

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI DOCUMENTI E DELL'ARCHIVIO

ALLEGATO 13 MANUALE DELLA CONSERVAZIONE DEI DOCUMENTI DIGITALI

INDICE

1	Introduzione al documento	3
1.1	Gestione versioni documento	3
1.2	Scopo e campo di applicazione del documento.....	3
1.3	Principi di redazione.....	3
1.4	Termini e definizioni	4
1.5	Acronimi.....	9
2	Nomine e individuazione dei compiti.....	10
2.1	Cliente/Soggetto Produttore: ESU.....	10
2.2	Referenti di processo	10
2.3	Responsabile della Conservazione	11
3.	La conservazione dei documenti	16
3.1	Il ruolo del Responsabile della Conservazione	17
4	Il sistema di creazione e gestione dei documenti.....	19
4.1	Controlli.....	19
4.2	Indicizzazione dei documenti	19
4.3	Gestione delle anomalie	19
4.4	Formato dei documenti elettronici	19
5	Il sistema di conservazione DIGITALE	20
5.1	Descrizione generale del servizio.....	20
6	Le tipologie documentali	21
	Decreto	21
	Registro di protocollo.....	21
	Contratto.....	21
	Documento protocollato	22
	FatturaPA.....	22
6.1	Fasi del processo per i versamenti da Interfaccia Utente WEB (caricamento manuale).....	23
6.2	Fasi del processo per i versamenti da connettore ADS	24
7	Il processo di conservazione	26
7.1	Processi di front-end.....	26
7.2	Processi di back-end.....	26
7.3	Tabella di Responsabilità	27
8	Procedure di ricerca ed esibizione	28
8.1	Requisiti software.....	28
9	Modifica dei documenti posti in conservazione	29
9.1	Procedura di rettifica: schema generale.....	29
10	Misure di sicurezza	30
10.1	ESU	30
10.2	TITT	30
11	Note conclusive	31
11.1	Protezione dei dati personali	31
12	Allegati	32
12.1	Documentazione contrattuale di riferimento	32

1 INTRODUZIONE AL DOCUMENTO

1.1 Gestione versioni documento

Versione:	01	Data Versione:	settembre 2014
Descrizione modifiche:	Nessuna		
Versione:	02	Data Versione:	settembre 2016
Descrizione modifiche:	Aggiornamento DPCM 13 novembre 2014		
Versione:	03	Data Versione:	aprile 2019
Descrizione modifiche:	Aggiornamento Manuale Conservazione a seguito adesione Convenzione SPC Cloud		
Versione:	04	Data Versione:	dicembre 2025
Descrizione modifiche:	Aggiornamento Manuale Conservazione a seguito modifiche organizzative e normative		

1.2 Scopo e campo di applicazione del documento

Il presente documento è il Manuale dei processi documentali del servizio di Conservazione digitale acquisito tramite la convenzione Consip SPC Cloud, dove tale servizio viene erogato dal Conservatore accreditato Telecom Italia Trust Technologies s.r.l.

Come richiesto dal DPCM del 2013 all'art. 8, il presente documento “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 d'ispezione da parte delle autorità di vigilanza preposte, il Manuale della Conservazione, integrato con il presente Manuale dei processi documentali per la conservazione, permette un agevole svolgimento di tutte le attività di controllo.

Si precisa che il presente documento integra e dettaglia il Manuale della Conservazione di Telecom Italia Trust Technologies disponibile nei siti:

<https://www.trusttechnologies.it/>

<http://www.agid.gov.it/>

1.3 Principi di redazione

La redazione del Manuale della Conservazione di ESU è ispirata ai seguenti principi:

- **Principio di Trasparenza**, il Manuale mira a fornire una chiara spiegazione del sistema di conservazione documentale e dei processi erogati;

- **Ottica di processo**, il documento mira a descrivere le fasi dei processi, non il dettaglio tecnico degli strumenti utilizzati, ad uso interno e a fini ispettivi;
- **Principio di Rilevanza**: nel Manuale sono contenute solamente le informazioni rilevanti, con un livello di dettaglio mirante ad agevolare le ispezioni, senza dettagli tecnici superflui;
- **Principio di Accuratezza**: le informazioni sono state revisionate da più persone, poste ai diversi livelli della catena decisionale.

1.4 Termini e definizioni

<i>ACCESSO</i>	operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici.
<i>ACCREDITAMENTO</i>	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.
<i>AFFIDABILITA'</i>	caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico.
<i>AGGREGAZIONE DOCUMENTALE INFORMATICA</i>	aggregazione 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.
<i>ARCHIVIAZIONE</i>	è il processo di trattamento e gestione dei documenti di uso corrente e/o nel medio lungo periodo. È passo propedeutico alla conservazione, per il quale non sono previsti particolari obblighi di legge.
<i>ARCHIVIO</i>	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.
<i>ARCHIVIO INFORMATICO</i>	archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico.
<i>AREA ORGANIZZATIVA OMOGENEA</i>	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.
<i>ATTESTAZIONE DI CONFORMITA' DELLE COPIE PER IMMAGINE SU SUPPORTO INFORMATICO DI UN DOCUMENTO ANALOGICO</i>	dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.

<i>AUTENTICITA'</i>	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.
<i>BASE DATI</i>	collezione di dati registrati e correlati tra loro.
<i>CERTIFICATORE ACCREDITATO</i>	soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza.
<i>CICLO DI GESTIONE</i>	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.
<i>CLASSIFICAZIONE</i>	attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici.
<i>CODICE</i>	decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni.
<i>CODICE ESEGUIBILE</i>	insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici.
<i>CONSERVATORE ACCREDITATO</i>	soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, dall'Agenzia per l'Italia digitale.
<i>CONSERVAZIONE</i>	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, descritto nel presente manuale di conservazione e che risponde a quanto stabilito nel DPCM 03/12/2013.
<i>COPIA ANALOGICA DI UN DOCUMENTO INFORMATICO</i>	documento analogico avente contenuto identico a quello del documento informatico da cui è tratto.
<i>COPIA DI SICUREZZA</i>	copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 del DPCM del 3 dicembre 2013.
<i>DOCUMENTO ANALOGICO</i>	Rappresentazione analogica di atti, fatti o dati giuridicamente rilevanti.
<i>DOCUMENTO INFORMATICO</i>	la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
<i>DATI PARTICOLARI</i>	dati personali (sensibili) idonei a rivelare l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale.

<i>ESIBIZIONE</i>	operazione che consente di visualizzare un documento conservato e di ottenerne copia.
<i>EVIDENZA INFORMATICA</i>	una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.
<i>EXTENSIBLE MARKUP LANGUAGE</i>	linguaggio derivato dall'SGML (Standard Generalized Markup Language), metalinguaggio che permette di creare altri linguaggi. Mentre l'HTML è un'istanza specifica dell'SGML, XML costituisce a sua volta un metalinguaggio, più semplice dell'SGML, largamente utilizzato per la descrizione di documenti sul Web. L'XML viene utilizzato per definire le strutture dei dati invece che per descrivere come questi ultimi devono essere presentati. Tali strutture vengono definite utilizzando dei marcatori (markup tags). Diversamente dall'HTML, l'XML consente all'utente di definire marcatori personalizzati, dandogli il controllo completo sulla struttura di un documento. Si possono definire liberamente anche gli attributi dei singoli marcatori.
<i>FASCICOLO INFORMATICO</i>	Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del Codice.
<i>FIRMA DIGITALE</i>	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 (art. 1 comma 1 lettera s) Decreto Legislativo del 7 marzo 2005 n. 82).
<i>FIRMA ELETTRONICA</i>	l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica (art. 1 comma 1 lettera q) Decreto Legislativo del 7 marzo 2005 n. 82).
<i>FIRMA ELETTRONICA QUALIFICATA</i>	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 (art. 1 comma 1 lettera r) Decreto Legislativo del 7 marzo 2005 n. 82).
<i>FIRMA ELETTRONICA AVANZATA</i>	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 (art. 1 comma 1 lettera q-bis) Decreto Legislativo del 7 marzo 2005 n. 82). Si vedano anche le regole tecniche, pubblicate nella G.U. il 21 maggio 2013.

FORMATO	modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
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. Detto anche token LegalDoc.
IMMODIFICABILITA'	caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso.
IMPRONTA DI UNA SEQUENZA DI SIMBOLI BINARI (o HASH)	una funzione matematica che genera, a partire da una evidenza informatica, una 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.
INSIEME MINIMO DI METADATI DEL DOCUMENTO INFORMATICO	complesso dei metadati, la cui struttura è descritta nell'allegato 5 del DPCM del 3 dicembre 2013, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta.
INTEGRITA'	insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato.
INTEROPERABILITA'	capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi.
LEGGIBILITA'	insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti.
MARCA TEMPORALE	il riferimento temporale che consente la validazione temporale, così come definita all'art. 1 comma 1 lettera i) DPCM del 30 marzo 2009. La marca temporale è opponibile ai terzi, definita anche nel DPCM 22 febbraio 2013, titolo IV.
SIGILLO ELETTRONICO	è stato introdotto nel nostro ordinamento con l'emanazione del Regolamento eIDAS. Sostanzialmente è equivalente a una firma elettronica qualificata, con la differenza che non afferisce a una persona fisica, bensì a una persona giuridica.
METADATI	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 del DPCM del 3 dicembre 2013.
PACCHETTO INFORMATIVO	contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare.

<i>PORTABLE DOCUMENT FORMAT</i>	formato di file creato da Adobe Systems nel 1993 per lo scambio di documenti. Il PDF è un formato a schema fisso basato su un linguaggio di descrizione di pagina che permette di rappresentare documenti in modo indipendente dall'hardware, dal software e dal sistema operativo; ogni PDF incapsula una descrizione completa del documento, che include testo, caratteri, immagini e grafica. PDF è uno standard aperto; recentemente la versione PDF/A (PDF Reference Version 1.4) è stata riconosciuta dall'International Organization for Standardization (ISO) con la norma ISO 19005:2005.
<i>POSTA ELETTRONICA CERTIFICATA</i>	sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici.
<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>PRODUTTORE</i>	persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con Responsabile della gestione documentale .
<i>RAPPORTO DI VERSAMENTO</i>	documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore; in LegalDoc è l'insieme degli Indici del Pacchetto di Archiviazione associati ad ogni documento inviato in conservazione in un'unica sessione, che fanno parte del pacchetto di versamento.
<i>RESPONSABILE DELLA CONSERVAZIONE</i>	il soggetto cui sono attribuite funzioni, adempimenti, attività e responsabilità relative al processo di conservazione ottica conformemente a quanto previsto all'art. 7 del DPCM 03/12/2013.
<i>RIFERIMENTO TEMPORALE</i>	informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici, così come definito all'art. 1 comma 1 lettera m) DPCM del 30 marzo 2009, definito anche nel DPCM 22 febbraio 2013.
<i>SCARTO</i>	operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale.
<i>STATICITA'</i>	Caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione.
<i>UTENTE</i>	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 AGLI ARCHIVI DI STATO	operazione con cui il Responsabile della conservazione di un organo giudiziario o amministrativo dello Stato 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.
---	--

1.5 Acronimi

CA	Certification Authority
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione, successivamente DigitPA ora Agenzia per l'Italia Digitale
D. LGS	Decreto Legislativo
DPCM	Decreto del Presidente del Consiglio dei Ministri
GU	Gazzetta Ufficiale della Repubblica Italiana
HSM	Hardware Security Module
PDF	Portable Document Format
PEC	Posta Elettronica Certificata
SG	Sistema di Gestione
SGD	Sistema di Gestione Documentale
SSL	Secure Socket Layer
TSA	Time Stamping Authority
TSS	Time Stamping Service
TU	Testo Unico
URL	Uniform Resource Locator
XML	Extensible Markup Language

2 NOMINE E INDIVIDUAZIONE DEI COMPITI

In questo capitolo sono individuati i differenti soggetti che intervengono a vario titolo nelle diverse fasi del processo di creazione dei documenti elettronici e conservazione elettronica documentale.

2.1 Cliente/Soggetto Produttore: ESU

ESU	
Sede Amministrativa	Via San Francesco, 122, 35121 Padova
Recapiti	049 823 5611
Sito web	www.esu.pd.it
Partita Iva	00815750286

2.2 Referenti di processo

Nominativo dei soggetti incaricati della gestione del sistema di creazione dei documenti e di invio dei documenti in conservazione.

Nome e Cognome	Responsabile della Conservazione interno – Stefano Ferrarese
Ente/Società	Direttore ESU
Data inizio incarico	1° Agosto 2014
Data termine incarico	1 Febbraio 2022

Nome e Cognome	Gabriele Verza
Ente/Società	Direttore ESU
Data inizio incarico	2 Febbraio 2022
Data termine incarico	Data di termine del contratto

Tipologia documentale di competenza	Documenti inerenti al Protocollo, contratti e atti repertoriati (Decreti e delibere)
Nome e Cognome	Referente di processo – Roberta Valente
Ente/Società	ESU
Data inizio incarico	1° Agosto 2014
Data termine incarico	31 Ottobre 2020

Tipologia documentale di competenza	Documenti inerenti al Protocollo, contratti e atti repertoriati (Decreti e delibere)
Nome e Cognome	Referente di processo – M. Cristina Betteto
Ente/Società	ESU
Data inizio incarico	1° Aprile 2021
Data termine incarico	Data di termine incarico

Tipologia documentale di competenza	Documenti di Gara
Nome e Cognome	Referente di processo – Ermanno Lion
Ente/Società	ESU
Data inizio incarico	2014
Data termine incarico	15 Febbraio 2016

Tipologia documentale di competenza	Documenti di Gara
Nome e Cognome	Referente di processo – Ezio Pavan
Ente/Società	ESU
Data inizio incarico	1° Aprile 2016
Data termine incarico	Data di termine incarico

Tipologia documentale di competenza	Fatture e documenti contabili e fiscali
Nome e Cognome	Referente di processo – Giampietro Parolin
Ente/Società	ESU
Data inizio incarico	31 Marzo 2015
Data termine incarico	Data di termine incarico

2.3 Responsabile della Conservazione

ESU, avvalendosi della facoltà prevista dall'art. 5, comma 1, b) del DPCM 03/12/2013 ha affidato lo svolgimento delle attività del **Responsabile del servizio della Conservazione** ad un soggetto terzo che, per competenza ed esperienza, garantisce lo svolgimento delle suddette attività.

Le attività sono state affidate a **Telecom Italia Trust Technologies** tramite la sottoscrizione del contratto esecutivo, CIG Z44385AE7A, per la fruizione dei servizi di Cloud Computing – Consip SPC Cloud lotto 1.

Telecom Italia Trust Technologies assume l'incarico di svolgere le attività delegate dal Responsabile della Conservazione in accordo con quanto previsto dal contratto, dagli allegati

contrattuali e dall'articolo dall'art. 5, comma 1, b) del DPCM 03/12/2013 e dalla precedente Deliberazione CNIPA 11/2004.

L'atto di affidamento per lo svolgimento delle attività del Responsabile del servizio della Conservazione è stato conferito da ESU a Telecom Italia Trust Technologies contestualmente alla sottoscrizione del contratto di adesione ai servizi di Cloud Computing SPC Cloud lotto 1 – Servizio SaaS di Conservazione Digitale.

Telecom Italia Trust Technologies S.r.l, di seguito TI Trust Technologies o TITT, è una società del gruppo Telecom Italia, che presenta forti competenze nei diversi ambiti tecnologici oggetto della presente offerta ed ha acquisito negli anni una profonda conoscenza del contesto di gara in qualità di principale attore nella progettazione, realizzazione e gestione dell'attuale piattaforma di Certification Authority (nel seguito CA) per numerosi clienti istituzionali della pubblica amministrazione. Tale conoscenza si estende anche e soprattutto alle modalità organizzative e operative specifiche dei servizi erogati.

Presente sul mercato dei servizi di certificazione digitale a norma da oltre dieci anni, l'offerta di TITT si caratterizza per gli altissimi livelli di sicurezza e di performance, che vanno ben oltre i requisiti tecnico-organizzativi previsti dalla legge e che sono verificati continuamente da AgID nel corso delle periodiche attività ispettive. Ciò grazie all'eccellenza delle proprie competenze e dei propri sistemi, supportati e integrati dalle infrastrutture del Gruppo Telecom Italia.

Il continuo aggiornamento di tali competenze e infrastrutture agisce trasversalmente sugli elementi comuni a tutti i servizi erogati:

- Certification Authority: la PKI per l'emissione e la gestione di certificati digitali necessari ai servizi di firma digitale e marcatura temporale dei documenti informatici.
- Posta Elettronica Certificata: per l'erogazione del servizio di certificazione delle comunicazioni di posta elettronica per la trasmissione dei documenti informatici da e verso la pubblica amministrazione.
- Conservazione: per la conservazione a norma dei documenti informatici che hanno validità per lunghi periodi temporali.
- Identity Provider (IdP) per il Servizio SPID: per la gestione dell'Identità Digitale SPID (Sistema Pubblico di Identità Digitale).
- Competence Center: il pool di risorse dedicato con know-how specifico sulle tecnologie di certificazione digitale e sulle strutture di PKI, continuamente aggiornato attraverso attività di scouting e di contatto con i principali vendor del settore. Il Competence Center è a disposizione dei clienti che necessitano di un supporto tecnico e consulenziale puntuale per risolvere le problematiche relative alla progettazione dei servizi, alla definizione delle policy di gestione, al disegno delle architetture ed al project management.
- Help Desk 24h/24: fornisce supporto in linea su hardware e software ed è a disposizione 24 ore su 24 per interventi urgenti quali la risoluzione di inconvenienti o la revoca dei certificati digitali.

TI Trust Technologies opera secondo un Sistema di Gestione della Qualità (SGQ) e della Sicurezza delle Informazioni (SGSI) certificato rispetto alle norme ISO 9001:2008 e ISO27001:2013 per i processi e le attività svolte all'interno dell'azienda in merito alla progettazione, sviluppo, system integration, delivery ed esercizio di servizi e soluzioni basati sulle tecnologie di crittografia a chiave pubblica.

Tutta l'infrastruttura di TITT opera all'interno di aree riservate dei Data Center di Telecom Italia, caratterizzate dai più elevati livelli di affidabilità e di sicurezza. In modo particolare, TITT fa della sicurezza dei dati, delle informazioni e dei servizi dei Clienti, una parte fondamentale

del proprio lavoro che non è solo tecnologia, ma si declina in un articolato sistema di componenti: qualità, legalità, valori e gestione integrata.

Sicurezza sinonimo di qualità: garantire e preservare la qualità dei servizi, integrando il concetto stesso di sicurezza in ogni fase dei processi operativi del Sistema Integrato per la Gestione della Qualità e della Sicurezza delle Informazioni (certificato secondo gli standard ISO9001:2008, ISO27001:2013 e WebTrust®).

Sicurezza sinonimo di rispetto della legalità: il Modello Organizzativo 231 adottato è finalizzato a garantire che tutte le operazioni (da quelle operative a quelle di natura amministrativa) siano “monitorate” a tutela delle risorse che operano per garantire la migliore qualità del servizio e di tutti coloro che entrano in contatto con l'organizzazione TI Trust Technologies (clienti, fornitori, stakeholders).

Sicurezza sinonimo di valori: TI Trust Technologies considera le informazioni come beni essenziali, da proteggere applicando una definizione di sicurezza delle informazioni molto solida ed estesa, basata su principi e requisiti fondamentali. Quale società appartenente al Gruppo Telecom Italia, TI Trust Technologies adotta rigide linee guida di sicurezza, focalizzando l'attenzione sull'organizzazione e sui processi, basati su obiettivi e valori fondamentali: tutela delle risorse umane interne ed esterne al Gruppo, salvaguardia del valore degli asset, immagine e reputazione, continuità operativa nell'erogazione dei servizi.

Sicurezza sinonimo di sistema: l'approccio alla sicurezza di TI Trust Technologies è frutto di un livello molto spinto delle componenti che lavorano in modo integrato per garantire il più alto livello di protezione ai nostri Clienti:

- **Sicurezza Fisica:** protezione dei perimetri esterni, controllo accessi alle sedi degli uffici del Data Center e dell'archivio, infrastrutture di sicurezza e prevenzione del Data Center (sistemi anti-intrusione, ridondanza dei cablaggi energia e rete, continuità elettrica, antincendio, antiallagamento, controllo HVAC –heating, ventilation & air conditioning), facility monitoring.
- **Sicurezza Logica:** firewalling, intrusion detection systems, antivirus, controllo delle vulnerabilità, ridondanza, protocolli sicuri, profilazione ed amministrazione delle utenze, credential management, vulnerability assessment & patching, backup and restore planning.
- **Continuità operativa:** l'infrastruttura di continuità operativa assicura il controllo e la mitigazione dei rischi che potrebbero derivare da eventuali blocchi operativi e, in ogni caso, il ripristino nel più breve tempo possibile. Il nostro piano di continuità operativa TI Trust Technologies prende in considerazione i seguenti scenari:
 - **distruzione o inaccessibilità** dei locali tali da rendere impossibile accedere ai siti necessari per l'erogazione dei servizi;
 - **indisponibilità del personale essenziale**, intesa come assenza prolungata di un numero considerevole o di tutte le persone necessarie per lo svolgimento dei servizi;
 - **interruzione del funzionamento delle infrastrutture**, che richiede l'attivazione del **sito di disaster recovery**. Si fa riferimento, ad esempio, al caso di interruzione dell'erogazione dell'energia elettrica o del funzionamento dei servizi di fonia, oppure alla violazione di una o più condizioni vincolanti per l'erogazione dei servizi di Certification Authority (ad esempio a causa del guasto

di uno o più dei dispositivi utilizzati per erogare i servizi di certificazione o della compromissione, anche accidentale, di una o più chiavi private di certificazione.

Dati identificativi e iscrizione a elenchi pubblici

I dati identificati di TI Trust Technologies sono descritti di seguito:

Denominazione e Ragione Sociale	TI Trust Technologies S.r.l.
Sede Legale	S.S. 148 Pontina, km. 29,100 00071 Pomezia RM
Telefono	+3906911971
Fax	+390691197331
Sede Operativa	S.R. 148 Pontina, km. 29,100 00071 Pomezia RM
Indirizzo Internet	https://www.trusttechnologies.it/
Call Center	800.28.75.24

Accreditamenti e qualificazioni

La Società è iscritta nei seguenti elenchi pubblici tenuti dall'autorità di vigilanza sui servizi da essa erogati:

- Dal 2015, [gestori dell'Identità Digitale](#) in ambito SPID;
- Dal 2014, [elenco dei conservatori accreditati](#) per il servizio di conservazione dei documenti informatici;
- Dal 2005 (già come IT Telecom), [elenco dei gestori del servizio di PEC](#) (Posta Elettronica Certificata);
- Dal 2000 (già come Saritel S.p.A., IT Telecom S.p.A. e I.T. Telecom S.r.l.), [elenco dei certificatori di firma qualificata](#).

Dal novembre 2012 la società ha ottenuto la Certificazione del proprio Sistema di Gestione della Sicurezza delle Informazioni (SGSI) alla normativa ISO 27001, a cura dell'Ente IMQ. L'obiettivo di TI Trust Technologies, con l'adozione dello standard ISO 27001, è quello di:

- garantire la robustezza e la congruenza dell'architettura di sicurezza posta a tutela delle risorse attraverso le quali vengono erogati i servizi ai clienti;
- consolidare, attraverso l'accreditamento di un organismo esterno riconosciuto dalla comunità internazionale, la capacità di erogare servizi tra i più innovativi nel campo della ICT security ed in linea allo standard di sicurezza ISO 27001;
- normalizzare l'infrastruttura interna attraverso la strutturazione programmata di controlli di natura organizzativa e procedurale;
- acquisire un elemento distintivo e di vantaggio rispetto alla concorrenza e come tale contribuire al miglioramento della propria posizione e di quella di Telecom Italia sul mercato;

- tutelare gli interessi propri e dei clienti, ponendo particolare attenzione agli aspetti elencati di seguito:
 - *riservatezza* o *confidenzialità* delle informazioni, attraverso lo sviluppo e l'implementazione di meccanismi e contromisure atte ad impedire che l'informazione sia disponibile o venga rivelata a individui, entità o processi non autorizzati;
 - *integrità* delle informazioni, attraverso lo sviluppo e l'implementazione di meccanismi e contromisure atte a impedire che l'informazione sia modificata o distrutta in maniera non autorizzata;
 - *disponibilità* delle informazioni, attraverso lo sviluppo e l'implementazione di meccanismi che consentano all'informazione di essere accessibile ed utilizzabile quando richiesta da un'entità autorizzata;
 - mantenimento del *livello di servizio*, attraverso lo sviluppo e l'implementazione di meccanismi che garantiscano la continuità del servizio erogato nel rispetto dei dati di targa e degli SLA definiti;
 - *conformità*, in termini di rispetto dei requisiti e dei vincoli di natura legale, normativa o contrattuale.
- Seguendo le linee guida sopra illustrate, la società ha predisposto una serie di attività in grado di portare a valori accettabili il livello di rischio residuo associato all'erogazione dei propri servizi, cercando, in tal modo, di soddisfare uno degli obiettivi strategici più importanti della propria *mission*.

Nel novembre 2016 IMQ, ente accreditato da Accredia per la valutazione di conformità EIDAS e ETSI EN 319 403, per la valutazione dei Prestatori di servizi fiduciari e dei servizi da essi forniti, ha certificato TI **TRUST TECHNOLOGIES** come **Qualified Trusted Service Provider per il servizio di Validazione Temporale elettronica**: con il riconoscimento dell'Agenzia per l'Italia Digitale, TI Trust Technologies può erogare servizi che hanno pieno valore legale in tutto il territorio dell'UE.

TITT eroga i servizi di Conservazione per conto di TIM, a seguito dell'aggiudicazione del Lotto 1 – Servizi di Cloud Computing - della “Procedura ristretta, suddivisa in 4 lotti, per l'affidamento dei servizi Cloud Computing, di Sicurezza, di realizzazione di Portali e Servizi online e di Cooperazione applicativa per le Pubbliche Amministrazioni (ID SIGEF 1403)” Consip S.p.A., ha stipulato un Contratto Quadro con il RTI Aggiudicatario, composto dalle aziende Telecom Italia S.p.A, Enterprise Services Italia S.r.l., Poste Italiane S.p.A. Postel S.p.A. e Postecom S.p.A..

3. LA CONSERVAZIONE DEI DOCUMENTI

L'implementazione e la gestione dei processi di creazione e conservazione dei documenti elettronici è un'operazione che si avvale di numerosi strumenti ed elementi, regolata da apposite discipline che vanno raccordate a quella generale della conservazione.

Di seguito si richiamano i principali strumenti ed elementi:

- **Documento informatico:** è una realtà immateriale e il tipo di supporto fisico sul quale esso è registrato è irrilevante per la natura del documento stesso.
Del documento informatico, a differenza di quello cartaceo, è possibile avere molteplici esemplari, tutti giuridicamente rilevanti e aventi identico valore legale. Per le sue caratteristiche, il documento informatico necessita di strumenti di validazione informatica efficaci e sicuri affinché ne siano garantite, in particolare, l'integrità e l'autenticità. Esemplicando, la gestione di un documento informatico non può prescindere dalla disponibilità di un elaboratore e dei relativi programmi necessari sia per "formare" il documento che per "leggerlo" e verificarne autenticità, integrità e paternità.
- **Documento analogico:** in generale, è quello che per la sua formazione utilizza una grandezza fisica che assume valori continui come, ad esempio, le tracce continue su carta per il documento cartaceo o le immagini continue per il film. Il supporto fisico su cui si può formare il documento analogico non è necessariamente quello cartaceo, ma può essere film, lastra o pellicola radiologica, microfilm, nastro audio e video. Il documento analogico può essere originale, a sua volta distinto in originale unico e non unico, o copia.
- **Firma digitale:** è l'elemento principale che interviene nella gestione elettronica del documento informatico dalla formazione, alla trasmissione, fino alla conservazione, poiché conferisce piena validità legale al documento cui è apposta, assicurando autenticità, integrità, non ripudiabilità.
- **Attestazione temporale:** per stabilire il momento temporale in cui un documento informatico è stato formato è necessario attribuirgli una "validazione temporale", definita come il risultato di una procedura informatica in grado di offrire un riferimento temporale opponibile ai terzi. Lo strumento per ottenere questo risultato è la marca temporale, una particolare firma elettronica che contiene l'ora e la data in cui è stata generata ed è opponibile ai terzi.

Il fine ultimo del processo di conservazione è rendere un documento inalterabile e imm modificabile, in modo che possa essere disponibile nel tempo nella propria autenticità ed integrità.

In linea generale non sono previste autorizzazioni preventive per l'adozione di criteri operativi per effettuare la conservazione. Per effettuare la riproduzione e la conservazione dei documenti su supporti digitali, tuttavia, è necessario rispettare le regole tecniche previste dal Ministero dell'Economia e delle Finanze con il Decreto del 17 giugno 2014, dai Decreti del Presidente del Consiglio dei Ministri del 3 dicembre 2013 e 13 novembre 2014.

3.1 Il ruolo del Responsabile della Conservazione

Come già per la deliberazione AIPA n. 42/2001, la deliberazione CNIPA n. 11/2004 (art. 5) le Regole Tecniche del DPCM 03/12/2013 enfatizzano il ruolo del Responsabile della Conservazione di documenti in formato digitale che assume un ruolo fondamentale all'interno del processo di conservazione, insieme ai suoi delegati o ai terzi affidatari.

La presenza del Responsabile della Conservazione è necessaria sia in ambito privato sia in ambito pubblico e vi sono attribuiti compiti debitamente elencati, riguardanti le funzioni, gli adempimenti, le attività e le responsabilità. Il Responsabile della Conservazione è tenuto a gestire il processo in coerenza con quanto stabilito dalla normativa in vigore.

Uno degli obiettivi principali del Responsabile della Conservazione è di definire ed impostare il processo per il trattamento della documentazione soggetta a conservazione.

Più in particolare (art. 7 del DPCM 03/12/2013):

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

m) predisporre il manuale di conservazione di cui all'art. 8 e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

[...]

Art. 5

Ai sensi dell'art. 44 del Codice dell'Amministrazione Digitale, la conservazione può essere svolta:

[...]

b) affidandola, in modo totale o parziale, ad altri soggetti, pubblici o privati che offrono idonee garanzie organizzative e tecnologiche, anche accreditati come conservatori presso l'Agenzia per l'Italia digitale.

Al Responsabile della Conservazione sono attribuiti compiti cruciali in ragione del controllo e della supervisione che egli attua sull'intero procedimento di conservazione.

Gli adempimenti comprendono non solo attività di pianificazione, ma anche attività di tipo operativo/esecutivo, che può essere necessario svolgere in sedi diverse e magari distanti tra di loro.

Le Regole Tecniche all'art. 5 consentono di delegare in tutto o in parte le attività previste ad altri soggetti interni alla struttura e/o di affidarle a soggetti terzi (pubblici o privati) i quali sono tenuti ad osservare le disposizioni contenute nel decreto stesso.

4 IL SISTEMA DI CREAZIONE E GESTIONE DEI DOCUMENTI

Si rimanda al Manuale di Gestione del Protocollo e degli Archivi (e/o a qualsiasi regolamento interno condiviso sulla gestione documentale) di ESU per la descrizione funzionale ed operativa del sistema di gestione informatica dei documenti adottato da esso, con particolare riferimento alle modalità di utilizzo dello stesso.

4.1 Controlli

Ai sensi di legge, ESU assicura che i documenti inviati in conservazione sono statici e non modificabili, ovvero redatti in modo tale per cui il contenuto non possa essere alterabile durante le fasi di conservazione ed accesso ed è immutabile nel tempo.

4.2 Indicizzazione dei documenti

ESU provvede all'indicizzazione dei documenti utilizzando le funzioni messe a disposizione dai sistemi di gestione dei documenti o dall'interfaccia web del servizio di Conservazione (Legal Archive) compilando la maschera di metadati associati ad ogni tipologia documentale e definiti in fase contrattuale.

4.3 Gestione delle anomalie

Il sistema di conservazione è configurato per accettare solo documenti in formati prestabiliti. Al venir meno di questa condizione, sopraggiungendo l'impossibilità di accettare il documento, il sistema lascia in attesa il documento in entrata senza immetterlo nel sistema di conservazione e contestualmente segnala l'anomalia a ESU.

4.4 Formato dei documenti elettronici

Le nuove Regole Tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 (GU Serie Generale n.59 del 12-3-2014 - Suppl. Ordinario n. 20) elencano in modo specifico i formati documentali da adottare per la conservazione a lungo termine dei documenti, ovvero le modalità di organizzazione delle informazioni in un codice binario nel loro allegato 2. Pertanto ESU ha deciso l'invio in conservazione soltanto di formati:

- .pdf
- .tif - tiff - gif - bmp
- .jpg - .jpeg
- .doc - .docx - .xls - .xlsx - .ppt - .pptx
- .ods - .odp - .odg - .odt
- .xml - .html - .xhtml - .pages - .json
- .txt - csv
- .dwg - .zip
- .eml - .msg
- .p7m - .p7s - .p7e
- Mp4

5 IL SISTEMA DI CONSERVAZIONE DIGITALE

5.1 Descrizione generale del servizio

Per la descrizione generale del servizio di Conservazione a norma si rimanda all'allegato "EVOCST01.TT.DPMU14001.07 - Descrizione del Servizio Conservazione a norma.pdf" reperibile anche sul sito <https://www.trusttechnologies.it/> dove è pubblicato e costantemente aggiornato alla versione più recente.

6 LE TIPOLOGIE DOCUMENTALI

Decreto

<i>Tipologia di documento</i>	Decreto (Atto monocratico)
<i>Natura del documento</i>	Originale digitale firmato digitalmente
<i>Data di decorrenza del processo di conservazione elettronica</i>	1° Aprile 2015
<i>Modalità di versamento</i>	Tipologia documentale inviata in conservazione in cooperazione applicativa tra Sistema di gestione documentale e Conservatore

Delibera

<i>Tipologia di documento</i>	Delibera (Atto collegiale)
<i>Natura del documento</i>	Originale digitale firmato digitalmente
<i>Data di decorrenza del processo di conservazione elettronica</i>	5 Settembre 2019
<i>Modalità di versamento</i>	Tipologia documentale inviata in conservazione in cooperazione applicativa tra Sistema di gestione documentale e Conservatore

Registro giornaliero di protocollo

<i>Tipologia di documento</i>	Registro giornaliero di protocollo
<i>Natura del documento</i>	Originale digitale
<i>Data di decorrenza del processo di conservazione elettronica</i>	1° Agosto 2014
<i>Modalità di versamento</i>	Tipologia documentale inviata in conservazione in cooperazione applicativa tra Sistema di gestione documentale e Conservatore

Contratto

<i>Tipologia di documento</i>	Contratto
<i>Natura del documento</i>	Originale digitale firmato digitalmente
<i>Data di decorrenza del processo di conservazione elettronica</i>	Da 1° Gennaio 2014 a 31 dicembre 2023 (manualmente) Da 1° gennaio 2024 informatizzato
<i>Modalità di versamento</i>	Tipologia documentale inviata in conservazione in cooperazione applicativa tra Sistema di gestione documentale e Conservatore

Documento protocollato

Tipologia di documento	Documento protocollato
Natura del documento	Originale digitale o copia digitale di originale analogico (scansione)
Data di decorrenza del processo di conservazione elettronica	13 marzo 2014
Modalità di versamento	Tipologia documentale inviata in conservazione in cooperazione applicativa tra Sistema di gestione documentale e Conservatore

FatturaPA attiva

Tipologia di documento	FatturaPA attiva
Natura del documento	Originale digitale firmato digitalmente
Data di decorrenza del processo di conservazione elettronica	1° aprile 2015
Modalità di versamento	Tipologia documentale inviata in conservazione in cooperazione applicativa tra Sistema di gestione documentale e Conservatore. Questa tipologia documentale è inviata in conservazione sia nella classe dedicata ai documenti protocollati, sia in apposita classe dedicata alla contabilità

FatturaPA passiva

Tipologia di documento	FatturaPA passiva
Natura del documento	Originale digitale firmato digitalmente
Data di decorrenza del processo di conservazione elettronica	1° aprile 2015
Modalità di versamento	Tipologia documentale inviata in conservazione in cooperazione applicativa tra Sistema di gestione documentale e Conservatore. Questa tipologia documentale è inviata in conservazione sia nella classe dedicata ai documenti protocollati, sia in apposita classe dedicata alla contabilità

Atto di liquidazione

<i>Tipologia di documento</i>	Atto di liquidazione
<i>Natura del documento</i>	Originale digitale firmato digitalmente
<i>Data di decorrenza del processo di conservazione elettronica</i>	5 settembre 2019
<i>Modalità di versamento</i>	Tipologia documentale inviata in conservazione in cooperazione applicativa tra Sistema di gestione documentale e Conservatore

PEC SIE (Sistema Informatico ESU)

<i>Tipologia di documento</i>	Documenti ricevuti/inviati tramite PEC
<i>Natura del documento</i>	Originale digitale
<i>Data di decorrenza del processo di conservazione elettronica</i>	Da 1° ottobre 2014 a termine contratto (giugno 2019)
<i>Modalità di versamento</i>	La conservazione dei messaggi e delle ricevute PEC SIE è un servizio integrato in Legalmail ed è erogato attraverso il servizio certificato e proprietario di InfoCert denominato LegalDoc all'interno della casella stessa

Di seguito l'analisi dettagliata del processo:

6.1 Fasi del processo per i versamenti da Interfaccia Utente WEB (caricamento web)

<i>Fase / Attività</i>	<i>Soggetti</i>	<i>Afferenza / Applicativi</i>	<i>Descrizione</i>
Redazione	Operatori ESU	Sistemi di video scrittura	Viene redatto il testo del documento.
Approvazione	Responsabili ESU	Eventuale firma digitale	Il documento viene approvato dai Responsabili competenti. Eventualmente vengono apposte le firme digitali a garanzia di integrità e immutabilità.

Versamento dei documenti	Referente di ESU	Interfaccia Utente WEB	I documenti vengono inviati al sistema di conservazione a seguito del caricamento manuale tramite una postazione pc, inserita nella rete internet di ESU, con compilazione manuale dei metadati e ricezione automatica dell'Indice di Conservazione/Rapporto di versamento.
Invio in conservazione	Referente di ESU	Legal Archive	Il sistema invia il documento in conservazione in modalità sincrona per ogni file.
Completamento del processo di conservazione	TITT	Legal Archive	Il sistema di conservazione Legal Archive eroga il processo di conservazione dei documenti secondo quanto dettagliato al capitolo 7.
Custodia dei supporti	TITT	Legal Archive	La custodia dei supporti è demandata a TITT come da accordi contrattuali.
Invio di Allegati	Referente di ESU	Legal Archive	L'invio di Allegati avviene mediante altro caricamento nell'interfaccia web avendo i medesimi metadati

6.2 Fasi del processo per i versamenti da connettore ADS

Fase / Attività	Soggetti	Afferenza / Applicativi	Descrizione
Redazione	Operatori ESU	Sistema di gestione documentale di ADS (moduli: Protocollo, Contabilità, Decreti)	Il documento viene ricevuto o redatto.
Estrazione CONNETTORE web service	Referente di ESU	Connettore sviluppato da ADS	L'operatore incaricato seleziona i documenti da inviare in conservazione attraverso apposita interfaccia del Gestionale ADS. Il connettore attraverso chiamate web service provvede all'invio in conservazione dei documenti selezionati.

<i>Completamento del processo di conservazione</i>	TITT	Legal Archive	Il sistema di conservazione eroga il processo di conservazione dei documenti secondo quanto dettagliato al capitolo 7.
<i>Custodia dei supporti</i>	TITT	Legal Archive	La custodia dei supporti è demandata ad TITT come da accordi contrattuali

7 IL PROCESSO DI CONSERVAZIONE

Il processo di conservazione attuato da TITT prevede l'utilizzo di diversi strumenti e l'intervento di soggetti che concorrono a rendere l'erogazione del servizio affidabile e rispondente ai requisiti richiesti dalla legge.

Ai fini del trattamento dei documenti destinati alla conservazione, il servizio si divide in due categorie di processi:

- processi di front-end;
- processi di back-end.

7.1 Processi di front-end

I processi di front-end sono erogati in modalità sincrona dal sistema Legal Archive, e sono finalizzati a mettere in comunicazione ESU con i servizi di back-end e sono richiamati in modalità on-line.

Per ciascuno dei servizi indicati di seguito si eseguono opportuni controlli di autenticazione del soggetto chiamante e di correttezza e accettabilità delle richieste:

- invio di un documento informatico o di un documento analogico opportunamente digitalizzato in conservazione;
- ricerca trasversale sulle classi documentali del documento da esibire;
- esibizione di un documento direttamente dal sistema Legal Archive;
- download del documento conservato con i relativi metadati contenuti nell'Indice di Conservazione.

7.2 Processi di back-end

I processi di back-end sono eseguiti dal sistema di Conservazione in modalità differita e sono i processi che, a partire dai documenti caricati sul sistema da ESU, implementano la conservazione in conformità alle regole tecniche contenute nel DPCM 03/12/2013.

Il processo di conservazione prevede l'elaborazione del singolo documento. Il documento viene, quindi, corredato da un file di indice, firmato digitalmente dal Responsabile del servizio della Conservazione, contenente informazioni sensibili ai fini della conservazione (indice del documento, impronte dei file che lo costituiscono, classificazione anagrafica dei firmatari). Ogni indice di conservazione di ogni file ha la firma del Responsabile del servizio della Conservazione, a garanzia della sua integrità e immutabilità.

7.3 Tabella di Responsabilità

<i>Attività</i>	<i>Responsabilità</i>	<i>ESU</i>	<i>Legal Archive Front-End</i>	<i>Legal Archive Back-End</i>	<i>Responsabile del servizio della Conservazione</i>
1. Formazione del documento	R – E				
2. Indicizzazione e archiviazione	R – E				
3. Acquisizione documento e creazione del file Indice di conservazione	V	R - E			
4. Invio al sistema di conservazione	R – E	R – E			
5. Verifica e accettazione del documento			E - V		
6. Creazione del file di Indice			E	R - V* - A	
7. Attestazione di corretto procedimento			E	R - V* - A	
8. Memorizzazione, creazione “copia di sicurezza” e chiusura del processo			E	R - V* - A	
[R-Responsabile; E-esegue; V- verifica; A-approva]					

(*) Tutte le verifiche in carico al Responsabile del servizio della Conservazione sono garantite anche dal servizio di auditing TITT.

8 PROCEDURE DI RICERCA ED ESIBIZIONE

Le procedure di esibizione del documento integrate in Legal Archive permettono, a partire dalla funzione di ricerca di estrarre dal sistema un documento di cui sia completata la procedura di conservazione.

L'applicazione realizzata in tecnologia web, permette ad un utente, precedentemente definito e in possesso delle debite autorizzazioni e credenziali, di accedere al sistema di conservazione da una qualsiasi stazione di lavoro (computer), purché collegata in rete e con disponibilità di un browser web.

Attraverso Legal Archive diventa possibile:

- estrarre un documento e visualizzarlo a video
- produrre copia cartacea o su altro supporto informatico del documento
- estrarre i visualizzatori memorizzati nel sistema di conservazione permettendone l'installazione sulla stazione dove si sta svolgendo l'esibizione
- prendere visione dei file a corredo che qualificano il processo di conservazione attestandone il corretto svolgimento
- verificare la validità delle firme digitali e delle marche temporali apposte nel processo di conservazione
- verificare l'integrità del documento.

L'esibizione del documento ottenuto tramite interrogazione al sistema Legal Archive rappresenta un'esibizione completa, legalmente valida ai sensi delle Regole Tecniche del 03/12/2013.

La funzione per l'esibizione è descritta in dettagli nel manuale utente "EVOCT01.IT_.DPMU14000.04-Conservazione-a-Norma-Manuale-Utente.pdf" disponibile sul sito www.trusttechnologies.it nella versione più aggiornata.

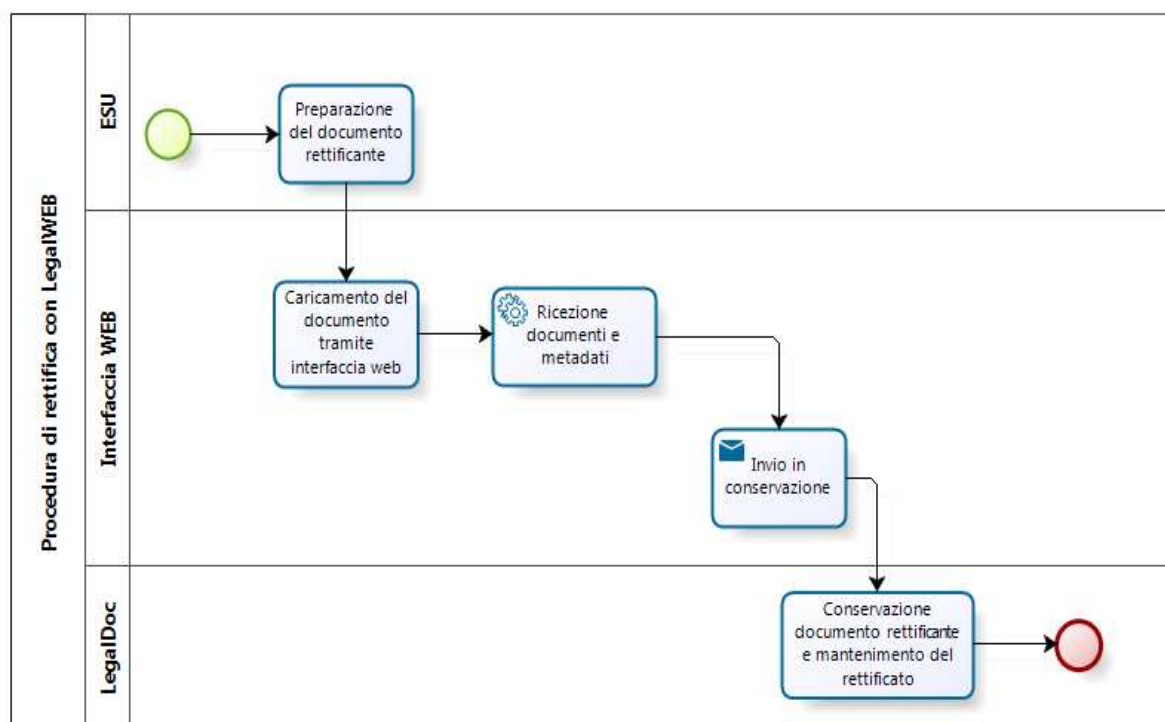
8.1 Requisiti software

Per la visualizzazione e la stampa del documento ottenuto con la procedura di esibizione da Legal Archive, ESU utilizza, per ognuno dei file costituenti il documento, il relativo viewer per i formati standard o depositato presso il sistema di conservazione per le altre tipologie di file.

9 MODIFICA DEI DOCUMENTI POSTI IN CONSERVAZIONE

In caso di modifica dei documenti già posti in conservazione, ESU provvede ad emanare ex novo un documento di rettifica che richiama il precedente e che verrà a sua volta conservato a norma; la riconducibilità del documento modificante a quello modificato è resa possibile grazie agli indici predisposti da ESU in fase di caricamento, che ne assicura la sistematicità e la coerenza.

9.1 Procedura di rettifica: schema generale



10 MISURE DI SICUREZZA

10.1 ESU

Per le misure di sicurezza nel trattamento dei documenti di ESU si rimanda all'apposito allegato al Manuale di Gestione del protocollo e degli archivi.

10.2 TITT

TITT opera in qualità di Conservatore accreditato, qualifica che viene rinnovata ogni due anni a valle di verifiche da parte degli organi di controllo (AGID, ACCREDIA). Si rimanda al Manuale della Conservazione la descrizione delle misure di sicurezza adottate.

11 NOTE CONCLUSIVE

11.1 Protezione dei dati personali

Nelle fasi di creazione, digitalizzazione, trattamento e invio in conservazione della documentazione cartacea e elettronica, ESU pone la massima cura al rispetto di quanto previsto in materia di privacy dal Regolamento UE n. 679/2016 (G.D.P.R “*General data Protection Regulation*”), dal D.lgs. 101/2018, nonché dai provvedimenti del Garante per la protezione dei dati personali.

Ai sensi dell'articolo 28 del GDPR, ESU ha nominato TI Trust Technologies Responsabile dei trattamenti dei dati necessari all'esecuzione del servizio.

In particolare, anche in considerazione del ruolo di Responsabile del servizio della Conservazione ricoperto, i compiti affidati a TI Trust Technologies attengono a qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la selezione, l'estrazione, l'interconnessione, la comunicazione, la cancellazione e la distruzione di dati.

TI Trust Technologies opera quale **Responsabile del trattamento** applicando le misure di sicurezza in base alle disposizioni legislative, regolamentari ed agli impegni contrattuali assunti.

L'informativa di cui all'articolo 13 del D.Lgs. 196/2003 (novellato dal GDPR) per i dati relativi al contratto è stata resa a ESU in allegato al materiale contrattuale da questi sottoscritto, ove viene altresì allo stesso consentito di esprimere il consenso per gli ulteriori trattamenti indicati.

12 ALLEGATI

12.1 Documentazione contrattuale di riferimento

Si fornisce di seguito un elenco dei documenti contrattuali a cui il Manuale si riferisce.

I documenti sotto riportati si intendono come riferimenti ufficiali: eventuali discrepanze fra quanto indicato nel Manuale e quanto presente nei documenti presenti nel seguente elenco si risolvono in favore di questi ultimi.

[1] Gara Cloud Lotto 1_Allegato D2_Contratto Esecutivo;

ID1800815750286001PJF - Progetto dei Fabbisogni_SPC Cloud - ESU Padova