ISTITUTO COMPRENSIVO STATALE - "E. TOTI"-LENTATE SUL SEVESO
Prot. 0007298 del 23/06/2026
I (Uscita)

tinexta
infocert

Manuale della Conservazione

tinexta
infocert

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

tinexta
infocert

STORAGE 34

SICUREZZA E PROTEZIONE DEI DATI 34

PROCEDURE DI GESTIONE E MONITORAGGIO 35

CONTROLLI PERIODICI E AUDIT 38

SPECIFICITÀ DEL CONTRATTO 40

tinexta
infocert

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.

tinexta
infocert

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 *bit* che può essere elaborata da una procedura informatica.
FASCICOLO INFORMATICO	Aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento.
FILE	Insieme di informazioni, dati o comandi logicamente correlati, raccolti sotto un unico nome e registrati, per mezzo di un programma di elaborazione o di scrittura, nella memoria di un computer.
FIRMA ELETTRONICA	Vedi articolo 3 del Regolamento eIDAS.
FIRMA ELETTRONICA AVANZATA	Vedi articoli 3 e 26 del Regolamento eIDAS.
FIRMA ELETTRONICA QUALIFICATA	Vedi articolo 3 del Regolamento eIDAS.
FLUSSO (BINARIO)	Sequenza di bit prodotta in un intervallo temporale finito e continuativo che ha un'origine precisa ma di cui potrebbe non essere predeterminato il suo istante di interruzione.
FORMATO CONTENITORE	Formato di file progettato per consentire l'inclusione ("imbustamento" o *wrapping*), in uno stesso file, di una o più evidenze informatiche soggette a differenti tipi di codifica e al quale possono essere associati specifici metadati.
FORMATO DEL DOCUMENTO INFORMATICO	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.

FUNZIONE DI *HASH* CRITTOGRAFICA	Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o *digest* (vedi) in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
GESTIONE DOCUMENTALE	Processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta, uso, selezione e conservazione dei documenti.
HASH	Termine inglese usato, impropriamente, come sinonimo d'uso di "impronta crittografica" o "*digest*" (vedi).
IDENTIFICATIVO UNIVOCO	Sequenza di numeri o caratteri alfanumerici associata in modo univoco e persistente ad un'entità all'interno di uno specifico ambito di applicazione.
IMPRONTA CRITTOGRAFICA	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di *hash* crittografica a un'evidenza informatica.
INTEGRITÀ	Caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità.
INTEROPERABILITÀ	Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi.
LEGGIBILITÀ	Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica.
MANUALE DI CONSERVAZIONE	Documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture.
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 (*FILE PACKAGE*)	Insieme finito di più file (possibilmente organizzati in una struttura di sottoalbero all'interno di un filesystem) che costituiscono, collettivamente oltre che individualmente, un contenuto informativo unitario e auto-consistente.
PACCHETTO DI VERSAMENTO	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione.
PACCHETTO INFORMATIVO	Contenitore logico che racchiude uno o più oggetti di conservazione con i relativi metadati, oppure anche i soli metadati riferiti agli oggetti di conservazione.
PATH	Percorso (*vedi*).
PATHNAME	Concatenazione ordinata del percorso di un file e del suo nome.
PERCORSO	Informazioni relative alla localizzazione virtuale del file all'interno del filesystem espressa come concatenazione ordinata del nome dei nodi del percorso.
PIANO 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

TIMELINE	Linea temporale virtuale su cui sono disposti degli eventi relativi ad un sistema informativo o a un documento informatico. Costituiscono esempi molto diversi di *timeline* un file di log di sistema, un flusso multimediale contenente essenze audio\video sincronizzate.
TITOLARE DELL'OGGETTO DI CONSERVAZIONE	Soggetto produttore degli oggetti di conservazione.
TRASFERIMENTO	Passaggio di custodia dei documenti da una persona o un ente ad un'altra persona o un altro ente.
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.

tinexta
infocert

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, comma3, 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 donnéès pour l'archivage. Transfert – Communication – Élimination – Restitution - Modification, ver. 2.1, 2018;
- METS - Metadata Encoding and Transmission Standard;
- PREMIS – PREservation Metadata: Implementation Strategies;
- EAD (3)/ISAD (G);
- EAC (CPF)/ISAAR (CPF)/NIERA (CPF);
- SCONS2/EAG/ISDIAH;
- 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 scegliere 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://conservatoriqualificati.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 metadatazione)
- Metadata Preservation (file XML di metadatazione secondo lo standard PREMIS)
- Schemas (file XSD di metadatazione)

- 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 SdI 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 metadatazione, 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.

tinexta
infocert

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:

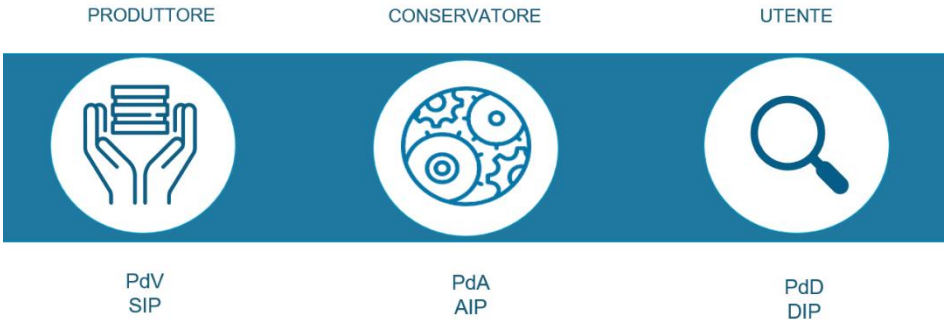


Figura 1 disegno di processo

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, immodificabilità 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**, contente 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 architetturale 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, contente 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 metadatazione.
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 autorizzazion

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 architetturali, 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 scelto 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 prioritizzate 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 indentificare 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 architetturalmente 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:

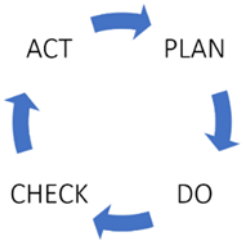


Figura 2 Rappresentazione del modello PDCA SMS

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

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

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

Nello specifico 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 consentedo 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.

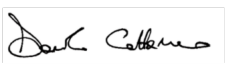
SPECIFICITÀ DEL CONTRATTO

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