osservato, che in ambito privato, con l'eccezione degli "archivi che rivestono interesse storico particolarmente importante", che divengono archivi specificamente disciplinati, l'obbligo di conservazione dei documenti è disciplinato dall'ordinamento vigente e, in particolare, dai termini prescrittivi del Codice civile nonché, per le scritture contabili, le fatture, le lettere e i telegrammi ricevuti e le copie delle fatture, delle lettere e dei telegrammi spediti, segnatamente dall'art. 2220 del c.c., il quale stabilisce l'obbligo di conservazione di dieci anni dalla data dell'ultima registrazione.

In ambito pubblico, oltre alle prescrizioni civilistiche, si rendono applicabili una serie di altre disposizioni specifiche, una su tutte, il Codice dei beni culturali e ambientali, emanato con il D.Lgs. 10 gennaio 2004, n. 42.

Inoltre, con riferimento agli archivi pubblici o privati, che rivestono interesse storico-artistico particolarmente importante, lo scarto del Pacchetto di Archiviazione avviene previa autorizzazione del Ministero per i beni e le attività culturali rilasciata al produttore secondo quanto previsto dalla normativa vigente in materia.

Pertanto, alla luce di quanto sopra sinteticamente rappresentato, tre mesi prima della scadenza del periodo di conservazione dei documenti, Argentea S.r.l. comunica al Cliente, in modalità certa, il termine di conservazione, elencando le possibili alternative:

- potrà richiedere una proroga della conservazione;
- potrà procedere allo scarto dei Pacchetti di Archiviazione versati, e nel caso delle Pubbliche Amministrazioni previa autorizzazione della Soprintendenza Archivistica così come prevede la normativa vigente in materia;
- potrà richiedere la restituzione dei dati conservati.



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

Al fine di raggiungere un soddisfacente grado d'interoperabilità nei processi di migrazione, la struttura dell'indice del Pacchetto di Archiviazione viene realizzata da Argentea S.r.l. in conformità con quanto previsto dallo standard "Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali", (c.d. SInCRO), ossia dalla norma UNI 11386 2020.

I Pacchetti di Archiviazione generati dal sistema di conservazione vengono trattati al solo scopo di soddisfare i requisiti della conservazione digitale dei documenti e delle richieste di produzione di pacchetti di distribuzione e di esibizione.

Il soddisfacimento dei requisiti della conservazione digitale implica che i Pacchetti di Archiviazione vengano firmati digitalmente dal Responsabile del servizio di conservazione o da un suo delegato e marcati temporalmente per assicurarne la validità nel corso del tempo.

La produzione di Pacchetti di Distribuzione o l'esibizione di Pacchetti di Archiviazione comporta invece la produzione di duplicati degli stessi che sono successivamente utilizzabili in altri processi. Il Pacchetto di Archiviazione memorizzato all'interno del sistema non subisce più alcuna modifica successiva alla firma digitale e all'apposizione della marca temporale.

7.10. Cessazione del Servizio di Conservazione

Il servizio di Conservazione viene erogato con la logica della sostenibilità e dell'impegno a lungo termine, ovvero per mantenere la disponibilità e la integrità delle informazioni connessa al servizio erogato con un impiego di risorse e infrastrutture concretamente assicurabile, nei limiti della ragionevolezza e con immutato livello di efficacia ed efficienza, nel medio e nel lungo periodo. A fronte dei suddetti obiettivi, è stata comunque stabilita una procedura, relativa all'Approccio a lungo termine e termination plan, per definire le modalità secondo le quali dovrà essere gestito l'evento di cessazione.

Qualora il Direttore Generale di ARGENTEA decida di cessare le operazioni di conservazione o modifichi la Mission Aziendale, il Responsabile del Sistema di Conservazione provvederà ad attivare il Termination Plan.

Le attività che verranno eseguite sono descritte nel dettaglio all'interno del documento relativo all'Approccio a lungo termine e termination plan.

Qualora venga richiesto, tale procedura viene resa disponibile fornendola al Soggetto produttore interessato.

7.11. Tabella riepilogativa delle fasi del processo di conservazione

Il processo di conservazione si articola nelle seguenti fasi:

FASE 1	Acquisizione da parte del sistema di conservazione del Pacchetto di Versamento per la sua presa in carico
---------------	--

Descrizione sintetica	Consiste nella ricezione dell'IPdV e dei documenti in esso contenuti
------------------------------	--

FASE 2	Verifica che il pacchetto di versamento e gli oggetti contenuti siano coerenti con le modalità previste nel presente Manuale di conservazione e con i formati di conservazione	
	Descrizione sintetica	In questa fase vengono condotti i controlli sull'IPdV

FASE 3	Preparazione del Rapporto di versamento	
	Descrizione sintetica	A seconda dell'esito del controllo sul PdV viene prodotto un rapporto di versamento. Che può avere esito positivo o negativo a seconda dei controlli effettuati nelle precedenti fasi. Nel caso il PdV venga rifiutato viene predisposto un Rapporto di Versamento con le indicazioni di tutte le anomalie riscontrate.

FASE 4	Sottoscrizione del Rapporto di versamento con firma digitale apposta da Argentea S.r.l. e Marcatura Temporale	
---------------	--	--

Descrizione sintetica	Il RdV viene firmato digitalmente dal Responsabile del servizio di Conservazione o da un suo delegato e viene marcato temporalmente. Il rapporto di versamento può essere scaricato dall'applicativo di conservazione. In caso di RdV con esito positivo Argentea S.r.l. prende in carico il versamento ufficialmente.
------------------------------	--

FASE 5	Preparazione e gestione del Pacchetto di Archiviazione	
	Descrizione sintetica	Il Pacchetto di Archiviazione è un insieme di metadati in grado di fornire prova dell'integrità dell'insieme dei documenti, ad esso correlati la cui conservazione decorre da una data determinata, la cui prova di integrità è fornita tramite una firma elettronica qualificata, corroborata da una marca temporale. La struttura del Pacchetto di Archiviazione è costruita sulla base delle specifiche della struttura dati (UNI 11386:2020) contenute nell'allegato 4 alle regole tecniche e secondo le modalità riportate nel manuale della conservazione

FASE 6	Sottoscrizione del Pacchetto di Archiviazione con firma digitale apposta da Argentea S.r.l. e apposizione di una validazione temporale con marca temporale alla relativa impronta. Tale operazione viene in breve chiamata anche "Chiusura del pacchetto di archiviazione"	
	Descrizione sintetica	Il Pacchetto di Archiviazione (PdA), viene costruito seguendo specifiche regole concordate con il soggetto produttore. La chiusura viene sancita dall'apposizione di opportuna marca temporale, per stabilirne l'istante di creazione, e firma digitale del Responsabile del servizio di Conservazione o di un suo delegato, per garantirne l'immodificabilità. Con la suddetta firma apposta in calce al Pacchetto di Archiviazione e la suddetta dichiarazione il conservatore NON SOTTOSCRIVE il contenuto e la semantica dei documenti conservati ma asserisce solamente che il processo di conservazione è stato eseguito correttamente, nel rispetto delle norme giuridiche e delle indicazioni contrattuali di servizio.

FASE 7	Preparazione e sottoscrizione con firma digitale di Argentea S.r.l. del Pacchetto di Distribuzione ai fini dell'esibizione richiesta dall'utente	
	Descrizione sintetica	Il Pacchetto di Distribuzione (PdD) è definito in base alle esigenze del richiedente. È generato a partire dai pacchetti di archiviazione. Nel caso più semplice il PdD contiene dei duplicati del PdA. In alternativa esso può essere costituito da una scelta di documenti conservati selezionati attraverso una o più interrogazioni.

FASE 8	Produzione di duplicati informatici effettuati su richiesta del Cliente in conformità a quanto previsto dalle regole tecniche in materia di formazione del documento informatico	
	Descrizione sintetica	Per duplicato informatico si intende il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario. I duplicati informatici hanno il medesimo valore giuridico, ad ogni effetto di legge, del documento informatico da cui sono tratti, se prodotti in conformità alle regole tecniche in materia di formazione del documento informatico, ovvero se contiene la stessa sequenza di bit del documento informatico di origine.

FASE 9	Eventuale scarto del Pacchetto di Archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dal <i>Contratto</i> di servizio, dandone preventiva informativa al Cliente al fine di raccoglierne il consenso	
	Descrizione	Alla scadenza dei termini di conservazione, il cliente può richiedere

sintetica	la cancellazione dei documenti.
-----------	---------------------------------

7.12. Audit Log

Il sistema di conservazione registra ogni evento rilevante del processo di conservazione.

In particolare sono gestiti i seguenti eventi:

- Creazione PdA
- Conservazione PdA
- Creazione Rapporto di Versamento
- Firma Rapporto di Versamento
- Download Documento
- Ricerca di un documento
- Login
- Creazione di un Pacchetto di Distribuzione
- Richiesta di Scarto
- Scarto dei documenti

I log di audit vengono inviati ad un sistema di log management che permette la consultazione dei dati con profili di utenti in sola lettura. Oltre al log di audit sono presenti altri log di servizio relativi ad altri eventi generati dal sistema durante il processo di conservazione.

8. IL SISTEMA DI CONSERVAZIONE

8.1. *Infrastruttura informatica datacenter*

Il servizio di Conservazione erogato da Argentea S.r.l. si avvale di un fornitore esterno per il servizio di Data Center. I Data Center dal quale sono erogati i servizi si trovano sul territorio nazionale e sono conformi ai requisiti della normativa ISO/IEC 27001:2005.

Nelle strutture che sono messe a disposizione dal Fornitore per l'erogazione dei servizi viene data grande importanza alla sicurezza degli ambienti e dei dati in essi contenuti. Per questo è presente tutta una serie di sistemi che permette di garantire integrità degli ambienti e dei servizi.

8.2. *Caratteristiche generali della soluzione di conservazione*

La soluzione, come meglio descritto in seguito, presenta le seguenti caratteristiche peculiari:

- architettura di produzione implementata su infrastruttura virtuale totalmente ridondata (HA) presso il Data Center del Fornitore, certificato Tier IV;
- continuità operativa garantita dall'utilizzo di una seconda infrastruttura in ambito metropolitano allineata in sincrono;
- ambiente di disaster recovery replicato in un sito a 70 km di distanza ed in grado di garantire valori di RTO, RPO e SDO adeguati all'applicazione in oggetto ed agli SLA previsti.

Il Sistema di Conservazione è sviluppato in modo modulare consentendo una facile scalabilità semplicemente aggiungendo unità e potenza elaborativa ai moduli sottoposti al maggior carico. L'esperienza del Fornitore nell'ambito della gestione di grandi volumi di dati ha permesso di creare architetture che si possono definire elastiche: "espandibili" in caso di aumento del carico di lavoro oppure "limitabili" nel caso di una riduzione delle necessità.

L'intera soluzione è stata progettata per essere quindi in grado di gestire l'elaborazione di grandi volumi di dati, scalando sia verticalmente che orizzontalmente in ognuna delle sue singole componenti, con un elevato livello di affidabilità, distribuendo su più server fisici nodi con il medesimo ruolo ed evitando single point of failure.

L'architettura modulare del sistema è implementata al 100% su infrastruttura di virtualizzazione e garantisce in sintesi i seguenti vantaggi:

Affidabilità - Totale ridondanza ai guasti HW

- ridondanza delle componenti hardware già a partire dal singolo datacenter;
- ridondanza dei sistemi su datacenter diversi;
- funzionalità di HA implementata dall'architettura virtuale;
- interconnessioni ridondate;
- replica dati tra i sistemi;
- utilizzo di servizi esterni garantiti.



Architettura scalabile

- sistema pensato per essere scalabile a livello fisico, virtuale ed applicativo,
- componenti di livello Enterprise ad alte prestazioni per la piattaforma di virtualizzazione, le componenti Applicative e DB;
- funzionalità di replica.

8.3. Componenti Logiche

Di seguito riportiamo l'immagine rappresentativa delle componenti logiche del sistema di conservazione:

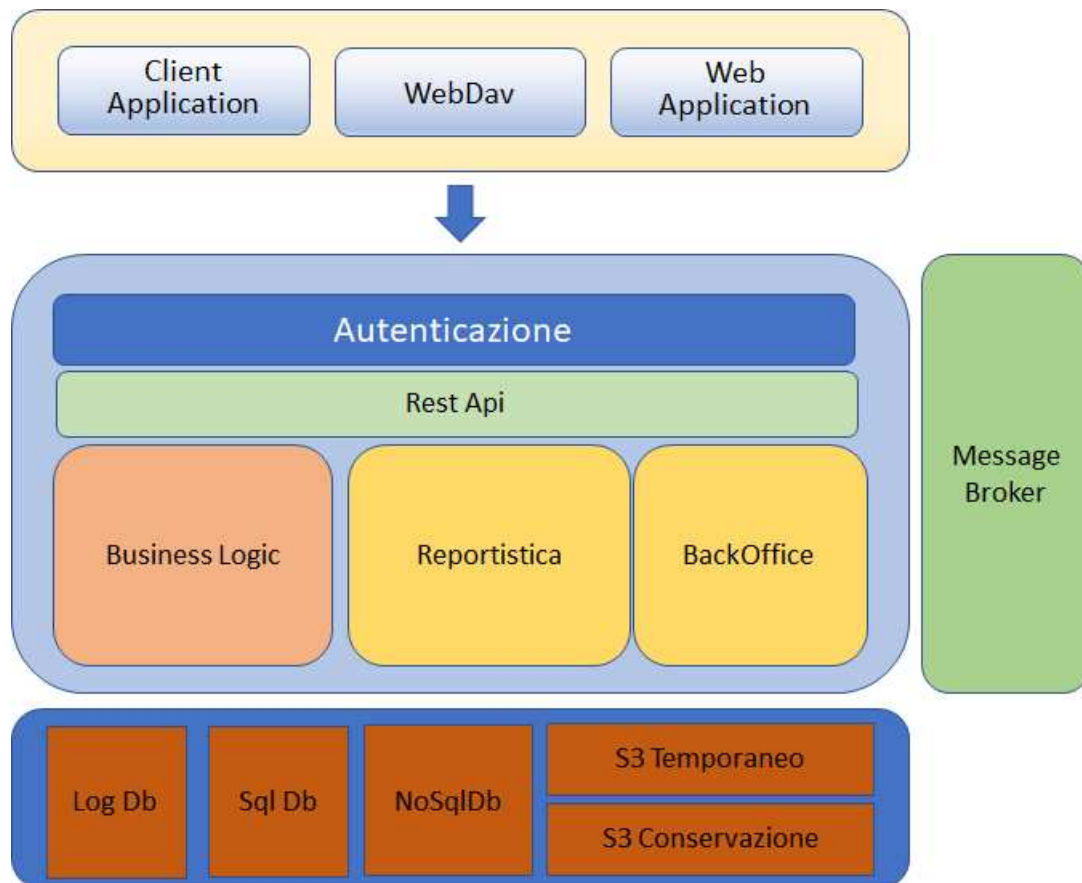


Figura 2: Rappresentazione delle componenti logiche

Come si evince dalla figura l'architettura è basata su una soluzione multi-tier a 3 livelli:

- **Presentation layer:** l'applicazione è fruibile quasi interamente tramite api rest, pertanto la parte di presentation è formata da un lato dall'applicazione web, dall'altro dalle api stesse. Essendo la parte di api gestita su servizi, risulta facilmente scalabile aumentando il numero di servizi dedicati;

- **Business logic (o application) layer:** l'implementazione delle regole che formano il dominio di business è stata suddivisa per contesto in più servizi. Questi servizi si occupano prevalentemente di rispondere alle richieste del cliente, di conservare i dati, ma anche di fornire della reportistica e delle utility per il backoffice;
- **Store (& Database) layer:** il livello di storing dei dati è diviso in quattro aree, la prima relativa alle profilazioni e configurazioni del sistema ed avviene mediante database relazionale, la parte di indicizzazione dei metadati e dei dati è stata convogliata verso un database nosql in modo da garantire prestazioni più elevate soprattutto in fase di reperimento dei dati; per immagazzinare i dati è stato pensato di utilizzare un ObjectStore con protocollo S3; l'ultima area invece è quella dei log, essendo una parte importante del servizio è stato deciso di affidarsi ad un aggregatore di log dedicato.

8.4. Componenti tecnologiche

Il sistema di conservazione è composto da varie parti e tecnologie, con l'obiettivo di trarre il meglio dalla loro sinergia.

Le principali componenti software che interagiscono all'interno del sistema sono:

- DB noSql per la gestione dei dati di sistema e dei metadati legati ai documenti in conservazione;
- DB relazionale per le operazioni di registrazione, autenticazione e configurazione
- Rest server per le interfacce di frontiera (Web e Web Service);
- un sistema di message broker per la gestione delle code e dei processi;
- sistema di registrazione e gestione dei dati di audit.

8.5. Componenti fisiche

La soluzione è composta da più infrastrutture fra loro interconnesse:

- un sito di Produzione completamente autosufficiente e con tutte le componenti ridondate in HA e collegato tramite fibre ottiche dedicate e di proprietà, con doppia via, al sito secondario. L'indirizzo del sito primario di produzione è Elmec Varese (BR4): Via Campo di Maggio 45-47, 21020 Brunello (VA) Italia
- un sito di BC pensato per permettere la ripartenza automatica dei sistemi in caso di problemi o down del sito principale
- un sito di DR predisposto alla replica dei dati e con le componenti necessarie ad una ripartenza completa del servizio. L'indirizzo del datacenter di disaster recovery è: Siziano (Supernap): Via Marche 8-10, 27010 Siziano (PV) Italia
- infrastruttura S3 di AWS è ospitato in differenti *Available Zone* descritte qui: https://aws.amazon.com/it/about-aws/global-infrastructure/regions_az/. Le *Available Zone* associate ad Argentea S.r.l. sono a Milano.

Tutte le componenti utilizzate sono di tipologia enterprise e, come tutte le soluzioni implementate dal Fornitore di Argentea S.r.l., utilizzano prodotti di marche ampiamente riconosciute e leader del mercato di riferimento.



8.5.1. Ambiente di Produzione

L'ambiente di produzione è ospitato su due siti in una infrastruttura virtuale sul quale sono installati i vari server applicativi.

Nel dettaglio sono presenti:

- il proxy in rete dmz
- il web server
- gli application server
- un nodo dedicato al DB server Postgres ed uno MongoDB
- il server virtuale per la gestione delle code del sistema di caricamento
- un nodo virtuale che implementa repository su ambiente S3
- link ed interfacce verso i sistemi di Firma e Marcatura.

La figura sottostante schematizza quanto implementato senza entrare nelle specifiche modalità di replica.

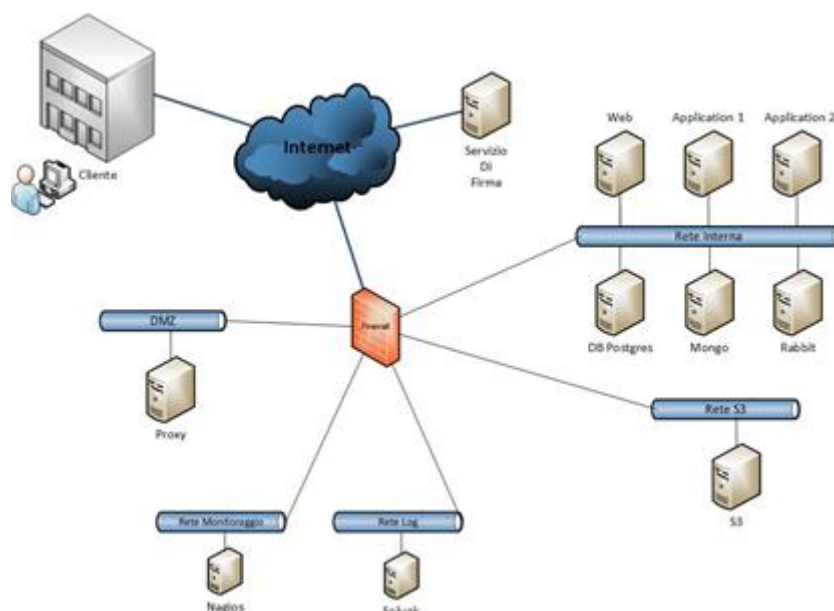


Figura 3: Rappresentazione della soluzione

8.5.2. Sito Secondario (DR)

Il sito secondario ospita un'infrastruttura virtuale sulla quale vengono riportati gli ambienti:

- storage S3 su cui vengono sincronizzati i dati in maniera applicativa che saranno resi disponibili ai server del sito secondario per ripristinare il servizio;
- collegamenti verso i sistemi esterni di firma e Marcatura temporale (sempre situati nel sito secondario);
- macchine virtuali replicate dal sito primario

La procedura di switch tra il sito primario ed il secondario è basata tramite il cambio dei puntamenti a livello di DNS.

La figura sottostante schematizza la modalità di replica delle componenti tra i vari sistemi.

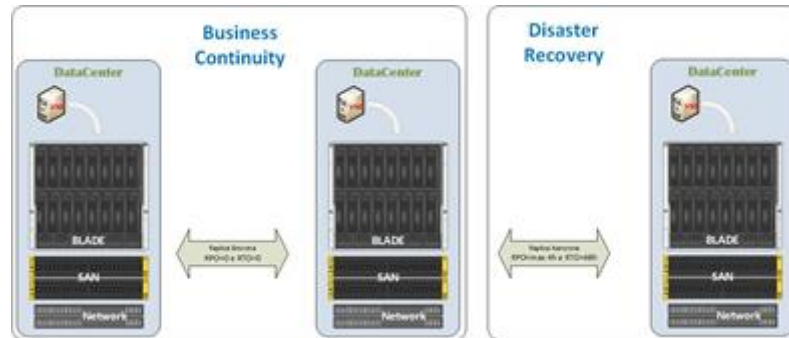


Figura 4: Rappresentazione della continuità della soluzione

Come si può notare è stata posta l'attenzione sia alla continuità operativa con un sistema di altissima affidabilità, sia al Disaster Recovery; questo ultimo può essere attivato attraverso apposito DRP (Disaster Recovery Plan) in caso di problemi sul sito di Produzione attivando il servizio con tempi e modi prestabiliti.

8.6. Politica di gestione degli accessi applicativi

L'accesso al sistema è garantito attraverso credenziali di autenticazione (Username e Password) le cui caratteristiche principali sono di seguito riportate:

- **Robustezza password;** le password che il sistema accetta devono rispettare le seguenti regole:
 - Lunghezza minima 8 caratteri
 - Contenere maiuscole e minuscole
 - Contenere almeno un carattere speciale tra: !@#\$%&()._-+?
 - La password non deve contenere lo Username
- **Scadenza password**

Tutte le utenze applicative comprese quelle amministrative richiedono il cambio obbligatorio della password dopo 90 giorni. Il profilo amministratore può impostare delle utenze "tecniche", utilizzate dalle procedure automatiche di versamento, per le quali non è prevista la scadenza della password.
- **Blocco utenza**

Nel caso in cui venga superato il numero massimo di tentativi consecutivi di inserimento errato della password viene bloccato l'accesso al sistema. I tentativi ammessi sono 3. Nel caso di utenza bloccata alla pagina di login compare il messaggio: "L'utente è stato disabilitato dopo troppi tentativi errati. Riprovare più tardi".

Lo sblocco dell'utenza avviene automaticamente dopo 30 minuti, passati quindi i 30 minuti l'utente può accedere nuovamente. Se l'utente ha dimenticato la password può effettuare il reset dal link "password dimenticata?" presente nella pagina di login. Il sistema invierà una mail all'indirizzo indicato con una password temporanea da modificare al primo accesso.

- **Gestione password precedenti**

Al fine di garantire uno standard di sicurezza adeguato non è consentito dal sistema utilizzare le 5 password precedenti.

- **Disattivazione Utenze**

Saranno resi inattivi gli utenti che negli ultimi 12 mesi non hanno effettuato alcun accesso.

- **Autenticazione a Due Fattori**

Il Sistema di Conservazione Argentea dà la possibilità agli utenti di attivare l'Autenticazione a due fattori – 2FA o anche detta Strong Authentication. Il secondo fattore di autenticazione (OTP) sarà fornito da un'app di autenticazione (il Sistema di Conservazione Argentea è compatibile con le principali).

- **Integrazione con Carta di Identità Elettronica (CIE)**

Il Sistema di Conservazione Argentea permette di ottenere l'integrazione con la Carta di Identità Elettronica senza oneri aggiuntivi.

8.7. Procedure di gestione e di evoluzione

In linea con quanto previsto dalla circolare n° 65, nell'allegato "REQUISITI DI QUALITÀ E SICUREZZA PER L'ACCREDITAMENTO E LA VIGILANZA", sono descritte le procedure in riferimento a:

- conduzione e manutenzione del sistema di conservazione;
- gestione e disponibilità dei log (vedi anche capitolo 9);
- monitoraggio del sistema di conservazione (vedi anche capitolo 9);
- change management (vedi paragrafo 8.7.1);
- verifica periodica di conformità a normativa e standard di riferimento (vedi paragrafo 8.7.2).

8.7.1. Change management

Per ogni operazione di upgrade - per evoluzione o bug fixing - di una qualsiasi componente del sistema di conservazione viene seguita una procedura al fine di garantire il minimo impatto su eventuali fermi del servizio ed avere la massima sicurezza possibile riguardo ai dati e documenti a sistema.

Tale procedura si basa sui seguenti assunti:

- ogni componente sviluppata è conservata in opportuno sistema di versionamento del codice;
- ogni componente sviluppato è testato in diverse fasi su sistemi logicamente separati (sviluppo, test, collaudo e produzione);
- i file di configurazione di ogni componente sono separati dai compilati in maniera da garantire un accesso più flessibile e veloce al personale addetto;
- sono state predisposte apposite macchine di deploy per la compilazione e creazione dei pacchetti delle varie componenti da installare;



Ogni aggiornamento del sistema passa da un flusso ben definito che consente contemporaneamente di mantenere stabile e sicura l'intera soluzione in uso dall'esterno e di sviluppare senza ostacoli nuove funzionalità.

In particolare vengono messi a disposizione 4 ambienti di lavoro: sviluppo, test, collaudo e produzione, logicamente separati. Tutti gli sviluppi vengono condotti e testati nell'ambiente sviluppo che è in uso esclusivo agli sviluppatori per le sue caratteristiche di continua trasformazione.

Qualsiasi altro attore esterno al team di sviluppo non ha nessun accesso a tale ambiente.

Il codice sviluppato viene conservato all'interno di un sistema di versionamento organizzato in maniera da permettere, qualora sia necessario, l'estrazione di una qualsiasi versione del software. Una volta che un nuovo modulo software è pronto, esso viene registrato nel sistema di versionamento associandogli un tag/versione.

Per operare l'installazione sull'ambiente di test, deputato ai test pre-collaudo, i sorgenti vengono scaricati su un ambiente di deploy, esterno all'ambiente di test stesso, direttamente dal sistema di versionamento, insieme a eventuali script automatici di compilazione, installazione e configurazione.

Sull'ambiente di test si effettuano i test per verificare la corretta implementazione dei moduli rilasciati ed effettua anche i test di regressione.

Solo se il processo di testing va a buon fine si procede con il rilascio dei nuovi moduli nell'ambiente di collaudo e produzione con la medesima procedura utilizzata per l'ambiente di test.

8.7.2. Verifica periodica di conformità a normativa e standard di riferimento

Argentea S.r.l., in qualità di conservatore, svolge una verifica periodica della conformità alle normative ed agli standard di riferimento. A tal proposito, viene effettuata una volta l'anno, una verifica sulla rispondenza ai requisiti di qualità e sicurezza avvalendosi dello strumento di check list, sulla base dell'allegato della circolare n° 65, attraverso il quale viene registrata l'aderenza o meno alla conformità richiesta.

9. MONITORAGGIO E CONTROLLI

In questo capitolo si riporta la descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione con l'evidenza delle soluzioni adottate in caso di anomalie.

9.1. *Condizione e manutenzione del sistema di conservazione, gestione log, monitoraggio Infrastruttura*

Il monitoraggio dell'infrastruttura è operativo 24 ore su 24/7/365, non solo per monitorare la gestione delle capacità ma anche per riscontrare qualsiasi evento anomalo a livello sistemistico, fino al sistema operativo.

I sistemi sono configurati per inviare agli operatori allarmi nel caso in cui il livello di utilizzo delle risorse superi una certa soglia oppure in caso di altri eventi anomali, compresi quelli che possono indicare una potenziale violazione di sicurezza. Gli allarmi vengono definiti sui sistemi tenendo in conto anche della criticità degli stessi o delle informazioni in essi eventualmente contenute.

Ove ciò avvenga, e quindi quando una risorsa è vicina alla saturazione oppure in caso di eventi anomali, è necessario aggiungere risorse (comunque da gestire come Change Request) o intraprendere le attività di verifica delle anomalie dei sistemi, anche al fine di verificare se si renda necessaria l'attivazione delle procedure.

Gli strumenti automatici di segnalazione, che vengono costantemente controllati dal personale, permettono l'impostazione di controlli "ad hoc" per ciascun servizio da monitorare, rilevando automaticamente le anomalie e segnalandole visivamente (e opzionalmente via email, sms, ecc.).

Per tutti i sistemi sono inseriti appositi controlli su tali strumenti atti a verificare i vari aspetti del servizio preso in esame, in modo da evidenziare qualsiasi tipo di anomalia.

Non appena compare un alert sullo strumento di monitoraggio, il personale addetto avvia immediatamente le opportune verifiche.

Ciascun alert è stato creato in modo da identificare in maniera precisa e rapida il sottostante servizio monitorato e ottenere:

- una breve descrizione del servizio monitorato;
- le verifiche e le ulteriori prove da compiere per assicurarsi dell'effettiva presenza di anomalie e raccogliere ulteriori dettagli;
- le operazioni da compiere nel caso si presenti una reale anomalia;
- le condizioni per cui è necessario avviare l'escalation.

E' a disposizione anche il tool MyElmec che consente di verificare puntualmente lo stato di funzionamento dell'intera infrastruttura, consentendo di individuare eventuali anomalie o situazioni da attenzionare per l'avvicinamento del limite di utilizzo delle risorse disponibili.

9.2. *Procedure di monitoraggio (applicativo)*

Argentea S.r.l., con l'ausilio e supporto del fornitore della piattaforma tecnologica ospitante la soluzione, assicura la verifica periodica del funzionamento, nel tempo, del sistema di conservazione. Il controllo della buona funzionalità del sistema di conservazione avviene tramite apposite funzionalità di monitoraggio del software. Esse mostrano l'esito delle operazioni automatiche eseguite sul sistema di conservazione come la generazione dei Pacchetti di Archiviazione, la chiusura dei Pacchetti di Archiviazione e la verifica dell'integrità degli archivi.

Unitamente all'esito delle predette operazioni vengono controllati anche i log delle operazioni medesime al fine di avere maggiore certezza di quanto effettivamente eseguito dal sistema di conservazione.

Il monitoraggio avviene inoltre anche a livello di processi di elaborazione sul sistema di conservazione. Questo permette di individuare eventuali casi di processi bloccati che potrebbero inficiare il funzionamento del sistema stesso.

Un ultimo controllo del buon funzionamento del sistema avviene tramite il monitoraggio delle tracciatore che vengono effettuate a livello di database. Tutte le operazioni eseguite determinano infatti la creazione di apposite revisioni che registrano tutte le modifiche intervenute sul sistema permettendo eventualmente di ripristinare i dati a seguito di situazioni anomale.

9.3. Verifiche sull'integrità degli archivi

Come previsto dalla normativa, Argentea S.r.l., assicura la verifica periodica, con cadenza non superiore a 36 mesi, dell'integrità degli archivi e della leggibilità degli stessi; assicura, inoltre, agli organismi competenti previsti dalle norme vigenti, l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza.

Il sistema di conservazione esegue periodicamente ed automaticamente le operazioni di controllo dell'integrità degli archivi. Tali operazioni vengono eseguite solo su una certa percentuale dell'archivio che viene definita nella configurazione del sistema di conservazione.

9.3.1. Pianificazione delle verifiche periodiche da effettuare

La verifica dell'integrità degli archivi viene effettuata sui filesystems in cui i documenti sono replicati, controllando tutti i file presenti nei PdA conservati.

Viene verificato che i file distribuiti nei filesystems siano identici mediante:

- controllo del nome e della dimensione dei file presenti sui filesystems;
- calcolo dell'hash di ogni singolo file. Il valore viene confrontato con l'hash del corrispondente file censito nell'IPdV del PdA.

Il controllo su ciascun PdA conservato viene effettuato a intervalli temporali. La prima verifica dell'integrità del PdA viene effettuata entro 36 mesi dalla conservazione del PdA. Le successive verifiche vengono effettuate entro 36 mesi dalla conclusione dell'ultima verifica effettuata.

9.3.2. Mantenimento della firma per il periodo di conservazione

Il sistema di conservazione si avvale di un altro fornitore terzo (Certificatore accreditato) per le attività di firma digitale e di marcatura temporale. Questo fornitore garantisce che gli elaboratori che offrono il servizio di marcatura temporale e di firma digitale sono protetti da livelli di protezione logica estremamente elevati. La medesima collocazione fisica del sistema garantisce gli elaboratori dalla possibilità di compromissioni fisiche grazie agli accorgimenti tecnici atti ad impedire accessi non autorizzati da persone e danneggiamenti da eventi accidentali. Non è infatti consentito l'accesso e la permanenza di una sola persona. I locali ove si svolgono le procedure di firma e marca sono dotati di sofisticati impianti di allarme, telecamere, microfoni, rilevatori di movimento (che si attivano soltanto quando nessuna persona vi è presente), al fine di controllare ogni movimento all'interno degli stessi.

9.4. Soluzioni adottate in caso di anomalie

Nell'ambito dell'Infrastruttura che ospita la soluzione di conservazione viene conservata e periodicamente esaminata dall'Amministratore un log delle operazioni svolte dagli utenti e dai processi, in modo che tali azioni possano essere

documentate ed attribuite a chi le ha eseguite o causate (Accountability), anche allo scopo di rilevare eventi di sicurezza, incidenti e vulnerabilità associati ai sistemi coinvolti nel processo di conservazione. Tali log sono archiviati e non sono accessibili agli utenti non autorizzati.

9.4.1. Procedura di ripristino in caso di corruzione o perdita dei dati:

In caso di anomalie riscontrate a seguito del monitoraggio delle funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi, sono presenti apposite procedure di emergenza (Contingency) da applicare in attesa del ripristino del servizio.

I sistemi su cui è ospitato il servizio effettuano il salvataggio automatico delle macchine virtuali e del dato contenuto secondo le politiche di Retention stabilite. Il controllo della corretta esecuzione dei backup è giornaliero ad opera degli addetti ed è agevolato dall'utilizzo di mail e dalla console del backup stessa.

L'evidenza del risultato viene riportata nel portale di gestione utente "MyElmec" al fine di dare visibilità completa dei processi a tutti gli addetti/interessati. L'eventuale processo di restore avviene inserendo la richiesta al reparto tecnico nel sistema di ticketing, a garanzia della corretta gestione e tracciatura di tutto il processo.

Eventuali urgenze o problematiche particolari possono essere gestite attraverso il canale ufficiale (il sistema di ticketing) e facendo riferimento al service manager assegnato al Gruppo, in grado di gestire ed eventualmente operare attività di prioritizzazione del ticket stesso.

Per gli errori riscontrati in fase di verifica applicativa si procede invece come già indicato al paragrafo 7.2.

9.4.2. Gestione dei log

L'elenco delle tipologie di log registrate è il seguente:

- audit: vengono tracciate tutte le attività di modifica ai sistemi
- secure: vengono tracciate tutte le attività di login/logout/failed login degli utenti
- log4j: log applicativi
- syslog: log generici che completano la ricostruzione degli eventi
- postgresql: log generati dal database
- apache: log generati dal motore web
- conservazione: log applicativi
- log antivirus

Il log più rilevante è ovviamente quello applicativo che registra tutti gli accessi al sistema e le operazioni di amministrazione e conservazione che vengono effettuate: creazioni di aziende, archivi ed utenze, assegnamento risorse, creazione di PdA, caricamenti di indici e files, validazioni, conservazioni ed errori durante questo tipo di operazioni.

Tali dati, memorizzati in un apposito sistema vengono salvati e storicizzati.

Il sistema permetta le consultazioni on-line tramite interfaccia Web di tutti i log gestiti.

<fine documento>

ACCORDO DI VERSAMENTO AL SISTEMA DI CONSERVAZIONE INDIVIDUATO DALL'ENTE DEI DOCUMENTI INFORMATICI PRODOTTI O REGISTRATI DALL'APPLICATIVO ORDINATIVO INFORMATICO FORNITO DA ARGENTEA

1. PREMESSA	2
2. IL SERVIZIO	2
2.1 IL SERVIZIO ORDINATIVO INFORMATICO	2
2.2 SIC – SISTEMA DI INTERFACCIA CONSERVAZIONE	2
3. TIPOLOGIE DI DOCUMENTI INFORMATICI OGGETTO DI CONSERVAZIONE	2
3.1 DOCUMENTI INFORMATICI PRODOTTI O REGISTRATI DALLA PROCEDURA MIF2 – STANDARD ABI	3
3.2 DOCUMENTI INFORMATICI PRODOTTI O REGISTRATI DALLA PROCEDURA MIF3 – STANDARD OIL/OPI	4
4. INVII ALLA CONSERVAZIONE	4
4.1 INDIVIDUAZIONE DOCUMENTI INFORMATICI DA CONSERVARE	4
4.2 TEMPISTICA DI INVIO AL SERVIZIO DI CONSERVAZIONE	5
4.3 ANOMALIE NEL PROCESSO DI INDIVIDUAZIONE DEI DOCUMENTI – MONITORAGGIO	5
5. CREAZIONE IPDV E PDV	6
5.1 CARATTERISTICHE DELL'IPDV	6
6. CLASSI DOCUMENTALI E METADATI ASSOCIATI	7
6.1 CLASSI DOCUMENTALI ORDINATIVO INFORMATICO MIF2 – STANDARD ABI	7
6.2 CLASSI DOCUMENTALI ORDINATIVO INFORMATICO MIF3 - STANDARD OIL/OPI	8
7. FASE DI INVIO AL SISTEMA DI CONSERVAZIONE	10
7.1 FLUSSO DI INVIO ALLA CONSERVAZIONE	10
7.2 INVIO DOCUMENTI	11
7.3 MONITORAGGIO DELLA FASE DI INVIO	11
7.4 CONSEGNA AL SISTEMA DI CONSERVAZIONE	11
7.5 RITORNI ATTESI DAL SISTEMA DI CONSERVAZIONE	11
8. APPENDICE A: XSD IPDV	12



1. PREMESSA

Il presente ACCORDO DI VERSAMENTO descrive LE MODALITA', LE TIPOLOGIE E LA TEMPISTICA DI VERSAMENTO per i documenti informatici prodotti o registrati dal Servizio Ordinativo Informatico ed inviati al Servizio di Conservazione indicato dall'Ente.

Nello specifico il Servizio di Conservazione individuato dall'Ente è il servizio offerto e contrattualizzato con Argentea.

2. IL SERVIZIO

2.1 IL SERVIZIO ORDINATIVO INFORMATICO

Gli Ordinativi di Pagamento ed Incasso informatico e le relative evidenze, rilasciate dalla Tesoreria in evasione degli stessi, sono evidenze elettroniche dotate di validità amministrativa e contabile, che sostituiscono a tutti gli effetti i documenti cartacei prodotti dall'Ente e dal Tesoriere.

Argentea, mette – da tempo - a disposizione degli Enti una soluzione informatica che permette la formazione e lo scambio dei documenti informatici da e per la Tesoreria.

Le soluzioni Ordinativo Informatico offerte da Argentea e denominate MIF2 ABI e MIF3 OIL/OPI si avvalgono di un modulo aggiuntivo (SIC – Sistema di Interfaccia Conservazione) in grado di individuare e predisporre i documenti informatici presenti negli archivi e di inviarli al Sistema di Conservazione contrattualizzato con l'Ente.

2.2 SIC – SISTEMA DI INTERFACCIA CONSERVAZIONE

Il modulo è stato sviluppato per soddisfare le richieste degli Enti che hanno la necessità di automatizzare l'invio dei documenti informatici al Servizio di Conservazione prescelto.

Le varie fasi per l'identificazione dei documenti informatici da inviare in conservazione, la formazione dei pacchetti di versamento e la ricezione delle evidenze di avvenuta ricezione/conservazione o di eventuali errori riscontrati dal Servizio di Conservazione sono meglio descritte nel seguito del documento.

3. TIPOLOGIE DI DOCUMENTI INFORMATICI OGGETTO DI CONSERVAZIONE

Il presente ACCORDO DI VERSAMENTO è rivolto esclusivamente alla tipologia di documenti individuati al successivo paragrafo 4.1, formati o registrati secondo quanto previsto dalle regole del Servizio Ordinativo Informatico di cui si avvale l'Ente.

Vengono individuati ed inviati al Servizio di Conservazione unicamente i documenti informatici validi, ovvero in corso di validità della firma digitale che ha sottoscritto il documento o per i quali sia stata prorogata la validità mediante apposizione di marca temporale.

All'interno del Servizio Ordinativo Informatico vengono sottoposti a marcatura temporale i soli Ordinativi di pagamento (mandati) e Ordinativi di incasso (reversali). Non vengono marcate temporalmente le ricevute informatiche e/o il giornale di cassa rilasciati dalle Tesorerie.

Ogni altro tipo di documento informatico che l'Ente intenda versare in autonomia al Servizio di Conservazione sarà oggetto di altro specifico Accordo o di integrazione al presente.

Il presente documento descrive il funzionamento delle procedure affinché il processo di individuazione e versamento al Servizio di Conservazione avvenga nel rispetto della normativa e di quanto previsto dal contatto.



3.1 DOCUMENTI INFORMATICI PRODOTTI O REGISTRATI DALLA PROCEDURA MIF2 – STANDARD ABI

I documenti informatici presenti negli archivi del Servizio Ordinativo Informatico nella versione MIF2 – Standard Abi ed oggetto dell'individuazione per il versamento in conservazione sono:

pacchetto mandati: ogni pacchetto di mandati, sottoscritto dall'incaricato dell'Ente, contiene uno o più mandati. La firma, posta in calce al pacchetto degli Ordinativi di pagamento, chiude e consolida il documento informatico 'mandati'; ogni pacchetto viene individuato secondo quanto previsto al successivo capitolo 4 ed inviato alla conservazione.

Inoltre al pacchetto può essere associata anche la ricevuta di servizio rilasciata dal Tesoriere ad attestazione dell'avvenuta ricezione degli ordini di pagamento.

Il pacchetto mandati può portare la marca temporale eventualmente apposta per garantirne la validità ed opponibilità oltre i termini di scadenza della firma digitale che ha sottoscritto il documento;

pacchetto reversali: ogni pacchetto di reversali, sottoscritto dall'incaricato dell'Ente, contiene una o più reversali. La firma, posta in calce al pacchetto degli Ordinativi di incasso, chiude e consolida il documento informatico 'reversali'; ogni pacchetto viene individuato secondo quanto previsto al successivo capitolo 4 ed inviato alla conservazione.

Inoltre al pacchetto può essere associata anche la ricevuta di servizio rilasciata dal Tesoriere ad attestazione dell'avvenuta ricezione degli ordini di incasso.

Il pacchetto mandati può portare la marca temporale eventualmente apposta per garantirne la validità ed opponibilità oltre i termini di scadenza della firma digitale che ha sottoscritto il documento;

quietanze mandati: ogni ricevuta di pagamento o di regolarizzazione sottoscritta dall'incaricato della Tesoreria e dimostrante l'avvenuta estinzione dell'ordinativo costituisce un documento informativo e viene individuata secondo quanto previsto al successivo capitolo 4 ed inviata alla conservazione.

Le ricevute di pagamento/regolarizzazione rilasciate dal Tesoriere non sono marcate temporalmente quindi non vengono inviate alla conservazione se il certificato che ha sottoscritto la ricevuta è scaduto;

bollette reversali: ogni ricevuta di incasso o di regolarizzazione sottoscritta dall'incaricato della Tesoreria e dimostrante l'avvenuta estinzione dell'ordinativo costituisce un documento informativo e viene individuata secondo quanto previsto al successivo capitolo 4 ed inviata alla conservazione.

Le ricevute di incasso/regolarizzazione rilasciate dal Tesoriere non sono marcate temporalmente quindi non vengono inviate alla conservazione se il certificato che ha sottoscritto la ricevuta è scaduto;

provvisori di entrata/uscita: ogni pacchetto contenente più ricevute di incasso o pagamento sottoscritto dall'incaricato della Tesoreria e dimostrante l'avvenuto incasso/pagamento di operazioni di iniziativa della Tesoreria, costituisce un documento informativo e viene individuato secondo quanto previsto al successivo capitolo 4 ed inviato alla conservazione.

I pacchetti di ricevute per operazioni di iniziativa della Tesoreria (provvisori) non sono marcati temporalmente quindi non vengono inviati alla conservazione se il certificato che ha sottoscritto la ricevuta è scaduto;

ricevute di servizio: qualora la ricevuta di servizio rilasciata dalla Tesoreria e sottoscritta digitalmente dalla stessa, attestante la corretta ricezione degli ordini, non sia abbinata al pacchetto dei mandati o delle reversali ai quali si riferisce, viene individuata ed inviata essa stessa in conservazione secondo quanto previsto al successivo capitolo 4.

Le ricevute di servizio, qualora non abbinate al pacchetto ordinativi, non sono marcate temporalmente e quindi non vengono inviate alla conservazione se il certificato che ha sottoscritto la ricevuta è scaduto.



3.2 DOCUMENTI INFORMATICI PRODOTTI O REGISTRATI DALLA PROCEDURA MIF3 – STANDARD OIL/OPI

I documenti informatici presenti negli archivi del Servizio Ordinativo Informatico nella versione MIF3 - Standard OIL/OPI ed oggetto dell'individuazione per il versamento in conservazione sono:

pacchetto mandati: ogni pacchetto di mandati, sottoscritto dall'incaricato dell'Ente, contiene uno o più mandati. La firma digitale chiude e forma il documento informatico 'mandati'; ogni pacchetto viene individuato secondo quanto previsto al successivo capitolo 4 ed inviato alla conservazione.

Il pacchetto mandati può portare la marca temporale eventualmente apposta per garantirne la validità ed opponibilità oltre i termini di scadenza della firma digitale che ha sottoscritto il documento;

pacchetto reversali: ogni pacchetto di reversali, sottoscritto dall'incaricato dell'Ente, contiene una o più reversali. La firma digitale chiude e forma il documento informatico 'reversali'; ogni pacchetto viene individuato secondo quanto previsto al successivo capitolo 4 ed inviato alla conservazione.

Il pacchetto reversali può portare la marca temporale eventualmente apposta per garantirne la validità ed opponibilità oltre i termini di scadenza della firma digitale che ha sottoscritto il documento;

ricevute di ricezione flusso: la ricevuta di ricezione del flusso (chiamata anche ricevuta di servizio) rilasciata dalla Tesoreria e sottoscritta digitalmente dalla stessa, attestante la corretta ricezione dell'ordine, costituisce un documento informatico e viene individuata ed inviata in conservazione secondo quanto previsto al successivo capitolo 4.

Le ricevute di ricezione non sono marcate temporalmente e quindi non vengono inviate alla conservazione se il certificato che ha sottoscritto la ricevuta è scaduto.

giornale di cassa: il flusso, con la movimentazione contabile (pagamento/incasso ordinativi e pagamento/incasso provvisori) effettuata dalla Tesoreria e relativa ad una giornata o ad un periodo, sottoscritto digitalmente dall'incaricato della Tesoreria costituisce un documento informatico e viene individuato e inviato alla conservazione secondo quanto previsto al successivo capitolo 4.

Il giornale di cassa non è marcato temporalmente, quindi non viene inviato alla conservazione se il certificato che ha sottoscritto il documento è scaduto.

4. INVII ALLA CONSERVAZIONE

Il modulo software SIC – Sistema di Interfaccia alle Conservazioni è schedato giornalmente (nelle ore serali/notturne) e si incarica di individuare i documenti informatici da inviare al Sistema di Conservazione, comporre i flussi relativi all'Indice del pacchetto di versamento ed al pacchetto di versamento stesso.

4.1 INDIVIDUAZIONE DOCUMENTI INFORMATICI DA CONSERVARE

Il modulo SIC, in modalità schedata (ore serali/notturne), procede con l'individuazione dei documenti da predisporre per l'invio al Sistema di Conservazione individuato dall'Ente o al sistema gestionale dell'Ente stesso.

Per poter essere inviati al Sistema di conservazione di riferimento o ai gestionali degli Enti i documenti devono:

- non essere archiviati come già inviati in conservazione con esito positivo;



- essere sottoscritti con certificato digitale in corso di validità o essere marcati temporalmente se il certificato fosse scaduto;
- in caso di ordinativi (mandati e reversali) aver ricevuto dalla Tesoreria la prevista ricevuta di ricezione del flusso (chiamata anche ricevuta di servizio);

Individuati i documenti sulla base di quanto sopra elencato, la procedura provvede a creare i pacchetti di versamento (PDV) con i relativi indici (IPDV).

Ogni pacchetto sarà creato per Ente/Tipologia/Giorno/Esercizio.

Le tipologie sono quelle previste al capitolo 3 del presente documento, mentre la selezione 'Giorno' corrisponde al giorno successivo all'apposizione della firma per gli Ordinativi (mandati e reversali) che hanno ottenuto la relativa ricevuta di servizio da parte della Tesoreria, mentre per ricevute applicative e giornali di cassa corrisponde al giorno successivo rispetto alla data di ricezione dei documenti stessi.

La procedura SIC salva su un database dedicato gli IPDV dei pacchetti inviati, oltre alle informazioni sugli invii effettuati verso il Sistema di Conservazione.

Viene chiesto al sistema di destinazione (Sistema di Conservazione o gestionale dell'Ente) di fornire un riferimento al documento conservato in modo da poter aggiornare il sistema mittente (archivi procedura Ordinativo Informatico) con gli estremi di avvenuta conservazione.

4.2 TEMPISTICA DI INVIO AL SERVIZIO DI CONSERVAZIONE

Il servizio di invio dei documenti alla conservazione (SIC – sistema di Interfaccia alle Conservazioni) prevede l'invio giornaliero dei documenti individuati come conservabili secondo quanto previsto al paragrafo 4.1.

L'esecuzione dei programmi che individuano i documenti da inviare alla conservazione è prevista nelle ore notturne (normalmente alle 5) per dar modo di inviare in conservazione il maggior numero di documenti possibili rispetto alle firme del giorno precedente e raccogliere dal Tesoriere il maggior numero di ricevute/giornale di cassa possibile.

Pertanto se un documento è stato firmato nella giornata 0, di norma viene inviato alla conservazione nella giornata +1.

L'invio può tardare per effetto di un allungamento non preventivato delle fasi precedenti la schedulazione dei programmi che individuano i documenti da inviare alla conservazione o per errori riscontrati in fase di invio.

4.3 ANOMALIE NEL PROCESSO DI INDIVIDUAZIONE DEI DOCUMENTI – MONITORAGGIO

Il processo prevede una fase di monitoraggio automatico con invio di segnalazioni alla struttura competente.

Eventuali documenti non conservabili verranno rianalizzati nella schedulazione successiva.

Eventuali anomalie riscontrate dalla procedura vengono segnalate via e-mail al servizio tecnico/informatico che presidia il processo.

- **ANOMALIA DI TIPO TECNICO**

per le anomalie di tipo tecnico vengono ingaggiati i tecnici software/sistemisti per le opportune verifiche e sistemazioni, con ripartenza del servizio.

- **ANOMALIA DI TIPO DOCUMENTALE**

per le anomalie di tipo documentale (ad esempio firma scaduta o documento non conservabile per vizi di forma) viene inviata una segnalazione alla Struttura di supporto alla Conservazione di Argentea



che contatta l'Ente, nella persona del Responsabile della Conservazione, per individuare le azioni opportune alla soluzione del problema.

5. CREAZIONE IPDV E PDV

La seconda fase attuata all'interno del modulo SIC consiste nel catalogare ogni singolo documento individuato come conservabile, associare allo stesso la propria 'classe documentale' ed estrarre dal documento stesso i metadati previsti per la classe documentale di appartenenza come descritta al capitolo 6.

E' questa la fase che compone l'Indice di Versamento, nel quale vengono elencati tutti i documenti (individuati da un loro 'nome') ed i rispettivi metadati. Il file così costruito costituisce per l'appunto l'Indice di Versamento che viene inviato al Sistema di Conservazione.

A seguire vengono inviati tanti documenti, quanti sono quelli elencati nell'indice e che sono stati precedentemente individuati come conservabili.

5.1 CARATTERISTICHE DELL'IPDV

L'IPdV è un file in formato XML che descrive un PdV, ovvero la specificità della classe documentale alla quale il versamento si riferisce.

L'IPdV generato dal sistema di interfaccia SIC3 ha un naming preciso, del tipo

IPDV-<codiceFiscaleEnte>_<esercizio>_<Progressivo>_Ordinativo|Ricevuta|GiornaleDiCassa.xml

utile a identificare univocamente il file dell'IPdV per ogni tipologia di documento inviato.

Come previsto dalla normativa ogni IPDV elenca i metadati previsti per la classe documentale di appartenenza del documento inviato. La classe documentale che identifica i documenti che vengono inviati è indicata nel tag docClass dell'IPDV.

Altro tag di fondamentale importanza è il tag <pdvid> che rappresenta un identificativo univoco della richiesta di versamento. Questo identificativo viene assegnato in modo automatico ed univoco dal sistema di interfaccia SIC3.

Successivamente l'indice elenca i metadati relativi a ogni singolo documento che partecipa al versamento.

A questo scopo bisogna introdurre nell'xml una sezione files che contiene un elenco di tag file, uno per ogni documento da mettere in conservazione.

Alcuni metadati sono comuni a tutte le tipologie di documento e devono essere introdotti obbligatoriamente:

- <docid> contiene l'identificativo univoco del documento lato versante. Normalmente tale dato viene ottenuto da un sistema documentale;
- filename indica il nome del documento, comprensivo di eventuale estensione, così come viene memorizzato su file system;
- mimetype indica il tipo di documento, nel senso informatico del termine, secondo la RFC 20464. Le tipologie di documento ammesse per la classe documentale scelta vengono definite in sede di accordo tra il Responsabile del Sistema di Conservazione e il Produttore. Nel caso di file firmati (tipicamente con estensione .p7m) il mimetype da indicare è quello del file sbustato. Se ad esempio si volesse



conservare il file miofile.pdf.p7m il mimetype corretto da indicare sarebbe application/pdf, se invece si volesse conservare miofile.txt.p7m il mimetype corretto da indicare sarebbe text/plain;

- closingDate indica la data di chiusura del documento, ovvero la data di ultima modifica precedente alla messa in conservazione;
- hash contiene l'impronta del documento. Il tag è corredato dall'attributo algorithm che specifica l'algoritmo di calcolo dell'impronta. L'algoritmo deve essere esplicitamente indicato nell'apposito attributo del tag hash.

Il resto dei metadati di un documento è variabile in numero e tipologia a seconda della classe documentale di appartenenza.

Ci sono tipicamente due tipi di metadati: singlemetadata e complexmetadata.

I primi sono di tipo flat, ovvero contengono un solo valore, i secondi raggruppano insiemi di metadati.

Un metadato di tipo simple è indicato nell'IPdV dal tag singlemetadata e normalmente contiene due sottotag, name e value. Il primo contiene il nome del metadato, il secondo il valore attuale relativo al documento in esame.

All'appendice A viene riportato l'xsd relativo agli IPdV creato dal SIC.

Nella compilazione di un IPdV le regole principali di cui si tiene conto sono:

- è importante che ogni IPdV abbia un naming specifico. Quello assegnato da SIC3 è:

IPdV

<codiceFiscaleEnte>_<esercizio>_<Progressivo>_Ordinativo|Ricevuta|GiornaleDiCassa.xml;

- i valori che vengono valorizzati dinamicamente in funzione del documento trattato hanno tutti il prefisso @ph_; tutti gli altri sono costanti;
- di particolare rilevanza è il tag <pdvid> che è unico all'interno dell'archivio e viene assegnato dal sistema di interfaccia SIC3;
- tutti i riferimenti alle date sono inseriti nello standard ISO8601;
- l'impronta dei file è un hash in SHA256 codificato in base64;
- l'elenco dei metadati obbligatori: devono essere presenti nell'IPdV eventualmente anche con valore vuoto.

6. CLASSI DOCUMENTALI E METADATI ASSOCIATI

6.1 CLASSI DOCUMENTALI ORDINATIVO INFORMATICO MIF2 – STANDARD ABI

Per i documenti informatici provenienti dal Sistema Ordinativo Informatico MIF2 – Standard ABI, individuati come indicato al paragrafo 4.1, le CLASSI DOCUMENTALI previste sono:

- **ORDINATIVI:** dove affluiscono i pacchetti mandati ed i pacchetti reversali;
- **RICEVUTE:** dove affluiscono le quietanze, le bollette, i provvisori e le eventuali ricevute di servizio se non accodate al pacchetto mandati/reversali.

La seguente tabella elenca i metadati ad esse associati dal MIF2:



Metadati ed extrainfo	Ordinativo	Metadati ed extrainfo	Ricevute
pdvId	id_flusso+"_Ordinativo"	pdvId	id_flusso+"_Ricevuta"
SIC_ID_Flusso		SIC_ID_Flusso	
docClass	3 _Ordinativo	docClass	4 _Ricevuta
Codice_Ente	Codice dell'ente	Codice_Ente	Codice dell'Ente
ABI_Tesoreria	Codice Abi del Tesoriere	ABI_Tesoreria	Codice Abi del Tesoriere
hash algorithm	SHA1	hash algorithm	SHA1
mimetype	application/xml	mimetype	application/xml
hash	hash del documento	hash	hash del documento
responsabileProcedimento	firmatario del documento	responsabileProcedimento	firmatario del documento
docid		docid	
filename	nome_documento+".xml.p7m"	filename	nome_documento+".xml.p7m"
documento	File base64 con estensione ".xml.p7m"	documento	File base64 con estensione ".xml.p7m"
oggettodocumento	MANDATI	oggettodocumento	RA_MANDATI
	REVERSALI		RA_REVERSALI
			PROVVISORI_ENTRATA
			PROVVISORI_USCITA
oggettoProcedimento	MANDATI	oggettoProcedimento	RA_MANDATI
	REVERSALI		RA_REVERSALI
			PROVVISORI_ENTRATA
			PROVVISORI_USCITA
SIC_Impronta		SIC_Impronta	
Nome_Marca_temporale			
Marca_temporale			
closingDate		closingDate	
Versione_foglio_di_stile	versione del foglio di stile M12	Versione_foglio_di_stile	versione del foglio di stile M12
destinatario_denominazione	Descrizione Banca Tesoriere	destinatario_denominazione	Descrizione Ente
destinatario_codicefiscale	Codice Fiscale Banca Tesoriere	destinatario_codicefiscale	Codice Fiscale Ente
soggettoproduttore_denominazione	Descrizione Ente	soggettoproduttore_denominazione	Descrizione Banca Tesoriere
soggettoproduttore_codicefiscale	Codice Fiscale Ente	soggettoproduttore_codicefiscale	Codice Fiscale Banca Tesoriere
soggettomittente_denominazione	Descrizione Ente	soggettomittente_denominazione	Descrizione Banca Tesoriere
soggettomittente_codicefiscale	Codice Fiscale Ente	soggettomittente_codicefiscale	Codice Fiscale Banca Tesoriere
numero	numero ordinativo	numero	numero ordinativo
progressivo	progressivo ordinativo	progressivo	progressivo ordinativo
dataEmissione	data emissione ordinativo	dataEmissione	data emissione ordinativo
codiceFunzione	codice funzione	codiceFunzione	codice funzione
esercizio	esercizio	esercizio	esercizio
anagraficaPartitaIva	Partita iva beneficiario/versante se presente	anagraficaPartitaIva	Partita iva beneficiario/versante se presente
anagraficaCodiceFiscale	Codice fiscale beneficiario/versante se presente	anagraficaCodiceFiscale	Codice fiscale beneficiario/versante se presente
		numeriRicevuteNumeroRicevuta	inserire i <i>numero_ricevute</i> separati da virgola
		qualificatore	tipologia di ricevuta
NB: Quando tra gli ordinativi è presente una marca temporale: si genera un file nome_documento+".tsr" che eredita le informazioni del documento che accompagna e se ne calcola il suo hash e il suo mimetype (application/octet-stream)			

6.2 CLASSI DOCUMENTALI ORDINATIVO INFORMATICO MIF3 - STANDARD OIL/OPI

Per i documenti informatici provenienti dal sistema Ordinativo Informatico MIF3 – Standard OIL/OPI, individuati come indicato al paragrafo 4.1 le CLASSI DOCUMENTALI previste sono:

- **ORDINATIVI:** dove affluiscono gli ordinativi di pagamento ed incasso (mandati e reversali);
- **RICEVUTE:** dove affluiscono le ricevute di ricezione del flusso (ricevute di servizio);
- **GIORNALE DI CASSA:** dove affluiscono i giornali di cassa giornalmente o periodicamente rilasciati dalla Tesoreria e contenenti tutti gli estremi delle operazioni di pagamento/incasso ordinativi e provvisori.

Le seguenti tabelle elencano i metadati ad esse associati dal MIF3:



METADATI ED EXTRAINFO	RICEVUTA DI 'RICEVUTO'
file.doc_id	identificativo del documento (assegnato al documento nella procedura di provenienza)
file.filename	nome del file p7m
file.mimetype	application/xml
file.closingDate	data_ora_creazione_flusso
mandatory. NumeroProtocollo	
mandatory. DataRegistrazioneProtocollo	
mandatory. 4 _SIC_ Impronta	Impronta
mandatory. AmministrazioniPartecipanti	
mandatory. 4 _indici_ ricevuta	numero del mandato o reversale al quale la RS si riferisce
mandatory. 4 _esercizio	esercizio
mandatory. AooDiRiferimento	
mandatory. OggettoProcedimento	Esito Ricezione Flusso
mandatory. DocumentiContenutiNelProcedimento	numero del mandato o reversale al quale la RS si riferisce
mandatory. ResponsabileProcedimento	Nominativo di chi ha sottoscritto digitalmente il documento
mandatory. AmministrazioneTitolareDelProcedimento	
mandatory. DataRegistrazioneProtocollo	
mandatory. NumeroProtocollo	
mandatory. Oggettodocumento	Esito Ricezione Flusso
mandatory. SoggettoMittente	
mandatori. Destinatario	Codice fiscale dell'Ente Denominazione dell'Ente
mandatory. SoggettoProduttore	codice fiscale della Banca Tesoriere denominazione della Banca Tesoriere
extraInfo. 4 _SIC_ ID Flusso	Identificativo Flusso
extraInfo. 4 _Codice_ Ente	Codice Ente Banca Tesoriera
extraInfo. 4 _ABI_ Tesoreria	Codice Abi Banca Tesoriera
extraInfo. 4 _numero_ ordinativo	numero del mandato o reversale al quale la RS si riferisce
extraInfo. 4 _Esercizio	esercizio

METADATI ED EXTRAINFO	REVERSALE	MANDATO
file.doc_id	identificativo del documento	identificativo del documento
file.filename	nome del file p7m	nome del file p7m
file.mimetype	application/xml	application/xml
file.closingDate	data ed ora di firma del documento	data ed ora di firma del documento
mandatory. NumeroProtocollo		
mandatory. DataRegistrazioneProtocollo		
Mandatory. 3 _SIC_ Impronta	Impronta	Impronta
mandatory. AmministrazioniPartecipanti		
Mandatory. 3 _indici_ ordinativi	numero reversale	numero mandato
Mandatory. 3 _esercizio	esercizio	esercizio
mandatory. AooDiRiferimento		
mandatory. OggettoProcedimento	Ordinativo di Incasso	Ordinativo di Pagamento
mandatory. DocumentiContenutiNelProcedimento	numero reversale	numero mandato
mandatory. ResponsabileProcedimento	nominativo del firmatario del documento	nominativo del firmatario del documento
mandatory. AmministrazioneTitolareDelProcedimento		
mandatory. DataRegistrazioneProtocollo		
mandatory. NumeroProtocollo		
mandatory. Oggettodocumento	Reversale	Mandato
mandatory. SoggettoMittente		
mandatori. Destinatario	Descrizione e Codice Fiscale Banca Tesoriere	Descrizione e Codice Fiscale Banca Tesoriere
mandatory. SoggettoProduttore	Descrizione e Codice Fiscale Ente	Descrizione e Codice Fiscale Ente
extraInfo. 3 _SIC_ ID Flusso	Identificativo flusso	Identificativo Flusso
extraInfo. 3 _Codice_ Ente	codice_ente	codice_ente
extraInfo. 3 _ABI_ Tesoreria	codice Abi Tesoreria	codice Abi Tesoreria
ExtraInfo. 3 _numero_ ordinativo	numero reversale	numero mandato
ExtraInfo. 3 _Esercizio	esercizio	esercizio
ExtraInfo. 3 _Codice_ Fiscale beneficiario versante	codice fiscale del versante quando presente	codice fiscale del beneficiario quando presente



METADATI ED EXTRAINFO	GIORNALE DI CASSA
file.doc_id	identificativo del documento
file.filename	nome del file p7m
file.mimetype	application/xml
file.closingDate	data_ora_creazione_flusso
mandatory. NumeroProtocollo	
mandatory. DataRegistrazioneProtocollo	
Mandatory. 434__SIC_Impronta	Impronta
mandatory. AmministrazioniPartecipanti	
Mandatory. 434__indici_giornale	numero del giornale di cassa
mandatory. numero_giornale_cassa	identificativo flusso
mandatory. esercizio	esercizio
mandatory.data inizio periodo riferimento giornale	data_inizio_periodo_riferimento
mandatory.data fine periodo riferimento giornale	data_fine_periodo_riferimento
mandatory. AooDIRiferimento	
mandatory. OggettoProcedimento	Giornale di Cassa
mandatory. DocumentiContenutiNelProcedimento	identificativo flusso
mandatory. ResponsabileProcedimento	Firmatario del documento
mandatory. AmministrazioneTitolareDelProcedimento	
mandatory. DataRegistrazioneProtocollo	
mandatory. NumeroProtocollo	
mandatory. Oggettodocumento	Giornale di Cassa
mandatory. SoggettoMittente	
mandatori. Destinatario	Denominazione e Codice fiscale Ente
mandatory. SoggettoProduttore	Denominazione e Codice Fiscale Tesoriere
extrainfo. 434__SIC_ID_Flusso	Sequence Interna
extrainfo. 434__Codice_Ente	Codice Ente
Extrainfo. 434__ABI_Tesoreria	Codice Abi Tesoreria
Extrainfo. 434__esercizio	esercizio
Extrainfo. 434__Numero_Reversale	informazioni con i numeri degli ordinativi o dei provvisori trattati nel giornale di cassa
Extrainfo. 434__Provvisorio_di_Entrata	
Extrainfo. 434__Numero_Mandato	
Extrainfo. 434__Provvisorio_di_Uscita	
Extrainfo. 434__Giroconto	
Extrainfo. 434__Anticipazione	
Extrainfo. 434__Fondo_di_cassa	
Extrainfo. 434__Deficit_di_cassa	

7. FASE DI INVIO AL SISTEMA DI CONSERVAZIONE

7.1 FLUSSO DI INVIO ALLA CONSERVAZIONE

Il processo di invio/versamento verso i sistemi di conservazione o gestionale dell'ente si compone dei seguenti passi:

1. Autenticazione al Sistema di Conservazione di destinazione;
2. Creazione del Pacchetto di Archiviazione – PDV – ovvero del contenitore dove depositare tutti i documenti che si vogliono inviare alla conservazione in un'unica soluzione;
3. Upload dell'Indice del Pacchetto di Versamento – IPDV;
4. Upload dei file indicati nell'Indice del Pacchetto di Versamento.



7.2 INVIO DOCUMENTI

L'invio dei dati avviene tramite canale sicuro e cifrato instaurato fra il Servizio Ordinativo Informatico/SIC dal quale provengono i documenti da inviare in conservazione ed il Servizio di Conservazione attivo sulla piattaforma tecnologica di Argentea residente presso Aruba Spa.

Il sistema di scambio messaggi fra la piattaforma di provenienza dei documenti e la piattaforma di conservazione è costantemente monitorato da procedure automatiche che ne segnalano alle competenti strutture eventuali anomalie.

7.3 MONITORAGGIO DELLA FASE DI INVIO

Anche la fase di invio dell'Indice del Pacchetto di Versamento (IPDV) e dei rispettivi documenti (PDV) prevede una fase di monitoraggio a carico della struttura tecnica di Argentea atta a rilevare eventuali anomalie di invio che vengono risolte con una nuova sottomissione nel caso il flusso risultasse non partito/consegnato.

Per ogni invio effettuato, il sistema di ricezione dei documenti posto a monte del Servizio di Conservazione restituisce un messaggio tecnico con l'esito dell'invio (positivo o negativo).

Nel caso l'esito sia negativo, il messaggio viene nuovamente inviato.

7.4 CONSEGNA AL SISTEMA DI CONSERVAZIONE

I documenti individuati, classificati ed inviati come dianzi descritto al Sistema di Conservazione vengono da questo presi in carico ed elaborati così come previsto dalle fasi di conservazione descritte nel Manuale di Conservazione di Argentea reperibile al sito:

<https://www.agid.gov.it/it/piattaforme/spid/identity-provider-accreditati/it-srl>

Il documento viene periodicamente aggiornato.

7.5 RITORNI ATTESI DAL SISTEMA DI CONSERVAZIONE

In seguito all'invio del PDV in conservazione il SIC - sistema di interfaccia si aspetta dei ritorni/notifiche che siano in grado di contro aggiornare gli archivi dell'Ordinativo Informatico. La procedura prevede tre tipi di messaggio:

- Ricevuta di Versamento (RdV);
- Ricevuta di Conservazione (RdC);
- ricevute per errore durante la validazione dell'IPDV.

I messaggi contenenti notifica di errori - riscontrati nella fase di conservazione - vengono vagliati dalla Struttura tecnica di Argentea e, risolta l'anomalia, il documento viene nuovamente inviato al Sistema di Conservazione.

Il Responsabile della Conservazione



8. APPENDICE A: XSD IPDV

```
<xs:schema          attributeFormDefault="unqualified"          elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="PDV">
    <xs:complexType>
      <xs:sequence>
        <xs:element type="xs:string" name="pdvid"/>
        <xs:element name="docClass">
          <xs:complexType>
            <xs:simpleContent>
              <xs:extension base="xs:string">
                <xs:attribute type="xs:string" name="namespace"/>
              </xs:extension>
            </xs:simpleContent>
          </xs:complexType>
        </xs:element>
        <xs:element name="files">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="file" maxOccurs="unbounded" minOccurs="1">
                <xs:complexType>
                  <xs:sequence>
                    <xs:element type="xs:string" name="docid"/>
                    <xs:element type="xs:string" name="filename"/>
                    <xs:element type="xs:string" name="mimetype"/>
                    <xs:element type="xs:string" name="closingDate"/>
                    <xs:element name="hash">
                      <xs:complexType>
                        <xs:sequence>
                          <xs:element type="xs:string" name="value"/>
                        </xs:sequence>
                      </xs:complexType>
                    </xs:element>
                    <xs:attribute type="xs:string" name="algorithm" default="SHA-256"/>
                  </xs:sequence>
                </xs:complexType>
              </xs:element>
              <xs:element name="metadata" minOccurs="0">
                <xs:complexType>
                  <xs:sequence>
                    <xs:element name="mandatory">
                      <xs:complexType>
                        <xs:sequence>
                          <xs:element name="singlemetadata" maxOccurs="unbounded" minOccurs="0">
                            <xs:complexType>
                              <xs:sequence>
                                <xs:element type="xs:string" name="namespace" />
                                <xs:element type="xs:string" name="name"/>
                                <xs:element type="xs:string" name="value"/>
                              </xs:sequence>
                            </xs:complexType>
                          </xs:element>
                        </xs:sequence>
                      </xs:complexType>
                    </xs:element>
                  </xs:sequence>
                </xs:complexType>
              </xs:element>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```



```
</xs:element>
<xs:element name="complexmetadata" maxOccurs="unbounded" minOccurs="0">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="singlemetadata" maxOccurs="unbounded" minOccurs="0">
        <xs:complexType>
          <xs:sequence>
            <xs:element type="xs:string" name="namespace"/>
            <xs:element type="xs:string" name="name"/>
            <xs:element type="xs:string" name="value"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
    </xs:sequence>
    <xs:attribute type="xs:string" name="namespace" use="optional"/>
    <xs:attribute type="xs:string" name="name" use="optional"/>
    <xs:attribute type="xs:string" name="namespaceNode" use="optional"/>
    <xs:attribute type="xs:string" name="nodeName" use="optional"/>
  </xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="extrainfos" minOccurs="0">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="singlemetadata" maxOccurs="unbounded" minOccurs="0">
        <xs:complexType>
          <xs:sequence>
            <xs:element type="xs:string" name="namespace"/>
            <xs:element type="xs:string" name="name"/>
            <xs:element type="xs:string" name="value"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="riferimento" minOccurs="0">
  <xs:complexType>
    <xs:sequence>
      <xs:element type="xs:string" name="pdvidref"/>
      <xs:element type="xs:string" name="docidref"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
```



```
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:schema>
```