SAN GIUSEPPE MOSCATI - AVELLINO
AZIENDA OSPEDALIERA DI RILIEVO NAZIONALE E DI ALTA SPECIALITÀ

Proponente: **UOC AFFARI GENERALI**

DELIBERAZIONE DEL DIRETTORE GENERALE N.ro 1368 del 23/12/2022

Provvedimento con Esecutività:

	Ordinaria

X	**Immediata**	**Motivazione:** immediata esecutività motivata dall'urgenza di rendere immediatamente operativo il suo contenuto

	Per Approvazione	**Atto soggetto a controllo ex art 35 L.R.C. n 32/94 e s.m.i.**

OGGETTO

Nomina del Responsabile della Conservazione ed adozione del Manuale di Conservazione dell'AORN S.G. Moscati - Linee Guida AgID sulla formazione gestione e conservazione dei documenti informatici di cui alle Determinazioni nn. 407/2020 e 371/2021.

Alla stregua dell'istruttoria compiuta e delle risultanze e degli atti tutti richiamati nelle premesse che seguono, costituenti istruttoria a tutti gli effetti di legge, nonché per espressa dichiarazione di regolarità tecnica ed amministrativa della stessa resa a mezzo di sottoscrizione della presente, da parte de **IL DIRETTORE** di **UOC AFFARI GENERALI**

Premesso
-che le disposizioni normative emanate dal Legislatore nel corso degli ultimi anni in materia di semplificazione ed innovazione, attribuiscono un ruolo di primo piano alla formazione, alla gestione ed alla conservazione dei documenti informatici. In tale contesto, la conservazione dei documenti nativi digitali e/o digitalizzati diviene fattore imprescindibile per la sostenibilità del processo di gestione stesso;
-che l'AgID (Agenzia per l'Italia Digitale), con l'emanazione delle Linee Guida di cui alla Determinazione n. 407/2020 (Adozione delle Linee Guida sulla Formazione, gestione e conservazione dei documenti informatici) ed alla Determinazione n. 371/2021 (Modifiche testo Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, allegato 5 - Metadati, allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati ed estensione dei termini di entrata in vigore), ha perseguito e realizzato l'obiettivo di aggregare in un corpo unico le regole tecniche di gestione del documento informatico, che in precedenza erano disciplinate, separatamente, in specifici DPCM, delineando, in tal modo, una regolamentazione esaustiva e completa (contenente regole e procedure), dell'intera vita del documento informatico, dalla sua formazione, alla trasmissione, all'archiviazione, alla conservazione ed alla sua disponibilità nel tempo.

Rilevato
- che ai fini della corretta gestione e conservazione dei documenti informatici, l'art. 44 comma 1 quater D.Lgs. 07/03/2005 n. 82 "Codice dell'amministrazione digitale" prevede, tra l'altro, che le Pubbliche Amministrazioni individuino la figura del Responsabile della Conservazione, che opera d'intesa, oltre che con i responsabili di cui al comma 1 bis del medesimo Decreto, anche con il Responsabile della gestione documentale;
- che, più in particolare, il Responsabile della Conservazione ha la responsabilità di garantire la corretta esecuzione del processo di conservazione a norma dei documenti informatici e che, nell'ambito di tale processo, gli eventuali dati personali vengano trattati nel rispetto della protezione dei dati personali, secondo l'attuale normativa in vigore (GDPR - Regolamento UE 2016/679);
-che, ai sensi di quanto previsto dalle recenti Linee Guida AGID, innanzi richiamate, nella Pubblica Amministrazione, il Responsabile della Conservazione è un ruolo previsto dall'organigramma del Titolare dell'oggetto di conservazione, che può essere ricoperto da un dirigente o un funzionario interno, formalmente designato e con specifiche competenze in materia, il quale definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia;
-che, più in particolare, al Responsabile della Conservazione, sono attribuite le seguenti competenze, previste dal paragrafo 4.5 delle Linee Guida AGID Determinazione n. 371/2021:
a) definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;
b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
c) genera e sottoscrive il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
d) genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
f) effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;
g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità. Adotta analoghe misure con riguardo all'obsolescenza dei formati;
h) provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
i) predispone le misure necessarie per la sicurezza fisica e logica del sistema di conservazione come previsto dalle vigenti Linee Guida;
j) assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
l) provvede per le amministrazioni statali centrali e periferiche a versare i documenti informatici, le aggregazioni informatiche e gli archivi informatici, nonché gli strumenti che ne garantiscono la consultazione, rispettivamente all'Archivio centrale dello Stato e agli archivi di Stato territorialmente competenti, secondo le tempistiche fissate dall' art.41, comma 1 del Codice dei beni culturali;

Dato atto
- che, sempre in base alle sopra citate Linee Guida AgID, tra i diversi compiti assegnati a tale figura professionale, rientra anche la predisposizione del Manuale di Conservazione (i cui contenuti sono definiti al paragrafo 4.6 delle Linee Guida di che trattasi),

che viene periodicamente, aggiornato dal Responsabile della Conservazione in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti;

Considerato
- che le Pubbliche Amministrazioni sono tenute a redigere, adottare con provvedimento formale e pubblicare sul proprio sito istituzionale il Manuale di Conservazione in una parte chiaramente identificabile dell'area "Amministrazione Trasparente", ai sensi di quanto previsto dall'art. 9 del D.Lgs n.33/2013;
- che in caso di affidamento del servizio di conservazione ad un Conservatore Esterno, le Pubbliche Amministrazioni possono descrivere nel proprio manuale anche le attività del processo di conservazione affidate al conservatore, in conformità con il contenuto del manuale predisposto da quest'ultimo, o rinviare, per le parti di competenza al manuale del conservatore esterno (cfr paragrafo 4.6 Linee Guida AgID di cui alla Determinazione 371/2021).

Dato atto, altresì
- di aver acquisito il parere favorevole del DPO in merito ai contenuti del Manuale di Conservazione, con particolare riferimento alla conformità degli stessi alla vigente normativa in materia di tutela dei dati personali;
-che il Direttore della UOC Sistemi Informativi ha verificato, in particolare, la conformità dei contenuti del Piano della Sicurezza, (Allegato 2 al Manuale di Conservazione), a quanto previsto dalle recenti Linee Guida AgID (Determinazione n. 371/2021 paragrafo 3.9 - Misure di Sicurezza), laddove si prevede che nel Piano della Sicurezza sono previste opportune misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali, ai sensi dell'art 32 del Regolamento UE 2016/679 (GDPR), nonché la descrizione della procedura da adottarsi nel caso di violazione dei dati personali, ai sensi degli art 33-34 del regolamento UE di cui innanzi.

Visti
- La Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.
- Il Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Il Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali.
- Il Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio. Il codice garantisce e disciplina la tutela e la valorizzazione del patrimonio e dei beni culturali. Tra i beni culturali citati vi sono gli archivi dei soggetti pubblici oltre che dei soggetti privati dichiarati di interesse storico;
- Il Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
- Il Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 – Regole tecniche per il protocollo informatico, abrogato con entrata in vigore delle Linee Guida AgID maggio 2021 in data 01.01.2022, fatte salve le disposizioni degli art. 2, c.1, art. 6, art.9, art. 18 commi 1 e 5, art. 20 e art. 21;
- Il 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;
- Il Decreto Legislativo 14 marzo 2013, n. 33 - Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni
- Il Regolamento UE n. 910/2014 (eIDAS) – Regolamento Europeo in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la Direttiva 1999/93/CE. Il regolamento fornisce una base normativa comune per interazioni elettroniche sicure fra cittadini, imprese e pubbliche amministrazioni e incrementa la sicurezza e l'efficacia dei servizi elettronici e delle transazioni di e-business e commercio elettronico nell'Unione Europea;
- Il Regolamento UE 679/2016 (GDPR) - Regolamento europeo in materia di protezione dei dati personali;
- Le Linee Guida AgID di cui alle Determinazioni n. 407 del 9.9.2020 - "Linee Guida sulla Formazione, gestione e conservazione dei documenti informatici" e n. 371 del 17.5.2021 – "Modifiche testo Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, allegato 5 - Metadati, allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati ed estensione dei termini di entrata in vigore".

Ritenuto
- pertanto, per quanto innanzi rappresentato, di proporre l'individuazione del Responsabile della Conservazione Aziendale, nella persona dell'Ing. Sara Santomauro, Collaboratore Tecnico Professionale, dipendente dell'AORN, in possesso delle specifiche competenze previste dalla vigente normativa, il cui nominativo è stato preventivamente condiviso, per le vie brevi, con la Direzione Amministrativa, attribuendo allo Stesso i compiti come in narrativa richiamati, senza alcun onere aggiuntivo a carico dell'Azienda;
- proporre, altresì l'approvazione e l'adozione del Manuale di Conservazione (con relativi allegati), predisposto, come da vigenti Linee Guida AgID, dal Responsabile della Conservazione sopraindicato, che sarà oggetto di periodico aggiornamento da parte di quest'ultimo in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti;
- di dare atto che, per le attività di che trattasi, l'Ing. Sara Santomauro, opererà d'intesa con altre figure aziendali (Responsabile trattamento dati personali, Responsabile della sicurezza, Responsabile dei sistemi informativi, Responsabile della gestione documentale), così come previsto dall'art. 44 comma 1 quater del D. Lgs. 07/03/2005 n.82 e s.m.i. "Codice dell'amministrazione digitale" (CAD);

Attestata
la conformità del presente atto alle norme sul trattamento dei dati di cui al D.lgs 196/2003 così come integrato con le modifiche introdotte dal D.Lgs 101/2018 per l'adeguamento della normativa nazionale al Regolamento UE 2016/679 (GDPR) e dalle novelle introdotte dalla legge 27 dicembre 2019 n 160, che contiene principi e prescrizioni per il trattamento dei dati personali, anche con riferimento alla loro "diffusione", e dichiarato di aver valutato la rispondenza del testo, compreso degli eventuali allegati, destinato alla diffusione per il mezzo dell'Albo Pretorio alle suddette prescrizioni e ne dispone la pubblicazione nei modi di legge;

Dichiarato
che la documentazione originale a supporto del presente provvedimento è deposita e custodita agli del Dipartimento/ U.O. proponente,
che non sussistono motivi ostativi a procedere essendo l'atto conforme alle disposizioni di legge in materia ed ai regolamenti e/o direttive dell'Ente, nonché coerente con gli obiettivi strategici individuati dalla Direzione Generale e le finalità istituzionali dell'Ente

Il Responsabile del procedimento dichiara l'insussistenza del conflitto di interesse, allo stato attuale, ai sensi dell'art. 6 bis della Legge n. 241/90 in relazione al citato procedimento e della Misura M4 del vigente Piano Anticorruzione.

PROPONE AL DIRETTORE GENERALE

Per quanto in premessa, che qui si intende integralmente riportato

-di individuare, quale Responsabile della Conservazione Aziendale, l'Ing. Sara Santomauro, Collaboratore Tecnico Professionale, dipendente dell'AORN, in possesso delle specifiche competenze richieste dalla vigente normativa, il cui nominativo è stato preventivamente condiviso, per le vie brevi, con la Direzione Amministrativa, attribuendo allo Stesso i compiti come in narrativa richiamati, senza alcun onere aggiuntivo a carico dell'Azienda;

- **di approvare ed adottare** il Manuale di conservazione (con relativi allegati), predisposto, come da vigenti Linee Guida AgID, dal Responsabile della Conservazione sopraindicato, che sarà oggetto di periodico aggiornamento da parte del responsabile della conservazione, in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti;

-di dare atto che, per le relative attività, l'Ing. Sara Santomauro, opererà d'intesa con altre figure aziendali (Responsabile trattamento dati personali, Responsabile della sicurezza, Responsabile dei sistemi informativi, Responsabile della gestione documentale), così come previsto dall'art. 44 comma 1 quater del D. Lgs. 07/03/2005 n.82 e s.m.i. "Codice dell'amministrazione digitale" (CAD);

- **di allegare** al presente provvedimento, quale parte integrante e sostanziale dello stesso, il Manuale di Conservazione di che trattasi (con relativi allegati);

- **di trasmettere**
- il presente provvedimento al Collegio sindacale, all'U.O.C. proponente, all'U.O.C. Gestione Economico Finanziaria, a tutte le Strutture Aziendali, al DPO, al RPCT, alla U.O.C. Sistemi Informativi per la pubblicazione sul sito istituzionale nella sezione Amministrazione Trasparente - Disposizioni Generali - Atti amministrativi generali – Regolamenti;

- **di conferire**
- al presente provvedimento immediata esecutività motivata dall'urgenza di rendere immediatamente operativo il suo contenuto.

Allegati alla presente:

PARERI (Nome File: PARERI.pdf - Impronta: 4c9a8f19aa03150edaf4df42c88bfdc8c579335003580e73b05faa02d6f5463e) - NON PUBBLICABILE: documentazione interna di supporto al provvedimento detenuta agli atti della UOC proponente;

Allegato 2 Piano della Sicurezza (Nome File: Allegato_2_Piano_della_Sicurezza.pdf - Impronta: 38f9456a17c1a2b3310ca3004a076b26631b52771b8078ebb8fd570a6a6f67ce) - NON PUBBLICABILE: documentazione interna di supporto al provvedimento detenuta agli atti della UOC proponente;

Allegato 1 sub B (Nome File: Allegato_1_sub_B.pdf - Impronta: d3f6f68717307e38711b4dffe0adbe2f4d206658cdd084be5b905dab9edc5fd8);

Allegato 1 sub A (Nome File: Allegato_1_sub_A.pdf - Impronta: d7071818839d72eb66f13780ee65888bde5f9732bd8003198fb9373070ab63fc);

Allegato 1 Disciplinare Tecnico (Nome File: Allegato_1_Disciplinare_Tecnico.pdf - Impronta: bb484a687bbbe421193642ed6087530c50b7b26fefee5d9b75edb75b2150bbe8);

manuale di conservazione (Nome File: manuale_di_conservazione.pdf - Impronta: abebf06384a14226f93fe362b05258a2391b11289c82ee1ff951ae242223c5ca);

IL RESPONSABILE DELL'ISTRUTTORIA: Verusio Giovanni

IL DIRETTORE

UOC AFFARI GENERALI - [Genzale Raffaela]

IL DIRETTORE GENERALE

Il Direttore Generale dell'A.O.R.N. S.G. Moscati, Dr. Renato Pizzuti , nominato con D.G.R.C. n. 329 del 21/06/2022 ed immesso nelle funzioni con D.P.G.R.C. n. 109 del 04/08/2022, coadiuvato dal Direttore Amministrativo Avv. **Chiara Di Biase** e dal Direttore Sanitario Dr. **Rosario Lanzetta** ha adottato la seguente Deliberazione

IN VIRTU' dei poteri conferitogli;

PRESO ATTO della dichiarazione di regolarità dell'istruttoria compiuta da **UOC AFFARI GENERALI**, nonché della dichiarazione di regolarità tecnica ed amministrativa resa dal Direttore/Dirigente proponente con la sottoscrizione della proposta.

Condivise le motivazioni in essa indicate e fatta propria la proposta del Direttore/Dirigente proponente;

VISTO IL PARERE IN ORDINE ALLA REGOLARITA' TECNICO/CONTABILE

C.U.P**.:**

C.I.G**.:**

IMPORTO TOTALE**:**

Motivazione/Annotazione

IL DIRETTORE UOC SERVIZIO ECONOMICO - FINANZIARIO

VISTI i pareri del Direttore Sanitario e del Direttore Amministrativo:

PARERE DEL DIRETTORE AMMINISTRATIVO:

X	**Favorevole**
	Non Favorevole

Motivazione (in caso di parere non favorevole)

PARERE FAVOREVOLE

Chiara Di Biase FIRMATO

PARERE DEL DIRETTORE SANITARIO:

X	**Favorevole**
	Non Favorevole

Motivazione (in caso di parere non favorevole)

PARERE FAVOREVOLE

Rosario Lanzetta FIRMATO

DELIBERA

Per quanto premesso nella proposta allegata, da intendersi come trascritto e riportato:

-di individuare, quale Responsabile della Conservazione Aziendale, l'Ing. Sara Santomauro, Collaboratore Tecnico Professionale, dipendente dell'AORN, in possesso delle specifiche competenze richieste dalla vigente normativa, il cui nominativo è stato preventivamente condiviso, per le vie brevi, con la Direzione Amministrativa, attribuendo allo Stesso i compiti come in narrativa richiamati, senza alcun onere aggiuntivo a carico dell'Azienda;

- di approvare ed adottare il Manuale di conservazione (con relativi allegati), predisposto, come da vigenti Linee Guida AgID, dal Responsabile della Conservazione sopraindicato, che sarà oggetto di periodico aggiornamento da parte del responsabile della conservazione, in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti;

-di dare atto che, per le relative attività, l'Ing. Sara Santomauro, opererà d'intesa con altre figure aziendali (Responsabile trattamento dati personali, Responsabile della sicurezza, Responsabile dei sistemi informativi, Responsabile della gestione documentale), così come previsto dall'art. 44 comma 1 quater del D. Lgs. 07/03/2005 n.82 e s.m.i. "Codice dell'amministrazione digitale" (CAD);

- di allegare al presente provvedimento, quale parte integrante e sostanziale dello stesso, il Manuale di Conservazione di che trattasi (con relativi allegati);

- di trasmettere
- il presente provvedimento al Collegio sindacale, all'U.O.C. proponente, all'U.O.C. Gestione Economico Finanziaria, a tutte le Strutture Aziendali, al DPO, al RPCT, alla U.O.C. Sistemi Informativi per la pubblicazione sul sito istituzionale nella sezione Amministrazione Trasparente - Disposizioni Generali - Atti amministrativi generali – Regolamenti;

- di conferire
- al presente provvedimento immediata esecutività motivata dall'urgenza di rendere immediatamente operativo il suo contenuto.

Trasmessa ai soggetti esterni sotto elencati a cura del servizio proponente:

DPO AZIENDALE;

Notificata ai soggetti interni sotto elencati:

UOC AFFARI GENERALI;

COLLEGIO SINDACALE;

UOC GESTIONE ECONOMICO - FINANZIARIA;

DIREZIONE GENERALE;

UOS URP E COMUNICAZIONE;

RESPONSABILE PREVENZIONE CORRUZIONE E TRASPARENZA;

UOC SERVIZIO DI PREVENZIONE E PROTEZIONE;

REFERENTE PRIVACY AZIENDALE;

UOC CONTROLLO DI GESTIONE E PROGRAMMAZIONE;

DIREZIONE AMMINISTRATIVA;

UOC GESTIONE RISORSE UMANE;

UOS TRATTAMENTO GIURIDICO E RAPPORTI SINDACALI;

UOS TRATTAMENTO ECONOMICO;

UOC TECNICO PATRIMONIO;

UOC AFFARI LEGALI;

UOS FORMAZIONE E AGGIORNAMENTO;

UOC SISTEMI INFORMATIVI;

UOS ADEMPIMENTI AMMINISTRATIVI CUP- TICKET ED ALPI;

UOC ACQUISIZIONE BENI E SERVIZI;

UOS ECONOMATO;

DIREZIONE SANITARIA;

UOC DIREZIONE MEDICA DEI PRESIDI OSPEDALIERI AORN MOSCATI;

UOS ORGANIZZAZIONE DEI SERVIZI SANITARI;

UOC FARMACIA;

UOS FARMACOVIGILANZA E DISPOSITIVO-VIGILANZA E FARMACOECONOMIA;

UOC MEDICINA PREVENTIVA DEL LAVORO E RADIOPROTEZIONE;

UOS FISICA MEDICA;

UOC RISCHIO CLINICO;

UOS MEDICINA LEGALE;

UFFICIO DI SEGRETERIA DEL COMITATO ETICO;

DIPARTIMENTO EMERGENZA E ACCETTAZIONE;

UOC ORTOPEDIA E TRAUMATOLOGIA;

UOC MEDICINA D'URGENZA;

UOS O.B.I. E P.S.;

UOC TERAPIA INTENSIVA P.O. LANDOLFI;

UOSD CHIRURGIA D'URGENZA;

UOC TERAPIA INTENSIVA;

DIPARTIMENTO CUORE E VASI;

UOSD CARDIOANESTESIA E RIANIMAZIONE;

UOC CARDIOLOGIA - U.T.I.C.;

UOS CARDIOLOGIA INVASIVA - EMODINAMICA;

UOS T.I. CARDIOLOGICA;

UOC CARDIOCHIRURGIA;

UOS CARDIOCHIRURGIA MININVASIVA;

UOC CHIRURGIA VASCOLARE;

UOS TRATTAMENTO ENDOVASCOLARE DELLE VASCULOPATIE;

UOSD DIAGNOSTICA CARDIOVASCOLARE;

DIPARTIMENTO MEDICO;

UOC GERIATRIA;

UOS VALUTAZIONE MULTIDIMENSIONALE GERIATRICA;

UOC NEFROLOGIA;

UOSD DERMATOLOGIA E DERMOCHIRURGIA;

UOC RECUPERO E RIABILITAZIONE FUNZIONALE;

UOSD GESTIONE INFETTIVOLOGICA NEI PAZIENTI IMMUNODEFICITARI E AIDS;

UOSD ALLERGOLOGIA IMMUNOLOGIA CLINICA;

UOSD MALATTIE ENDOCRINE NUTRIZIONE E DEL RICAMBIO;

UOC MALATTIE INFETTIVE E TROPICALI;

UOC MEDICINA GENERALE;

UOS ANGIOLOGIA;

UOC MEDICINA GENERALE AD INDIRIZZO EPATOLOGICO E GESTIONE PUNTO DI PRIMO SOCCORSO;

UOSD PNEUMOLOGIA;

UOS ENDOSCOPIA TORACICA ED INTERVENTISTICA;

DIPARTIMENTO DI CHIRURGIA GENERALE E SPECIALISTICA;

UOC CHIRURGIA ONCOLOGICA;

UOC UROLOGIA;

UOC BREAST UNIT;

UOSD GASTROENTEROLOGIA;

UOSD UROLOGIA FUNZIONALE;

UOC CHIRURGIA TORACICA;

UOC CHIRURGIA GENERALE;

DIPARTIMENTO ONCO EMATOLOGICO;

UOC EMATOLOGIA;

UOS DH EMATOLOGICO;

UOS TERAPIE CELLULARI AVANZATE;

UOSD TERAPIA DEL DOLORE;

UOC ONCOLOGIA;

UOS NEOPLASIE NELL'ANZIANO;

UOC RADIOTERAPIA ONCOLOGICA;

UOC SERVIZIO IMMUNO TRASFUSIONALE;

DIPARTIMENTO MATERNO INFANTILE;

UOC OSTETRICIA E GINECOLOGIA;

UOC NEONATOLOGIA;

UOC PEDIATRIA;

UOS GENETICA MEDICA;

UOS SUB INTENSIVA PEDIATRICA;

UOC FISIOPATOLOGIA DELLA RIPRODUZIONE;

UOSD GINECOLOGIA SOCIALE;

DIPARTIMENTO DEI SERVIZI;

UOC ANATOMIA E ISTOLOGIA PATOLOGICA;

UOC MEDICINA NUCLEARE;

UOC MICROBIOLOGIA E VIROLOGIA;

UOC LABORATORIO ANALISI;

UOS CENTRO EMOSTASI;

UOC RADIOLOGIA;

UOS RISONANZA MAGNETICA;

UOS T.C.;

UOSD ECOGRAFIA;

UOSD LABORATORIO ANALISI P.O. LANDOLFI;

UOSD RADIOLOGIA SOLOFRA;

UOSD RADIOLOGIA INTERVENTISTICA BODY;

UOSD LABORATORIO DI GENETICA;

DIREZIONE STRATEGICA;

DIPARTIMENTO TESTA COLLO;

UOC NEUROLOGIA;

UOC NEUROCHIRURGIA;

UOC OCULISTICA;

UOS PATOLOGIA RETINICA MEDICA E CHIRURGICA;

UOC ORL;

UOSD NEURORADIOLOGIA;

UOSD UNITÀ STROKE;

UOSD SERVIZIO DI PSICOLOGIA CLINICA OSPEDALIERA;

Allegati alla presente:

PARERI (Nome File: PARERI.pdf - Impronta: 4c9a8f19aa03150edaf4df42c88bfdc8c579335003580e73b05faa02d6f5463e) - NON PUBBLICABILE: documentazione interna di supporto al provvedimento detenuta agli atti della UOC proponente;

Allegato 2 Piano della Sicurezza (Nome File: Allegato_2_Piano_della_Sicurezza.pdf - Impronta: 38f9456a17c1a2b3310ca3004a076b26631b52771b8078ebb8fd570a6a6f67ce) - NON PUBBLICABILE: documentazione interna di supporto al provvedimento detenuta agli atti della UOC proponente;

Allegato 1 sub B (Nome File: Allegato_1_sub_B.pdf - Impronta: d3f6f68717307e38711b4dffe0adbe2f4d206658cdd084be5b905dab9edc5fd8);

Allegato 1 sub A (Nome File: Allegato_1_sub_A.pdf - Impronta: d7071818839d72eb66f13780ee65888bde5f9732bd8003198fb9373070ab63fc);

Allegato 1 Disciplinare Tecnico (Nome File: Allegato_1_Disciplinare_Tecnico.pdf - Impronta: bb484a687bbbe421193642ed6087530c50b7b26fefee5d9b75edb75b2150bbe8);

manuale di conservazione (Nome File: manuale_di_conservazione.pdf - Impronta: abebf06384a14226f93fe362b05258a2391b11289c82ee1ff951ae242223c5ca);

DIRETTORE GENERALE

(Renato Pizzuti)

FIRMATO DIGITALMENTE DA
PIZZUTI RENATO
23.12.2022 13:33:18 UTC

SAN GIUSEPPE MOSCATI - AVELLINO
AZIENDA OSPEDALIERA DI RILIEVO NAZIONALE E DI ALTA SPECIALITÀ

MANUALE DI CONSERVAZIONE DELL'AZIENDA OSPEDALIERA DI RILIEVO NAZIONALE SAN GIUSEPPE MOSCATI DI AVELLINO

Indice

INTRODUZIONE **1**

1. SCOPO E AMBITO DEL PRESENTE DOCUMENTO **2**

2. PRINCIPI DI REDAZIONE DEL MANUALE **3**

3. NORMATIVA DI RIFERIMENTO **5**

4. STANDARD DI RIFERIMENTO **6**

5. DEFINIZIONI E ACRONIMI **8**

6. MODELLO ORGANIZZATIVO DELLA CONSERVAZIONE: RUOLI E RESPONSABILITÀ **10**

6.1 SISTEMA E ATTORI 10
6.2 TITOLARE O PRODUTTORE 11
6.3 UTENTE 11
6.4 RESPONSABILE DELLA CONSERVAZIONE 12
6.5 CONSERVATORI 13
6.6 ORGANISMI DI TUTELA E VIGILANZA 14

7. STRUTTURA ORGANIZZATIVA PER IL SISTEMA DI CONSERVAZIONE **15**

7.1 ORGANIGRAMMA 15
7.2 STRUTTURE ORGANIZZATIVE 15
7.3 COMPITI E RESPONSABILITÀ DEI CONSERVATORI 15
7.4 PUBBLICO UFFICIALE 16

8. OGGETTI SOTTOPOSTI A CONSERVAZIONE, MODALITÀ E METADATI **17**

8.1 OGGETTI/TIPOLOGIE DOCUMENTALI SOTTOPOSTI A CONSERVAZIONE 17
8.2 MODALITÀ DI CONSERVAZIONE E METADATI 17

9. PROCESSO DI CONSERVAZIONE (CONSERVATORI ESTERNI) **20**

9.1 PREMESSA 20
9.2 DEFINIZIONE DEI DOCUMENTI INFORMATICI E DELLE AGGREGAZIONI DOCUMENTALI INFORMATICHE 20
9.3 DEFINIZIONE DEI PACCHETTI 21
9.4 FASI DEL VERSAMENTO E LOGICHE DI CONSERVAZIONE 21
9.5 PRESA IN CARICO DEI PACCHETTI DI VERSAMENTO 22
9.6 DESCRIZIONE DEL PROCESSO DI CONSERVAZIONE 22
9.7 INDICE DEL PACCHETTO DI ARCHIVIAZIONE E RAPPORTO DI VERSAMENTO 22
9.8 IL PROCESSO DI ESIBIZIONE DI UN PACCHETTO DI DISTRIBUZIONE 23
9.9 ESIBIZIONE A NORMA 24
9.10 PRODUZIONE COPIE E DUPLICATI 24
9.11 DESCRIZIONE DEL SISTEMA DI CONSERVAZIONE 24
9.12 PROCEDURE DI MONITORAGGIO E CONTROLLO DEL SISTEMA DI CONSERVAZIONE 24
9.13 COPIE DI SICUREZZA 24
9.14 SCARTO DEI PACCHETTI DI ARCHIVIAZIONE 24
9.15 INTEROPERABILITÀ 25
9.16 FUNZIONALITÀ PER LA VERIFICA E IL MANTENIMENTO DELL'INTEGRITÀ DEGLI ARCHIVI 25
9.17 MANTENIMENTO DELLA FIRMA PER IL PERIODO DI CONSERVAZIONE 25
9.18 NORMATIVE IN VIGORE NEI LUOGHI DOVE SONO CONSERVATI I DOCUMENTI 25
9.19 FASI DEL PROCESSO DI CONSERVAZIONE E RESPONSABILITÀ 25

10 TRATTAMENTO DEI DATI PERSONALI 28
10.1 TUTELA E DIRITTI DEGLI INTERESSATI 28
10.2 MODALITÀ DEL TRATTAMENTO 28
10.3 FINALITÀ DEL TRATTAMENTO 28
10.4 SICUREZZA DEI DATI 28
11. DISPOSIZIONI FINALI 30

Allegati

ALLEGATO 1 – DISCIPLINARE TECNICO
ALLEGATO 1 SUB A – MANUALE DI CONSERVAZIONE TI TRUST TECHNOLOGIES
ALLEGATO 1 SUB B – MANUALE DI CONSERVAZIONE INFOCERT
ALLEGATO 2 – PIANO DELLA SICUREZZA

INTRODUZIONE

Le disposizioni normative emanate dal legislatore nel corso degli ultimi anni in materia di semplificazione ed innovazione, attribuiscono un ruolo di primo piano alla formazione, alla gestione ed alla conservazione dei documenti informatici.

In tale contesto, la conservazione dei documenti nativi digitali e/o digitalizzati diviene fattore imprescindibile per la sostenibilità del processo di gestione stesso; è fondamentale, infatti, garantire la conservazione documentale in modo autentico e accessibile anche nel lungo periodo, così come avviene tradizionalmente per i documenti analogici.

Le nuove regole tecniche per la conservazione dei documenti informatici ai sensi delle nuove Linee Guida AgID (di cui alla Determinazione AgID n. 407/2020 come successivamente modificata con Determinazione 371/2021), hanno abrogato le precedenti regole tecniche, (DPCM 3 dicembre 2013-Regole tecniche in materia di sistema di conservazione).

Obiettivo generale delle Linee Guida è aggregare in un corpo unico le regole tecniche di gestione del documento informatico che in precedenza erano disciplinate separatamente, in specifici DPCM. Viene delineata in tal modo una disciplina esaustiva e completa, contenente regole e procedure, nell'ambito di un corpo unico, che norma l'intera vita del documento informatico, dalla sua formazione, alla trasmissione, all'archiviazione, alla conservazione ed alla disponibilità nel tempo.

Le Linee Guida garantiscono un adattamento costante ai cambiamenti imposti dall'incessante rivoluzione digitale. In tal senso è stata predisposta l'emanazione di un testo "statico" che contiene la base normativa della materia e una serie di "allegati" i cui contenuti più "flessibili" potranno adeguarsi agevolmente all'evoluzione tecnologica.

Nella parte riservata alla conservazione dei documenti informatici le Linee Guida disciplinano tutti gli aspetti rilevanti: dal sistema di conservazione, agli oggetti conservati, ai modelli organizzativi e ai ruoli ed alle responsabilità.

In particolare, nelle suddette Linee Guida vengono definiti, tra l'altro il ruolo ed i compiti del Responsabile della Conservazione, che opera secondo quanto previsto dall'art 44 comma 1 quater nonché i contenuti del Manuale di conservazione.

1. SCOPO E AMBITO DEL PRESENTE DOCUMENTO

Il presente Manuale della Conservazione, predisposto dal Responsabile della Conservazione, è un documento dell'AORN S.G. Moscati che descrive i ruoli, le responsabilità e l'organizzazione logica e fisica del sistema di conservazione dei documenti digitali, i processi attuati nell'ambito della conservazione, gli oggetti e le tipologie documentarie da destinare a conservazione. Il presente documento e i dati contenuti sono oggetto di periodico aggiornamento. La responsabilità dell'aggiornamento è in capo al Responsabile della conservazione, che vi provvede a seguito di variazioni normative o avvenute nel ciclo di produzione e conservazione dei documenti informatici.

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

Il sistema conserva i documenti informatici e i documenti amministrativi informatici con i metadati ad essi associati; le aggregazioni documentali informatiche (fascicoli e serie) con i metadati ad esse associati contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che costituiscono le aggregazioni medesime, nel rispetto di quanto indicato per le Pubbliche Amministrazioni nell'articolo 67 comma 2, del DPR 445/2000 e s.m.i. e art. 44, comma 1- bis del D.Lgs 82/2005 e sm.i.(CAD).

2. PRINCIPI DI REDAZIONE DEL MANUALE

La redazione del Manuale di Conservazione 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 del processo e non solo il dettaglio tecnico degli strumenti utilizzati, ad uso interno e a fini ispettivi;
- Principio di Rilevanza: nel Manuale sono contenute solo le informazioni rilevanti, con un livello di dettaglio mirante ad agevolare le ispezioni, senza dettagli tecnici superflui;
- Principio di Accuratezza: le informazioni sono revisionate da più persone, poste ai diversi livelli della catena decisionale.

I contenuti del Manuale di conservazione sono definiti dalle recenti Linee Guida AgID, innanzi richiamate, in base alle quali lo stesso deve indicare:

- i dati dei soggetti che nel tempo hanno assunto la responsabilità del sistema di conservazione, descrivendo in modo puntuale, in caso di delega, i soggetti, le funzioni e gli ambiti oggetto della delega stessa;
- la struttura organizzativa comprensiva delle funzioni, delle responsabilità e degli obblighi dei diversi soggetti che intervengono nel processo di conservazione;
- la descrizione delle tipologie degli oggetti digitali sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di oggetti e delle eventuali eccezioni;
- la descrizione delle modalità di presa in carico di uno o più pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento;
- la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione;
- la modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;
- la descrizione del sistema di conservazione, comprensivo di tutte le componenti tecnologiche, fisiche e logiche, opportunamente documentate e delle procedure di gestione e di evoluzione delle medesime;
- la descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie;
- la descrizione delle procedure per la produzione di duplicati o copie;
- i tempi entro i quali le diverse tipologie di oggetti digitali devono essere trasferite in conservazione e i tempi di scarto così come indicati nel Piano di conservazione allegato al Manuale di Gestione documentale;
- le modalità con cui viene richiesta la presenza di un pubblico ufficiale, indicando anche quali sono i casi per i quali è previsto il suo intervento;

- le normative in vigore nei luoghi dove sono conservati gli oggetti digitali.

Le medesime Linee Guida prevedono che le Pubbliche Amministrazioni sono tenute a redigere, adottare con provvedimento formale e pubblicare sul proprio sito istituzionale il Manuale di conservazione. La pubblicazione è realizzata in una parte chiaramente identificabile dell'area "Amministrazione trasparente", ai sensi di quanto previsto dall'art. 9 del d.lgs. 33/2013.

In caso di affidamento del servizio di conservazione ad un Conservatore Esterno, le Pubbliche Amministrazioni possono descrivere nel proprio manuale anche le attività del processo di conservazione affidate al conservatore, in conformità con il contenuto del Manuale di conservazione predisposto da quest'ultimo, o rinviare, per le parti di competenza, al Manuale del conservatore esterno.

Alla luce dei principi richiamati e delle disposizioni delle recenti Linee Guida, il presente documento descrive il modello organizzativo ed il processo di conservazione dei documenti informatici prodotti o ricevuti, adottato dall'AORN dal punto di vista organizzativo, tecnico ed operativo, definendo i soggetti coinvolti e i ruoli svolti dagli stessi nel modello organizzativo di funzionamento dell'attività di conservazione.

A seconda della tipologia degli oggetti sottoposti a conservazione e dei rapporti con il soggetto che realizza tale processo, il presente Manuale è integrato con il Disciplinare Tecnico (**Allegato 1**), che definisce le specifiche operative e le modalità di descrizione e di versamento nel Sistema di conservazione digitale dei documenti informatici e delle aggregazioni documentali informatiche.

Al Disciplinare Tecnico, sono acclusi i Manuali di conservazione dei Soggetti individuati dall'AORN quali Conservatori Esterni: Ti Trust Technologies (**Allegato 1 sub A**) e Infocert (**Allegato 1 sub B**).

Al Manuale di conservazione è, altresì, accluso (**Allegato 2**) il Piano di Sicurezza del sistema di gestione informatica dei documenti, nel quale sono previste opportune misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali, ai sensi dell'art. 32 del Regolamento UE 2016/679 (GDPR), nonché la descrizione della procedura da adottarsi nel caso di violazione dei dati personali, ai sensi degli artt. 33-34 del Regolamento UE di cui innanzi, quale allegato non pubblicabile.

Il presente Manuale di conservazione è applicato dall'AORN S.G. Moscati di Avellino, quale soggetto Produttore che sottopone a conservazione digitale le seguenti tipologie documentali: Registro giornaliero di protocollo; PEC; Delibere e Determine informatizzate; Delibere e Determine digitalizzate; Fatture Elettroniche attive e notifiche; Fatture Elettroniche passive e notifiche; Contratti; Cartelle cliniche digitalizzate. In particolare, il processo di conservazione è affidato al Conservatore Esterno TI Trust Technologies per le seguenti classi documentali: Registro giornaliero di protocollo, Delibere informatizzate, Determine informatizzate, Delibere digitalizzate, Determine digitalizzate, Contratti, e per l'area sanitaria Cartelle Cliniche digitalizzate, mentre il processo di conservazione è affidato al Conservatore Esterno Infocert per le seguenti classi documentali: PEC, Fatture Elettroniche attive e notifiche e Fatture Elettroniche passive e notifiche, conservatori accreditati AgID, di seguito indicati come Conservatori.

Gli accordi tra AORN S.G. Moscati di Avellino ed i Conservatori per l'affidamento in outsourcing del processo di conservazione sono stati formalizzati da parte dell'Ente mediante sottoscrizione dei relativi contratti di adesione al servizio.

3. NORMATIVA DI RIFERIMENTO

- Legge 7 agosto 1990, n. 241 e s.m.i. - Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;

- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;

- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. - Codice in materia di protezione dei dati personali;

- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. - Codice dei Beni Culturali e del Paesaggio. Il codice garantisce e disciplina la tutela e la valorizzazione del patrimonio e dei beni culturali. Tra i beni culturali citati vi sono gli archivi dei soggetti pubblici oltre che dei soggetti privati dichiarati di interesse storico;

- Decreto Legislativo 7 marzo 2005, n. 82 e s.m.i. - Codice dell'amministrazione digitale (CAD);

- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche per il protocollo informatico, abrogato con entrata in vigore delle Linee Guida AgID maggio 2021 in data 01.01.2022, fatte salve le disposizioni degli art. 2, c.1, art. 6, art. 9, art. 18 commi 1 e 5, art. 20 e art. 21;

- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 - Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;

- Decreto Legislativo 14 marzo 2013, n. 33 - Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni;

- Regolamento UE n. 910/2014 (eIDAS) – Regolamento europeo in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE. Il Regolamento fornisce una base normativa comune per interazioni elettroniche sicure fra cittadini, imprese e pubbliche amministrazioni e incrementa la sicurezza e l'efficacia dei servizi elettronici e delle transazioni di e - business e commercio elettronico nell'Unione Europea;

- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);

- Linee Guida AgID - Linee Guida sulla formazione, gestione e conservazione dei documenti informatici approvate con Determinazione n. 407 del 9.9.2020 così come successivamente modificata dalla Determinazione n. 371 del 17.5.2021, in vigore, il 01.01.2022.

4. STANDARD DI RIFERIMENTO

- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;

- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);

- ETSI TS 101 533-1 v1.3.1 (2012-04) - Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management;

- ETSI TR 101 533-2 v1.3.1 (2012-04) - Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors;

- ICA - ISAD (G): General International Standard Archival Description - Second Edition - Adopted by the Committee on Descriptive Standards Stockholm, Sweden, 19-22 September 1999. Traduzione italiana a cura di Stefano Vitali, con la collaborazione di Maurizio Savoja, Firenze 2000. Standard dell'ICA (International Council on Archives - Conseil International des Archives) che fornisce delle norme generali per l'elaborazione di descrizioni archivistiche;

- ISO 14721:2012 – Open Archival Information System – Reference model (CCSDS 650.0-M-2, Recommend Practice, Magenta Book June 2012): definisce concetti, modelli e funzionalità inerenti agli archivi digitali e ciò che è richiesto per garantire una conservazione permanente, o per un lungo termine indefinito, di informazioni digitali. Questa versione sostituisce la prima (ISO 14721:2003 - CCSDS 650.0-B-1 – Blue Book, January 2002) di cui è disponibile una traduzione in italiano (Sistema informativo aperto per l'archiviazione: traduzione italiana: OAIS. Sistema informativo aperto per l'archiviazione, a cura di Giovanni Michetti, Roma, ICCU 2007);

- ISO 16363:2012 - Space data and information transfer systems - Audit and certification of trustworthy digital repositories (CCSDS 652.0-M-1 Recommend Practice, Magenta Book September 2011);

- ISO 15836: 2009: Information and documentation – The Dublin Core metadata element set. Sistema di metadati del Dublin Core (questa versione sostituisce la precedente: ISO 15836:2003);

- ISO 23081-1:2006: Information and documentation – Records management processes – Metadata for records – Part 1- Principles. Quadro di riferimento per lo sviluppo di un Sistema di metadati per la gestione documentale;

- ISO/TS 23081-2:2007: Information and documentation – Records management processes – Metadata for records – Part 2- Conceptual and implementations issues. Guida pratica per l'implementazione;

- ISO 23081-2:2009: Information and documentation – Managing Metadata for records – Part 2- Conceptual and implementations issues. Guida pratica per l'implementazione;

- LTO4: standard "open" sviluppato alla fine del 1990. LTO 4 è una tecnologia di storage dei dati su nastro.

- SAML: Security Assertion Markup Language è uno standard informatico per lo scambio di dati di autenticazione e autorizzazione (dette asserzioni) tra domini di sicurezza distinti, tipicamente un identity provider (entità che fornisce informazioni di identità) e un service provider (entità che fornisce servizi). Il formato delle asserzioni SAML è basato su XML. SAML è mantenuto da OASIS Security Services Technical Committee.

- SQL: (Structured Query Language) è un linguaggio standardizzato per database basati sul modello relazionale (RDBMS).

- UNI 11386:2010 - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI SInCRO): Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali: definisce la struttura dell'insieme di dati a supporto del processo di conservazione; in particolare, precisa e integra alcune disposizioni contenute nella Deliberazione CNIPA 19 febbraio 2004, n. 11, individuando gli elementi informativi necessari alla creazione dell'indice di conservazione e descrivendone sia la semantica sia l'articolazione per mezzo del linguaggio formale XML. L'obiettivo della norma è di consentire agli operatori del settore di utilizzare una struttura-dati condivisa al fine di raggiungere un soddisfacente grado d'interoperabilità nei processi di migrazione, grazie all'adozione dello Schema XML appositamente elaborato.

- UNI ISO 15489-1:2006: Informazione e documentazione – Gestione dei documenti di archivio – Principi generali sul record management.

- UNI ISO 15489-2:2007: Informazione e documentazione – Gestione dei documenti di archivio – Linee guida sul record management.

5. DEFINIZIONI E ACRONIMI

Si riportano, di seguito, alcune definizioni contenute nell'allegato n. 1 alle vigenti Linee Guida, rilevanti ai fini del presente Manuale.

Accesso: operazione che consente di prendere visione dei documenti informatici.

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.

Area organizzativa omogenea: un insieme di funzioni e di uffici individuati dall'Ente al fine di gestire i documenti in modo unitario e coordinato, secondo quanto disposto dall'art. 50 comma 4 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i. Essa rappresenta il canale ufficiale per l'invio di istanze e l'avvio di procedimenti amministrativi.

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.

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.

Esibizione: operazione che consente di visualizzare un documento conservato.

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.

Manuale di conservazione: documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture.

Manuale di gestione documentale informatico: documento che descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Metadati: dati associati a un documento informatico, o a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081- 1:2017.

Oggetto di conservazione: oggetto digitale versato in un sistema di conservazione.

PdA - Pacchetto di archiviazione: pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel manuale di conservazione.

PdD - Pacchetto di distribuzione: pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione.

PdV - 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.

Piano di conservazione: documento, allegato al manuale di gestione documentale 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 e s.m.i.

Piano della sicurezza: documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi.

Presa in carico: accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione e, in caso di affidamento del servizio all'esterno, dagli accordi stipulati tra il titolare dell'oggetto di conservazione e il responsabile del servizio di conservazione.

Produttore dei PdV: persona fisica, 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.

RdV - 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 della conservazione: soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.

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 (D.Lgs 82/2005).

Titolare dell'oggetto di conservazione: soggetto produttore degli oggetti di conservazione.

6. MODELLO ORGANIZZATIVO DELLA CONSERVAZIONE: RUOLI E RESPONSABILITÀ

6.1 SISTEMA E ATTORI

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo
Responsabile del servizio di conservazione	Funzione esercitata dai Conservatori Esterni		A decorrere dalla data di adesione al servizio
Responsabile della conservazione del Produttore	Ing. Sara Santomauro	Definizione delle policies di conservazione	A decorrere dalla data del provvedimento di nomina
Responsabile funzione archivistica di conservazione	Funzione esercitata dai Conservatori Esterni		A decorrere dalla data di adesione al servizio
Titolare del trattamento dei dati personali	AORN S.G. Moscati di Avellino		Dalla data del provvedimento d'individuazione del titolare
Responsabile esterno del trattamento dei dati personali	Funzione esercitata dai Conservatori Esterni		Dalla data dell'atto di nomina ed a decorrere dalla data di adesione al servizio
Responsabile della sicurezza dei sistemi per la conservazione	Funzione esercitata dai Conservatori Esterni		A decorrere dalla data di adesione al servizio
Responsabile sistemi informativi per la conservazione	Funzione esercitata dai Conservatori Esterni		A decorrere dalla data di adesione al servizio
Responsabile sviluppo e manutenzione del sistema di conservazione	Funzione esercitata dai Conservatori Esterni		A decorrere dalla data di adesione al servizio

6.2 TITOLARE O PRODUTTORE

Nel Disciplinare Tecnico (Allegato 1) e nei Manuali di Conservazione dei Conservatori Esterni (Allegato 1 sub A e B) acclusi al presente Manuale il "Produttore" è il Soggetto Produttore dell'archivio digitale.

I recapiti e i riferimenti amministrativi e anagrafici del Produttore/Soggetto Produttore sono di seguito riportati:

Produttore/Soggetto Produttore	AORN S.G. Moscati di Avellino
Sede Amministrativa	Contrada Amoretta - Avellino -
Recapiti	0825/203111
Sito web	www.aornmoscati.it
PEC	protocollo.generale@pec.aornmoscati.it
Partita IVA	01948180649

6.3 UTENTE

Si identifica come utente una persona, ente o sistema che interagisce con i servizi di un sistema per la conservazione dei documenti informatici al fine di fruire delle informazioni di interesse.

L'utente può richiedere al Responsabile della conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge. Il Sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, ai documenti informatici conservati e consente la produzione di un Pacchetto di distribuzione direttamente acquisibile dai soggetti autorizzati.

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

Nel ruolo dell'utente si possono definire al momento solo specifici soggetti abilitati del Produttore, in particolare gli operatori indicati dal Produttore, che possono accedere esclusivamente ai documenti versati dal Produttore stesso o solo ad alcuni di essi secondo le regole di visibilità e di accesso concordate tra i conservatori e il Produttore.

Si identificano gli utenti del Sistema di conservazione nelle seguenti persone:

- Nominativo - Ing. Sara Santomauro, Responsabile della Conservazione del Produttore;
- Eventuali ulteriori utenti, addetti alla funzione archivistica di conservazione del Produttore.

L'abilitazione e l'autenticazione di tali operatori/utenti avviene in base alle procedure di gestione utenze indicate nel Piano della sicurezza dei Conservatori esterni, come sopra individuati.

6.4 RESPONSABILE DELLA CONSERVAZIONE

Nelle recenti Linee Guida AgID, innanzi richiamate, vengono definiti, tra l'altro il ruolo ed i compiti del Responsabile della conservazione che opera secondo quanto previsto dall'art. 44 comma 1 quater[1].

Il Responsabile della conservazione:

- è un ruolo previsto dall'organigramma del Titolare dell'oggetto di conservazione;
- può essere un dirigente o un funzionario interno formalmente designato e in possesso di idonee competenze giuridiche, informatiche ed archivistiche;
- può essere svolto dal responsabile della gestione documentale o dal coordinatore della gestione documentale, ove nominato.

Il responsabile della conservazione definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia e, sotto la propria responsabilità, può delegare lo svolgimento delle proprie attività o parte di esse a uno o più soggetti, che all'interno della struttura organizzativa, abbiano specifiche competenze ed esperienze.

In particolare, il responsabile della conservazione:

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

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

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

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

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

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

g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;

---

[1] L'art. 44, comma 1-quater, del CAD prevede che: "Il responsabile della conservazione, che opera d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei sistemi informativi, può affidare, ai sensi dell'articolo 34, comma 1-bis, lettera b), la conservazione dei documenti informatici ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative, e tecnologiche e di protezione dei dati personali. Il responsabile della conservazione della pubblica amministrazione, che opera d'intesa, oltre che con i responsabili di cui al comma 1-bis, anche con il responsabile della gestione documentale, effettua la conservazione dei documenti informatici secondo quanto previsto all'articolo 34, comma 1-bis".

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

i) predispone le misure necessarie per la sicurezza fisica e logica del sistema di conservazione;

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

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

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

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

Il ruolo di Responsabile della Conservazione del Produttore (AORN) è ricoperto dal dipendente: Ing. Sara Santomauro – Collaboratore Tecnico Professioanle.

6.5 CONSERVATORI

I Conservatori esterni intesi come Enti Conservatori o come Soggetti che svolgono attività di conservazione, sono stati individuati dall'AORN in: TI Trust Technologies ed Infocert, che, a seconda delle classi documentali così come specificate nel Disciplinare Tecnico (Allegato 1), garantiscono la conservazione, archiviazione e gestione dei Documenti informatici e degli altri oggetti digitali; erogano servizi di accesso basati sui contenuti digitali conservati; forniscono supporto, formazione e consulenza al Produttore per i processi di dematerializzazione.

Di fatto, quindi i conservatori si impegnano alla conservazione dei documenti trasferiti e ne assumono la funzione di Responsabili della conservazione ai sensi della normativa vigente, garantendo il rispetto dei requisiti previsti dalle norme in vigore nel tempo per i sistemi di conservazione.

Di seguito si riportano i dati identificativi dei Conservatori esterni dell'AORN:

- **Denominazione sociale** TI Trust Technologies S.r.l.

  Sede legale S.S. 148 Pontina, km 29,100 – 00071 Pomezia (Roma)

  C.F. e P.IVA 04599340967

  Sito web https://www.trusttechnologies.it/

- **Denominazione sociale** InfoCert S.p.A.

  Sede legale Piazza Sallustio, 9 – 00187 - Roma

  C.F. e P.IVA 07945211006

  Sito web https://www.infocert.it/

6.6 ORGANISMI DI TUTELA E VIGILANZA

"Lo spostamento, anche temporaneo dei beni culturali mobili" compresi gli archivi storici e di deposito è soggetto ad autorizzazione della Soprintendenza archivistica (D.Lgs 22 gen. 2004, n. 42 e s.m.i., art. 21, c. 1, lettera b).

Anche "Il trasferimento ad altre persone giuridiche di complessi organici di documentazione di archivi pubblici, nonché di archivi di privati per i quali sia intervenuta la dichiarazione ai sensi dell'articolo 13", sia che comporti o non comporti uno spostamento, rientra tra gli interventi soggetti ad autorizzazione della Soprintendenza Archivistica (D.Lgs 22 gen. 2004, n. 42 e s.m.i., art.21, c. 1, lettera e).

La disposizione si applica anche:

- all'affidamento a terzi dell'archivio (outsourcing), ai sensi del D.lgs 22 gen. 2004, n. 42 e s.m.i., art.21, c. 1, lettera e)

- al trasferimento di archivi informatici ad altri soggetti giuridici, nell'ottica della conservazione permanente sia del documento sia del contesto archivistico.

Resta ferma, inoltre, la competenza del Ministero della Cultura in materia di tutela dei sistemi di conservazione sugli archivi pubblici e privati che rivestono interesse storico particolarmente importante, così come disciplinato dalla normativa sui beni culturali.

I sistemi di conservazione delle pubbliche amministrazioni ed i sistemi di conservazione dei conservatori accreditati sono soggetti alla vigilanza dell'AgID, e per tale fine i Sistemi di conservazione dei Conservatori esterni prevedono la materiale conservazione dei dati e delle copie di sicurezza sul territorio nazionale e l'accesso ai dati presso la sede del Produttore.

7. STRUTTURA ORGANIZZATIVA PER IL SISTEMA DI CONSERVAZIONE

7.1 ORGANIGRAMMA

Si rinvia agli organigrammi descritti nei Manuali di Conservazione dei Conservatori esterni

7.2 STRUTTURE ORGANIZZATIVE

Si rinvia alle strutture organizzative descritte nei Manuali di Conservazione dei Conservatori esterni

7.3 COMPITI E RESPONSABILITÀ DEI CONSERVATORI

I Conservatori Esterni assolvono i seguenti compiti assumendone le relative responsabilità:

- **Compiti Organizzativi**

I conservatori provvedono alla realizzazione di una base di dati relativa ai documenti informatici che il Produttore versa in conservazione, gestita secondo i principi di sicurezza illustrati nel proprio Manuale e nel Contratto, ed attuati adottando procedure di tracciabilità tali da garantire la corretta conservazione, l'accessibilità a ogni singolo documento e la sua esibizione.

I Conservatori si occupano altresì di definire:

- le caratteristiche ed i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare e organizzare gli stessi in modo da garantire la corretta conservazione e la sicurezza dei dati, anche al fine di poterli prontamente produrre, ove necessario;
- le procedure di sicurezza e tracciabilità che consentano di risalire in ogni momento alle attività effettuate durante l'esecuzione operativa di conservazione;
- le procedure informatiche ed organizzative per la corretta tenuta dei supporti su cui vengono memorizzati i documenti informatici oggetto di conservazione;
- le procedure informatiche ed organizzative atte ad esibire la documentazione conservata, in caso di richieste formulate da chi ne abbia titolo;

- **Compiti di Manutenzione e Controllo**

I Conservatori provvedono a:

- mantenere un registro cronologico del software dei programmi in uso nelle eventuali diverse versioni succedute nel tempo ed un registro cronologico degli eventi di gestione del sistema di conservazione comprensivo delle risoluzioni adottate per rimuovere eventuali anomalie;
- implementare specifici controlli di sistema per individuare e prevenire l'azione di software che possano alterare i programmi ed i dati;
- verificare la corretta funzionalità del sistema e dei programmi in gestione;
- analizzare e valutare periodicamente la registrazione degli eventi rilevanti ai fini della sicurezza (analisi del log di sistema);

- definire e documentare le procedure di sicurezza da rispettare per l'apposizione del riferimento temporale;
- mantenere e gestire i dispositivi di firma in conformità con le procedure stabilite dal certificatore qualificato che ha rilasciato i relativi certificati;
- verificare la validità delle marche temporali utilizzate dal sistema di conservazione;
- verificare il buon funzionamento del filesystem.

- **Compiti Operativi**

I Conservatori effettuano le seguenti attività:

- supervisione dell'intero sistema di conservazione digitale, verificando accuratamente i processi di apposizione delle firme digitali, dei riferimenti temporali e delle marche temporali, in modo che la procedura rispetti la normativa, assicurandosi che tutto il processo si realizzi secondo le procedure descritte nel Manuale;
- sincronizzazione dell'ora di sistema di tutti i sistemi utilizzati, verifica e controllo della sincronizzazione del clock di sistema per consentire registrazioni accurate e comparabili tra loro;
- mantenimento della documentazione descrittiva del processo di conservazione aggiornata nel corso del tempo.

- **Compiti per la protezione dei dati e delle procedure informatiche**

I Conservatori sono garanti, di tutte le misure necessarie per la sicurezza fisica, logica e ambientale dei dati e del sistema preposto alla loro conservazione, comprensivo delle copie di sicurezza dei supporti di memorizzazione, al fine di proteggere le informazioni da possibili violazioni in termini di riservatezza, integrità e disponibilità delle informazioni stesse.

Dovranno quindi predisporre e verificare che gli strumenti informatici in dotazione siano protetti secondo criteri che dovranno essere sempre aggiornati, con la tecnologia e la normativa di tutela della privacy, per garantirne il corretto funzionamento contro i cosiddetti malicious code e contro gli accessi non autorizzati sia logici che fisici.

Sono altresì responsabili della definizione ed adozione, attraverso un'analisi del rischio, degli appropriati controlli di sicurezza delle informazioni.

7.4 PUBBLICO UFFICIALE

Nei casi previsti dalla normativa, il ruolo di Pubblico ufficiale è svolto dal Responsabile della conservazione, Dirigente/Funzionario, o da altri dallo stesso formalmente designati, quale il Responsabile della Funzione archivistica di conservazione per l'attestazione di conformità all'originale di copie di documenti informatici conservati.

8. OGGETTI SOTTOPOSTI A CONSERVAZIONE, MODALITÀ E METADATI

8.1 OGGETTI/TIPOLOGIE DOCUMENTALI SOTTOPOSTI A CONSERVAZIONE

L'AORN S.G. Moscati di Avellino invia in conservazione le seguenti tipologie documentali:

- Registro giornaliero di protocollo;
- PEC;
- Delibere informatizzate;
- Determine informatizzate;
- Delibere digitalizzate;
- Determine digitalizzate;
- Fatture Elettroniche attive e notifiche;
- Fatture Elettroniche passive e notifiche;
- Contratti;
- Cartelle cliniche digitalizzate.

8.2 MODALITÀ DI CONSERVAZIONE E METADATI

Di seguito la descrizione delle modalità di conservazione delle varie tipologie documentali prodotte dall'AORN e dei relativi metadati:

- **Registro giornaliero di protocollo.** Per la conservazione di questa tipologia documentale, l'Azienda utilizza la piattaforma Legal Archive di TI Trust Technologies. Il registro giornaliero conservato è un file PDF e la classe documentale utilizzata è "Registro giornaliero di Protocollo" e viene inviato al servizio di conservazione ogni giorno. I metadati utilizzati sono: Hash, Nome_Documento, UID_Documento, Data di chiusura, Versione, Destinatario, Soggetto produttore, Oggetto, Cod_IPA, Amministrazione, Cod_AOO, Responsabile, Numero, Anno, Soggetto produttore, Numero prima registrazione, Numero ultima registrazione, Data prima registrazione, Data ultima registrazione, Codice registro.

- **PEC.** Il servizio PEC dell'Azienda è fornito da Infocert. Il servizio di conservazione è attivato per tutte le caselle istituzionali tramite la piattaforma Webmail di Infocert. Il documento conservato è un file EML contenente il messaggio con eventuali allegati. Le PEC vengono inviate al servizio di conservazione entro 24 ore dalla ricezione. I metadati utilizzati sono quelli standard per la conservazione PEC del servizio Infocert, ossia: A, Allegati, CC, Da, Data, Indirizzo, Message ID, Oggetto, Oggetto documento, Riferimento Message ID, Trasporto. Il servizio di conservazione delle PEC è individuale per ciascuna casella.

- **Delibere e Determine informatizzate.** Per la conservazione a norma di delibere e determine, è utilizzata la piattaforma Legal Archive di TI Trust Technologies. Le delibere e le determine vengono inviate al sistema di conservazione 15 giorni dopo la loro pubblicazione.

Sia per le delibere che per le determine, è utilizzata la classe documentale "Determina" con gli stessi metadati: Hash, Nome_Documento, UID_Documento, Data di chiusura, Versione, Destinatario, Soggetto produttore, Oggetto, Produttore, Anno, Numero, Autore, CodiceUOR, Codice Identificativo AOO, Responsabile del procedimento, Identificazione del conservatore, Firmatario Ente, Ruolo Firmatario, Tipologia.
La distinzione tra delibere e determine è evidenziata attraverso i metadati "Nome_documento" e "UID documento". I vari documenti che formano l'atto (proposta, pareri, eventuali allegati, attestato di pubblicazione) vengono conservati singolarmente all'interno della piattaforma. I documenti che appartengono allo stesso atto hanno lo stesso valore nel campo "numero" e lo stesso valore nel campo "oggetto".

- **Delibere e Determine digitalizzate.** È in corso un processo di digitalizzazione dei documenti dell'archivio storico dell'albo pretorio, l'estrapolazione dei metadati e la conservazione a norma dell'atto così digitalizzato. Il documento conservato è un PDF.
  La piattaforma che verrà utilizzata per la conservazione a norma di questi documenti è Legal Archive di TI Trust Technologies. Sarà utilizzata la classe documentale "Determine" e gli stessi metadati degli atti di delibere e determine attualmente presenti in conservazione.

- **Fatture Elettroniche attive e notifiche e Fatture Elettroniche passive e notifiche.** Per la conservazione a norma delle fatture elettroniche, è utilizzata la piattaforma LegalDoc di Infocert, Conservatore accreditato AgID. Il documento conservato è un PDF.
  Per le fatture elettroniche attive è utilizzata la classe documentale "legal_invoice_pacon i seguenti metadati: Periodo di imposta, Data documento, Data inizio periodo di imposta, Serie numerazione, Codice CIG, Codice CUP, Codice fiscale emittente, Codice fiscale, Codice PA, Denominazione emittente, Denominazione, Indirizzo e-mail, Identificativo Sdi, Località, Nome file SOGEI, Note, Numero documento, Partita IVA emittente, Partita IVA, Provincia, Totale importo.
  Per le fatture elettroniche passive è invece utilizzata la classe documentale "legal_invoice_pa_pass" con i seguenti metadati: Periodo di imposta, Data documento, Codice Identificativo Gara, Codice Unitario Progetto, Codice fiscale emittente, Codice Fiscale, Codice Ufficio IPA, Data protocollo, Denominazione emittente, Denominazione, Identificativo univoco dato da SDI, Nome file SOGEI, Numero documento - Numero Fattura, Numero protocollo attribuito dal ricevente, Partita IVA emittente, Partita IVA, Stato della Fattura, Parametro interno per identificare il flusso di alimentazione.
  Per quanto riguarda le notifiche attive e passive, le classi utilizzate sono "notifica_pa" e "notifica_pa_pass" con i seguenti metadati: Periodo di imposta, Data documento, Codice fiscale emittente, Codice fiscale, Codice PA, Denominazione emittente, Denominazione, Id esterno, Identificativo SDI, Nome file SOGEI, Numero documento, Partita IVA emittente, Partita IVA.

- **Contratti.** Per la conservazione a norma dei contratti nativi digitali è utilizzata la piattaforma Legal Archive di TI Trust Technologies. I contratti vengono inviati al sistema di conservazione entro 24 ore dopo la sua sottoscrizione. La classe documentale scelta è "Contratti" e i metadati utilizzati sono: Hash, Nome_Documento, UID_Documento, Data di chiusura, Versione, Destinatario, Soggetto produttore, Oggetto, Data_del_documento, Data Contabile, Cod_BU, Cod_Archivio, Tipo_Documento, Oggetto_Doc, Cod_Rapporto, Cod_SottoRapp, Cod_Cliente, Cod_Promotore, Cod_Fornitore. I contratti in formato cartaceo continueranno ad essere conservati nell'apposito archivio aziendale.

- **Cartelle cliniche digitalizzate**. È in atto un continuo processo di digitalizzazione delle cartelle cliniche cartacee che interessa sia l'archivio storico sia le nuove cartelle prodotte dall'Azienda. Il trattamento è lo stesso per tutte le cartelle e prevede: digitalizzazione, estrapolazione dei metadati e invio in conservazione sulla piattaforma Asap-Arc di Trust Technologies.

La classe documentale scelta è "Documento Amministrativo Informatico" con la seguente personalizzazione: Hash, Contesto, Nome_Documento, UID_Documento, Data di chiusura, Versione, Destinatario, Soggetto produttore, Oggetto, Nome_Paziente, Cognome_Paziente, Nominativo_Paziente, Codice_Fiscale_Paziente, Data_Nascita, Nosologico, Numero_SDO, Data_Ammissione, Data_Dimissione, Codice_ISTAT, Codice_Struttura.

9. PROCESSO DI CONSERVAZIONE (CONSERVATORI ESTERNI)

9.1 PREMESSA

Si riporta di seguito la descrizione del processo di conservazione affidato ai Conservatori Esterni.

Il Produttore, al momento dell'invio in conservazione, associa ad ogni documento informatico (Rif. Allegato 5 delle nuove Linee Guida AgID Determinazione n. 371/2021 del 17 Maggio 2021), un file dei parametri di conservazione e un file di indici entrambi di tipo XML.

Al documento viene inoltre associato dal sistema di conservazione un file di ricevuta (file IPdA, ovvero un Indice del pacchetto di archiviazione) nonché un identificativo univoco generato dal sistema stesso, definito token.

Il file IPdA, firmato dal Responsabile della conservazione e marcato temporalmente, attesta la correttezza del processo, e dà certezza al momento temporale.

La struttura del file IPdA rispecchia quanto richiesto nell'Allegato 5 (Metadati) delle Linee Guida AgID vigenti.

Il documento rappresenta l'unità minima di elaborazione nel senso che viene memorizzato ed esibito come un tutt'uno; non è possibile estrarre dal sistema parti di un documento.

Un documento conservato presso il sistema di conservazione, quindi, ha le seguenti caratteristiche:

- è costituito da un file;
- è memorizzato sui supporti previsti dalla procedura di conservazione;
- è identificato in maniera univoca attraverso il token;
- è conservato insieme al file dei parametri di conservazione, al file di indici del documento e al file di ricevuta (file IPdA).

Come stabilito dalle Regole tecniche per il protocollo informatico ai sensi delle Linee Guida AgID, Determinazione n. 371/2021 del 17 Maggio 2021, i documenti sono statici e non modificabili, ovvero sono redatti in modo tale per cui il contenuto non è alterabile durante le fasi di conservazione ed accesso, e sono immutabili nel tempo.

In pratica, il documento non contiene macroistruzioni né codici eseguibili.

Le caratteristiche di staticità ed immodificabilità del documento inviato al sistema di conservazione digitale sono assicurate dal Produttore.

Per il formato dei file conservabili nel sistema di conservazione si rinvia ai "Manuali del Sistema di conservazione" dei Conservatori Esterni.

9.2 DEFINIZIONE DEI DOCUMENTI INFORMATICI E DELLE AGGREGAZIONI DOCUMENTALI INFORMATICHE

I Sistemi di conservazione gestiti dai Conservatori Esterni (Sistemi), conservano documenti informatici, in particolare documenti amministrativi informatici, con i metadati ad essi associati e le loro aggregazioni documentali informatiche.

I documenti informatici e le loro aggregazioni documentali informatiche sono trattati nel sistema nella forma di Unità documentarie e Unità archivistiche e sono inviati in conservazione sotto forma di Pacchetti di versamento (PdV), che contengono sia i documenti che i relativi metadati.

I documenti informatici (Unità documentarie) sono suddivisi in tipologie documentarie, che identificano gruppi documentali omogenei per natura e funzione giuridica, modalità di registrazione o di produzione.

Tale suddivisione è funzionale all'individuazione, per ogni singola tipologia documentaria, di set di metadati standard e di articolazioni o strutture di composizione omogenee.

Per ogni tipologia documentaria i Conservatori definiscono:

- il set dei metadati descrittivi da inserire nei PdV, ritenuti essenziali per la corretta conservazione dei documenti, in coerenza con quanto stabilito nell'Allegato 5 delle nuove Linee Guida AgID Determinazione n. 371/2021 del 17 Maggio 2021;
- l'articolazione o struttura di riferimento della corrispondente Unità documentaria ai fini della predisposizione del PdV per l'invio al Sistema di conservazione;
- le indicazioni operative per la produzione del PdV e l'invio dello stesso al Sistema.

9.3 DEFINIZIONE DEI PACCHETTI

In generale si definisce "pacchetto" un 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.

Nell'ambito del processo di conservazione distinguiamo tra:

- pacchetto di versamento: insieme di documenti che il Produttore invia al sistema di conservazione in una sessione, ognuno corredato dall'IPdA;
- pacchetto di archiviazione: un pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento. Ad ogni documento il Sistema di conservazione associa un file XLM, detto Indice del Pacchetto di Archiviazione (IPdA). L'insieme degli Indici del Pacchetto di Archiviazione associati ai file componenti un pacchetto è detto rapporto di versamento;
- pacchetto di distribuzione: un pacchetto informativo inviato dal sistema di conservazione all'utente in risposta a una sua richiesta, ovvero è la risposta alla ricerca effettuata dal Produttore tramite interfaccia disponibile, che porta all'esibizione del documento conservato. Il documento da esibire è accompagnato sempre dall'IPdA.

9.4 FASI DEL VERSAMENTO E LOGICHE DI CONSERVAZIONE

Il processo di conservazione si basa su di una logica di conservazione caratterizzata dal versamento da parte del Produttore degli oggetti da conservare (Documenti informatici e aggregazioni documentali informatiche) secondo la tempistica seguente:

- la stampa giornaliera dei registri (di protocollo e di repertorio) entro la giornata lavorativa successiva a quella della registrazione;
- le fatture passive e gli altri documenti contabili entro i termini previsti dalla normativa di settore;

- tutti gli altri documenti non oltre 12 mesi dalla data di registrazione degli stessi nel sistema di gestione documentale.

9.5 PRESA IN CARICO DEI PACCHETTI DI VERSAMENTO

Relativamente alle funzioni di "Invio al sistema di conservazione del pacchetto di versamento", "Validazione del pacchetto di versamento", "Descrizione del rapporto di versamento", si rimanda ai "Manuali del Sistema di conservazione" dei Conservatori Esterni.

9.6 DESCRIZIONE DEL PROCESSO DI CONSERVAZIONE

Il sistema di conservazione permette di mantenere e garantire nel tempo l'integrità e la validità legale di un documento informatico, nel rispetto della normativa vigente.

Il sistema consente le funzionalità di:

- Accettazione del pacchetto di versamento;
- Conservazione del pacchetto di archiviazione: il documento, ricevuto dal Conservatore in formato digitale statico non modificabile, viene conservato a norma di legge per tutta la durata prevista ed è contenuto in un pacchetto di archiviazione;
- Rettifica del pacchetto di archiviazione: un documento inviato in conservazione può essere rettificato dall'invio di un documento successivo. La rettifica è una modifica logica, nel pieno rispetto del principio di tracciabilità e si applica al pacchetto di archiviazione;
- Scarto/cancellazione del pacchetto di archiviazione: un documento inviato in conservazione può essere cancellato. Il sistema di conservazione terrà comunque evidenza del documento all'interno dell'archivio a norma, nel rispetto del principio di tracciabilità; la cancellazione si applica al pacchetto di archiviazione, inoltre lo scarto è l'operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale;
- Esibizione del pacchetto di distribuzione: il documento richiesto via web viene richiamato direttamente dal sistema di conservazione digitale ed esibito, con garanzia della sua opponibilità a terzi;
- Ricerca dei documenti informatici indicizzati: il Produttore può eseguire una ricerca tra i documenti conservati trasversalmente sulle classi documentali;
- Visualizzazione delle statistiche di conservazione.

Il sistema di conservazione dei Conservatori Esterni integra il sistema di conservazione del Produttore e ne estende i servizi con funzionalità di stoccaggio digitale.

Le fasi di creazione, utilizzo e archiviazione dei documenti sono organizzate liberamente, in quanto il servizio di conservazione dei Conservatori interviene solamente nella fase di conservazione e solo per i documenti che il Produttore sceglie di conservare.

9.7 INDICE DEL PACCHETTO DI ARCHIVIAZIONE E RAPPORTO DI VERSAMENTO

Come già anticipato, l'Indice del Pacchetto di Archiviazione è un file in formato XML, marcato temporalmente e firmato digitalmente dal Responsabile della conservazione, generato dal sistema di

conservazione secondo la vigente normativa, che contiene le informazioni di conservazione del documento e viene con esso conservato.

In particolare nel file sono riportati:

- informazioni sull'applicazione che ha generato l'IPdA
- il token del documento
- l'operazione eseguita
- conservazione,
- rettifica,
- scarto
- cancellazione
- il bucket (area di conservazione) associato al Soggetto Produttore e la policy utilizzata
- il nome dei file che compongono il documento, incluso il file dei parametri di conservazione ed il file di indici, e le rispettive impronte
- eventuali informazioni relative al documento rettificante e rettificato
- il tempo di creazione (timestamp) del file IPdA.
- l'insieme degli IPdA di un pacchetto forma il rapporto di versamento.

Il file IPdA è reso disponibile con il documento di riferimento ad ogni operazione di conservazione e richiesta di esibizione.

Per i dettagli sulle modalità di gestione delle fasi previste (memorizzazione, creazione del file IPdA e marcatura temporale dello stesso) si rimanda ai "Manuali del Sistema di conservazione" dei Conservatori Esterni.

9.8 IL PROCESSO DI ESIBIZIONE DI UN PACCHETTO DI DISTRIBUZIONE

Le procedure di esibizione permettono di estrarre dal sistema di conservazione un pacchetto di distribuzione per cui sia stata completata correttamente la procedura di conservazione, di rettifica o di cancellazione, utilizzando il relativo token.

Insieme ai file costituenti il pacchetto di distribuzione, sono rese disponibili anche le informazioni che qualificano il processo di conservazione, ossia il file IPdA.

Non è possibile esibire parti singole di documento.

Il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, al documento informatico conservato, attraverso la produzione di un pacchetto di distribuzione.

In particolare ogni documento inserito nel sistema di conservazione è identificato in maniera univoca mediante una stringa denominata token.

Il token consente il reperimento di ciascun documento e la sua corretta esibizione, nonché la fruizione dei servizi di rettifica, di ricerca e di cancellazione logica.

Le procedure del sistema mantengono e aggiornano ad ogni nuovo invio il database di tutti i token; il database viene interrogato ad ogni richiesta di rettifica, scarto e cancellazione, ricerca ed esibizione confrontando il token inviato con quelli memorizzati.

La procedura assicura di agire solo sul documento richiesto, e solo se in possesso dei dovuti profili di autorizzazione.

9.9 ESIBIZIONE A NORMA

L'esibizione del pacchetto di distribuzione ottenuto tramite interrogazione al sistema di conservazione rappresenta un'esibizione completa, legalmente valida.

Un apposito strumento di esibizione e verifica permette di richiamare agevolmente un documento conservato e consente di ottenere in modo automatico sia la verifica delle firme digitali e delle marche temporali apposte che le verifiche di integrità dei documenti conservati e di tutti gli altri elementi conservati.

Si rimanda ai Manuali del Sistema di conservazione dei Conservatori Esterni, per il dettaglio delle funzionalità di verifica del sistema di conservazione e precisamente al par 7.6 per TI Trust Technologies e al par. 6 per Infocert.

9.10 PRODUZIONE COPIE E DUPLICATI

Si rimanda al "Manuale del Sistema di conservazione" di TI Trust Technologies, par 7.7

Si rimanda al "Manuale del Sistema di conservazione" di Infocert, par. 6

9.11 DESCRIZIONE DEL SISTEMA DI CONSERVAZIONE

Si rimanda al "Manuale del Sistema di conservazione" di TI Trust Technologies, par. 8

Si rimanda al "Manuale del Sistema di conservazione" di Infocert, par. 7

9.12 PROCEDURE DI MONITORAGGIO E CONTROLLO DEL SISTEMA DI CONSERVAZIONE

Si rimanda al "Manuale del Sistema di conservazione" di TI Trust Technologies, par. 9

Si rimanda al "Manuale del Sistema di conservazione" di Infocert, par. 7

9.13 COPIE DI SICUREZZA

Si rimanda al "Manuale del Sistema di conservazione" di TI Trust Technologies, par. 7.7

Si rimanda al "Manuale del Sistema di conservazione" di Infocert, par. 6

9.14 SCARTO DEI PACCHETTI DI ARCHIVIAZIONE

Si rimanda al "Manuale del Sistema di conservazione" di TI Trust Technologies, par. 7.8

Si rimanda al "Manuale del Sistema di conservazione" di Infocert, par. 6

9.15 INTEROPERABILITÀ

Si rimanda al "Manuale del Sistema di conservazione" di TI Trust Technologies, par. 7.9

Si rimanda al "Manuale del Sistema di conservazione" di Infocert, par. 6

9.16 FUNZIONALITÀ PER LA VERIFICA E IL MANTENIMENTO DELL'INTEGRITÀ DEGLI ARCHIVI

Si rimanda al "Manuale del Sistema di conservazione" di TI Trust Technologies, par. 9.2

Si rimanda al "Manuale del Sistema di conservazione" di Infocert, par. 7

9.17 MANTENIMENTO DELLA FIRMA PER IL PERIODO DI CONSERVAZIONE

Il sistema di conservazione di TI Trust Technologies si avvale di un fornitore terzo per le attività di firma digitale e di marcatura temporale. Questo fornitore garantisce che gli elaboratori che offrono il servizio di marcatura temporale e di firma digitale sono protetti da livelli di protezione logica estremamente elevati. La medesima collocazione fisica del sistema garantisce gli elaboratori dalla possibilità di compromissioni fisiche grazie agli accorgimenti tecnici atti ad impedire accessi non autorizzati da persone e danneggiamenti da eventi accidentali.

Nel sistema di conservazione di InfoCert, al buon esito del processo di conservazione, il Responsabile del servizio della conservazione di InfoCert appone la propria firma digitale su ogni pacchetto di archiviazione, mediante un sistema di firma automatica erogato dalla CA Certification Authority InfoCert, che si avvale di un dispositivo crittografico ad alte prestazioni HSM. Per maggiori dettagli si rinvia ai rispettivi manuali dei Conservatori esterni.

9.18 NORMATIVE IN VIGORE NEI LUOGHI DOVE SONO CONSERVATI I DOCUMENTI

I documenti informatici sono conservati in Italia; pertanto al sistema di conservazione di TI Trust Technologies e di Infocert sono applicabili le norme italiane.

9.19 FASI DEL PROCESSO DI CONSERVAZIONE E RESPONSABILITÀ

Il servizio di conservazione digitale dei documenti informatici predisposto dal Conservatore risponde alla esigenza di conservare documenti informatici della Pubblica Amministrazione.

Il servizio permette di conservare i documenti informatici del Produttore, garantendone l'integrità e la validità legale nel tempo nonché la loro "esibizione a norma".

Il sistema di conservazione opera secondo i modelli organizzativi che garantiscono la sua distinzione logica dal sistema di gestione documentale del Produttore.

Pertanto, la conservazione non viene svolta all'interno della struttura organizzativa del Produttore (soggetto titolare dei documenti informatici da conservare), ma è affidata ai Conservatori indicati in precedenza, che espleteranno le attività per le quali hanno ricevuto formale delega, nei limiti della stessa e per le quali operano in modo autonomo e ne sono responsabili.

La sequenza di attività che vanno dalla fase propedeutica alla formazione dei documenti informatici alla fase di conservazione degli stessi è di seguito schematicamente rappresentata.

Sistemi	**Fase**	**Descrizione e MACRO FASI del processo di conservazione**	**Attività a carico di:** **Produttore/Conservatore**	
Sistema di gestione documentale del Produttore	1	Produzione/formazione/emissione a norma dei documenti informatici e contestuale generazione dei relativi metadati	X	
	2	Produzione del pacchetto di versamento	X	
	3	Deposito in conservazione del pacchetto di versamento e dei relativi documenti informatici completi di metadati	X	
Servizio di Fatturazione PA e PEC	1	Produzione/formazione/emissione a norma dei documenti informatici e contestuale generazione dei relativi metadati		X
	2	Produzione del pacchetto di versamento		X
	3	Deposito in conservazione del pacchetto di versamento e dei relativi documenti informatici completi di metadati		X
Sistema di Firma Digitale	4	Servizio di Firma Automatica e di eventuale apposizione marca temporale, da effettuare sui documenti tributari prima dell'invio al sistema di conservazione.	X	X

Sistemi	***Fase***	***Descrizione e MACRO FASI del processo di conservazione***	***Attività a carico di:*** ***Produttore/Conservatore***	
Sistema di conservazione digitale dei documenti informatici	5	Acquisizione da parte del sistema di conservazione del pacchetto di versamento prodotto dal Produttore per la sua presa in carico		X
	6	Verifica che il pacchetto di versamento ed i documenti informatici in esso descritti siano coerenti e conformi alle prescrizioni stabilite dal Contratto di servizio		X
	7	Eventuale rifiuto del pacchetto di versamento o dei documenti informatici, nel caso in cui le verifiche di cui alla fase 6 abbiano evidenziato delle anomalie		X

	8	Generazione, in modo automatico, del rapporto di versamento relativo a ciascun pacchetto di versamento		X
	9	Invio al Produttore del rapporto di versamento		X
	10	Preparazione e gestione del pacchetto di archiviazione		X
	11	"Chiusura" del pacchetto di archiviazione mediante sottoscrizione con firma digitale di TI Trust Technologies e apposizione di marca temporale		X
	12	Richieste di esibizione dei documenti informatici conservati	X	
	13	Preparazione del pacchetto di distribuzione ai fini dell'esibizione richiesta dall'utente con tutti gli elementi necessari a garantire l'integrità e l'autenticità degli stessi		X
	14	Richiesta del Produttore di duplicati informatici	X	
	15	Produzione di duplicati informatici su richiesta del Produttore		X

10 TRATTAMENTO DEI DATI PERSONALI

10.1 TUTELA E DIRITTI DEGLI INTERESSATI

In materia di trattamento dei dati personali i Conservatori, come innanzi individuati, garantiscono la tutela degli interessati in ottemperanza a quanto disposto dal D. Lgs. 196/2003 e s.m.i. così come modificato dal D. Lgs 101/2018 e s.m.i. e dal Regolamento UE 2016/679 e s.m.i.

In particolare, agli interessati sono fornite le informative di cui all'art. 13 del Regolamento UE 2016/679 GDPR in materia di protezione dei dati personali. Nella suddetta informativa il Produttore è informato sui diritti di accesso ai dati personali ed altri diritti.

10.2 MODALITÀ DEL TRATTAMENTO

I dati personali sono trattati con strumenti automatizzati per il tempo strettamente necessario a conseguire gli scopi per cui sono stati raccolti.

Specifiche misure di sicurezza, come descritte nei "Manuali del Sistema di Conservazione" dei Conservatori e nei Contratti sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati.

10.3 FINALITÀ DEL TRATTAMENTO

Il trattamento dei dati è finalizzato all'erogazione del servizio di conservazione digitale dei documenti informatici: i dati raccolti sono utilizzati così come definito con i Conservatori esterni per l'attivazione del Servizio di conservazione digitale dei documenti informatici. I Conservatori esterni utilizzeranno i dati raccolti per lo svolgimento dell'attività connessa e/o derivante dal Servizio di conservazione digitale dei documenti informatici del Produttore.

Per motivi d'ordine pubblico, nel rispetto delle disposizioni di legge per la sicurezza e la difesa dello Stato, per la prevenzione, accertamento e/o repressione dei reati, i documenti informatici ed i dati forniti ai Conservatori potranno essere comunicati a soggetti pubblici, quali forze dell'ordine, Autorità pubbliche e autorità Giudiziaria per lo svolgimento delle attività di loro competenza.

10.4 SICUREZZA DEI DATI

Come previsto dalle norme vigenti in materia, i Conservatori esterni adottano idonee e preventive misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei documenti informatici, di danneggiamento delle risorse hardware su cui i documenti informatici sono registrati ed i locali dove i medesimi vengono custoditi nonché l'accesso non autorizzato ai documenti stessi e i trattamenti non consentiti dalla legge o dai regolamenti aziendali.

Le misure di sicurezza adottate dai Conservatori esterni, per i cui dettagli si rinvia ai rispettivi manuali, assicurano:

- l'integrità dei documenti informatici, da intendersi come salvaguardia dell'esattezza dei dati, difesa da manomissioni o modifiche da parte di soggetti non autorizzati;

- la disponibilità dei dati e dei documenti informatici da intendersi come la certezza che l'accesso sia sempre possibile quando necessario; indica quindi la garanzia di fruibilità dei documenti informatici, evitando la perdita o la riduzione dei dati anche accidentale utilizzando un sistema di backup;

- la riservatezza dei documenti informatici da intendersi come garanzia che le informazioni siano accessibili solo da persone autorizzate e come protezione delle trasmissioni e controllo degli accessi stessi.

11. DISPOSIZIONI FINALI

Il presente Manuale, come indicato nelle Linee Guida, è oggetto di aggiornamento periodico da parte del Responsabile della conservazione, in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Le disposizioni/attività indicate nel presente documento si intendono integrate con quanto specificatamente indicato nel Disciplinare Tecnico (Allegato 1), con acclusi i Manuali di conservazione dei Conservatori Esterni TI Trust Technologies (Allegato 1 sub A) e Infocert (Allegato 1 sub B), e nel Piano della sicurezza (Allegato 2).

Per tutto quanto non espressamente previsto dal presente Manuale si fa rinvio e riferimento alla vigente normativa in materia.

SAN GIUSEPPE MOSCATI - AVELLINO
AZIENDA OSPEDALIERA DI RILIEVO NAZIONALE E DI ALTA SPECIALITÀ

MANUALE DI CONSERVAZIONE DELL'AZIENDA OSPEDALIERA DI RILIEVO NAZIONALE SAN GIUSEPPE MOSCATI DI AVELLINO

ALLEGATO 1
DISCIPLINARE TECNICO

Indice

INTRODUZIONE **1**

1. FORMATI GESTITI **2**

1.1 CARATTERISTICHE GENERALI DEI FORMATI 2

1.2 FORMATI PER LA CONSERVAZIONE 3

2. LA TIPOLOGIA DEI PACCHETTI INFORMATIVI GESTITI **6**

2.1 SPECIFICHE DEL PACCHETTO DI VERSAMENTO 6

2.2 SPECIFICHE DEL RAPPORTO DI VERSAMENTO 6

3. TIPOLOGIE DEI DOCUMENTI POSTI IN CONSERVAZIONE **7**

4. METADATI DA ASSOCIARE ALLE DIVERSE TIPOLOGIE DI DOCUMENTI **8**

4.1 METADATI MINIMI DA ASSOCIARE A QUALSIASI DOCUMENTO INFORMATICO 8

4.2 METADATI MINIMI DEL DOCUMENTO INFORMATICO AMMINISTRATIVO 8

4.3 METADATI UTILIZZATI 9

5. DISPOSIZIONI FINALI **10**

INTRODUZIONE

Il presente Disciplinare Tecnico definisce le specifiche operative e le modalità di descrizione e di versamento nel Sistema di conservazione digitale dei documenti informatici e delle aggregazioni documentali informatiche. Analogamente ai Manuali della Conservazione dei Conservatori Esterni, tale documento viene periodicamente aggiornato, dal Responsabile della Conservazione, in base alla eventuale ridefinizione delle tipologie documentali che il Produttore intende portare in conservazione nel Sistema di Conservazione di TI Trust Technologies e nel Sistema di Conservazione di InfoCert, nonché sulla base dell'evoluzione tecnologica e dell'obsolescenza dei formati, nonché dell'evoluzione della normativa di settore.

1. FORMATI GESTITI

La leggibilità di un documento informatico dipende dalla possibilità e dalla capacità di interpretare ed elaborare correttamente i dati binari che costituiscono il documento, secondo le regole stabilite dal formato con cui esso è stato rappresentato.

Il formato di un documento informatico è la convenzione usata per rappresentare il contenuto informativo mediante una sequenza di byte.

Nel seguito vengono fornite le indicazioni sui formati dei documenti informatici che per le loro caratteristiche sono, al momento attuale, da ritenersi coerenti con la conservazione digitale a lungo termine.

Infatti, una possibile soluzione al problema dell'obsolescenza, che porta all'impossibilità di interpretare correttamente formati non più supportati al fine di renderli visualizzabili, è quella di selezionare formati standard.

1.1 CARATTERISTICHE GENERALI DEI FORMATI

	Caratteristica	Descrizione della Caratteristica
1	**APERTURA**	Un formato si dice "aperto" quando è conforme a specifiche pubbliche, cioè disponibili a chiunque abbia interesse ad utilizzare quel formato. La disponibilità delle specifiche del formato rende sempre possibile la decodifica dei documenti rappresentati in conformità con dette specifiche, anche in assenza di prodotti che effettuino tale operazione automaticamente. Questa condizione si verifica sia quando il formato è documentato e pubblicato da un produttore o da un consorzio al fine di promuoverne l'adozione, sia quando il documento è conforme a formati definiti da organismi di standardizzazione riconosciuti. In quest'ultimo caso tuttavia si confida che quest'ultimi garantiscono l'adeguatezza e la completezza delle specifiche stesse. In relazione a questo aspetto, sono da privilegiarsi formati già approvati dagli Organismi di standardizzazione internazionali quali ISO e OASIS.
2	**SICUREZZA**	La sicurezza di un formato dipende da due elementi: ▪ il grado di modificabilità del contenuto del file; ▪ la capacità di essere immune dall'inserimento di codice maligno.
3	**PORTABILITÀ**	Per portabilità si intende la facilità con cui i formati possano essere usati su piattaforme diverse, sia dal punto di vista dell'hardware che del software, inteso come sistema operativo. Di fatto si ottiene mediante l'impiego fedele di standard documentati e accessibili e dalla loro diffusione sul mercato.
4	**FUNZIONALITÀ**	Per funzionalità si intende la possibilità da parte di un formato di essere gestito da prodotti in-ormatici, che prevedono una varietà di funzioni

		messe a disposizione del Produttore per la formazione e gestione del documento informatico.
5	**SUPPORTO ALLO SVILUPPO**	Il supporto allo sviluppo è la modalità con cui si mettono a disposizione le risorse necessarie alla manutenzione e sviluppo del formato e i prodotti informatici che lo gestiscono (organismi preposti alla definizione di specifiche tecniche e standard, società, comunità di sviluppatori, ecc.).
6	**DIFFUSIONE**	La diffusione è l'estensione dell'impiego di uno specifico formato per la formazione e la gestione dei documenti informatici. Questo elemento influisce sulla probabilità che esso venga supportato nel tempo, attraverso la disponibilità di più prodotti informatici idonei alla sua gestione e visualizzazione.

1.2 FORMATI PER LA CONSERVAZIONE

Oltre al soddisfacimento delle caratteristiche precedentemente elencate, la scelta dei formati idonei alla conservazione si è orientata verso formati capaci di far assumere al documento le fondamentali caratteristiche di immodificabilità e staticità.

Pertanto, alla luce delle suddette considerazioni, i formati adottati per la conservazione delle diverse tipologie di documenti informatici, in accordo con quanto previsto dai Conservatori, sono i seguenti:

Formato PDF/A	**Descrizione**	
	Il PDF (Portable Document Format) è un formato creato da Adobe nel 1993 che attualmente si basa sullo standard ISO 32000. Questo formato è stato concepito per rappresentare documenti complessi in modo indipendente dalle caratteristiche dell'ambiente di elaborazione del documento. Il formato è stato ampliato in una serie di sotto-formati tra cui il PDF/A.	
Caratteristiche e dati informativi		
	Informazioni gestibili	testo formattato, immagini, grafica vettoriale 2D e 3D, filmati.
	Sviluppato da	Adobe Systems - http://www.adobe.com/
	Estensione	.pdf
	Tipo MIME	Application/pdf
	Formato aperto	SI
	Specifiche tecniche	Pubbliche
	Standard	ISO 19005-1:2005 (vesr. PDF 1.4)

	Altre caratteristiche	assenza di collegamenti esterni assenza di codici eseguibili assenza di contenuti crittografati il file risulta indipendente da codici e collegamenti esterni che ne possono alterare l'integrità e l'uniformità nel lungo periodo le più diffuse suite d'ufficio permettono di salvare direttamente i file nel formato PDF/A sono disponibili prodotti per la verifica della conformità di un documento PDF al formato PDF/A
	Software necessario alla visualizzazione	Adobe Reader

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

		opportuno file xslt, produrne una copia human readable con Microsoft Internet Explorer / Firefox / Google Chrome o altri browser.

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

2. LA TIPOLOGIA DEI PACCHETTI INFORMATIVI GESTITI

2.1 SPECIFICHE DEL PACCHETTO DI VERSAMENTO

Riferimento paragrafo 6 Manuale del Sistema di Conservazione di TI Trust Technologies (Allegato 1 sub A).

Riferimento paragrafo 6 Manuale del Sistema di Conservazione di Infocert (Allegato 1 sub B).

2.2 SPECIFICHE DEL RAPPORTO DI VERSAMENTO

Riferimento paragrafo 7 Manuale del Sistema di Conservazione di TI Trust Technologies (Allegato 1 sub A).

Riferimento paragrafo 6 Manuale del Sistema di Conservazione di Infocert (Allegato 1 sub B).

3. TIPOLOGIE DEI DOCUMENTI POSTI IN CONSERVAZIONE

L'AORN S.G. Moscati di Avellino porta in conservazione i seguenti tipi di documenti:

- Area amministrativa:
- Registro giornaliero di protocollo
- PEC
- Delibere informatizzate
- Determine informatizzate
- Delibere digitalizzate
- Determine digitalizzate
- Fatture elettroniche attive e notifiche
- Fatture elettroniche passive e notifiche
- Contratti
- Cartelle cliniche digitalizzate

Tutti i documenti vengono riversati in conservazione utilizzando la piattaforma Legal Archive di Trust Technologies, ad eccezione delle PEC e delle Fatture Elettroniche attive e notifiche e Fatture elettroniche passive e notifiche la cui conservazione è affidata alla piattaforma LegalDoc di Infocert.

4. METADATI DA ASSOCIARE ALLE DIVERSE TIPOLOGIE DI DOCUMENTI

Con il termine "metadati" si indicano tutte le informazioni significative associate al documento informatico, escluse quelle che costituiscono il contenuto del documento stesso.

I metadati riguardano principalmente, ma non esclusivamente, i modi, i tempi ed i soggetti coinvolti nel processo della formazione del documento informatico, della sua gestione e della sua conservazione.

Metadati sono anche le informazioni riguardanti gli autori, gli eventuali sottoscrittori e le modalità di sottoscrizione e la classificazione del documento.

I metadati che seguono devono essere associati al documento dal Produttore prima del versamento in conservazione.

I metadati, seppur chiaramente associati al documento informatico, possono essere gestiti indipendentemente dallo stesso. In relazione ai diversi tipi di documenti informatici posti in conservazione, è previsto un "set minimo" di metadati come di seguito specificato.

4.1 METADATI MINIMI DA ASSOCIARE A QUALSIASI DOCUMENTO INFORMATICO

I metadati che seguono devono essere associati ad ogni documento informatico, a prescindere dalla specializzazione che questo assume (amministrativo, fiscale, ecc.).

Al documento informatico immodificabile, il Produttore dovrà associare i metadati che sono stati generati durante la sua formazione.

L'insieme minimo dei metadati è costituito da:

1. l'identificativo univoco e persistente
2. il riferimento temporale (data di chiusura)
3. l'oggetto
4. il soggetto che ha formato il documento
    a. nome
    b. cognome
    c. Codice Fiscale
5. l'eventuale destinatario
    a. nome
    b. cognome
    c. Codice Fiscale (unico dato obbligatorio del destinatario).

4.2 METADATI MINIMI DEL DOCUMENTO INFORMATICO AMMINISTRATIVO

Le Pubbliche Amministrazioni formano gli originali dei propri documenti amministrativi informatici attraverso gli strumenti informatici riportati nel Manuale di gestione.

Detto documento amministrativo informatico è identificato e trattato nel sistema di gestione informatica dei documenti del Produttore.

Pertanto, al documento amministrativo informatico, il Produttore deve associare, oltre ai metadati di cui al punto precedente, anche l'insieme minimo dei metadati ai sensi delle nuove Linee Guida AgID di cui alle Determinazioni 407/2020 e 371/2021:

- numero di protocollo del documento;
- data di registrazione di protocollo;
- mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti;
- oggetto del documento;
- data e protocollo del documento ricevuto, se disponibile;
- l'impronta del documento informatico.

4.3 METADATI UTILIZZATI

Si fa riferimento al Manuale della conservazione, in cui sono specificati per ogni tipologia documentale i metadati utilizzati.

5. DISPOSIZIONI FINALI

Il presente documento, come indicato nelle Linee Guida, è oggetto di aggiornamento periodico, da parte del Responsabile della Conservazione, in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.
Il presente documento costituisce allegato al Manuale di conservazione (Allegato 1).
Al presente Disciplinare Tecnico sono acclusi i Manuali di conservazione dei Conservatori Esterni TI Trust Technologies (Allegato 1 sub A) e Infocert (Allegato 1 sub B).
Per tutto quanto non espressamente previsto dal presente manuale si fa rinvio e riferimento alla vigente normativa in materia.

Manuale di Conservazione

Telecom Italia Trust Technologies S.r.l. - Documento pubblico – Tutti i diritti riservati

VERSIONI DEL DOCUMENTO		
Revisione	Descrizione delle modifiche	Emissione
00	Prima emissione	22/10/2014
01	Aggiornamento Template, Indice, Nomenclatura, Normativa, Ruoli e responsabilità	22/03/2016
02	Revisione generale del documento con interventi principali su: 1. Cap. 1 - Scopo del documento: precisazione relative alle modalità di commercializzazione dei servizi, degli aspetti contrattuali e dei ruoli; 2. Par. 3.1 - Normativa di riferimento: Revisione e integrazione delle fonti normative; 3. Cap. 4 - Ruoli e responsabilità: sintesi e chiarimenti sui ruoli; modifica del Responsabile del servizio di Conservazione; 4. Cap. 5 - Struttura organizzativa per il SERVIZIO : precisazioni in merito alle nomine per il trattamento dei dati e sull'organizzazione; 5. Cap. 6 - Oggetti sottoposti a conservazione: precisazioni in merito alle modalità di conservazione 6. Cap. 7 - Il processo di conservazione: precisazioni e miglioramento della descrizione del processo. 7. Par. 7.1- Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico: migliorata la rappresentazione delle modalità 8. Par. 7.2 - Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti: migliorata la descrizione delle verifiche effettuate 9. Par. 7.6 - Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione.: Migliorata la descrizione delle attività effettuate 10. Par. 7.7 - Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti: Precisazioni sulle copie e le duplicazioni 11. Par. 7.9.1 - Cessazione del SERVIZIO: Precisazione sui termini dell'attività e sugli obblighi di accesso 12. Par. 8.1.1 - Sistema di versamento (SV).e Par. 8.1.4 - Sistema di accesso: Eliminate alcune tabelle di dettaglio ridondanti 13. Par. 8.4 - Procedure di gestione e di evoluzione: Eliminazione di alcune informazioni ridondanti 14. Per. 9.3 - SLA e soluzioni adottate in caso di anomalie: Ridefinizione ed aggiornamento degli SLA	04/05/2017
03	Aggiornamento Cap. 4 – Ruoli e responsabilità: aggiornamento delle date effettive di nomina dei Responsabili;	02/08/2017
04	Revisione generale del documento con interventi principali su: 1. Cap. 1 - Scopo del documento: Aggiornamento della qualifica di Conservatore Accreditato; Riferimenti del Conservatore 2. Par.2.2- Acronimi: Inserimento acronimi per nuovi formati trattati; 3. Par. 3.1 - Normativa di riferimento: Inserimento riferimento alla normativa GDPR (Regolamento UE 2016/679); 4. Cap. 4 - Ruoli e responsabilità: Aggiornamento ruoli (Responsabile sicurezza e Responsabile Trattamento Dati); 5. Par. 6.1 - Oggetti conservati: inserimento nuovi formati; 6. Par. 6.2 - Il pacchetto di versamento (PdV) e par. 6.3 - Il pacchetto di archiviazione (PdA): aggiornamento informazioni relative alle modalità di gestione e trattamento dei pacchetti; 7. Cap. 7- Il processo di conservazione: aggiornamento della descrizione dei sotto processi a seguito dell'introduzione di nuovi formati e nuove tipologie di documenti; 8. Par. 8.2 - Componenti tecnologiche: aggiornamento delle informazioni relative ad elementi infrastrutturali 9. Par. 8.2.1 - Servizi Erogati: Aggiornamento dei siti di riferimento a seguito dell'introduzione di nuove tipologie di documenti.	25/05/2018
05	Inserimento cap. 11 - Protezione dei dati personali	29/08/18

06	1. Aggiornamento dati identificativi (par. 1.1) e struttura organizzativa (par. 1.2) del Conservatore 2. Correzione di refusi e riferimenti nel testo 3. Modifica definizione di 'sicurezza' (cap. 2) 4. Aggiornamento della tabella n. Tabella 9 - Formati ammessi per la conservazione 5. Revisione terminologia par. 7.9	08/11/2018
07	1. Aggiornamento dati identificativi (par. 1.1) e struttura organizzativa (par. 1.2) del Conservatore 2. Correzione di refusi e riferimenti nel testo	17/02/2021
08	1. Revisione generale del documento per adeguamento Linee Guida AgID in materia di formazione, gestione, conservazione dei documenti informatici; 2. Correzione di refusi e riferimenti nel testo; 3. Aggiornamento del paragrafo 1.2; 4. Modifica del nome del paragrafo "Par. 7.9.1 - Cessazione del SERVIZIO" in "Cessazione del SERVIZIO";	12/01/2022
09	1. Correzione di refusi e riferimenti nel testo; 2. Aggiornamento dati identificativi (par. 1.1) cambio indirizzo posta elettronica;	05/04/2022

Telecom Italia Trust Technologies è proprietaria delle informazioni contenute nel presente documento, che può essere liberamente divulgato all'esterno del Gruppo Telecom Italia, con riserva di tutti i diritti rispetto all'intero contenuto.

Indice degli argomenti

1 Scopo del documento 6
1.1 Dati identificativi del conservatore 7
1.2 Struttura organizzativa del conservatore 8

2 Terminologia (Glossario, Acronimi) 8
2.1 Glossario 8
2.2 Acronimi 14

3 Normativa e standard di riferimento 15
3.1 Normativa di riferimento 15
3.2 Standard di riferimento 16

4 Ruoli e responsabilità 17

5 Struttura organizzativa per il SERVIZIO 21
5.1 Organigramma 21
5.2 Strutture organizzative 21
5.2.1 Attività relative al contratto con i Soggetti Produttori 22
5.2.2 Attività relative alla gestione dei sistemi informativi 24

6 Oggetti sottoposti a conservazione 24
6.1 Oggetti conservati 25
6.2 Il pacchetto di versamento (PdV) 27
6.3 Il pacchetto di archiviazione (PdA) 27
6.4 Il pacchetto di distribuzione (PdD) 30

7 Il processo di conservazione 31
7.1 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico 31
7.2 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti 32
7.3 Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico 32
7.4 Rifiuto del pacchetto di versamento 33
7.5 Preparazione e gestione del pacchetto di archiviazione 33
7.6 Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione. 34
7.7 Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti 35
7.8 Scarto dei pacchetti di archiviazione 35
7.9 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori 36
7.9.1 Cessazione del SERVIZIO 37

8 Il sistema di conservazione 37
8.1 Componenti logiche 38
8.1.1 Sistema di versamento (SV). 38
8.1.2 Sistema di gestione dati (SGD) 39

8.1.3 Sistema di memorizzazione (SM) 40
8.1.4 Sistema di accesso 40
8.2 Componenti tecnologiche 41
8.2.1 Servizi Erogati 42
8.2.1.1 Scalabilità sui volumi 42
8.3 Componenti fisiche 43
8.3.1 Piattaforma di esercizio primario del SERVIZIO 43
8.4 Procedure di gestione e di evoluzione 44

9 Monitoraggi e controlli 45
9.1 Procedure di monitoraggio 46
9.2 Verifica l'integrità degli archivi 47
9.3 SLA e soluzioni adottate in caso di anomalie 47

10 Assistenza al Cliente 48

11 Protezione dei dati personali 48

1 Scopo del documento

Il presente documento è il Manuale di Conservazione del Conservatore Qualificato Telecom Italia Trust Technologies S.r.l. (in breve TI Trust Technologies o TI.TT), redatto ai sensi delle Linee guida sulla formazione, gestione e conservazione dei documenti informatici. Il Manuale di conservazione è un documento informatico che illustra l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.

Il presente manuale di conservazione è un documento informatico e come tale anch'esso sottoposto al processo di conservazione digitale.

I SERVIZI di conservazione (di qui in avanti, per brevità, il SERVIZIO o i SERVIZI) sono erogati in tutto o in parte da TI.TT tramite specifiche ed idonee infrastrutture tecnologiche, come descritto nella seguente documentazione ed in altri documenti eventualmente in essa richiamati:

- il presente Manuale di Conservazione;
- le Descrizioni delle tipologie di servizi pubblicate da TI.TT sul proprio sito https://www.trusttechnologies.it/download/documentazione;
- gli eventuali documenti denominati "Specificità del Contratto", nel quale sono illustrati elementi tipici delle singole forniture verso determinati Clienti Finali e che costituiscono allegati al presente Manuale di Conservazione.

Nell'ambito dei rapporti contrattuali si identificano i soggetti di seguito indicati:

- **VENDITORE**: soggetto che stipula il contratto di vendita dei SERVIZI nei confronti del CLIENTE FINALE e degli UTILIZZATORI;
- **CLIENTE FINALE**: il soggetto che acquisisce i SERVIZI erogati da TI.TT tramite il VENDITORE, affinché siano utilizzati da:
  - sé medesimo;
  - soggetti afferenti alla propria organizzazione;
  - soggetti che abbiano un rapporto contrattuale con il CLIENTE FINALE, ovvero con una struttura od un'organizzazione a questi collegata da un rapporto contrattuale;
- **UTILIZZATORE**: il soggetto che usa il SERVIZIO erogato da TI.TT;

I SERVIZI erogati da TI.TT sono regolati dalla documentazione di natura contrattuale descritta di seguito, cui si fa riferimento secondo l'ordine di prevalenza indicato in caso di contestazione o di discordanza tra le condizioni ed i termini convenuti tra le Parti:

1. Contratto di Vendita: contratto di vendita del singolo SERVIZIO intercorrente tra il Venditore ed il Cliente Finale;
2. Scheda di attivazione del SERVIZIO e Scheda di configurazione del SERVIZIO, secondo i modelli resi disponibili al momento della richiesta di attivazione effettuata dal Cliente;
3. Modulo Accettazione Condizioni ed Informativa (codice CAITPRIN.TTSOCF16002)
4. Condizioni Specifiche (codice CAITPRIN.TT.SOCF17001);
5. Condizioni Generali (codice CAITPRIN.TT.SOCF16000): esse saranno applicabili al rapporto contrattuale in essere tra TI.TT ed il Cliente Finale e/o l'Utilizzatore, fatto salvo quanto convenuto specificamente nel Contratto di Vendita e/o in altri documenti specificamente richiamati.

TI.TT rende disponibili le versioni aggiornate di tutta la documentazione rilevante da un punto di vista contrattuale mediante pubblicazione agli indirizzi seguenti (o comunque opportunamente ed idoneamente referenziati):

- https://www.trusttechnologies.it/download/documentazione/;
- https://www.trusttechnologies.it/legale_e_privacy.

Con la sottoscrizione delle condizioni che regolano i SERVIZI CN e della MODULISTICA prevista per la loro attivazione, TI.TT, affidatario del servizio di conservazione ha designato formalmente, al proprio interno, il **Responsabile del servizio di Conservazione**.

I SERVIZI sono erogati da TI.TT come operatore **certificato e qualificato** in conformità alla Normativa italiana in materia di Conservazione dei Documenti Informatici ed al Regolamento (UE) N. 910/2014 del Parlamento Europeo

e del Consiglio del 23 luglio 2014 (EIDAS) ed alla normativa per la sua attuazione. Pertanto, il presente MANUALE DI CONSERVAZIONE costituisce anche Certificate Practice Statement ai fini dell'applicazione di tale normativa.

Torna al sommario

1.1 Dati identificativi del conservatore

La società TI.TT è una società del Gruppo TIM (Direzione e coordinamento di TIM S.p.A.) con unico socio TIM S.p.A.

Il responsabile del presente Manuale di conservazione è Salvatore Nappi.

Denominazione sociale	Telecom Italia Trust Technologies s.r.l.
Indirizzo sede legale	S. R.148 Pontina, km. 29,100 00071 - Pomezia (RM)
Amministratore Delegato	Nappi Salvatore
n. P.IVA	04599340967
n. telefono (centralino) n. fax	+390682659601 +390682659619
Sito internet	www.trusttechnologies.it
Indirizzo Pec	TI.TT@ttpec.telecomitalia.it
Referente tecnico cui rivolgersi in caso di problemi tecnico operativi Indirizzo n. telefono indirizzo posta elettronica	CALL CENTER: S. R.148 Pontina, km. 29,100 00071 - Pomezia (RM) 800.28.75.24 conservazione-operation@telecomitalia.it

Tabella 1 - Dati identificativi del soggetto conservatore

Torna al sommario

1.2 Struttura organizzativa del conservatore

L'organizzazione di TI Trust Technologies (illustrata nel diagramma sopra) si articola nelle seguenti funzioni ed attività che rispondono all'Amministratore Delegato Ing. Salvatore Nappi e delle quali si evidenziano più oltre i presidi dei processi operativi:

- **Marketing & Sales**, con la responsabilità di assicurare il presidio specialistico delle attività di commercializzazione del portafoglio di offerta:
- **Operations**, con la responsabilità di assicurare lo sviluppo applicativo ed il supporto tecnico per le piattaforme dell'offerta di competenza.

Alle dirette dipendenze dell'A.D. opera, inoltre, un'area di staff denominata **Compliance, Governance & Security**.

Le funzioni e le aree di attività sono direttamente collegate con il governo e lo sviluppo del business e dell'azienda nel suo insieme, assicurando la gestione e sviluppo dell'operatività, il relativo sistema di offerta, lo sviluppo del know-how e la redditività economica.

2 Terminologia (Glossario, Acronimi)

Nel presente capitolo, sono riportati il Glossario dei termini e gli Acronimi ricorrenti nel testo o che sono comunque significativi in relazione al SERVIZIO.

Torna al sommario

2.1 Glossario

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.
Allegato	Documento che compone l'Unità documentaria per integrare le informazioni contenute nel documento principale. È redatto contestualmente o precedentemente al documento principale. La sua presenza è facoltativa.
Annesso	Documento che compone l'Unità documentaria, generalmente prodotto e inserito nell' unità documentaria in un momento successivo a quello di creazione dell'Unità documentaria, per fornire ulteriori notizie e informazioni a corredo del Documento principale.
Apertura	Elemento caratteristico di un formato conforme a specifiche pubbliche, cioè disponibili a chiunque abbia interesse ad utilizzarlo. Gli organismi di standardizzazione internazionali considerati dalla normativa sono ISO e ETSI.

Application server	Tipologia di server che fornisce l'infrastruttura e le funzionalità di supporto, sviluppo ed esecuzione di applicazioni nonché altri componenti server in un contesto distribuito. Si tratta di un complesso di servizi orientati alla realizzazione di applicazioni ad architettura multilivello ed enterprise, con alto grado di complessità, spesso orientate per il web (applicazioni web).
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.
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.
Cluster	Insieme di dispositivi di elaborazione connessi in maniera più o meno stretta che operano insieme in modo tale da poter essere considerati un unico sistema.
Codice	Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni.
Comunità di riferimento	Un gruppo ben individuato di potenziali Utenti che dovrebbero essere in grado di comprendere un particolare insieme di informazioni. La Comunità di riferimento può essere composta da più comunità di Utenti [da OAIS].
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.
Contenuto informativo	Insieme delle informazioni che costituisce l'obiettivo originario della conservazione. È composto dall'Oggetto-dati e dalle Informazioni di rappresentazione [da OAIS].
Data center	Struttura utilizzata per ospitare computer e componenti associati quali dispositivi di telecomunicazioni e di storage, in generale con adeguati livelli di prestazioni e di sicurezza.
Diffusione	Estensione dell'impiego di uno specifico formato per la formazione e la gestione dei documenti informatici affinché sia più probabile che esso venga supportato nel tempo. La questione ha impatti sul fatto che un formato possa avere la disponibilità di più prodotti informatici idonei alla sua gestione e visualizzazione.
Digest	Vedi impronta crittografica.
Disaster recovery	Insieme delle misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi di business per imprese, associazioni o enti, a fronte di gravi emergenze che ne intacchino la regolare attività.
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	Documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario.
Esibizione	Operazione che consente di visualizzare un documento conservato e di ottenerne copia.
Estratto di documento informatico	Parte del documento tratto dal documento originale.
Estratto per riassunto di documento informatico	Documento nel quale si attestano in maniera sintetica fatti, stati o qualità desunti da documenti informatici.
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 di simboli binari (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.
File di indice	Indice dell'AIP: file XML che contiene tutti gli elementi del Pacchetto di archiviazione, derivati sia dalle informazioni contenute nel SIP (o nei SIP) trasmessi dal Produttore, sia da quelle generate dal Sistema di conservazione nel corso del processo di conservazione.
File-manifesto	File che contiene metadati riferiti ad un file o ad un pacchetto di file.
Filesystem	Sistema di gestione dei file, strutturato mediante una o più gerarchie ad albero, che determina le modalità di assegnazione dei nomi, memorizzazione e organizzazione all'interno di uno storage.
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.
Formato del documento informatico	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
Formato "deprecato"	Formato in passato considerato ufficiale il cui uso è attualmente sconsigliato a favore di una versione più recente.
Funzionalità	Possibilità da parte di un formato di essere gestito da prodotti informatici, che prevedono una varietà di funzioni messe a disposizione dell'utente per la formazione e gestione del documento informatico.
Funzione di hash crittografica	Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o digest in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
Identificativo univoco	Sequenza di 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.
Informazioni descrittive	Elementi che descrivono il pacchetto informativo e consentono di ricercarlo nel sistema di conservazione. In base alle caratteristiche della tipologia di oggetto contenuto nel Pacchetto, tali informazioni possono essere un sottoinsieme di quelle presenti nel pacchetto informativo, possono coincidere o possono anche essere diverse.
Informazioni sulla conservazione (PDI)	Informazioni necessarie a conservare il Contenuto informativo e garantiscono che lo stesso sia chiaramente identificato e che sia chiarito il contesto in cui è stato creato. Sono costituite da metadati che definiscono la provenienza, il contesto, l'identificazione e l'integrità del Contenuto informativo oggetto della conservazione [da OAIS].
Informazioni sulla rappresentazione	Informazioni che associano un Oggetto-dati a concetti più significativi.
Informazioni sull'impacchettamento	Informazioni che consentono di mettere in relazione nel Sistema di conservazione, in modo stabile e persistente, il Contenuto informativo con le relative Informazioni sulla conservazione.
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.
Log di sistema	Registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati.
Manuale di conservazione	Documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture.
Marca temporale	Sequenza di caratteri che rappresentano una data e/o un orario per accertare l'effettivo avvenimento di un certo evento. La data è di solito presentata in un formato compatibile, in modo che sia facile da comparare con un'altra per stabilirne l'ordine temporale. La pratica dell'applicazione di tale marca temporale è detta timestamping.
Memorizzazione	Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici.
Metadati	Dati associati a un o documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017.
Oggetto 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 un formato predefinito e concordato descritto nel manuale di conservazione.
Pacchetto informativo	Contenitore logico che racchiude uno o più oggetti di conservazione con i relativi metadati, oppure anche i soli metadati riferiti agli oggetti di conservazione.
Pathname	Concatenazione ordinata del percorso di un file e del suo nome.
Percorso (path)	Informazioni relative alla localizzazione virtuale del file all'interno del filesystem espressa come concatenazione ordinata del nome dei nodi del percorso.
Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi.
Piano di classificazione (titolario)	Struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata.
Piano di conservazione	Strumento integrato con il sistema di classificazione, per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445.
Portabilità	Caratteristica che definisce il livello di facilità con cui i formati possano essere usati su piattaforme diverse, sia dal punto di vista dell'hardware che del software, inteso come sistema operativo. TI.TT, utilizzando gli standard sopra descritti, è possibile rispettare questo criterio. La portabilità è fondamentale perché un cliente possa esportare i propri dati presso un altro outsourcer qualora, alla fine del contratto, non intenda rinnovarlo. Essa è altresì importante per poter viceversa importare i dati di un nuovo cliente provenienti da un altro outsourcer che utilizzi gli standard descritti dalla normativa.
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 di conservazione	Insieme delle attività finalizzate alla conservazione dei documenti informatici di cui al paragrafo 4.7 delle Linee guida sulla formazione, gestione e conservazione dei documenti informatici.
Produttore dei PdV	Persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale.
Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.
Registro di protocollo	Registro informatico ove sono memorizzate le informazioni prescritte dalla normativa per tutti i documenti ricevuti e spediti da un ente e per tutti i documenti informatici dell'ente stesso.
Registro particolare	Registro informatico individuato da una pubblica amministrazione per la memorizzazione delle informazioni relative a documenti soggetti a registrazione particolare.
Repertorio	Registro su cui vengono annotati con un numero progressivo i fascicoli secondo l'ordine cronologico in cui si costituiscono all'interno delle suddivisioni del piano di classificazione.
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	Soggetto che definisce e attua le politiche complessive del sistema di

conservazione	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.
Responsabile della gestione documentale	Soggetto responsabile della gestione del sistema documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445.
Responsabile del trattamento dei dati	Persona con conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, in grado di assolvere i compiti di cui all'articolo 39 del Regolamento (UE) 2016/679.
Responsabile della sicurezza dei sistemi di conservazione	Soggetto che assicura il rispetto dei requisiti di sicurezza all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID.
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Soggetto che assicura lo sviluppo e la manutenzione del sistema all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID.
Riferimento temporale	Informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento.
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.
Serie	Raggruppamento di documenti con caratteristiche omogenee (vedi anche aggregazione documentale informatica).
Sicurezza	La sicurezza di un formato dipende da due elementi: il grado di modificabilità del contenuto del file e la capacità di essere immune dall'inserimento di codice maligno. Nel sistema di conservazione a norma di TI.TT i pacchetti di versamento vengono sottoposti a scansione antivirus con verifica dei file e archivi compressi multilivello. Ogni file compresso è quindi controllato anche se si tratta di compressioni ripetute (tecnica utilizzata per evitare che l'antivirus controlli i file di un archivio compresso). Gli antivirus utilizzati sono costantemente aggiornati. L'invio dei file, inoltre, avviene attraverso linee controllate da firewall e Intrusion detector.
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 classificazione	Strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata.
Sistema di conservazione	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; per i privati è il sistema che consente la tenuta di

	un documento informatico.
Supporto allo sviluppo	È la modalità con cui si mettono a disposizione le risorse necessarie alla manutenzione e sviluppo del formato e i prodotti informatici che lo gestiscono (organismi preposti alla definizione di specifiche tecniche e standard, società, comunità di sviluppatori, ecc.).
Testo unico	Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni.
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.
Unità archivistica	Insieme organizzato di Unità documentarie o Documenti raggruppati dal Produttore per le esigenze della sua attività corrente in base al comune riferimento allo stesso oggetto, attività o fatto giuridico. Può rappresentare una unità elementare di una Serie [da ISAD].
Unità documentaria	Aggregato logico costituito da uno più Documenti che sono considerati come un tutto unico. Costituisce l'unità elementare in cui è composto l'archivio.
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.

Tabella 2 – Glossario

Torna al sommario

2.2 Acronimi

ACRONIMO	SIGNIFICATO
AgID:	Agenzia per l'Italia digitale
CA:	Certification Autorithy
CAD:	Codice dell'amministrazione digitale
CRL:	Certificate Revocation List, è la lista dei certificati revocati o sospesi, ovvero lista di certificati che sono stati resi non validi prima della loro naturale scadenza
DICOM	Digital Imaging and Communications in Medicine
DIP:	Dissemination Information Package (Pacchetto di distribuzione)
eIDAS	Regolamento (UE) № 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
FEA	Firma elettronica avanzata.
FEQ	Firma elettronica qualificata.

GDPR	Regolamento (UE) № 679/2016 del Parlamento Europeo e del Consiglio, del 27 aprile 2016 ("General Data Protection Regulation"), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.
HL7	Health Level 7
HSM:	Hardware Security Module, è l'insieme di hardware e software che realizza dispositivi sicuri per la generazione delle firme in grado di gestire in modo sicuro una o più coppie di chiavi crittografiche
ISO:	International organization for Standardization
IR:	Informazioni sulla rappresentazione
IRse:	Informazioni sulla rappresentazione semantiche
IRSI:	Informazioni sulla rappresentazione sintattiche
OAIS:	Open archival information system.
PDI:	Preservation description information (informazioni sulla conservazione).
PdA (AiP)	Pacchetto di Archiviazione.
PdD (DiP)	Pacchetto di Distribuzione.
PdV (SiP)	Pacchetto di Versamento.
PEC:	Posta Elettronica Certificata.
SIP:	Submission Information Package (Pacchetto di versamento).
SMTP:	Simple Mail Transfer Protocol (SMTP) è il protocollo standard per la trasmissione via internet di e-mail.
TSA:	Time Stamping Autorithy, è il soggetto che eroga la marca temporale.
UNI SInCRO:	UNI 11386:2020 – Supporto all'Interoperabilità nella conservazione e nel Recupero degli oggetti digitali.

Tabella 3 - Acronimi

Torna al sommario

3 Normativa e standard di riferimento

Si riporta di seguito un elenco dei principali riferimenti normativi relativi al SERVIZIO.

Torna al sommario

3.1 Normativa di riferimento

Normativa di riferimento
Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
Decreto legislativo 30 giugno 2003, n. 196 e s.m.i. "Codice in materia di protezione dei dati personali", integrato con le modifiche introdotte dal DECRETO LEGISLATIVO 10 agosto 2018, n. 101, recante "Disposizioni per

l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679;
GDPR-General Data Protection Regulation – Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 Aprile 2016
Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
Regolamento (UE) № 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE;
Indice del Manuale di Conservazione, versione 2 dello schema AgID, pubblicato il 16 gennaio 2015
Linee Guida AgID in materia di formazione, gestione e conservazione dei documenti informatici del 9 settembre 2020;
Regolamento sui criteri di fornitura per i servizi di conservazione del 6 giugno 2021;

Tabella 4 - Normativa di riferimento

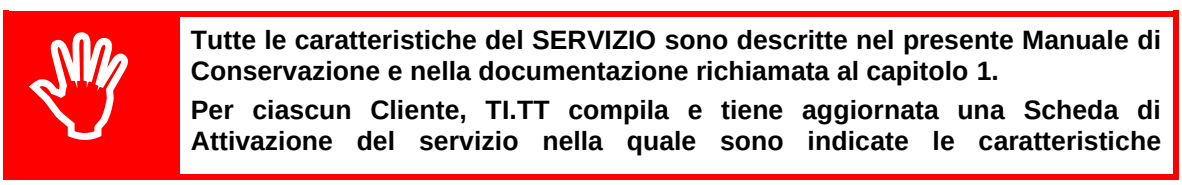
Torna al sommario

3.2 Standard di riferimento

Con riguardo alle previsioni contenute nell'allegato 4 alle Linee guida AgID in materia di formazione, gestione e conservazione dei documenti informatici (d'ora in poi Linee Guida AgID), si riportano di seguito gli standard per la conservazione dei documenti informatici:

Standard di riferimento
ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
ISO 9001 – Sistemi di gestione per la qualità – Requisiti.
ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
ETSI TR 101 533-2 V1.3.1 (2012-04)Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
UNI 11386:2020 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

Tabella 5 - Standard di riferimento



specifiche che assume il servizio per il Cliente.

La Scheda di attivazione del servizio viene sottoposta al Cliente prima dell'attivazione del servizio per consentirgli di verificarne il contenuto ed una copia sottoscritta deve essere riconsegnata a TI.TT. Lo stesso avverrà per ogni successiva modifica o integrazione della scheda.

Torna al sommario

4 Ruoli e responsabilità

Il SERVIZIO descritto nel presente Manuale di Conservazione è strutturato in modo tale da poter garantire l'esecuzione delle attività affidate a TI.TT, in qualità di Conservazione Qualificato ha designato al proprio interno il Responsabile del servizio di Conservazione.

In tale contesto TI.TT, non sottopone a nessun trattamento di verifica il contenuto dei documenti che le sono inviati dal Produttore dei Pdv per sottoporli al processo di conservazione.

Il Responsabile del servizio di conservazione non è responsabile del contenuto dei documenti.

I Ruoli individuati nel Processo di Conservazione, nel rispetto delle Linee Guida sono illustrati nella tabella seguente:

Ruolo	Descrizione
Titolare dell'Oggetto di Conservazione	Il Soggetto produttore, nonché proprietario dell'archivio. Il responsabile del servizio di conservazione sottoscrive i pacchetti di distribuzione.
Produttore dei PdV	Il produttore dei PdV è la persona fisica, interna al Titolare dell'oggetto di conservazione, 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.
Utenti abilitati	Persona, ente o sistema che interagisce con i servizi del sistema di conservazione dei documenti informatici. L'utente abilitato può richiedere al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge e nelle modalità previste dal manuale di conservazione.
Responsabile della Conservazione	Il responsabile della conservazione definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.
Conservatore	Assicura, dalla presa in carico fino all'eventuale scarto, la conservazione degli oggetti digitali sottoposti a conservazione, tramite l'adozione di regole, procedure e tecnologie, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità. Le attività a carico del conservatore sono svolte dalla figura del Responsabile del servizio di Conservazione (RSC).

Le attività e le responsabilità

Lo svolgimento del processo di conservazione richiede la collaborazione e l'interazione degli attori indicati nel seguito, con la specificazione delle responsabilità e delle attività di competenza.

Ruolo	Attività di competenza	Nominativo
Responsabile del servizio di conservazione	Il Responsabile del servizio di conservazione espleta le seguenti funzioni: - Definisce e attua politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione; - Definisce le caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente; - Verifica la corretta erogazione del servizio di conservazione all'ente produttore; - Gestisce le convenzioni, definisce gli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione (acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento, preparazione e gestione del pacchetto di archiviazione, preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta, scarto dei pacchetti di archiviazione) L'attività propria del responsabile del servizio di conservazione vuole garantire la conservazione degli oggetti digitali. Il responsabile del servizio di conservazione garantisce l'aggiornamento delle informazioni sulla rappresentazione. Il responsabile del servizio di conservazione anche tramite la struttura organizzativa succitata garantisce il rispetto delle attività di propria competenza elencate al paragrafo 4.5 delle Linee Guida AgID. In qualità di responsabile del servizio di conservazione si occupa inoltre delle politiche complessive del sistema di conservazione. È responsabile inoltre delle specifiche del sistema di conservazione sulla base della normativa vigente e dell'erogazione del servizio ai soggetti produttori. il responsabile del servizio di conservazione genera il rapporto di versamento. Il responsabile del servizio di conservazione appone la firma digitale e la marca temporale sul pacchetto di archiviazione. Il responsabile del servizio di conservazione garantisce l'esibizione del pacchetto di distribuzione qualora la comunità di riferimento lo richiedesse. Il responsabile del servizio di conservazione sottoscrive i pacchetti di distribuzione.	**Giantommaso Lafavia**
Responsabile della sicurezza dei sistemi per la conservazione	Il Responsabile della sicurezza dei sistemi per la conservazione espleta le seguenti attività - Rispetta e monitora i requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; - Segnala eventuali difformità al Responsabile del servizio di conservazione e individua e pianifica le necessarie azioni correttive.	**Massimiliano Medros**
Responsabile della funzione archivistica di	Il Responsabile della funzione archivistica di conservazione espleta le seguenti funzioni:	**Maria Chiara Lanzillotta**

conservazione	- Definisce e gestisce il 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; - Definisce il set di metadati di conservazione dei documenti e dei fascicoli informatici; questa attività sarà espletata con il supporto del soggetto produttore - Monitora il processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione; - Collabora con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza; - Supporta il responsabile del servizio di conservazione nell'acquisizione del pacchetto di versamento ed è presente nelle verifiche e controlli dell'autorità di competenza. - Si occupa dell'aggiornamento alle normative e della formazione dell'organizzazione. Il responsabile della funzione archivistica di conservazione opera a stretto contatto con il responsabile del servizio di conservazione. Le principali mansioni affidate al responsabile della funzione archivistica di conservazione sono di seguito riportare: - Gestisce le modalità di trasferimento, esibizione e fruizione dei documenti informatici - Definisce le informazioni sulla rappresentazione e sulle informazioni della conservazione. Questa attività sarà espletata con il supporto del soggetto produttore. - Coadiuva il responsabile del servizio di conservazione nelle procedure di chiusura del pacchetto di archiviazione - Si interfaccia con il soggetto produttore qualora sia necessario procedere allo scarto delle tipologie documentarie. - Forma e aggiornare la struttura organizzativa coinvolta nel processo di conservazione.	
Responsabile del trattamento dei dati personali	Il Responsabile del trattamento dei dati personali: - Garantisce il rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; - Garantisce che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza; - Coordina l'attivazione del servizio di conservazione a seguito della sottoscrizione di un contratto; - Coordina le attività di chiusura del servizio al termine del contratto.	**Giantommaso Lafavia**
Responsabile dei sistemi informativi per la	Il Responsabile dei sistemi informativi per la conservazione espleta le seguenti attività - Gestisce l'esercizio delle componenti hardware e software del sistema di conservazione;	**Francesca Mazzanti**

conservazione	- Monitora il mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore; - Segnala eventuali difformità degli SLA al Responsabile del servizio di conservazione e individua e pianifica le necessarie azioni correttive; - Pianifica lo sviluppo delle infrastrutture tecnologiche del sistema di conservazione; - Controlla e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.	
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Il Responsabile dello sviluppo e della manutenzione del sistema di conservazione espleta le seguenti attività - Coordina lo sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione; - Pianifica e monitora progetti di sviluppo del sistema di conservazione; - Monitora gli SLA relativi alla manutenzione del sistema di conservazione; - Si interfaccia con l'ente produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche; - Gestisce inoltre lo sviluppo di siti web e portali connessi al servizio di conservazione; - Coordina le attività di change management.	**Marco Donatone**

Tabella 6 - Ruoli e Responsabilità

Responsabile del servizio di conservazione

Il Responsabile del servizio di conservazione di TI.TT è Giantommaso Lafavia. La sua nomina è stata formalizzata in data 04/10/2016 e controfirmata per accettazione.

Dalla nomina formalizzata in data 01/03/2009, fino alla nomina di Giantommaso Lafavia, il ruolo di Responsabile del servizio conservazione è stato ricoperto da Guido Allegrezza.

Il Responsabile della sicurezza dei sistemi per la conservazione

A far data dal 23 marzo 2018 il responsabile della sicurezza dei sistemi di conservazione del conservatore TI.TT è Massimiliano Medros, che in pari data è stato nominato Responsabile della Sicurezza per il Sistema di Gestione della Sicurezza delle Informazioni ed ha assunto il ruolo di Security Manager dell'azienda. Opera nell'ambito dell'area di staff di cui al par. 5.1 e per il ruolo di Responsabile della Sicurezza, riporta all'AD. La nomina è stata formalizzata e controfirmata per accettazione dal responsabile designato. Il precedente responsabile era Enrico Cavallo, la cui revoca è avvenuta contestualmente alla nomina dell'attuale Responsabile.

Il Responsabile della funzione archivistica di conservazione

A far data dal 03 gennaio 2022 questo ruolo è ricoperto da Maria Chiara Lanzillotta La nomina è stata formalizzata in forma scritta ed è stata controfirmata per accettazione dal responsabile designato. La precedente responsabile era Stefania Rampazzo, la cui revoca è avvenuta contestualmente alla nomina dell'attuale Responsabile.

Il Responsabile del trattamento dei dati personali

A far data dal 12 marzo 2018 questo ruolo è ricoperto dall'Ing. Giantommaso Lafavia. La nomina è stata formalizzata in forma scritta ed è stata controfirmata per accettazione dal responsabile designato. Il precedente responsabile era Cinzia Villani, la cui revoca è avvenuta contestualmente alla nomina dell'attuare Responsabile.

Il Responsabile dei sistemi informativi per la conservazione

Il responsabile dei sistemi informativi di conservazione del conservatore TI.TT è Francesca Mazzanti. La nomina è stata formalizzata e controfirmata per accettazione dal responsabile designato. La nomina decorre dal 22/10/2014.

Il responsabile dei sistemi informativi gestisce le componenti hardware e software del sistema di conservazione. Inoltre, il responsabile dei sistemi informativi verifica il mantenimento degli SLA erogati dai fornitori. Segnala eventuali difformità e gestisce le eventuali anomalie. Il responsabile dei sistemi informativi gestisce la manutenzione delle attrezzature informatiche con il supporto dei collaboratori.

Il Responsabile dello sviluppo e della manutenzione del sistema di conservazione

Il Responsabile dello sviluppo e della manutenzione del sistema di conservazione del conservatore TI.TT è Marco Donatone. La nomina è stata formalizzata e controfirmata per accettazione dal responsabile designato. La nomina decorre dal 19/01/2016. In qualità di soggetto responsabile dello sviluppo e manutenzione del sistema di conservazione coordina e gestisce i rapporti con i fornitori per le attività legate allo sviluppo del sistema di conservazione. Il responsabile monitora e verifica le operazioni del sistema di conservazione. Si interfaccia con il soggetto produttore in riferimento ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software. Gestisce inoltre l'intero sviluppo di siti web e portali connessi con il sistema di conservazione

Torna al sommario

5 Struttura organizzativa per il SERVIZIO

5.1 Organigramma

TI.TT si configura come conservatore che svolge attività di conservazione, che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia. Secondo quanto stabilito dalle Linee Guida AgID e, secondo quanto previsto dalla normativa in materia di protezione dei dati personali, il conservatore TI.TT assume il ruolo di responsabile del trattamento dei dati, come individuato da specifico atto scritto.

Tutte le persone coinvolte nell'erogazione dei servizi della Società sono state incaricate al trattamento dei dati. Il soggetto Produttore si configura come titolare del trattamento dei dati contenuti nei documenti oggetto di conservazione.

Si riporta l'articolazione organizzativa preposta all'erogazione del SERVIZIO:

Figura 1 - Articolazione organizzativa per l'erogazione del SERVIZIO

Torna al sommario

5.2 Strutture organizzative

Il SERVIZIO è svolto da TI.TT con infrastrutture proprie, senza ricorrere a terze parti per le attività ordinarie di erogazione del servizio.

È individuato il Responsabile del Servizio di Conservazione e non sono previste attività delegate a terzi (rif. Paragrafo 4.4 delle Linee Guida AgID).

Riguardo alle principali attività del SERVIZIO, si descrive di seguito l'articolazione funzionale ed organizzativa che ne assume le responsabilità e le modalità di presa in carico.

Torna al sommario

5.2.1 Attività relative al contratto con i Soggetti Produttori

L'erogazione del SERVIZIO da parte di TI.TT viene espletata a seguito della sottoscrizione di un contratto di vendita (v. capitolo 1) con il soggetto produttore. Il processo di definizione della proposta e di acquisizione dell'accettazione è svolto in collaborazione fra le funzioni "Marketing & Sales" e "Operations" (attività commerciali e di provisioning del SERVIZIO) della società.

Il perfezionamento del contratto consente l'attivazione del SERVIZIO.

Una volta che il Soggetto Produttore ha perfezionato la documentazione di attivazione e che il SERVIZIO è stato correttamente attivato e configurato sulla piattaforma di erogazione, è possibile attivare le fasi del processo di conservazione dei documenti inviati dal Produttore.

La prima parte del processo di conservazione è relativa all'**acquisizione e verifica dei pacchetti di versamento**, che viene gestita dal responsabile del servizio di conservazione, che si interfaccia per la scelta sulle informazioni sulla rappresentazione con il Produttore.

La generazione del rapporto di versamento sarà effettuata di conseguenza dopo le verifiche in conformità alla normativa e agli standard di riferimento, da parte del responsabile del servizio di conservazione, coadiuvato dal responsabile della funzione archivistica.

Il responsabile del servizio di conservazione, per i pacchetti accettati, provvede alla **preparazione e alla gestione del pacchetto di archiviazione**. Detto pacchetto viene così firmato e marcato digitalmente, così da poter essere fruito a chi ne farà richiesta, secondo la normativa vigente, come pacchetto di distribuzione.

Il processo di ***cessazione*** si attiva qualora un Soggetto Produttore arrivi alla scadenza naturale del suo contratto con TI.TT e non intenda rinnovarlo.

Tra le attività che il Soggetto produttore può affidare al Conservatore nella figura del RsC, in conformità alle Linee Guida AgID, sono elencate di seguito:

- definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;
- gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
- genera e sottoscrive il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
- genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
- effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
- effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;
- al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;
- predispone le misure necessarie per la sicurezza fisica e logica del sistema di conservazione come previsto dal par. 4.11 delle Linee guida AgID;

Restano comunque in capo al Soggetto Produttore le seguenti attività:

- la predisposizione del manuale di conservazione interno ad opera del Responsabile della Conservazione, in conformità al paragrafo 4.7 delle Linee Guida AgID, curandone l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti;
- assicurare che la conservazione della documentazione di natura fiscale avvenga entro le scadenze dettate dalla normativa di settore (DM 17 giugno 2014);

- assicurare la corretta formazione della documentazione secondo quanto disposto dalle Linee guida AgID;
- assicurare che venga rispettato l'assolvimento degli obblighi fiscali della documentazione fiscale dettati dalla normativa di settore;
- autorizzare la procedura di scarto per quei pacchetti di archiviazione contenenti i documenti destinati allo scarto;
- assicurare la presenza di un pubblico ufficiale/notaio, 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;
- Assicurare agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza (esibizione dei documenti).

La seguente tabella descrive nel dettaglio le attività, le responsabilità e chi si occupa della loro realizzazione, relativamente al ciclo di vita contrattuale dell'adesione al SERVIZIO.

Attività	Responsabilità	Area di competenza
Attivazione del servizio di conservazione (a seguito della sottoscrizione di un contratto).	Responsabile del servizio di conservazione Venditore Coordinatore attività di delivery	Infrastructure & Document Management
Acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento.	Responsabile del servizio di conservazione, supporto del Responsabile della funzione archivistica di conservazione	Infrastructure & Document Management
Preparazione e gestione del pacchetto di archiviazione.	Responsabile del servizio di conservazione	Infrastructure & Document Management
Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta.	Responsabile del servizio di conservazione	Infrastructure & Document Management
Scarto dei pacchetti di archiviazione.	Responsabile del servizio di conservazione, supporto del Responsabile della funzione archivistica di conservazione, previa autorizzazione da parte del soggetto produttore	Infrastructure & Document Management
Chiusura del servizio di conservazione (al termine di un contratto).	Responsabile del servizio di conservazione Coordinatore attività di delivery	Infrastructure & Document Management

Tabella 7 - Attività, responsabilità e ruoli del processo di provisioning

Torna al sommario

5.2.2 Attività relative alla gestione dei sistemi informativi

Per ciò che riguarda i processi di gestione dei sistemi informativi dedicati al SERVIZIO, le attività di conduzione e manutenzione del sistema di conservazione sono garantite dal responsabile dei sistemi informativi per la conservazione.

Il monitoraggio del sistema di conservazione è in carico al responsabile dei sistemi informativi per la conservazione per quanto concerne i sistemi informativi e le soluzioni per garantire lo SLA (Service Level Agreement). Il responsabile della sicurezza dei sistemi per la conservazione è invece colui che coordina e garantisce il monitoraggio dei requisiti per la sicurezza dei sistemi e degli ambienti, come descritto nel Piano della Sicurezza Generale dei Servizi Erogati da TI.TT e dal Piano della Sicurezza del Servizio di Conservazione.

Il *change management* della piattaforma dedicata al servizio di conservazione è invece un processo controllato e seguito dal responsabile dello sviluppo e della manutenzione del sistema di conservazione. Esso serve per garantire la leggibilità nel tempo dei documenti conservati ed evitare che l'obsolescenza dei sistemi possa pregiudicarne l'esibizione.

Per quanto riguarda gli adeguamenti dei sistemi informativi della conservazione agli standard e alle normative specifiche, le indicazioni provengono dal responsabile della funzione archivistica di conservazione, che si occupa delle verifiche periodiche di conformità a normativa e standard di riferimento. Il responsabile della funzione archivistica di conservazione ha quindi il compito di aggiornare TI.TT sulle normative a gli standard di riferimento e provvederà a tenere dei corsi di aggiornamento alle strutture organizzative coinvolte nel processo di conservazione.

La seguente tabella descrive nel dettaglio le attività, le responsabilità e chi si occupa della loro realizzazione, relativamente alla gestione dei sistemi informativi:

Attività	Responsabilità	Area di competenza
Conduzione e manutenzione del sistema di conservazione;	Responsabile dei sistemi informativi	Infrastructure & Document Management
Monitoraggio del sistema di conservazione;	Responsabile dei sistemi informativi	Infrastructure & Document Management
Change management;	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Infrastructure & Document Management
Verifica periodica di conformità a normativa e standard di riferimento	Responsabile della funzione archivistica di conservazione	Infrastructure & Document Management

Tabella 8 - Attività, responsabilità e ruoli della gestione dei sistemi informativi

Torna al sommario

6 Oggetti sottoposti a conservazione

La rappresentazione degli oggetti digitali sottoposti al processo conservazione è parte integrante del contratto di affidamento del servizio di conservazione.

Torna al sommario

6.1 Oggetti conservati

Il Sistema di conservazione, gestito da TI.TT, conserva diverse tipologie documentarie con i metadati ad esse associati e le loro aggregazioni documentali informatiche (aggregazioni), che includono i fascicoli informatici (fascicoli) e le serie informatiche.

Il sistema gestisce gli oggetti digitali sottoposti a conservazione distinti per ogni singolo soggetto produttore e anche per singola struttura, consentendo di definire configurazioni e parametrazioni ad hoc per ogni Soggetto Produttore, in base a quanto da questi indicato nelle Schede di Attivazione e di Configurazione all'atto dell'attivazione e alle successive variazioni.

Per mantenere anche nel Sistema le informazioni relative alla struttura dell'Archivio e dei relativi vincoli archivistici, le unità documentarie possono essere versate corredate di un set di metadati di profilo archivistico che include gli elementi identificativi e descrittivi del fascicolo, con riferimento alla voce di classificazione, alla segnatura archivistica. I fascicoli possono essere versati nel sistema quando sono completi e dichiarati chiusi, descritti da un set di metadati che include obbligatoriamente, oltre alle informazioni di identificazione, classificazione e descrizione, anche il tempo di conservazione previsto. Nel caso delle serie, la chiusura può avvenire a cadenza annuale o comunque secondo una definizione temporale definita dal soggetto produttore.

I documenti informatici, (unità documentarie) e i fascicoli (unità archivistiche) delle amministrazioni pubbliche sono suddivisi secondo un piano di classificazione che identifica gruppi documentali omogenei per natura e/o funzione giuridica (Titolo, classe, sottoclasse), modalità di registrazione o di produzione.

Le tipologie documentarie trattate da TI.TT assieme ai loro specifici metadati e articolazioni, sono dettagliatamente indicate all'interno della Descrizione del SERVIZIO, pubblicata sul sito di TI.TT (v. capitolo 1).

L'unità documentaria rappresenta l'unità minima elementare di riferimento di cui è composto un Archivio, pertanto rappresenta il riferimento principale per la costruzione dei Pacchetti informativi secondo il modello OAIS.

All'unità documentaria e agli elementi che la compongono sono associati set di metadati che la identificano e la descrivono. Coerentemente con quanto sopra riportato l'unità documentaria è pertanto logicamente strutturata su tre livelli: unità documentaria, documento, File.

Tutti i formati gestiti da TI.TT sono elencati e descritti in un registro interno al sistema di conservazione "Registro dei Formati" in cui ogni formato è corredato da informazioni descrittive relative alla eventuale versione, e al *mimetype*.

All'atto dell'attivazione del SERVIZIO, nelle Schede di Attivazione e di Configurazione, il produttore seleziona fra quelli resi disponibili da TI.TT i formati che il SERVIZIO accetterà, per ogni tipologia documentaria gestita.

Di seguito, viene fornito un riepilogo dei formati al momento ammessi per la conservazione:

Formato	Proprietario	Estensione	Tipo	Aperto	Standard
PDF - PDF/A[1]	Adobe Systems http://www.adobe.com/	.pdf	application/pdf	Si	ISO 32000-1 (PDF); ISO 19005-1:2005 (vers. PDF 1.4); ISO 19005-2:2011 (vers. PDF 1.7)
TIFF	Aldus Corporation (acquisita Adobe)	.tif	image/tiff	No	ISO 12639 (TIFF/IT); ISO 12234 (TIFF/EP)
JPG e JPEG 2000	Joint Photographic Experts Group	.jpg, .jpeg, .jp2 (JPEG 2000)	image/jpeg	Si	ISO/IEC 10918:1 (JPG); ISO/IEC 15444-1 (JPEG 2000)
Office Open XML (OOXML)	Microsoft	.docx, .xlsx, .pptx	application/vnd.openxmlformats-officedocument.*	Si	ISO/IEC DIS 29500:2008

[1] Il PDF/A è stato sviluppato con l'obiettivo specifico di rendere possibile la conservazione.

ODF Open Document Format	OASIS	.ods, .odp, .odg, .odb	application/vnd.oasis.opendocument.text	Si	ISO/IEC 26300:2006; UNI CEI ISO/IEC 26300
XML Extensible Markup Language	W3C	.xml	application/xml text/xml	Si	
TXT	-	.txt	ASCII, UTF-8, UNICODE	Si	ISO 646, RFC 3629, ISO/IEC 10646
PEC ed EMAIL	-	.eml	message/RFC822	No	RFC 2822/MIME
HL7	Health Level 7	.pdf; .cda; .p7m;	application/(.pdf; p7m; cda)	SI	HL7 Implementation Guide for CDA® Release 2 - ISO/HL7 10781:2015
DICOM	ACR e NEMA	.dcm	image/dcm	SI	DICOM (ISO 12052:2006)

Tabella 9 - Formati ammessi per la conservazione

Il modello OAIS prevede che, ad ogni oggetto digitale portato in conservazione, venga associato un insieme di informazioni (metadati) che ne permetta in futuro una facile reperibilità. In questo insieme di metadati troviamo le informazioni sulla rappresentazione (IR), classificabili in sintattiche (IRsi) e semantiche (IRse), il cui obiettivo è fornire tutte le informazioni necessarie per poter leggere ed interpretare la sequenza di bit dell'oggetto conservato. Inoltre, ad un sistema di conservazione che rispetti la normativa italiana, è richiesto il requisito di leggibilità degli oggetti dati, previsto dal paragrafo 4.1 delle Linee guida AgID, e dal comma 1 dell'art. 44 del Codice dell'amministrazione digitale.

Risulta necessario affrontare tre tematiche importanti:

- La prima riguarda "cosa" e "come" associare ad un oggetto digitale conservato in merito alle informazioni sulla rappresentazione;
- La seconda si riferisce al "come" rispettare il requisito di leggibilità;
- La terza si riferisce a "cosa" e "come" fornire nel momento in cui quell'oggetto deve essere distribuito agli utenti.

Per soddisfare questi requisiti, all'attivazione del servizio il produttore indica le informazioni sulla rappresentazione necessarie alla consultazione dei documenti versati, ovvero:

1. Strumenti per la leggibilità: tipicamente legati al formato dell'oggetto conservato.
2. Informazioni sulla rappresentazione sintattica: tipicamente legate al formato dell'oggetto conservato.
3. Informazioni sulla rappresentazione semantica: tipicamente legate alla descrizione archivistica dell'oggetto conservato.

Sebbene le informazioni sulla rappresentazione sintattica (tipo 2) possano essere considerate le basi su cui poggiare le successive conservazioni di oggetti di uno specifico formato, poiché sono le informazioni necessarie a produrre/creare gli strumenti che ne permettono la leggibilità (tipo 1), resta fondamentale fornire fin dal principio, insieme all'oggetto conservato, gli strumenti necessari per poterlo leggere.

Concludendo, per soddisfare l'eventuale necessità di una disponibilità immediata dell'oggetto conservato, possiamo affermare che il sistema di conservazione deve avere almeno conservato gli strumenti per la leggibilità (visualizzatori) degli oggetti digitali versati in conservazione.

Si ritiene per tanto necessaria la capacità del software di generare, per ogni soggetto produttore, un insieme di descrizioni archivistiche "speciali" che diano modo al responsabile del servizio di conservazione di conservare le tre tipologie di informazioni sulla rappresentazione.

Si tenga presente che le tre descrizioni archivistiche speciali sotto riportate non hanno nessuna associazione con le informazioni sulla rappresentazione:

1. "Viewer" di tipologia "Unità documentaria" con file di indice di tipo multi-indice.
2. Fascicolo Informazioni sulla rappresentazione di tipologia "Fascicolo".
3. Informazioni sulla rappresentazione di tipologia "Unità Documentaria" con file di indice di tipo indice singolo.

Torna al sommario

6.2 Il pacchetto di versamento (PdV)

Si tratta del pacchetto informativo inviato dal produttore al sistema di conservazione, utilizzando gli strumenti e le modalità messi a disposizione da TI.TT, Il Produttore può scegliere, al momento dell'attivazione del servizio fra le opzioni disponibili per il trasferimento dei pacchetti di versamento descritte secondo le modalità e protocolli riportati nel Documento di Descrizione del Servizio.

In questo sistema di conservazione possono essere trasferiti pacchetti di versamento conformi a quanto previsto dalle Linee guida: esso supporta PdV eventualmente accompagnati da IR nel formato definito nell'allegato 5 delle Linee Guida AgID e nel formato CSV.

La fase relativa alla preparazione del PdV e il conseguente invio al sistema di conservazione possono avvenire in modi diversi, essendo fortemente dipendente dalla situazione specifica del soggetto produttore e dagli accordi stipulati con il conservatore.

In condizioni generali il pacchetto di versamento, prodotto e traferito dal produttore al sistema di conservazione, è costituito dall'insieme dei file che saranno oggetto di conservazione, accompagnati da un file detto file di indice o file dei metadati.

Il file di indice dovrà contenere i metadati per ricercare i documenti all'interno del sistema. Le informazioni sono concordate con il conservatore e configurate nel sistema di conservazione per ciascuna descrizione archivistica, nella stessa configurazione saranno anche implementate le regole di validazione dei metadati, concordate sempre con il conservatore.

La struttura e la forma del file di indice dipendono sia dalla modalità di trasferimento, scelta tra le tre disponibili, sia dalla natura dei file che costituiscono il pacchetto e dalle eventuali relazioni tra gli stessi. Una volta che i pacchetti di versamento sono stati acquisiti, questi vengono trasformati in pacchetti di archiviazione (PdA).

Nel sistema di conservazione di TI.TT i metadati possono essere di vari tipi.

Ci si è attenuti all'allegato 5 "Metadati" delle Linee Guida AgID. In aggiunta ai metadati previsti, vengono gestiti i seguenti tipi:

- Stringa;
- Numero;
- Data;
- Hash (SHA256 del file);
- *MIME Type* (per poter poi associare un documento alle informazioni di rappresentazione);

Inoltre, per ogni metadato è possibile definire:

- Obbligatorietà;
- Ricercabilità;

Torna al sommario

6.3 Il pacchetto di archiviazione (PdA)

Il pacchetto di archiviazione è l'elemento fondamentale del sistema di conservazione, è il pacchetto informativo che racchiude in sé tutti gli elementi sufficienti e necessari per una conservazione a lungo termine.

Il principio su cui si basa l'architettura del modello dati del sistema di conservazione è quello di un'assoluta auto consistenza del pacchetto informativo nel momento in cui è costituito il PdA stesso, tale obiettivo viene raggiunto grazie all'aderenza al modello funzionale e al modello-dati previsto in OAIS.

La coerenza di un pacchetto informativo è data da due componenti logiche fondamentali:

- l'insieme delle informazioni statiche che prevedono un set complesso di metadati che descrivono in maniera "piatta" tutti gli elementi identificativi, descrittivi, gestionali, tecnologici, etc., relativi ad uno e uno solo pacchetto informativo;

- l'insieme delle relazioni di contesto che permettono la correlazione logica del pacchetto informativo agli altri pacchetti informativi e in generale ad un qualsiasi contesto di natura archivistico-gerarchica.

Quest'ultimo elemento è quello che ci permette di ricostruire il vincolo archivistico e quindi di ricondurre, ad esempio, ad una stessa pratica o ad uno stesso fascicolo tutti i documenti relativi ad un medesimo affare o procedimento amministrativo.

Concretamente, si può prevedere che nel sistema si conserveranno all'interno di un medesimo pacchetto informativo (e quindi incapsulate in una medesima busta) le seguenti componenti, codificate in un'XML:

- l'oggetto digitale possibilmente in un formato standard non proprietario;
- l'impronta del documento generata con funzione di hash;
- il set di metadati gestionali (UNI SInCRO);
- il viewer necessario per la visualizzazione del documento stesso, o in alternativa, si inserisce il puntatore/riferimento al viewer comune a più pacchetti informativi per quel formato di file del documento;
- la documentazione tecnica necessaria alla comprensione del viewer stesso (anch'esso può essere un puntatore/riferimento che rimanda alla componente digitale descritta per più pacchetti informativi) oppure la documentazione per la comprensione del documento digitale e/o della classe documentale di riferimento.

La forza innovativa del sistema di conservazione risiede, oltre che negli elementi informativi che sono stati descritti sopra e che permettono una perfetta *compliance* al modello OAIS, anche nel livello descrittivo adottato.

Si assume che il livello di descrizione minimo che garantisca una gestione efficace di tutti i dati e metadati necessari per la conservazione e che permette quella necessaria contestualizzazione archivistica del documento, è rappresentato dall'unità archivistica. Essa rappresenta un livello di aggregazione minimo nel quale racchiudere le informazioni comuni a più documenti e contenuti digitali per relazionare i documenti afferenti al medesimo oggetto, pratica, procedimento o processo.

Tale livello diventa un file contenente i metadati identificativi e descrittivi, secondo il modello sopra proposto. Ovviamente esso non contiene un oggetto digitale, nella stretta accezione OAIS, ma diventa un container da conservare. Oltre ai metadati tipici (ad esempio, denominazione del fascicolo, estremi cronologici del fascicolo, riferimenti al procedimento amministrativo associato) esso conterrà due puntatori fondamentali:

- uno o più puntatori agli oggetti digitali contenuti nel fascicolo (un fascicolo può contenere uno o più data object);
- uno o più puntatori alla struttura archivistica di riferimento (quindi alla serie/sottoserie della rappresentazione attuale dell'archivio); in altre parole un fascicolo potrà riferirsi ad una o più serie archivistiche.

Ciascun livello archivistico, così come previsto dalla modalità descrittiva multi livellare degli standard internazionali riconosciuti dalla comunità scientifica archivistica (v. ISAD/EAD), diverrà esso stesso oggetto di descrizione.

Si assume però che il livello di descrizione sufficiente e necessario per una corretta conservazione della risorsa digitale sia rappresentato proprio dall'unità archivistica (che può assumere di volta in volta la forma di aggregato logico legato a concetti di fascicolo, pratica o quant'altro). Tale livello, pertanto, diventa elemento conservato e incorporato (embedded) a tutti gli effetti al PdA che contiene l'oggetto digitale che rappresenta il documento informatico da conservarsi a norma.

L'insieme, costituito dal *data object*, dai suoi metadati e dalle relazioni fra i documenti e fra questi e la struttura di archivio, costituisce il nucleo minimo e sufficiente della conservazione a lungo termine.

In concreto, una volta che i PdV sono stati accettati nel sistema, (e sono quindi stati oggetto di controlli sui metadati previsti dal contratto di servizio) essi sono pronti ad essere trasformati in PdA e quindi diventare l'oggetto della conservazione a lungo termine.

Il documento informatico, così trattato, sarà arricchito dei metadati previsti nel contratto di servizio, ma anche di tutti quei metadati tecnologici, relativi al documento stesso e al *viewer*, necessari per ostacolare l'obsolescenza tecnologica.

All'atto della conservazione verrà composto il pacchetto di archiviazione (PdA). Lo schema seguente mostra sinteticamente come sarà costruito il PdA:

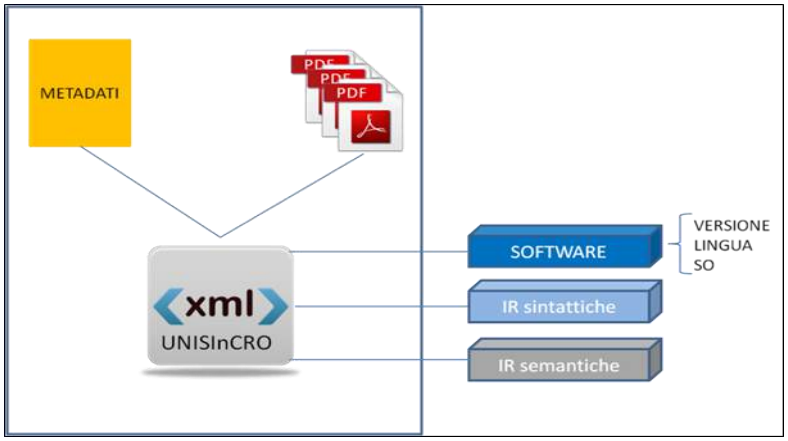


Figura 2 - Pacchetto di archiviazione (PdA)

Schema del PdA e dei collegamenti con le informazioni sulla rappresentazione

Ad ogni oggetto versato nel sistema di conservazione verrà associato:

- l'UID del software per la visualizzazione.
- l'UID del fascicolo delle informazioni sulla rappresentazione sintattica.
- l'UID del fascicolo delle informazioni sulla rappresentazione semantica.

In un sistema OAIS *compliant*, si definisce pacchetto di archiviazione un pacchetto informativo composto dall'insieme delle informazioni che costituiscono l'obiettivo originario della conservazione e dalle relative informazioni sulla conservazione. In un contesto OAIS il pacchetto di archiviazione dove essere auto-consistente, ovvero, deve prevedere tutte le informazioni necessarie al recupero e alla ricostruzione dell'oggetto conservato e delle informazioni ad esso associate.

Si riporta la struttura dell'indice del pacchetto di archiviazione.

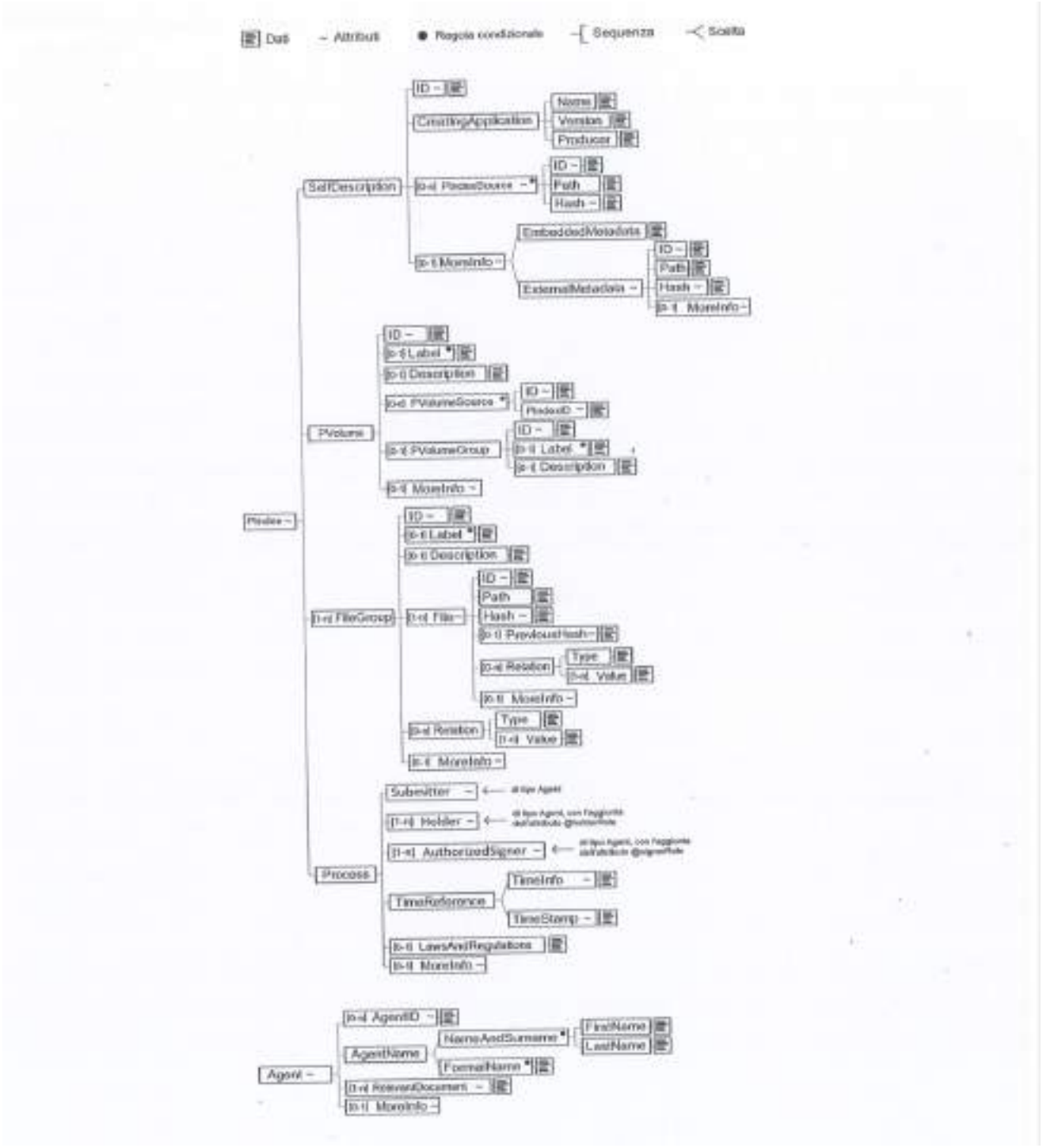


Figura 3: struttura dell'indice del pacchetto di archiviazione

Torna al sommario

6.4 Il pacchetto di distribuzione (PdD)

Nel modello OAIS, il pacchetto di distribuzione è strutturato nel modello dati, come il pacchetto di archiviazione (PdA). La differenza sta nella sua destinazione in quanto esso viene concepito per essere fruito ed utilizzato dall'utente finale (esibizione).

In questo caso, un PdD può anche non coincidere con un PdA originale conservato nel *data center*, anzi, molto spesso, ragioni di opportunità inducono a distribuire pacchetti informativi che sono un'estrazione del contenuto informativo di un PdA (negando ad esempio l'accesso ad una parte di esso). Può anche verificarsi il caso di PdD che sono il frutto di più PdA che vengono "spacchettati" e rimpacchettati per un più fruibile utilizzo da parte dell'utente.

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

Il sistema di conservazione gestisce un archivio dei **software** eseguibili, ciascuno dei quali utile a visualizzare un determinato formato file cui appartengono i documenti conservati.

I software dell'archivio sono associati ad una descrizione archivistica in modo tale che, al momento della generazione dei pacchetti di distribuzione dei documenti informatici da esibire, vengano automaticamente inclusi anche e solo i software necessari alla loro visualizzazione.

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

- I documenti richiesti nel formato previsto per la loro visualizzazione.
- Un'estrazione dei metadati associati ai documenti.
- L'indice di conservazione firmato e marcato.
- I *viewer* necessari alla visualizzazione dei documenti del pacchetto.

Inoltre, nei pacchetti di distribuzione, è possibile inserire tutta la catena di documentazione necessaria a rispondere alle esigenze del modello OAIS.

Torna al sommario

7 Il processo di conservazione

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

I pacchetti di versamento, di norma, raggiungono il SERVIZIO attraverso l'interazione diretta tra il Cliente e la piattaforma di esercizio primario (vedi par. 8.3.1).

Ove richiesto dalla tipologia dei dati [2] (ad esempio dati sanitari) l'interazione avviene, invece, tramite elementi (HW e/o SW) installati presso il Cliente e gestiti dal Conservatore, che assicurano la cifratura del canale di trasmissione e dei Pacchetti di Versamento (Gateway, v. Figura 5).

In dettaglio le modalità di trasferimento utilizzate sono:

1) **Upload manuale**: avviene tramite l'autenticazione al sito di erogazione della conservazione a Norma. Un'apposita Web-App consente agli utenti profilati sulla piattaforma di accedere e caricare uno ad uno i file da conservare inserendo di volta in volta i relativi metadati;
2) **SFTP**: è costituita da un collegamento SFTP (Secure File Transfert Protocol) criptato punto-punto con la piattaforma del cliente e autorizzato dai firewall e dall'intero *layer* di sicurezza. Il Cliente ottiene le credenziali di autenticazione e può accedere dalla piattaforma tramite un set predefinito di IP statici. In modalità automatica si può quindi procedere all'upload dei pacchetti di versamento nella folder SFTP dedicata, costituiti da un file di indice e di una cartella contenente i documenti da porre in conservazione
3) **Web Services (A2A)**: con credenziali personalizzate e accesso consentito dal *layer* di sicurezza, il Cliente può raggiungere i *web services* di conservazione esposti da TI.TT. La modalità è detta Application To Application (A2A). L'applicazione del Cliente, dopo l'autenticazione, potrà utilizzare le chiamate per eseguire tutte le operazioni previste dalla conservazione.

4) **DICOM**: consente l'acquisizione di immagini DICOM utilizzando procedure standard Storage/Storage Commitment e Query/Retrieve DICOM 3.0;

[2] La tipologia dei dati viene dichiarata dal Cliente al momento della attivazione del servizio e su di essa non vengono effettuate verifiche/controlli da parte del Conservatore

5) **HI7**: consente l'acquisizione di documenti utilizzando il messaggio standard Hl7 (ver. 2.6 o successive) "MDM T10";
6) **Modalità Custom**: relativa a clienti che richiedono una progettazione puntuale delle esigenze, con metadati personalizzati e aggiuntivi rispetto allo standard, oppure modalità di invio dei documenti da conservare ibridi o comunque diversi da quelli standard (gli standard sono l'Upload Manuale, l'SFTP e l'A2A).

Torna al sommario

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

Il sistema esegue per i PdV acquisiti i seguenti controlli:

- la conformità dell'Indice del pacchetto di versamento allo schema stabilito dal sistema di conservazione;
- la conformità delle tipologie documentarie che devono essere congruenti con quanto previsto nell'ambito delle pattuizioni contrattuali stipulate con i singoli soggetti produttori;
- la conformità dei metadati da quanto previsto dagli accordi;
- l'integrità dei componenti, verificando per ogni file versato, che l'impronta fornita dal produttore coincida con quella calcolata dal sistema di conservazione;
- il controllo di ammissibilità dei formati;

Sui documenti informatici versati al sistema di conservazione sono eseguiti i controlli di validazione della documentazione rispetto alle regole ed agli standard previsti dalle classi documentali di appartenenza.

Il processo di convalida riguarda almeno i seguenti aspetti:

- la verifica dell'integrità del documento memorizzato sul supporto rispetto all'impronta associata allo stesso;
- la verifica che il formato del dato sia coerente con quanto dichiarato nei suoi metadati;

Alla prova dell'esito positivo dei test preliminari, il sistema produce un rapporto chiamato rapporto di versamento (RdV) in cui sono riportate e validate le informazioni ricevute nel pacchetto di versamento (PdV).

In caso di esito negativo l'intero pacchetto di versamento viene sospeso e viene notificato tramite e-mail l'evento al gruppo di competenza, che procederà a contattare i referenti del soggetto produttore per definire, a seconda dei casi, le azioni da intraprendere.

Inoltre, la notifica è automaticamente inviata ai contatti del Soggetto Produttore indicati all' attivazione del servizio.

Tutte le notifiche sono riportate nei file di log del sistema di conservazione a loro volta sottoposti a conservazione con cadenza periodica.

Torna al sommario

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

La prima parte del processo di conservazione è relativa all'acquisizione e verifica dei pacchetti di versamento, che viene gestita dal responsabile del servizio di conservazione.

Il sistema effettua dei controlli preliminari, volti alla validazione del pacchetto di versamento in entrata nel sistema.

Il risultato della convalida è riepilogato da un esito in formato XML (rapporto di versamento). Gli oggetti digitali, per i quali l'esito della convalida è risultato positivo, possono quindi essere inseriti in un PdA.

Il rapporto di versamento viene quindi firmato e marcato digitalmente e messo a disposizione del soggetto produttore come evidenza della presa in carico dei documenti, in una o più delle modalità seguenti specificate nel Documento di Descrizione del Servizio:

- Per i soggetti che effettuano i **versamenti tramite il protocollo SFTP**, il rapporto di versamento viene copiato in una cartella apposita, visibile al solo soggetto produttore, il quale, attraverso una procedura automatica, ne riscontra la presenza e può effettuarne il download. La ritenzione di tali rapporti nella

specifica cartella è di 3 mesi, dopo i quali i rapporti sono comunque visibili e scaricabili tramite l'interfaccia *web based* a disposizione del personale designato dal Soggetto Produttore.

- Per i soggetti che effettuano i **versamenti tramite l'upload da web**, il rapporto di versamento è a disposizione dalla stessa interfaccia *web based*, attraverso una pagina di ricerca che consente la visualizzazione e il download.
- Per i soggetti che effettuano i **versamenti tramite *web services*** ricevono il rapporto di versamento attraverso un apposito comando dallo stesso applicativo che invia i documenti.
- Per i soggetti che lo richiedano può essere inviato il rapporto di versamento anche attraverso il servizio di Posta Elettronica.

Tutti i rapporti di versamento sono conservati insieme ai documenti informatici sottoposti al processo conservazione e per lo stesso periodo di tempo relativo ai documenti stessi.

Tutti i soggetti, a prescindere dalla modalità di versamento dei dati, sono in grado di recuperare i rapporti di versamento delle conservazioni effettuate attraverso l'interfaccia *web based* a disposizione del personale designato dal soggetto produttore.

Torna al sommario

7.4 Rifiuto del pacchetto di versamento

Il PdV viene sottoposto ai controlli di validazione descritti nel paragrafo 7.2. Qualora il PdV non abbia superato tutti i controlli previsti, il sistema rifiuta il pacchetto di versamento e notifica all'utente l'avvenuto errore. La notifica avviene attraverso interfaccia grafica nell'area designata alle notifiche e attraverso l'invio di un messaggio mail.

In aggiunta, oltre alla notifica mail e web il sistema dettaglia nei log la causa d'errore.

Torna al sommario

7.5 Preparazione e gestione del pacchetto di archiviazione

Una volta a disposizione i pacchetti informativi presso la piattaforma di TI.TT, il processo di conservazione può avere inizio.

È possibile separare i versamenti in diversi pacchetti di archiviazione dividendoli in base a diverse logiche:

- Per file di metadati;
- Per chiamata diretta (WS);
- In base ai Megabyte;
- In base al tempo.

Ad ogni buon conto, nella definizione dei PdV, è consigliato il rispetto delle seguenti configurazioni:

- Massimo 4 GB di documenti conservati per PdA (al fine di supportare il formato ISO);
- Massimo 80mila documenti/file (allegati inclusi) per PdA (al fine di minimizzare le probabilità dei PdV);
- Massimo 5 MB per ogni file inviato mediante WS e fino a 350 MB per invii tramite SFTP (al fine di ottimizzare le prestazioni dei canali di trasmissione);

Una volta che la creazione dei pacchetti di archiviazione è completata, l'applicazione effettuerà la lettura dei metadati associati ai file da conservare.

Ogni file dovrà infatti avere almeno un record contenente i valori che lo contraddistinguono e attraverso i quali sarà possibile effettuare la sua ricerca, dopo la conservazione.

I metadati associati ai file da conservare sono concordati prima dell'esercizio del servizio tra il Cliente e TI.TT attraverso la "scheda di configurazione del servizio", un documento contenente diverse informazioni che servono a determinare la struttura, le proprietà e il contesto dei dati che saranno conservati.

La struttura utilizzata nella costruzione dei PdA fa riferimento alla norma UNI SInCRO che è lo standard nazionale riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione

In concreto, il pacchetto di archiviazione è un'entità logica contenuta in un'alberatura di file e cartelle e definita nel file indice UNI SInCRO generato nel corso del processo di conservazione e contenente tutte le informazioni inviate dal PdV o definite sul sistema di conservazione.

La conservazione si conclude con la firma digitale e la marca temporale dell'indice UNI SInCRO e termina con la messa a disposizione del cliente di questa evidenza di avvenuta conservazione (indice P7M) da parte del responsabile del servizio di conservazione.

Il sistema di conservazione si occupa autonomamente di tutte le fasi di conservazione, tracciandone ogni passaggio e ogni esito nei file di log.

Torna al sommario

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

Sui pacchetti di archiviazione conservati, gli, utenti con profilo di esibizione o ricerca possono effettuare ricerche e ottenere pacchetti di distribuzione.

Il PdD, coincidente con il PdA, contiene:

- tutti gli elementi presenti nel PdA;
- i documenti del PdA richiesto;
- un'estrazione delle informazioni di conservazione dei documenti e dei fascicoli;
- l'indice di conservazione firmato e marcato e le informazioni sulla conservazione associate ai documenti;
- (quando richiesto) i *viewer* necessari alla visualizzazione dei documenti del pacchetto e le informazioni sulla rappresentazione;
- le informazioni sull'impacchettamento e le informazioni descrittive associate al pacchetto informativo.

In linea generale il PdD può essere erogato dal sistema di conservazione come unico file in formato ZIP e in formato ISO a seconda della richiesta dell'utente.

Il sistema di conservazione di TI.TT garantisce l'esibizione dell'archivio informatico. Il sistema permette di richiedere, di generare e di scaricare i PdD, completi di file di evidenza della conservazione e delle informazioni di rappresentazione. Inoltre, nei PdD è contenuta tutta la catena di documentazione necessaria a rispondere alle esigenze dello standard OAIS.

Il Soggetto Produttore, in fase di attivazione del servizio segnala al *provisioning* di TI.TT, su apposita documentazione correlata dagli allegati autorizzativi e di identificazione, i propri delegati alla visualizzazione e al download dei documenti informatici originali ai fini dell'esibizione.

Verranno così inviate le credenziali per accedere al *portale della conservazione* con la modalità del canale separato (username via mail e password OTP via cellulare) e un manuale di utilizzo del portale.

Tali credenziali serviranno per il collegamento al portale di conservazione, all'indirizzo https://conservazione.trusttetchnologies.it. Il collegamento avviene tramite connessione sicura SSL con certificato della Certification Authority TI.TT.

Una volta accreditato dal portale, l'utente ha accesso ai servizi opportunamente profilati alla sua utenza.

A quel punto i produttori sono in grado di:

- Visualizzare direttamente i documenti informatici originali conservati da remoto;
- Scaricare i documenti informatici conservati (duplicati) e i file di evidenza della conservazione (indice di conservazione UNI SInCRO);
- Richiedere e scaricare i PdD da consegnare alle autorità competenti, in caso di necessità;

Nel pacchetto informativo è compreso anche il necessario per la rappresentazione (*viewer* nella versione coerente alla visualizzazione dei PdD) e le informazioni sul sistema operativo in grado di supportare l'applicazione.

Va sottolineato che l'esibizione dei file digitali conservati deve avvenire in modo che le autorità possano verificare la coerenza della firma digitale e la marca temporale apposta durante il processo di conservazione.

Tale procedura, non potendo essere effettuata stampando l'evidenza firmata della conservazione, deve necessariamente prevedere un supporto informatico.

Torna al sommario

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

Il Soggetto Produttore, in fase di attivazione del servizio segnala al *provisioning* di TI.TT, su apposita documentazione correlata dagli allegati autorizzativi e di identificazione, i propri delegati alla visualizzazione e al download dei documenti informatici originali, che ricevono le credenziali per accedere al *portale della conservazione* con la modalità del canale separato (username via mail e password OTP via cellulare) e un manuale di utilizzo del portale[3]..

Detta piattaforma, consente al Soggetto Produttore di effettuare sia la produzione di duplicati, sia l'esibizione a norma dei documenti informatici conservati.

Una volta accreditato dal portale, l'utente ha accesso ai servizi opportunamente profilati alla sua utenza.

A quel punto i soggetti produttori sono in grado di:

- Visualizzare direttamente i documenti informatici originali conservati;
- Scaricare i documenti informatici conservati (duplicati) e i file di evidenza della conservazione (indice di conservazione UNI SInCRO);
- Richiedere e scaricare i PdD da consegnare alle autorità competenti, in caso di necessità.

La procedura per visualizzare i documenti informatici conservati è semplice e intuitiva. È tuttavia disponibile online un manuale, presso lo stesso portale della conservazione.

Il soggetto produttore o un suo delegato all'attività di consultazione e produzione di duplicati informatici, ricerca i documenti attraverso i campi che l'interfaccia grafica mette a disposizione. Si tratta degli stessi metadati con i quali sono stati accompagnati i file durante l'invio al sistema di conservazione.

Una volta visualizzati i file conservati, l'ente produttore può richiedere al SISTEMA un duplicato, attraverso una funzione disponibile sul portale. Detta funzione consente di scaricare un file di tipo ISO o di tipo ZIP, attraverso il canale criptato SSL del portale.

Sarà così possibile per l'ente produttore avere una copia del pacchetto di distribuzione contenente i documenti conservati, il *viewer* per la loro corretta visualizzazione, l'indice di conservazione firmato e marcato e un'estrazione dei metadati associati ai documenti.

Qualora sia richiesta l'attestazione di conformità all'originale di copie di documenti informatici originali, conservati dal sistema di conservazione, nello specifico caso di documenti che rischiano di divenire illeggibili per obsolescenza tecnologica, sarà cura del Soggetto Produttore provvedere a richiedere la presenza di un pubblico ufficiale per assolvere a tale obbligo.

Torna al sommario

7.8 Scarto dei pacchetti di archiviazione

Il paragrafo 4.11 delle Linee guida AgID stabilisce che possono essere oggetto di selezione e scarto, all'interno del sistema di conservazione, i documenti informatici e le aggregazioni documentali informatiche, alla scadenza dei termini di conservazione previsti dalla norma, dandone informativa al soggetto produttore e nel rispetto della normativa sui beni culturali.

Il Sistema di Gestione Dati, grazie alla propria concezione, permette di gestire al meglio lo scarto del materiale documentario non destinato alla conservazione permanente, ma caratterizzato invece da tempi di conservazione limitati e diversificati.

Negli archivi correnti gestiti secondo criteri aggiornati è presente, nel piano di classificazione e conservazione, un metadato, definibile per ciascuna tipologia di documento o fascicolo (descrizione archivistica), che stabilisce i tempi di conservazione.

[3] Il collegamento avviene tramite connessione sicura SSL con certificato della Certification Authority TI.TT

Sarà dunque il sistema di gestione dati (SGD) ad incaricarsi di avvisare il responsabile del servizio di conservazione attraverso una o più notifiche impostabili, circa la scadenza dei tempi di conservazione dei documenti, e a supportarlo nell'effettuazione dello scarto, a mantenere al proprio interno, ove richiesto, i metadati della documentazione fisicamente scartata.

Il sistema di conservazione consente di produrre un elenco dei PdA che hanno superato il tempo di conservazione e di inviarlo al Soggetto Produttore. Una volta validato definitivamente l'elenco di scarto dal Soggetto Produttore, questi provvederà a trasmettere l'autorizzazione di scarto al conservatore. Solo dopo aver ricevuto l'autorizzazione, il conservatore provvederà alla cancellazione dei pacchetti di archiviazione, contenuti nell'elenco di scarto.

Il processo di selezione e scarto provvederà ad eliminare fisicamente i file presenti nel *file system* e a cancellare tutti i riferimenti nel database, mantenendo però l'indice di conservazione (in quanto contiene la lista dei file scartati) e aggiungendo automaticamente ai metadati dei PdA, una nota che indica il fatto che il PdA è stato sottoposto a processo di scarto includendo data e ora di esecuzione.

L'operazione di scarto verrà tracciata sul sistema mediante la produzione delle informazioni essenziali sullo scarto, inclusi gli estremi della richiesta di nulla osta allo scarto e il conseguente provvedimento autorizzatorio.

Nei casi di archivi pubblici o privati di particolare interesse culturale, le procedure di scarto avvengono previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo. L'ente produttore, una volta ricevuto il nulla-osta dal Ministero, provvede ad adeguare, se necessario, l'elenco di scarto. Una volta che l'elenco di scarto è definitivo, l'ente produttore lo trasmette al conservatore. Solo dopo aver ricevuto l'autorizzazione dall'ente produttore, il conservatore provvederà alla cancellazione dei pacchetti di archiviazione, contenuti nell'elenco di scarto.

Torna al sommario

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

Per una corretta erogazione di un servizio di conservazione a norma che risponda alle caratteristiche richieste dal modello OAIS, una qualsiasi applicazione di conservazione deve essere in grado di esportare i documenti conservati in un formato che garantisca l'integrità della conservazione stessa.

L'applicazione del sistema di conservazione, essendo progettata secondo lo standard OAIS è in grado di esportare i singoli pacchetti di archiviazione generati durante gli anni, seguendo le regole che permettono successivamente di importare i pacchetti in un altro sistema OAIS *compliant*.

Sono di seguito presentate le situazioni e le soluzioni previste per i flussi di migrazione dei dati conservati da un soggetto conservatore ad un altro.

Si ricorda che, in accordo con il modello OAIS, tutti i conservatori aderenti sono tenuti all'interoperabilità dei sistemi, che si concretizza con l'adozione e la produzione di pacchetti di distribuzione in formato standard, importabili su qualunque sistema di conservazione a norma.

In caso di movimentazione di dati da un conservatore ad un altro o da un conservatore ad un utente autorizzato, si utilizzano canali sicuri e criptati:

- Per i download dei PdD eseguiti da web, il requisito è evaso utilizzando gli appositi servizi https esposti;
- Per gli upload, anche massivi, eseguiti con chiamate SOAP (A2A) è sempre utilizzato il protocollo sicuro https;
- Per la copia dei PdD su supporti ottici, fisici o altro hardware (e.g. flash-memory), allo scopo di trasportare i dati da un conservatore ad un altro o in generale per il mantenimento dei dati conservati all'esterno dei CED del conservatore qualificato, sono adottate procedure che garantiscono i requisiti di riservatezza indicati dalla normativa di riferimento.

TI.TT è in grado di importare dati da altri *outsourcer* previa la verifica della loro piena conformità agli standard di riferimento.

Torna al sommario

7.9.1 Cessazione del SERVIZIO

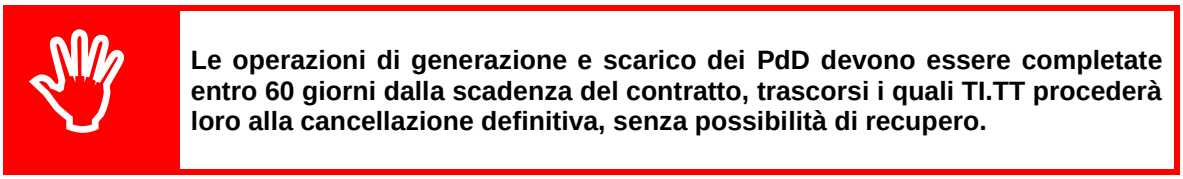
Di seguito viene tracciato l'iter procedurale della Cessazione del SERVIZIO, cioè le azioni da effettuare alla scadenza dei contratti con i clienti, qualora non vengano rinnovati.

I referenti indicati dal Cliente in fase di attivazione, dovranno collegarsi alla piattaforma web dedicata alla generazione e allo scarico dei PdD contenenti tutti i documenti conservati, fino alla scadenza.

TI.TT fornirà supporto telefonico in orario di ufficio, per eventuali problemi (v. capitolo Assistenza al Cliente10). Gli utenti avranno a disposizione un manuale, scaricabile direttamente dal sito di TI.TT, che descrive tutte le attività da espletare per queste operazioni.

Ove le dimensioni dei PdD lo richiedano e sulla base degli accordi con i singoli Clienti, TI.TT procederà al loro trasferimento sui supporti forniti dal Cliente, che gli saranno riconsegnati.

Al termine delle predette operazioni, TI.TT disattiverà l'accesso al portale web e cancellerà definitivamente i dati, senza possibilità di recupero.



Torna al sommario

8 Il sistema di conservazione

Il modello dei dati che viene utilizzato come base per l'implementazione del sistema di conservazione è lo standard ISO 14721:2012 OAIS Open Archival Information System esplicato nella gestione di tre differenti tipologie di pacchetti informativi:

- Il pacchetto di versamento (PdV): il documento digitale o l'insieme dei documenti digitali, corredati da tutti i metadati descrittivi, versati dal soggetto produttore nel sistema di conservazione.
- Il pacchetto di archiviazione (PdA): uno o più PdV sono trasformati in pacchetto di archiviazione per la conservazione. Il PdA ha un insieme completo di informazioni sulla conservazione che si aggiungono al file di metadati.
- Il pacchetto di distribuzione (PdD): il documento digitale o l'insieme dei documenti digitali, corredati da tutti o da parte dei metadati previsti nel PdA, finalizzati alla presentazione e distribuzione dei documenti conservati.

In termini generali, il modello OAIS definisce le componenti logiche comuni a tutti e tre i pacchetti informativi sopra descritti. Il modello dati utilizzato dal sistema di conservazione prevede una strettissima aderenza a tale modello concettuale rivisitandolo ed ampliandolo con elementi di contestualizzazione provenienti dalla tradizione archivistica italiana.

Inoltre, l'obiettivo del sistema di conservazione è quello di garantire non solo la gestione e la conservazione dell'insieme informativo e descrittivo del singolo documento (o collezione di documenti, nell'accezione OAIS, in riferimento a AIC, *Archival Information Collection*), ma anche di tutte le informazioni di contesto dei metadati e, soprattutto, delle relazioni fra i documenti che servono per la ricostruzione del vincolo archivistico e, quindi, del fascicolo digitale di riferimento.

Come illustrato nella seguente figura il sistema di conservazione è conforme al modello OAIS.

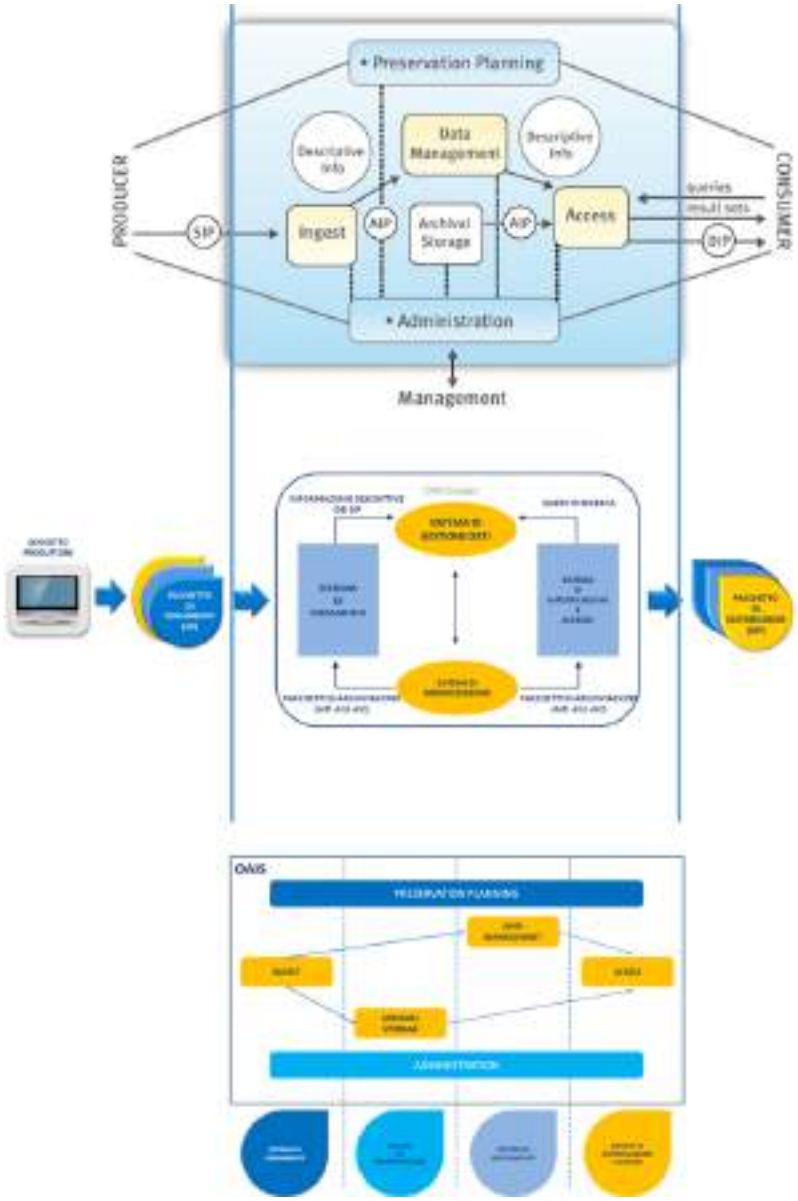


Figura 4 - Sistema di conservazione e conformità al modello OAIS

Torna al sommario

8.1 Componenti logiche

Nel rispetto dello standard, il sistema è formato da quattro macro-componenti funzionali:

8.1.1 Sistema di versamento (SV).

Il sistema di versamento è la porta di ingresso dell'intero sistema ed ha il compito di ricevere i pacchetti di versamento da parte dei soggetti produttori, di verificarne l'aderenza al contratto di servizio di conservazione e ai requisiti di conservazione, di preparare i pacchetti di archiviazione ed infine di inviare ai sistemi opportuni, le informazioni e i dati per garantire la conservazione a norma dei documenti informatici ricevuti.

Rispetto alla pluralità di situazioni documentarie possibili, il sistema si comporterà applicando le regole d'ingresso definite all'attivazione del SERVIZIO. Esattamente come avviene in un archivio di deposito tradizionale, le regole avranno lo scopo di stabilire:

- Le caratteristiche minime che la documentazione deve possedere per poter essere accettata in ingresso;

- I tempi di versamento della documentazione dotata di tali caratteristiche;
- Le modalità di versamento;
- I metadati di ciascun versamento che dovranno anch'essi essere conservati dal sistema.

In particolare, per quanto riguarda il primo punto, il sistema può gestire due ordini di caratteristiche:

- Caratteristiche tecnologiche, riferite ai singoli oggetti digitali;
- Caratteristiche archivistiche, ossia la presenza di alcuni metadati di contesto.

Le caratteristiche archivistiche possono riguardare, ad esempio, l'appartenenza di ciascun documento ad un fascicolo, o la possibilità di ricondurre un fascicolo all'attività di un determinato ufficio.

Le caratteristiche tecnologiche riguardano esclusivamente i documenti digitali, e possono riferirsi al formato con cui sono stati prodotti, alla validità della firma, e/o della marca temporale. Poiché i documenti informatici potrebbero giungere al sistema dopo un considerevole lasso di tempo dalla loro formazione, a causa dei tempi di chiusura delle relative pratiche, è quanto mai opportuno che il sistema si incarichi di verificare la sussistenza dei requisiti di base per la conservazione.

Una volta che la documentazione avrà superato i controlli di qualità previsti, il sistema di versamento dovrà applicare le regole previste dal *preservation planning* per costruire i pacchetti di archiviazione a partire dai PdV inviati dal produttore.

Innanzitutto, viene generata la cosiddetta "descrizione del pacchetto" che consiste in una serie di informazioni descrittive (descrizioni associate) che consentirà l'accesso al documento informatico da parte dell'utente. Infatti, sulla base di queste descrizioni, è possibile effettuare ricerche ed è a partire da queste descrizioni che verranno costruiti i PdD differenti, a seconda delle necessità dell'utente.

Sui documenti versati nel sistema di conservazione è possibile quindi avviare un'attività di validazione sia dei file che dei metadati rispetto alle regole ed agli standard previsti dalle descrizioni archivistiche di appartenenza. I risultati della convalida possono essere allegati al documento oggetto della convalida per essere eventualmente portati in conservazione insieme al documento. Il processo di convalida include:

- La verifica dell'integrità del documento memorizzato sul supporto rispetto all'impronta associata allo stesso;
- La verifica che il formato del contenuto binario sia coerente con quanto dichiarato nei suoi metadati;
- La compilazione metadati: alcuni metadati potrebbero essere compilati in questa fase in maniera automatica (ad esempio potrebbero essere aggiunte le informazioni relative all'utente che ha effettuato il versamento e la data di versamento).

Il risultato della convalida è riepilogato da un esito in formato XML nel rapporto di versamento. I documenti informatici, per i quali l'esito della convalida è risultato positivo, possono quindi essere inseriti in un PdA.

L'esito restituito contiene, in un file in formato XML, la lista dei file, il relativo *hash* e l'identificativo univoco che è stato assegnato al file dal sistema di conservazione e che potrà essere utilizzato per accedere al file.

Torna al sommario

8.1.2 Sistema di gestione dati (SGD)

Completa l'architettura, il Sistema di Gestione Dati che ha il compito di gestire le informazioni legate al contesto archivistico e alle descrizioni dei documenti; questa macro-componente è in pratica il collante dell'intero sistema. Il Sistema di Gestione Dati è il cuore archivistico del sistema ed è la componente che consente di avere una visione unitaria dell'archivio e quindi consente di accedervi.

Il Sistema di Gestione Dati ha una duplice valenza: da una parte offre servizi al Sistema di Accesso per consentire le ricerche e la navigazione e dall'altra consente all'ente produttore di gestire il proprio deposito digitale. Il Sistema di Gestione Dati rappresenta il collante archivistico dell'intero sistema di conservazione e per questo riteniamo questa componente essenziale per consentire ad un soggetto produttore di gestire al meglio il proprio deposito digitale.

Il Soggetto produttore attraverso questo modulo potrà vedere l'archivio come il complesso sistema di relazioni che in effetti è e, tramite le funzionalità che esso offre, potrà compiere tutte quelle operazioni tipicamente archivistiche necessarie per la gestione di un archivio (di deposito). Per esempio, il Sistema di Gestione Dati, grazie alla propria particolare concezione, permette di gestire al meglio lo scarto del materiale documentario non destinato alla conservazione permanente, ma caratterizzato invece da tempi di conservazione limitati e diversificati.

Torna al sommario

8.1.3 Sistema di memorizzazione (SM)

Il Sistema di Memorizzazione ha lo scopo di gestire in modo semplice e sicuro la conservazione a lungo termine dei documenti informatici, integrando una serie di servizi specifici di monitoraggio dello stato fisico e logico dell'archivio ed effettuando, per ogni documento conservato, una continua verifica di caratteristiche come la leggibilità, l'integrità, il valore legale, l'obsolescenza del formato e la possibilità di applicare la procedura di scarto d'archivio.

Nell'ambito del sistema complessivo, quindi, il Sistema di Memorizzazione ha il compito di garantire il mantenimento della validità nel tempo dei singoli "documenti digitali", preoccupandosi di aspetti quali l'affidabilità, l'autenticità e l'accessibilità.

Il Sistema di Memorizzazione, in primo luogo acquisisce quanto inviato dal Sistema di versamento durante la fase di versamento e, verificandone preventivamente l'affidabilità, provvederà a gestirne lo storage. Sui documenti conservati verranno applicate opportune politiche di gestione atte a garantire, non solo la catena ininterrotta della custodia dei documenti, ma anche la piena tracciabilità delle azioni conservative finalizzate a garantire nel tempo la salvaguardia della fonte.

Torna al sommario

8.1.4 Sistema di accesso

Il modulo per la gestione degli accessi orchestra il flusso di informazioni e servizi necessari per fornire le funzionalità di accesso al cosiddetto "consumer" ovvero all'utente che ha la necessità di accedere ad un determinato documento.

A seguito di una ricerca impostata dall'utente, il modulo di Gestione Accesso richiede i risultati della ricerca al Sistema di Gestione Dati che, organizzando le informazioni descrittive dei PdA, è in grado di rispondere alla richiesta; l'utente una volta individuato il documento desiderato (o i documenti, o addirittura un intero fascicolo o PdA) potrà inoltrare una richiesta di accesso ai dati, questa genererà la richiesta al modulo di Generazione PdD il quale interagendo sia con il Sistema di Gestione Dati che con il Sistema di Memorizzazione recupererà le informazioni necessarie (PdA e informazioni descrittive) per produrre il Pacchetto di distribuzione corrispondente alla richiesta.

Attraverso la piattaforma di conservazione è possibile definire un numero illimitato di ruoli attraverso la definizione di profili d’uso che verrà illustrata più avanti.

Le funzionalità di ricerca saranno implementate dal Sistema di Gestione Dati, mentre il Sistema di Accesso fornirà le interfacce per l'interrogazione e per la ricezione e visualizzazione dei risultati.

Le modalità dell'accesso, in generale, permettono quindi di poter ricercare il documento singolo o le aggregazioni di documenti, mediante tutti i criteri derivabili dai metadati ad esso direttamente associati, per poi risalire al suo contesto archivistico.

L’accesso alle funzionalità offerte dal sistema è regolato anche da un sottosistema di autorizzazione che permette di suddividere l’utenza applicativa in gruppi ai quali è possibile assegnare permessi di esecuzione di specifiche operazioni. I singoli permessi (capabilities)sono assegnabili ad un gruppo tramite la definizione di “Profilo d’uso” Grazie ai “profili d’uso”, definibili autonomamente dall’amministratore dell’applicazione, ogni utente potrà accedere ad uno o più Soggetti Produttori e avere visibilità su una o più descrizioni archivistiche, nonché è possibile assegnare visualizzazioni di singoli pulsanti e/o menù.

Il sottosistema per la firma digitale nel contesto della conservazione digitale si configura come elemento fondamentale per consentire di attuare la conservazione a norma dei documenti di un preciso flusso di lavoro. Il processo essenziale per completare la procedura consiste nella firma dell’indice di conservazione (UNI 11386:2020) dei PdA nonché nell'apposizione di una marca temporale su tale file.

Essendo presenti diversi dispositivi in grado di fornire queste funzionalità, l'architettura del sistema di conservazione prevede di demandare ad un apposito sottosistema il compito di interfacciarsi con essi. Ciò consente al Sistema di Memorizzazione di utilizzare qualunque dispositivo di firma digitale, dato che le eventuali differenze nell'implementazione vengono mascherate dal sottosistema stesso.

Resta l'obbligo che la firma digitale, in questo contesto relativa al responsabile del servizio di conservazione deve essere apposta utilizzando un dispositivo di firma di un tipo approvato da AgID ed un certificato rilasciato da una Certification Authority (CA) appartenente all'elenco dei certificatori accreditati presso AgID.

La marca temporale consiste in un'ulteriore firma digitale apposta da un soggetto esterno, Time Stamping Authority (TSA), il quale registra e memorizza presso la propria struttura organizzativa l'impronta del file e la relativa data di firma. In questo caso il soggetto esterno non è, dunque, una persona fisica ma un Ente certificatore.

Il sistema di conservazione è in grado di richiedere in modo automatico ed on-line la marca temporale alle TSA utilizzate nel sistema.

Torna al sommario

8.2 Componenti tecnologiche

I moduli e le componenti necessarie alla conservazione sono tutti erogati internamente da TI.TT Le componenti core del sistema di conservazione sono suddivise in modo da rispettare i più ristrettivi standard di sicurezza:

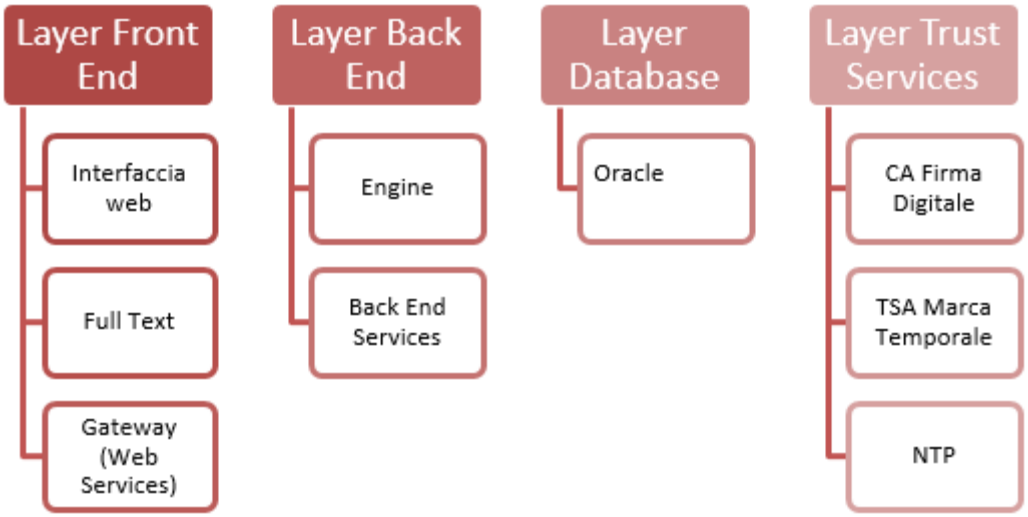


Figura 5 - Componenti core del sistema di conservazione

Torna al sommario

Front End:

L'applicazione è pensata per essere scalabile, aumentando il numero dei Web container, attraverso una logica di server clustering gestita automaticamente dal sistema, che, a seconda del livello di carico di ciascun server, distribuirà al meglio le richieste dei client.

- **L' Interfaccia Web** è erogata in modalità sicura ed espone i servizi di consultazione, esibizione e download;
- **Full-text Engine**: è l'applicazione che abilita le funzionalità di full-text;
- **Gateway / Web Services**: insieme di servizi web e/o elementi hw/sw che permettono, ad applicazioni di terze parti, di versare documenti nel sistema di conservazione o di interrogarlo sullo stato di un documento;

Back End:

- I Back End Services rappresentano il core della logica applicativa e l'interfaccia verso le basi dati (Oracle) e gli storage. Il Back End ha in carico la gestione e la distribuzione dei processi tra i vari nodi del cluster.
- Il database, gli storage e le componenti critiche degli ambienti di conservazione sono soggetti a procedure di backup tali da mantenere correttamente allineati gli ambienti di erogazione e di DR.

Il Sistema di conservazione è sviluppato secondo le specifiche J2EE, nell'ottica di fornire una soluzione Enterprise; è un insieme di applicazioni clusterizzabili che permette una facile scalabilità e una gestione automatica dei processi.

Vista l'esperienza di TI.TT nella gestione dei grandi volumi di dati è sempre stato un obiettivo per l'azienda il creare una architettura elastica, che possa essere espansa in caso di aumento del carico di lavoro oppure ridotta nel caso di un calo delle necessita.

L'intera soluzione è stata progettata per essere in grado di gestire l'elaborazione di grandi volumi di dati. A tale scopo, il sistema può essere scalato sia verticalmente che orizzontalmente e, le singole componenti, possono essere distribuite su più server. La compatibilità con la virtualizzazione e il *cloud computing* è garantita previa raggiungibilità dei servizi di firma.

L'architettura è basata su una soluzione multi-tier a 3 livelli:

- Presentation layer;
- Business logic (o application) layer;
- Database layer.

L'estrema elasticità del sistema permette di sostituire, upgradare a caldo oppure di aggiungere a piacere applicazioni in uno o più nuovi nodi di un eventuale cluster:

- **Back End** (Services): rappresenta il core della logica applicativa e l'interfaccia verso le basi dati a cui l'applicazione attinge. Il Back End ha in carico la gestione e la distribuzione dei processi tra i vari nodi del cluster. È implementato tramite Spring ed espone le sue funzionalità remotamente via protocollo HTTP/HttpInvoker. Non si necessita di un container J2EE ma è sufficiente l'utilizzo di un Servlet Container quale Apache Tomcat 6 per il deploy dello stesso.
- **Engine**: è il motore di conservazione.
- **Front End** (Interfaccia Web): è un'applicazione J2EE stateful realizzata con pagine web dinamiche, cui gli utenti potranno accedere per monitorare il sistema.

Di seguito la lista dei browser dichiarati compatibili che non richiedono l'installazione di plug-in per l'accesso:

- Google Chrome 23 o superiore.
- Internet Explorer 8 o superiore.
- Opera 12 o superiore.
- Safari 6 o superiore.

L'applicazione è pensata per essere scalabile, aumentando il numero dei Web container, attraverso una logica di server clustering gestita automaticamente dal sistema, che, a seconda del livello di carico di ciascun server, distribuirà al meglio le richieste dei client.

In un'ottica di installazione su ambienti virtuali, il sistema consente un'ampia scalabilità al crescere degli utenti coinvolti e, cosa più importante, al crescere dei volumi di documenti da conservare, permettendo di reagire tempestivamente alle nuove esigenze del cliente.

Torna al sommario

8.2.1 Servizi Erogati

Sottodominio	Descrizione
https://conservazione.trusttechnologies.it	Sito di esibizione
https://cons-datisensibili.trusttechnologies.it/asap_arc/	Sito di esibizione

Tabella 10 - Servizi Erogati

Torna al sommario

8.2.1.1 Scalabilità sui volumi

La conservazione dei documenti, rispetto ai volumi, è soggetta a due variabili:

- Crescita dei documenti;
- Crescita dei dati.

La crescita dei documenti, vista la dimensione fisica degli oggetti, è sicuramente la parte più critica in termini di scalabilità. Per questo motivo il sistema di conservazione è stato sviluppato per essere indipendente dal sistema hardware che conserva i file. Oltre ad essere svincolato dal sistema hardware, il software è in grado di distribuire i documenti da conservare su più storage in funzione di regole che dipendono dalla tipologia di documenti o dalla disponibilità di risorse. Per questo motivo, al crescere dei volumi, è possibile affiancare agli esistenti altri storage con caratteristiche tecnologiche anche differenti rispetto ai presenti.

Il Sistema di Conservazione è stato progettato per supportare numeri elevati di utenti che vi accedono per consultare documenti in esso conservati. In ogni caso, trattandosi di un applicativo sviluppato a tre livelli ed impiegando le più moderne tecnologie di implementazione software, è possibile far crescere la componente Interfaccia Web in funzione del numero di utenti. Anche la componente database è assolutamente scalabile in funzione del numero di utenti.

Riepilogando:

- necessità di maggiore capacità elaborativa => si aggiungono application server e/o core e RAM;
- necessità di maggiore capacità elaborativa sui Database e Repository/Content Server => si aggiungono ulteriori server ai rispettivi cluster e/o core e RAM;
- necessità di archiviare una maggior quantità di dati => si aggiungono nuovi dischi agli storage;
- Alla saturazione di uno storage se ne aggiunge un altro;
- necessità di maggiore banda fra il sito principale e l'eventuale sito di disaster recovery: la presenza di accessi in Fibra Ottica sulle due sedi consente di ampliare agevolmente la banda disponibile per il collegamento.

Torna al sommario

8.3 Componenti fisiche

8.3.1 Piattaforma di esercizio primario del SERVIZIO

La soluzione è stata implementata sia su una piattaforma di esercizio primario sia su una piattaforma gemella, per la funzionalità di Disaster Recovery, che in condizioni normali funge da ambiente di collaudo.

La piattaforma di esercizio primario eroga il SERVIZIO con macchine fisiche ridondate, che garantiscono cioè l'alta affidabilità dei processi, in modo che, qualora un processo relativo ad un software dovesse avere un blocco nell'erogazione, la piattaforma continua ad erogare il servizio con la macchina gemella.

Per questo motivo, esistono due macchine gemelle di erogazione dei processi relativi al Front End e due macchine gemelle per i processi del Back End.

La configurazione sfrutta l'algoritmo di Round Robin, garantendo così oltre all'alta affidabilità, anche la scalabilità dei processi. Infine, i bilanciatori sul sito primario consentono di erogare i servizi in alta affidabilità mentre, il cluster dei servizi di backend, permette di estendere le stesse garanzie all'intera infrastruttura.

È disponibile un sito di *Disaster Recovery*, nel Data Center TIM di Via Oriolo Romano n.257 a Roma, come ulteriore protezione dei sistemi dagli eventi di natura disastrosa che si possono verificare sul sito di erogazione principale di Pomezia. La piattaforma sul sito secondario è realizzata con caratteristiche funzionali simili a quelle del sito primario.

Il Data Center di Via di Oriolo Romano è conforme ai principali standard di sicurezza internazionale ed in particolare implementa un Sistema di Gestione della Sicurezza delle Informazioni certificato ISO 27001.

L'architettura *High Level* distribuita sui 3 siti (Produzione, Pomezia2 e DR) si compone di diverse tecnologie abilitanti al fine di indirizzare in modo ottimale le esigenze per ogni linea di erogazione.

Per il sito di DR si ottengono RPO (*Recovery Point Objective,* riferito alla perdita dei dati) tendente a zero con l'utilizzo delle seguenti tecniche:

- Replica dei dati residenti su DB utilizzando tecnologie di replica a livello software (log *shipping e standby DB*), che consentono di avere sul sito remoto una copia consistente a livello applicativo per architetture complesse multi-istanza;
- Replica dei dati residenti su file system effettuata attraverso tecnologie di data *replication host-based.*

Tale soluzione consente di garantire protezione e ridondanza dei dati rendendo possibile la ricostruzione completa degli ambienti tramite funzionalità di allineamento massivo offerte dalle tecnologie di *data replication* a livello *array.*

Torna al sommario

8.4 Procedure di gestione e di evoluzione

Gli interventi di manutenzione oltre a garantire operatività e funzionalità ai sistemi, hanno un alto profilo di qualità in termini sia di manutenibilità che di verificabilità delle applicazioni; per ottenere tali risultati è condizione essenziale un approccio di tipo metodologico e strutturato, che consente di:

- valutare l'impatto: prima di operare la modifica, in sede di definizione degli interventi di manutenzione, deve essere valutato con precisione l'impatto che la modifica avrà sul funzionamento dell'intero sistema;
- controllare l'azione: è necessario procedere nell'esecuzione degli interventi rispettando sia gli standard e le regole proprie del processo di produzione del software che le modalità di erogazione del servizio, aggiornando coerentemente la documentazione al fine di preservare nel corso del tempo il livello di manutenibilità del sistema.

Vengono di seguito sinteticamente illustrati i processi di sviluppo e manutenzione evidenziando in particolare le fasi connesse alla gestione della configurazione:

Figura 6 - Processi di sviluppo e manutenzione

L'analisi di impatto ha l'obiettivo di determinare la portata dell'intervento richiesto ai fini della sua pianificazione e relativa implementazione. Si articola in:

- valutare la richiesta di manutenzione per ciò che riguarda l'impatto potenziale sui sistemi software esistenti, sulla documentazione, sulle strutture dati;
- determinare una stima preliminare delle risorse necessarie;
- documentare la portata della modifica e conseguentemente aggiornare il documento di richiesta di modifica.

Dopo la loro analisi, le modifiche possono essere raggruppate come una **release** di manutenzione schedulata, con conseguente pianificazione, il cui obiettivo è determinarne i contenuti e la tempificazione. Le principali attività sono:

- selezione delle richieste di modifica per la prossima release;
- raggruppamento delle modifiche e schedulazione del lavoro;
- preparazione di un documento di pianificazione della release e, introduzione nel sistema di gestione delle configurazioni;

- aggiornamento della richiesta di modifiche approvata.

Attività afferenti alle modifiche design prevedono:

- analisi della richiesta approvata ed eventuale revisione della struttura architetturale;
- revisione e sviluppo della progettazione funzionale e tecnica;
- aggiornamento della documentazione di progetto e del dizionario dati;
- recupero e rimpiazzo di tutti i documenti modificati;
- aggiornamento della richiesta di intervento.

Le principali attività relative alle modiche sorgenti sono:

- realizzare ed eseguire lo unit test delle modifiche nel codice;
- memorizzare o rimpiazzare il codice, sotto il controllo del sistema di gestione delle configurazioni;
- aggiornare la richiesta di manutenzione in modo da rispecchiare i moduli o le unità modificate.

I rilasci saranno strutturati e qualificati; il significato della codifica usata da TI.TT è chiara ed univoca. In particolare, sono previste le seguenti tipologie di rilasci:

- Livello di manutenzione (Maintainance Level);
- Rilascio di aggiornamento (Release);
- Versione (Version).

Gli interventi di manutenzione evolutiva sono assimilabili ad un insieme di piccoli progetti con durate ipotizzabili che oscillano secondo i requisiti individuati.

Tali attività presentano le caratteristiche tipiche di ogni progetto, ovvero: definizione dei requisiti, definizione di una soluzione tecnica, stima dei costi e dei tempi, formalizzazione dell'incarico, pianificazione, analisi dei rischi ed esecuzione delle attività progettuali, accettazione del prodotto e autorizzazione dei pagamenti.

La manutenzione correttiva consiste nell'adeguamento del software in relazione ad un difetto o malfunzionamento. Le attività di manutenzione correttiva, mirate alla risoluzione dei problemi, sono svolte nel rispetto dei livelli di servizio (SLA) richiesti.

Il team di manutenzione prende in carico la gestione della richiesta di correzione e diventa, quindi, responsabile per il completamento dell'intervento; ove necessario, potrà contattare l'Utente finale per richiedere ulteriori informazioni d'approfondimento sulla richiesta inviata. Se non diversamente specificato dal Committente, l'attivazione dell'intervento è tracciata mediante un sistema di ticketing; mediante questo sarà possibile avere evidenza dello stato del singolo processo e dei livelli di servizio raggiunti.

Il gruppo di lavoro impegnato individua gli oggetti coinvolti dall'attività, eventuali effetti collaterali su altri oggetti software, attua la manutenzione richiesta, nel rispetto delle modalità definite (fasi e prodotti per le singole fasi), dichiarando, alla terminazione dei lavori di sviluppo e test, la disponibilità al rilascio in esercizio.

Nel corso dello svolgimento dell'intervento il team di manutenzione provvederà a mantenere aggiornato il sistema centrale di gestione delle segnalazioni relativamente allo stato dell'intervento.

Le attività di aggiornamento del software sono accompagnate da altrettanti aggiornamenti della documentazione relativa rispetto alle modifiche effettuate.

Torna al sommario

9 Monitoraggi e controlli

Il presente capitolo descrive le procedure di monitoraggio delle funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate. (Linee Guida paragrafo 4.10).

Torna al sommario

9.1 Procedure di monitoraggio

Tipo anomalia	Descrizione	Modalità di gestione
Errori temporanei	È il caso di errori dovuti a problemi temporanei che pregiudicano il versamento, ma si presume non si ripresentino a un successivo tentativo di Versamento	Il produttore deve provvedere a rinviare l'unità documentaria in un momento successivo. L'operazione potrebbe dover essere ripetuta più volte qualora il problema, seppur temporaneo, dovesse protrarsi nel tempo.
Versamenti non conformi alle regole concordate	È il caso in cui il versamento non viene accettato perché non conforme alle regole concordate (firma non valida, Formato file non previsto, file corrotto, mancanza di Metadati obbligatori, ecc.).	Il conservatore invia via e-mail una segnalazione dell'anomalia ai referenti del soggetto produttore, con i quali viene concordata la soluzione del problema.
Errori interni o dovuti a casistiche non previste o non gestite	In alcuni casi è possibile che il sistema di conservazione risponda con un messaggio di errore generico che non indica le cause dell'anomalia riscontrata in quanto dovuta a un errore interno o perché legata a una casistica non prevista, non gestita o non gestibile dal sistema di conservazione.	I referenti del soggetto produttore segnalano il problema via e-mail al soggetto conservatore, che si attiverà per la sua risoluzione.

Tabella 11 - Procedure di monitoraggio

Le anomalie vengono affrontate con diverse metodologie, secondo la natura dell'anomalia stessa e la collocazione dell'evento che l'ha generata nel processo di conservazione; quindi, oltre alle procedure atte a garantire l'integrità degli archivi, esistono anche procedure atte a risolvere anomalie in altre componenti del sistema.

Le caratteristiche comuni e le specificità delle procedure di risoluzione delle anomalie dipendono da diversi fattori organizzativi e tecnologici:

- tutte le funzionalità del sistema che inseriscono o modificano dati nel Data Base e file nell'area SFTP o nel File System operano in modalità transazionale;
- il backup del Data Base assicura il *restore* all'ultima transazione completata correttamente;
- dell'Area di SFTP/Upload riservata a ciascun soggetto produttore e viene effettuato backup;

Il File System è sottoposto a backup full a caldo con frequenza giornaliera;

Non è quindi possibile far fronte a tutte le possibili anomalie con le stesse procedure, ma sono necessarie procedure specifiche secondo la natura dell'anomalia stessa.

La tabella seguente illustra le misure adottate per risolvere eventuali anomalie, classificate in ragione della collocazione delle informazioni nell'ambito del sistema nel momento in cui si è verificata l'anomalia:

File System	Si effettua la restore tramite le funzioni standard del file server per tutti i file inseriti nel File system fino all'ultimo back up; per i file inseriti successivamente all'ultimo back up si eseguono opportune procedure di quadratura tra Data Base e File system, che provvedono a riportare il sistema in stato di congruenza. Le procedure di recupero debbono essere eseguite sia sul sito primario che sul secondario.
Database	Si effettua la restore tramite le funzioni standard di Oracle dal sito primario o dal sito secondario (nel caso di indisponibilità del DB primario)
Area SFTP/Upload	In caso di problemi riscontrati prima del backup, si richiede al soggetto produttore la ritrasmissione dei PdV.

Tabella 12 - Misure adottate per risolvere eventuali anomalie

I servizi ed i sistemi gestiti da TI.TT sono controllati in modo automatico da due diversi sistemi di monitoraggio che consentono la visualizzazione e la notifica degli allarmi:

Il "Sistema Esterno" consente il controllo dei servizi erogati in rete dall'infrastruttura effettuando accessi periodici ai servizi tramite collegamento esterno in ADSL su rete internet.

Il "Sistema Interno" utilizza un Network Management System completamente gestito dagli addetti della CA che consente di mantenere il controllo della rete e dei sistemi fornendo importanti informazioni per la corretta gestione sistemistica.

Come previsto dalla normativa, i riferimenti temporali applicati alle registrazioni effettuate dai sistemi gestiti da TI.TT in qualità di Gestore di PEC e Certificatore Accreditato, costituiscono validazione temporale opponibile a terzi. TI.TT dispone di un sistema di riferimento temporale che garantisce il funzionamento di tutti i suoi servizi in conformità ai requisiti previsti dalla normativa in vigore.

La sincronizzazione temporale dei sistemi gestiti da TI.TT per l'erogazione dei servizi di conservazione rispetto alla scala di Tempo Universale Coordinato (UTC), è garantita dall'utilizzo di due orologi di qualità con NTP server incorporato che, mediante l'esecuzione di uno script periodico, mantengono allineati i server della piattaforma.

La rilevazione di qualsiasi anomalia viene registrata e successivamente risolta dal personale autorizzato da TI.TT.

Tutti i controlli seguono una pianificazione stabilita dal responsabile dello sviluppo e della manutenzione dei sistemi di conservazione. Detta pianificazione viene messa in atto attraverso piattaforme e software ad hoc, in grado di eseguire controlli "terzi" in modo automatico ed inviare le eventuali notifiche al responsabile dei sistemi informativi.

Torna al sommario

9.2 Verifica l'integrità degli archivi

La funzionalità di verifica di integrità degli archivi digitali permette di verificare l'integrità del documento informatico dal momento della sua conservazione, confrontando l'impronta attuale con quella contenuta nell'Indice di Conservazione. Tale funzionalità viene applicata durante il processo di conservazione subito dopo la fase di memorizzazione nel *file system,* e risulta poi utile, nell'assolvimento dei requisiti di verifica periodica della leggibilità dei documenti, come richiesto dalla normativa.

Questa funzionalità è presente nel sistema come processo schedulabile, e può essere quindi pianificato a piacere da parte del responsabile del servizio di conservazione o di un suo delegato. A ogni verifica effettuata viene generato un report in formato xml che può essere consultato da parte del responsabile del servizio di conservazione per attestare la corretta esecuzione della verifica o per diagnosticare eventuali anomalie.

Torna al sommario

9.3 SLA e soluzioni adottate in caso di anomalie

Di seguito viene descritta la tabella dei livelli di servizio garantiti, suddivisi per attività relativa al servizio di conservazione a norma di TI.TT.

RIFERIMENTO	DESCRIZIONE	MONITORAGGIO[4]
Tempestività di attivazione delle utenze: numero medio di ore lavorative per l'attivazione di una utenza	L'indicatore rappresenta il numero medio di ore lavorative necessarie per il censimento, l'attivazione e l'invio delle credenziali all'utente.	Calcolo QUADRIMESTRALE 5 giorni lavorativi

[4] Tutti i valori sono calcolati al netto degli interventi di manutenzione programmata e dei tempi per attività in carico al Cliente. Inoltre, il calcolo viene effettuato considerando come base l'orario di lavoro 9-18, dei soli giorni lavorativi.

Disponibilità del servizio agli utenti	L'indicatore rappresenta la percentuale di disponibilità del servizio di conservazione.	Calcolo QUADRIMESTRALE 99,50%

L'indicazione delle condizioni di esclusione delle responsabilità di TI.TT è contenuta nelle Condizioni Generali e Specifiche del SERVIZIO richiamate al capitolo 1, cui si rinvia.

Torna al sommario

10 Assistenza al Cliente

Il servizio di assistenza di TI.TT è in grado di risolvere sia problematiche di natura commerciale che tecnica.

L'Help Desk è raggiungibile tramite numero verde nazionale (**800.28.75.24**) e fornisce:

1) Informazioni di natura commerciale: dal lunedì al venerdì dalle 9.00 alle 18.00, festivi esclusi;
2) Assistenza ai clienti: dal lunedì al venerdì dalle 9:00 alle 18.00, festivi esclusi;
3) Segnalazione di inconvenienti (apertura ticket di lavorazione): 24 ore su 24, 7 giorni su 7.

Un team di tecnici specializzati è in grado di supportare il cliente in tutto il ciclo di vita del servizio.

Le procedure di accesso ai servizi di assistenza tecnica prevedono l'identificazione del cliente mediante codici di riconoscimento associati al nome del Soggetto Produttore.

Questa prima fase di identificazione ha il duplice scopo di impedire un utilizzo fraudolento e di fornire ai tecnici la specifica esatta del servizio sottoscritto dal cliente per il quale si richiede supporto.

Terminata la fase di identificazione i tecnici provvedono ad una prima analisi dell'anomalia segnalata (analisi di 1° livello), assegnando un grado di severità e un codice di priorità.

Questa fase prevede anche l'apertura di uno specifico "cartellino di guasto" (trouble ticket) con un numero progressivo per il tracciamento storico ed una successiva analisi comparativa dei guasti e delle loro cause al fine di adottare azioni correttive.

Nel corso dell'analisi di 1° livello è possibile, qualora non siano necessari interventi ulteriori da parte di specialisti, la immediata risoluzione del problema.

In caso contrario l'anomalia verrà fatta scalare ai tecnici specialistici di 2° livello che, nel 100% dei casi, sono in grado di risolvere il problema.

Alla soluzione dell'anomalia il cliente viene avvisato del ripristino completo del servizio e guidato nella verifica della funzionalità al fine di chiudere il "cartellino di guasto".

Torna al sommario

11 Protezione dei dati personali

Nell'ambito del Gruppo Telecom Italia è operativo un sistema organizzativo e normativo interno per garantire che tutti i trattamenti di dati personali si svolgano nel rispetto delle disposizioni di legge vigenti, richiamate al par. 3.1 oltre che ai principi di correttezza e liceità dichiarati nel Codice Etico del Gruppo TIM.

Ai sensi dell'art. 28 del GDPR il Cliente finale (d'ora in avanti anche il "Titolare") nomina TI.TT **Responsabile del trattamento** dei dati personali che il Titolare invia al SERVIZIO, esclusivamente per la finalità relativa alla sua erogazione. La nomina ha luogo contestualmente alla sottoscrizione da parte del Cliente finale delle condizioni di utilizzo del servizio e della modulistica per la sua attivazione ed è valida fino alla cessazione delle attività e comunque non oltre la scadenza del contratto di vendita, ovvero fino alla revoca anticipata per qualsiasi motivo da parte del Titolare. La cessazione delle attività o la revoca anticipata comportano automaticamente l'immediata cessazione dei trattamenti e la restituzione e/o la cancellazione dei dati personali sottoposti ai trattamenti.

Il Responsabile, nell'ambito delle indicazioni, delle condizioni e delle istruzioni fornite dal Titolare:

- tratta i dati dichiarati dal Titolare nella documentazione di attivazione del SERVIZIO;
- effettua i trattamenti relativi alla Conservazione a norma dei documenti informatici;
- effettua i trattamenti mediante strumenti elettronici o comunque automatizzati e/o con strumenti cartacei;
- dichiara di fornire garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti degli interessati del Titolare.

In relazione al SERVIZIO reso al Cliente Finale, TI.TT conferma quanto segue:

- TI.TT conserva nel proprio Registro dei Trattamenti le informazioni previste dal GDPR e relative al servizio contrattualizzato con l'azienda cliente. La registrazione sarà mantenuta anche successivamente alla data di cessazione del servizio contrattualizzato;
- Nel caso TI.TT rilevi violazioni dei dati personali nell'ambito dei trattamenti previsti dal SERVIZIO (c.d. "data breach") e svolti per conto del Cliente Finale, TI.TT gliene darà tempestiva segnalazione;
- Ove applicabile in relazione al SERVIZIO, nel rispetto dei contratti in corso e delle normative in vigore, TI.TT fornirà al Titolare il supporto per permettere l'esercizio degli ulteriori diritti previsti dal GDPR da parte delle persone fisiche interessate;
- I servizi erogati al Titolare in virtù dei contratti in corso sono stati acquisiti da terze parti soggette a stringenti vincoli contrattuali o sviluppati da TI.TT secondo metodologie già conformi al principio della *privacy by design* e *by default*. In particolare, tramite l'applicazione del processo di *risk analysis* e l'adozione di policy interne di sicurezza e compliance Privacy, TI.TT ha definito ed applica adeguate misure di sicurezza per la protezione dei dati personali trattati nelle proprie piattaforme. Ad esse si aggiungono, ove applicabile e in relazione al SERVIZIO, le misure di sicurezza specifiche per rispondere alle esigenze del Titolare e previste dai contratti in corso. L'elenco delle misure definite da TI.TT per la protezione dei dati personali è pubblicato sul sito di TI.TT all'indirizzo: https://www.trusttechnologies.it/download/legale-e-privacy/ ;
- In caso di nuovi servizi o di interventi sui servizi caratterizzati da un rischio significativo per i diritti e le libertà delle persone fisiche TI.TT effettua il Privacy Impact Assessment (PIA);
- TI.TT effettua i trattamenti dei dati personali in infrastrutture collocate sul territorio italiano. Nei casi previsti da accordi con il Titolare si applicano le garanzie previste dal GDPR per il trasferimento extra-EU, previa autorizzazione del Titolare;
- TI.TT fornirà supporto per lo svolgimento delle attività di verifica dei trattamenti che svolge in qualità di responsabile, previo accordo che stabilisca le modalità e i corrispettivi;
- I riferimenti del Data Protection Officer del Gruppo TIM sono i seguenti:
  recapito: Data Protection Officer, via Gaetano Negri, 1 - 20123 Milano
  indirizzo e-mail: dpo.trusttechnologies@telecomitalia.it
- Ulteriori dettagli sui trattamenti sono disponibili sull'informativa pubblicata da TI.TT sul proprio sito, all'indirizzo https://www.trusttechnologies.it/download/legale-e-privacy/

Torna al sommario

Firmato digitalmente da: Danilo Cattaneo
Ruolo: AMMINISTRATORE DELEGATO
Organizzazione: INFOCERT SPA/07945211006
Data: 05/05/2022 10:18:51

Manuale della Conservazione

di InfoCert S.p.A.

InfoCert
TINEXTA GROUP

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

© InfoCert S.p.A. – All right reserved

INDICE DEL DOCUMENTO

1. SCOPO E AMBITO DEL DOCUMENTO 4
2. TERMINOLOGIA 5
3. NORMATIVA E STANDARD DI RIFERIMENTO 13
4. RUOLI E RESPONSABILITÀ 17
PROFILO DI INFOCERT 17
RESPONSABILI INFOCERT 20
5. OGGETTI SOTTOPOSTI A CONSERVAZIONE 29
FORMATI 30
METADATI 31
6. IL PROCESSO DI CONSERVAZIONE 33
CONTROLLI DI VERSAMENTO 34
HANDOVER E INTEROPERABILITÀ 38
7. I SISTEMI DI CONSERVAZIONE 40
FIRMA DIGITALE CON DISPOSITIVO HSM DEI PdA 40
MARCA TEMPORALE DEI PdA 40
SICUREZZA E PROTEZIONE DEI DATI 42
PROCEDURE DI GESTIONE E MONITORAGGIO 44
CONTROLLI PERIODICI E AUDIT 48
8. SPECIFICITÀ DEL CONTRATTO 50

© InfoCert S.p.A. – All right reserved

© InfoCert S.p.A. – All right reserved

1. SCOPO E AMBITO DEL DOCUMENTO

Il presente documento è il **manuale della conservazione di InfoCert S.p.A.** (del Gruppo Tinexta), ai sensi delle **Linee Guida AgID**, Agenzia per l'Italia Digitale, su formazione, gestione e conservazione dei documenti informatici, 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 InfoCert, può liberamente far riferimento al presente documento nel proprio Manuale della Conservazione.

© InfoCert S.p.A. – All right reserved

2. 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.

© InfoCert S.p.A. – All right reserved

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.

© InfoCert S.p.A. – All right reserved

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

© InfoCert S.p.A. – All right reserved

	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.

© InfoCert S.p.A. – All right reserved

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.

© InfoCert S.p.A. – All right reserved

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

© InfoCert S.p.A. – All right reserved

	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

© InfoCert S.p.A. – All right reserved

	Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali.

© InfoCert S.p.A. – All right reserved

3. NORMATIVA E STANDARD DI RIFERIMENTO

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

- 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 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 [interamente abrogate dalle Linee Guida AgID a partire da gennaio 2022];
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche per il

© InfoCert S.p.A. – All right reserved

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;
- Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 [interamente abrogate dalle Linee Guida AgID a partire da gennaio 2022];
- 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.
- eIDAS (electronic IDentification Authentication and Signature) EU Regulation 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.
- 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.
- 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).

© InfoCert S.p.A. – All right reserved

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;

© InfoCert S.p.A. – All right reserved

- 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 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.

© InfoCert S.p.A. – All right reserved

4. 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 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 InfoCert);
e) **CONSERVATORE** (InfoCert).

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

Quest'ultimo affida in *full outsourcing* il servizio di conservazione a 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 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 INFOCERT

InfoCert si pone sul mercato europeo come **Trust Service Provider** qualificato ai sensi del Reg. UE 910/2014 (eIDAS), leader del mercato italiano nei servizi di digitalizzazione e dematerializzazione, nonché una delle principali Certification Authority a livello europeo,

© InfoCert S.p.A. – All right reserved

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.

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.

Inoltre, dal 2019, InfoCert ha ottenuto la **qualifica AgID Cloud Marketplace** (CSP Tipo B Infrastruttura e SaaS per LegalDoc).

Infine, da febbraio 2022, InfoCert è anche tra le prime aziende italiane iscritta nell'elenco del **marketplace AgID dei servizi di conservazione**.

Denominazione sociale	InfoCert S.p.A.
Sede Legale:	Piazza Sallustio, 9, 00187 Roma Tel.+39 06 836691

© InfoCert S.p.A. – All right reserved

Sedi Operative:	• Piazza da Porto, 3, 35131 Padova • Via Via Carlo Bo, 11, 20143 Milano • Via Marco e Marcelliano, 45, 00147 Roma Tel: +39 06836691
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 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-Archive*), 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 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).

© InfoCert S.p.A. – All right reserved

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.

InfoCert, inoltre, nello svolgimento delle proprie attività, ha conseguito le seguenti certificazioni:

RESPONSABILI 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	Nicola Maccà	• 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;	da luglio 2018

© InfoCert S.p.A. – All right reserved

RUOLI	NOMINATIVI	ATTIVITA'	PERIODI
		• 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.	
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;	da settembre 2015

© InfoCert S.p.A. – All right reserved

RUOLI	NOMINATIVI	ATTIVITA'	PERIODI
		• collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza; • controlli periodici a campione sulla leggibilità dei documenti conservati.	
Responsabile Sicurezza dei sistemi per la conservazione	Giovanni Belluzzo	• Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; • Segnalazione delle eventuali difformità al Responsabile del servizio e individuazione e pianificazione delle necessarie azioni correttive.	da luglio 2018
Responsabile trattamento dati personali (Privacy Officer)	Ilenia Gentilezza	• Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali. • Garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.	da marzo 2020
Responsabile sistemi	Francesco Griselda	• Presidio ed evoluzione dei sistemi informativi per la	da ottobre 2020

© InfoCert S.p.A. – All right reserved

RUOLI	NOMINATIVI	ATTIVITA'	PERIODI
informativi per la conservazione		conservazione nel rispetto delle procedure ISO9001 ISO14000 ISO20000 ISO27000. • Gestione dell'esercizio delle componenti hardware e software di base del sistema di conservazione. • Monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore in collaborazione con Il Responsabile della manutenzione del sistema di conservazione. • Segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di Conservazione e individuazione e pianificazione delle necessarie azioni correttive. • Pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione. • Controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di Conservazione. • Coordinamento dello sviluppo e manutenzione delle componenti hardware e software di base del sistema di conservazione.	

© InfoCert S.p.A. – All right reserved

RUOLI	NOMINATIVI	ATTIVITA'	PERIODI
Responsabile sviluppo e manutenzione del sistema di conservazione	Lucia Bortoletto	• Sviluppo e manutenzione del sistema di conservazione nel rispetto delle procedure ISO9001 ISO14000 ISO20000 ISO27000. • Coordinamento dello sviluppo e manutenzione delle componenti software del sistema di conservazione. • Pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione. • Monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione. • Interfaccia con l'ente produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche in collaborazione con il Responsabile funzione archivistica di conservazione. • Gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.	da luglio 2018

© InfoCert S.p.A. – All right reserved

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

RUOLI	NOMINATIVI PRECEDENTI	PERIODI
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
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

Operativamente, la suddivisione interna delle attività può essere così schematizzata:

© InfoCert S.p.A. – All right reserved

Responsabili>> Attività	del servizio	della funzione archivistica	del trattamento dei dati personali	della sicurezza dei sistemi	dei sistemi	dello sviluppo e della manutenzione	soggetto produttore
1. Condizioni Generali di Contratto	R						
2. Richiesta di attivazione	R	V	V	V	V	V-E	
3. Atto di affidamento	R						
4. Specifiche Tecniche di integrazione	V			A	A	R-E	
5. Impegno alla riservatezza	V		R	A			
6. Acquisizione del documento da conservare	R				E	V	
7. Metadatazione ed archiviazione	A	R			E	V	
8. Eventuale attestazione della conformità di quanto memorizzato nel documento d'origine da parte di un PU	R						
9. Creazione del pacchetto di versamento							R
10. Invio al sistema di conservazione del							R

© InfoCert S.p.A. – All right reserved

Responsabili>> Attività	del servizio	della funzione archivistica	del trattamento dei dati personali	della sicurezza dei sistemi	dei sistemi	dello sviluppo e della manutenzione	soggetto produttore
pacchetto di versamento							
11. Validazione Del pacchetto di versamento	R				E	V	
12. Generazione del pacchetto di archiviazione	R				E	V	
13. Memorizzazione e duplicazione	R			V	E	V	
14. Invio dell'IPdA al soggetto produttore	R					E	V
15. Scarto dei pacchetti di archiviazione	R	V			A	E	A
16. Chiusura del servizio di conservazione al termine di un contratto	R	V			A	E	A
17. Conduzione e manutenzione del sistema di conservazione	A				R	E	V
18. Monitoraggio del sistema di conservazione	A	V			R	E	

© InfoCert S.p.A. – All right reserved

Responsabili>> Attività	del servizio	della funzione archivistica	del trattamento dei dati personali	della sicurezza dei sistemi	dei sistemi	dello sviluppo e della manutenzione	soggetto produttore
19. Change management		V		V	A	R	
20. Verifica periodica di conformità a normativa e standard di riferimento	A	R	V	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 interno. Il processo di conservazione è normalmente effettuato da procedure totalmente automatizzate, che non necessitano dell'intervento di altri soggetti o delegati. InfoCert si riserva, come specificato nelle Condizioni generali del Contratto, la possibilità di avvalersi di partner tecnologici per l'esecuzione di operazioni, singole attività, servizi relativi a funzioni o fasi del processo di conservazione, a terzi soggetti, fornitori esterni, che per conoscenza, esperienza, capacità e affidabilità forniscano idonee garanzie.

© InfoCert S.p.A. – All right reserved

5. 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 InfoCert e associato a un file XML, detto Indice del Pacchetto di Archiviazione (IPdA o indice di conservazione UNI SInCRO) firmato digitalmente e marcato temporalmente dal Responsabile del servizio di 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.

© InfoCert S.p.A. – All right reserved

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 (firmato e marcato dal Responsabile del servizio di 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 (firmato e marcato dal Responsabile del servizio di 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'.

I visualizzatori di alcuni formati (definiti in InfoCert come 'standard' perché maggiormente richiesti) sono automaticamente assegnati all'atto dell'attivazione del proprio ambiente di conservazione e sono forniti da 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)

© InfoCert S.p.A. – All right reserved

Formato	Estensione	MIME-Type	Standard
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, dovrà segnalarlo nei 'Dati Tecnici di attivazione' (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.

Inoltre, il Responsabile del servizio della conservazione mantiene un archivio di tutte le componenti hardware e software obsolete, non più compatibili con i programmi di visualizzazione garantiti e/o depositati dal soggetto produttore, nel caso questi siano i soli strumenti che consentono di rendere leggibili i documenti conservati associati a tale *viewer*.

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.

L'**Allegato 5 delle Linee Guida AgID** introduce i metadati minimi per il documento informatico, il documento amministrativo informatico e per le aggregazioni documentali.

© InfoCert S.p.A. – All right reserved

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

© InfoCert S.p.A. – All right reserved

6. 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;*
3. *il sistema crea i pacchetti di archiviazione; il Responsabile del servizio firma digitalmente l'indice di conservazione UNI SInCRO di ogni singolo pacchetto di archiviazione a garanzia di integrità, immodificabilità e autenticità;*
4. *l'indice di conservazione viene marcato temporalmente, a garanzia della sua data-certazione; il sistema restituisce al produttore l'indice di conservazione come ricevuta (rapporto di versamento);*

© InfoCert S.p.A. – All right reserved

5. *il database del sistema viene aggiornato, il pacchetto di archiviazione viene indicizzato, memorizzato e ridondato più volte (ogni pacchetto è soggetto a controlli periodici di integrità e leggibilità a distanza di tempo);*
6. *il documento conservato può essere ricercato attraverso i metadati, su richiesta dell'utente in possesso delle apposite credenziali, in qualsiasi momento, ed esibito mediante un pacchetto di distribuzione, che contiene tutte le evidenze del processo.*

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 creazione, utilizzo e archiviazione 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:

© InfoCert S.p.A. – All right reserved

- 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 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.

Al terzo rifiuto del pacchetto, sarà necessario contattare il servizio di assistenza tecnica di 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') 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

© InfoCert S.p.A. – All right reserved

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, 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.

© InfoCert S.p.A. – All right reserved

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 firmato e marcato temporalmente dal Responsabile del servizio della conservazione stesso).

In caso di anomalie, se il documento risulta corrotto in uno dei repository, il sistema tenta il ripristino automatico con il dato presente nel repository integro. Se invece ambedue le copie sono alterate, 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 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.

© InfoCert S.p.A. – All right reserved

La procedura può essere attivata per varie ragioni, sia alla chiusura del contratto, sia in continuità di servizio, 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 (al termine della quale viene inviata una notifica al soggetto produttore).

Lo scarto è, quindi, espressamente richiesto a InfoCert dal soggetto produttore, mediante '**MODULO LIBERATORIA E RICHIESTA SCARTO**' e apposita lista di token firmata digitalmente dal Responsabile della Conservazione interno.

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.

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 InfoCert sono conformi allo standard di interoperabilità UNI SInCRO: l'interrogazione di tali archivi restituisce le informazioni secondo il suddetto standard.
L'adozione di tale standard permette l'interoperabilità e la trasferibilità dei dati in modo semplificato.

Nel caso il soggetto produttore decida di rescindere o interrompere il contratto di affidamento del servizio di conservazione, questi può effettuare il **download** dei propri Pacchetti di Distribuzione in autonomia, attraverso la procedura di esibizione, o, in alternativa,

© InfoCert S.p.A. – All right reserved

richiedendo il **servizio di restituzione** (su supporto da concordare in base a volume ed esigenze).

Il soggetto produttore provvede ad inviare anche copia della **liberatoria** denominata '**MODULO DI RESTITUZIONE DATI**' sottoscritta digitalmente dal proprio Responsabile della conservazione interno.

Al termine della procedura di handover verso il nuovo Conservatore, i pacchetti verranno cancellati.

Seguendo i dettami dello standard OAIS, il versamento in 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 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'.

© InfoCert S.p.A. – All right reserved

7. I SISTEMI DI CONSERVAZIONE

I sistemi sono organizzati su più siti nel territorio italiano (**Padova**, **Modena**, **Milano**), con applicazioni software in architettura distribuita, molteplici componenti e con una serie di servizi di interesse generalizzato condivisi con altre applicazioni (marca temporale, HSM, supporti di conservazione).

I servizi sono accessibili online, tramite portale o chiamate applicative.

Dal punto di vista architetturale **LegalDoc** è realizzato utilizzando la tecnologia dei Web Services, secondo architettura REST su protocollo HTTPS. È protetto da firewall configurati in alta affidabilità e costantemente aggiornati per assicurare i massimi livelli di protezione possibile. L'intero sistema 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.

Dal punto di vista architetturale **SAFE LTA** è organizzato in *hybrid cloud architecture AWS*, servizi API REST, *elastic search engine* e *ingestion engine* configurabili. Ed è basato sulle specifiche *eArchiving building block* del *Connecting Europe Facility* (CEF), un modello di conservazione a lungo termine derivante dallo standard OAIS e utilizzato a livello internazionale.

FIRMA DIGITALE CON DISPOSITIVO HSM DEI PdA

Al buon esito del processo di conservazione, il Responsabile del servizio della conservazione di InfoCert appone la propria firma digitale su ogni pacchetto di archiviazione, mediante un sistema di firma automatica erogato dalla CA - Certification Authority - InfoCert, che si avvale di un dispositivo crittografico ad altre prestazioni HSM.

MARCA TEMPORALE DEI PdA

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* - InfoCert, che la restituisce firmata con un certificato emesso dalla TSA - *Time Stamping Authority* - InfoCert. Il TSS è sincronizzato via radio con l'I.N.RI.M di Torino (Azienda Nazionale di Ricerca Metrologica, già “Galileo Ferraris”) ed è protetto contro la manomissione

© InfoCert S.p.A. – All right reserved

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 InfoCert e dei suoi partner tecnologici supporta la memorizzazione dei file sia su storage magnetici ad alte performance che su sistema *Object Storage S3*. 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 dei documenti che contengono dati sensibili ed eventualmente anche degli altri.

I sistemi di storage sono stati valutati da 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 LegalDoc, lo storage magnetico ad alte performance rappresenta sia il supporto primario di conservazione posto fisicamente presso la sede InfoCert di Padova, sia il supporto secondario posto nel sito di *disaster recovery* di Modena.

I due sistemi sono interconnessi mediante collegamenti ad alta velocità dedicati, completamente ridondati e protetti da misure di sicurezza. I collegamenti consentono la replicazione dei dati conservati eliminando il rischio di distruzione di tutte le copie delle informazioni in caso di danno irreparabile a livello di sito.

Questo secondo sistema funge anche da copia di sicurezza.

L'allineamento tra il sito primario e il sito secondario avviene coerentemente con le politiche generali di Disaster Recovery definite in InfoCert che garantiscono RTO e RPO inferiori alle 48

© InfoCert S.p.A. – All right reserved

ore.

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

SAFE LTA è interante erogato su cloud AWS.

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

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 ISO/IEC 27001:2013**. Nella policy di sicurezza di 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.*

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**.

© InfoCert S.p.A. – All right reserved

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. 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.

© InfoCert S.p.A. – All right reserved

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, 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 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 InfoCert, infatti, sono costantemente impegnati nell'attività di *technology watch*

© InfoCert S.p.A. – All right reserved

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, 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.

Particolare attenzione viene quindi posta nel mantenimento di livelli di servizio, attraverso l'adozione di un modello di *Service Management System* conforme alla citata norma ISO/IEC 20000 ha permesso infatti 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 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:

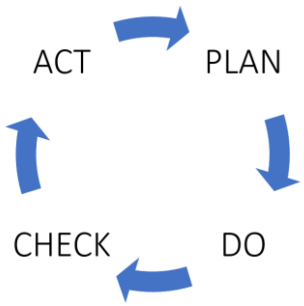


Figura 2 Rappresentazione del modello PDCA SMS

© InfoCert S.p.A. – All right reserved

- istituzione del sistema - SMS (Plan) in cui si definiscono e si pianificano le politiche e i requisiti per la gestione dei servizi inerenti il campo di applicazione; si stabiliscono gli obiettivi di gestione del servizio a tutti i livelli pertinenti;
- implementazione ed attuazione del sistema-SMS (Do) e dei processi di design, transition, delivery e improvement continuo dei servizi sulla base di quanto definito nel service management plan, con particolare attenzione al controllo delle modifiche al SMS valutando e limitando I rischi;
- azioni di monitoraggio e revisione del sistema-SMS (Check);
- attuazione di misure a miglioramento del sistema-SMS (Act) ove sono pianificate e attuate idonee azioni correttive sulla base dei risultati della fase precedente.

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

- allineare i servizi di business con i bisogni correnti e futuri del cliente
- coordinare i requisiti del mercato sui servizi offerti con gli 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 InfoCert ha definito degli SLA baseline di riferimento in relazione ai seguenti KPI (*Key Performance Indicator*):

- orario di servizio
- disponibilità di servizio.

Inoltre, InfoCert si è dotata di una soluzione di monitoraggio denominata **NEW RELIC**, un Software as a Service che permette la completa gestione dei dati ai team DEVOPS.
Questa è una piattaforma di osservabilità di secondo livello, in grado di identificare e prevedere problemi di tipo infrastrutturale e applicativo.
Utilizzando un evoluto sistema di gestione e raccolta dati effettua un monitoring full-stack, fornisce gli strumenti per la prevenzione e l'ottimizzazione dei servizi, oltre ad un'efficiente gestione di segnalazione degli incident. Inoltre, è stata sviluppata l'integrazione con la piattaforma di controllo ***Cloudwatch***, tool nativo di AWS, che consente di avere il pieno controllo e la gestione delle metriche di tutte le componenti presenti in cloud.

© InfoCert S.p.A. – All right reserved

Il tool è composto da tre elementi fondamentali:

- AGENT: risiedono sui server e collezionano le metriche 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;

- NEWRELIC ANALYTICS PLATFORM: è il cuore dello strumento, dove vengono raccolte ed elaborate le metriche e che consente di gestire, aggregare ed elaborare i dati, definendo la modalità di visualizzazione e gestione degli alert;

- LOCATIONS: server nei quali risiedono gli script che simulano la user experience, possono essere privati o pubblici e grazie a questa diversa collocazione è possibile verificare il corretto funzionamento di un servizio sia della rete interna che da rete pubblica.

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 InfoCert, segnalando in modo puntuale le componenti impattate.
Il monitoring della disponibilità del servizio viene svolta coerentemente con le procedure generali di 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 NEW RELIC 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 InfoCert.

© InfoCert S.p.A. – All right reserved

CONTROLLI PERIODICI E AUDIT

In 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

© InfoCert S.p.A. – All right reserved

- 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.

© InfoCert S.p.A. – All right reserved

8. SPECIFICITÀ DEL CONTRATTO

I servizi sono regolati dai seguenti documenti contrattuali, che contengono e descrivono tutte le esigenze richieste dai soggetti produttori e sono resi disponibili in fase di attivazione o su richiesta:

1. ***Condizioni Generali di Contratto*** che regola la vendita del servizio di conservazione nelle diverse modalità di erogazione;
2. ***Richiesta di attivazione*** che comporta l'adesione al servizio e disciplina le condizioni economiche;
3. ***Dati tecnici per l'attivazione*** con cui il soggetto produttore fornisce tutte le informazioni necessarie su tipologie documentali, metadati, configurazioni e numero di utenze di accesso di cui necessita;
4. ***Atto di affidamento*** che rappresenta la formalizzazione dell'affidamento ad InfoCert del servizio di conservazione, la nomina del Responsabile del trattamento dei dati personali ai sensi del Regolamento UE n. 679/2016 GDPR, e stabilisce espressamente quali attività di fatto vengano assunte da InfoCert e quali, al contrario, rimangano a carico dell'affidatario, soggetto produttore, come stabilito dalle Linee Guida AgID;
5. ***Allegato Tecnico*** che descrive le modalità di fornitura del servizio e l'infrastruttura tecnico-tecnologica utilizzata per la sua erogazione;
6. ***Manuale Utente*** che risponde alla necessità di documentare operativamente il processo attraverso le varie schermate;
7. **Impegno alla riservatezza NDA** (NON-DISCLOSURE AGREEMENT);
8. **Specifiche Tecniche di integrazione a LegalDoc**, che fornisce tutte le informazioni tecniche necessarie ad operare l'integrazione tra i Sistemi di Gestione documentali del produttore e LegalDoc (sia tramite web services che con LegalDoc Connector);
9. **Descrizione dei codici di errore**, per fornire una casistica esaustiva dei possibili messaggi di errore di versamento in LegalDoc e delle azioni che è necessario intraprendere per porvi rimedio
10. **File di configurazione** LegalDoc, inviato da InfoCert all'attivazione del servizio, contenente i dati di configurazione del soggetto produttore, delle user d'accesso,

© InfoCert S.p.A. – All right reserved

delle policy associate e delle tipologie documentali, comprensivi di metadati e formati configurati.

Per SAFE LTA le informazioni su integrazioni, errori di versamento e configurazioni sono disponibili su https://developers.infocert.digital/safe-lta/

© InfoCert S.p.A. – All right reserved

ATTESTATO DI PUBBLICAZIONE

Delibera N.ro 1368 del 23/12/2022

Certificato di pubblicazione

Si certifica che la presente Delibera viene pubblicata all'Albo Pretorio on line dell'Azienda in data 23/12/2022 e vi rimarrà per 15 giorni consecutivi

Il Responsabile della Pubblicazione Delibere e Determine

Notificata ai soggetti interni sotto elencati:

UOC AFFARI GENERALI;

COLLEGIO SINDACALE;

UOC GESTIONE ECONOMICO - FINANZIARIA;

DIREZIONE GENERALE;

UOS URP E COMUNICAZIONE;

RESPONSABILE PREVENZIONE CORRUZIONE E TRASPARENZA;

UOC SERVIZIO DI PREVENZIONE E PROTEZIONE;

REFERENTE PRIVACY AZIENDALE;

UOC CONTROLLO DI GESTIONE E PROGRAMMAZIONE;

DIREZIONE AMMINISTRATIVA;

UOC GESTIONE RISORSE UMANE;

UOS TRATTAMENTO GIURIDICO E RAPPORTI SINDACALI;

UOS TRATTAMENTO ECONOMICO;

UOC TECNICO PATRIMONIO;

UOC AFFARI LEGALI;

UOS FORMAZIONE E AGGIORNAMENTO;

UOC SISTEMI INFORMATIVI;

UOS ADEMPIMENTI AMMINISTRATIVI CUP- TICKET ED ALPI;

UOC ACQUISIZIONE BENI E SERVIZI;

UOS ECONOMATO;

DIREZIONE SANITARIA;

UOC DIREZIONE MEDICA DEI PRESIDI OSPEDALIERI AORN MOSCATI;

UOS ORGANIZZAZIONE DEI SERVIZI SANITARI;

UOC FARMACIA;

UOS FARMACOVIGILANZA E DISPOSITIVO-VIGILANZA E FARMACOECONOMIA;

UOC MEDICINA PREVENTIVA DEL LAVORO E RADIOPROTEZIONE;

UOS FISICA MEDICA;

UOC RISCHIO CLINICO;

UOS MEDICINA LEGALE;

UFFICIO DI SEGRETERIA DEL COMITATO ETICO;

DIPARTIMENTO EMERGENZA E ACCETTAZIONE;

UOC ORTOPEDIA E TRAUMATOLOGIA;

UOC MEDICINA D'URGENZA;

UOS O.B.I. E P.S.;

UOC TERAPIA INTENSIVA P.O. LANDOLFI;

UOSD CHIRURGIA D'URGENZA;

UOC TERAPIA INTENSIVA;

DIPARTIMENTO CUORE E VASI;

UOSD CARDIOANESTESIA E RIANIMAZIONE;

UOC CARDIOLOGIA - U.T.I.C.;

UOS CARDIOLOGIA INVASIVA - EMODINAMICA;

UOS T.I. CARDIOLOGICA;

UOC CARDIOCHIRURGIA;

UOS CARDIOCHIRURGIA MININVASIVA;

UOC CHIRURGIA VASCOLARE;

UOS TRATTAMENTO ENDOVASCOLARE DELLE VASCULOPATIE;

UOSD DIAGNOSTICA CARDIOVASCOLARE;

DIPARTIMENTO MEDICO;

UOC GERIATRIA;

UOS VALUTAZIONE MULTIDIMENSIONALE GERIATRICA;

UOC NEFROLOGIA;

UOSD DERMATOLOGIA E DERMOCHIRURGIA;

UOC RECUPERO E RIABILITAZIONE FUNZIONALE;

UOSD GESTIONE INFETTIVOLOGICA NEI PAZIENTI IMMUNODEFICITARI E AIDS;

UOSD ALLERGOLOGIA IMMUNOLOGIA CLINICA;

UOSD MALATTIE ENDOCRINE NUTRIZIONE E DEL RICAMBIO;

UOC MALATTIE INFETTIVE E TROPICALI;

UOC MEDICINA GENERALE;

UOS ANGIOLOGIA;

UOC MEDICINA GENERALE AD INDIRIZZO EPATOLOGICO E GESTIONE PUNTO DI PRIMO SOCCORSO;

UOSD PNEUMOLOGIA;

UOS ENDOSCOPIA TORACICA ED INTERVENTISTICA;

DIPARTIMENTO DI CHIRURGIA GENERALE E SPECIALISTICA;

UOC CHIRURGIA ONCOLOGICA;

UOC UROLOGIA;

UOC BREAST UNIT;

UOSD GASTROENTEROLOGIA;

UOSD UROLOGIA FUNZIONALE;

UOC CHIRURGIA TORACICA;

UOC CHIRURGIA GENERALE;

DIPARTIMENTO ONCO EMATOLOGICO;

UOC EMATOLOGIA;

UOS DH EMATOLOGICO;

UOS TERAPIE CELLULARI AVANZATE;

UOSD TERAPIA DEL DOLORE;

UOC ONCOLOGIA;

UOS NEOPLASIE NELL'ANZIANO;

UOC RADIOTERAPIA ONCOLOGICA;

UOC SERVIZIO IMMUNO TRASFUSIONALE;

DIPARTIMENTO MATERNO INFANTILE;

UOC OSTETRICIA E GINECOLOGIA;

UOC NEONATOLOGIA;

UOC PEDIATRIA;

UOS GENETICA MEDICA;

UOS SUB INTENSIVA PEDIATRICA;

UOC FISIOPATOLOGIA DELLA RIPRODUZIONE;

UOSD GINECOLOGIA SOCIALE;

DIPARTIMENTO DEI SERVIZI;

UOC ANATOMIA E ISTOLOGIA PATOLOGICA;

UOC MEDICINA NUCLEARE;

UOC MICROBIOLOGIA E VIROLOGIA;

UOC LABORATORIO ANALISI;

UOS CENTRO EMOSTASI;

UOC RADIOLOGIA;

UOS RISONANZA MAGNETICA;

UOS T.C.;

UOSD ECOGRAFIA;

UOSD LABORATORIO ANALISI P.O. LANDOLFI;

UOSD RADIOLOGIA SOLOFRA;

UOSD RADIOLOGIA INTERVENTISTICA BODY;

UOSD LABORATORIO DI GENETICA;

DIREZIONE STRATEGICA;

DIPARTIMENTO TESTA COLLO;

UOC NEUROLOGIA;

UOC NEUROCHIRURGIA;

UOC OCULISTICA;

UOS PATOLOGIA RETINICA MEDICA E CHIRURGICA;

UOC ORL;

UOSD NEURORADIOLOGIA;

UOSD UNITÀ STROKE;

UOSD SERVIZIO DI PSICOLOGIA CLINICA OSPEDALIERA;

Trasmessa ai soggetti esterni sotto elencati a cura del servizio proponente:

DPO AZIENDALE;

Esecutività

Il presente atto è immediatamente esecutivo

Il Responsabile della Pubblicazione Delibere e Determine

FIRMATO

FIRMATO DIGITALMENTE DA RUSSO BRUNELLA
23.12.2022 13:44:56 UTC