Manuale di Conservazione

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 di conservazione: 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 - Deprovisioning 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 (SIP) e par. 6.3 - Il pacchetto di archiviazione (AIP): 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;	25/05/2018

	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.	
05	Inserimento cap. 11 - Protezione dei dati personali	29/08/18

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 13
3 Normativa e standard di riferimento 14
3.1 Normativa di riferimento 14
3.2 Standard di riferimento 14
4 Ruoli e responsabilità 15
5 Struttura organizzativa per il servizio di conservazione 19
5.1 Organigramma 19
5.2 Strutture organizzative 20
5.2.1 Attività relative al contratto con i Soggetti Produttori 20
5.2.2 Attività relative alla gestione dei sistemi informativi 21
6 Oggetti sottoposti a conservazione 22
6.1 Oggetti conservati 22
6.2 Il pacchetto di versamento (SIP) 25
6.3 Il pacchetto di archiviazione (AIP) 25
6.4 Il pacchetto di distribuzione (DIP) 29
7 Il processo di conservazione 30
7.1 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico 30
7.2 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti 30
7.3 Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico 31
7.4 Rifiuto del pacchetto di versamento 31
7.5 Preparazione e gestione del pacchetto di archiviazione 32
7.6 Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione. 32
7.7 Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti 33
7.8 Scarto dei pacchetti di archiviazione 34
7.9 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori 35
7.9.1 Deprovisioning del SERVIZIO 35
8 Il sistema di conservazione 36
8.1 Componenti logiche 37
8.1.1 Sistema di versamento (SV). 37
8.1.2 Sistema di gestione dati (SGD) 38

8.1.3 Sistema di memorizzazione (SM) 39
8.1.4 Sistema di accesso 39
8.2 Componenti tecnologiche 40
8.2.1 Servizi Erogati 41
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 43

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

10 Assistenza al Cliente 47

11 Protezione dei dati personali 48

1 Scopo del documento

Il presente documento è il Manuale della Conservazione del Conservatore Accreditato Telecom Italia Trust Technologies S.r.l. (in breve TI Trust Technologies o TI.TT), redatto ai sensi della normativa richiamata al successivo capitolo 3, nel quale sono illustrate le regole generali e le procedure seguite dalla società per l'erogazione dei propri servizi di Conservazione digitale dei documenti informatici (di qui in avanti, per brevità, il SERVIZIO o i SERVIZI)

Il presente documento:

- è pubblicato a garanzia dell'affidabilità del SERVIZIO nei confronti dei Clienti che lo utilizzano e contiene le modalità operative dei servizi indicati;
- descrive le regole e le procedure utilizzate per implementare il processo di conservazione di documenti informatici, trasferiti da Cliente Finale a TI.TT;
- descrive le modalità per l'esibizione dei documenti informatici sottoposti al processo di conservazione;
- descrive le procedure di sicurezza adottate nell'erogazione del SERVIZIO;
- descrive le competenze, i compiti e le responsabilità del **Responsabile del servizio di conservazione**, al quale il soggetto produttore affida le attività relative al SERVIZIO;
- è liberamente disponibile per la consultazione ed il download sul sito predisposto da TI.TT: http://www.trusttechnologies.it/download;
- è un documento informatico e come tale anch'esso sottoposto al processo di conservazione digitale.

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 assume il ruolo di **Responsabile del servizio di Conservazione**, cui il CLIENTE FINALE affida la gestione del processo di conservazione.

I SERVIZI sono erogati da TI.TT come operatore **certificato ed accreditato** 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 Marco Donatone, in qualità di

Responsabile dello sviluppo e della manutenzione del sistema di conservazione.

Denominazione sociale	Telecom Italia Trust Technologies s.r.l.
Indirizzo sede legale	S. R.148 Pontina, km. 29,100 00071 - Pomezia (RM)
Amministratore Delegato	Leopoldo Genovesi
n. P.IVA	04599340967
n. telefono (centralino) n. fax	+3906911971 +390691197331
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 Servizi-ca@telecomitalia.it

Tabella 1 - Dati identificativi del soggetto conservatore

Torna al sommario

1.2 Struttura organizzativa del conservatore

L'organizzazione di TI.TT (illustrata nel diagramma a lato) si articola nelle seguenti funzioni ed attività che rispondono all'Amministratore Delegato:

- **Sales** (attività di commercializzazione del portafoglio di offerta);
- **Business Development** (sviluppo e a profittabilità del portafoglio dell'offerta);
- **Operations** (sviluppo applicativo e supporto tecnico per le piattaforme dell'offerta di competenza), a sua volta articolata in Identity & Certification Authority (Service Management) e Infrastructure & Document Management Infrastrutture, Delivery e Assurance (conduzione operativa dei sistemi, provisioning, Service Management).

Figura 1 - Organigramma

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

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.

Le aree di attività sono coordinate da risorse che operano come referenti con il Responsabile della struttura.

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 a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici.
accreditamento	Riconoscimento, da parte dell'Agenzia per l'Italia digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione.
affidabilità	Caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico.
aggregazione documentale informatica	Aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente.
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 organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività.
attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.
autenticità	Caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico.
certificatore accreditato	Soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, dall' Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza.
ciclo di gestione	Arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo.
classificazione	Attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati.
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 accreditato	Soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, dall'Agenzia per l'ItaliaDigitale.
conservazione	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione.
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.
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.
esibizione	Operazione che consente di visualizzare un documento conservato e di ottenerne copia.
evidenza informatica	Sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.
fascicolo informatico	Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del Codice.
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.
formato	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
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	Funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
identificativo univoco	Sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione.
impronta	Sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash.
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	Insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato.
interoperabilità	Capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi.

leggibilità	Insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti.
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	Strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 delle regole tecniche del sistema di conservazione.
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 detto timestamping.
memorizzazione	Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici.
metadati	Insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 del DPCM 3 dicembre 2013.
pacchetto di archiviazione	Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del presente decreto e secondo 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.
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 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.
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 nell'ambito dell'organizzazione di appartenenza.
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.
processo di conservazione	Insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 10 delle regole tecniche del sistema di conservazione.
produttore	Persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale.

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 gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi	Dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione.
responsabile della conservazione	Soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 delle regole tecniche del sistema di conservazione.
responsabile del trattamento dei dati	Persona fisica, persona giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.
responsabile della sicurezza	Soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza.
riferimento temporale	Informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento.
scarto	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale.
serie	Unità Archivistiche o Unità Documentarie ordinate secondo un sistema di classificazione o conservati insieme perché: - sono il risultato di un medesimo processo di sedimentazione o archiviazione o di una medesima attività; - appartengono ad una specifica tipologia documentaria; - a ragione di qualche altra relazione derivante dalle modalità della loro produzione, acquisizione o uso. (fonte: ISAD).
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 riversamento 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.
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	Sistema di conservazione dei documenti informatici di cui all'articolo 44 del Codice.
sistema di gestione informatica dei documenti	Nell'ambito della pubblica amministrazione, è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445; per i privati è il sistema che consente la tenuta di un documento informatico.
Soggetto produttore o Titolare	Persona fisica o giuridica, la Pubblica Amministrazione o l'Ente titolare dei documenti informatici da conservare. Nelle pubbliche amministrazioni il Produttore ed il Titolare fanno parte della stessa amministrazione.
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.
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.
Versamento:	Azione di trasferimento di SIP dal Produttore al Sistema di conservazione.
utente	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.

Tabella 2 – Glossario

Torna al sommario

2.2 Acronimi

ACRONIMO	SIGNIFICATO
AgID:	Agenzia per l'Italia digitale
AIP:	Archival Information package (Pacchetto di archiviazione)
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)
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).
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 11386:2010 – Supporto all'Interoperabilità nella conservazione e nel Recupero.

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;
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;
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;
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.
Indice del Manuale di Conservazione, versione 2 dello schema AgID, pubblicato il 16 gennaio 2015

Tabella 4 - Normativa di riferimento

Torna al sommario

3.2 Standard di riferimento

Con riguardo alle previsioni contenute nel DPCM 3 dicembre 2013, 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);

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 11386:2010 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

Tutte le caratteristiche del servizio di Conservazione di TI Trust Technologies sono descritte nel presente Manuale di Conservazione e nella documentazione richiamata al capitolo 1.

Per ciascun Cliente, TI Trust Technologies compila e tiene aggiornata una Scheda di Attivazione del servizio nella quale sono indicate le caratteristiche 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 ad TI Trust Technologies. 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 Responsabile del servizio di Conservazione designato dal Soggetto Produttore.

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

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

Seguendo quanto indicato dalle Regole tecniche vigenti e sulla base del modello OAIS (standard ISO 14721:2012), che definisce le caratteristiche di un archivio finalizzato alla conservazione a lungo termine di documenti informatici e alla fruizione degli stessi da parte di una comunità di riferimento, si possono identificare i seguenti ruoli fondamentali Produttore, Utente, Responsabile.

Produttore

Il produttore è la 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 il responsabile della gestione documentale. Nel contratto di affidamento del servizio di conservazione tra soggetto produttore e il conservatore si regoleranno i rapporti di servizio, la responsabilità delle parti e le condizioni economiche.

Il responsabile della funzione archivista del conservatore di TI Trust Technologies avrà cura di definire con i soggetti responsabili interni all'ente Produttore, gli oggetti da sottoporre al processo di conservazione con le relative informazioni di rappresentazione e di conservazione.

Le modalità di versamento verranno altresì specificate nel documento “DESCRIZIONE DEL SERVIZIO”, allegato al contratto di affidamento del servizio. Il soggetto produttore mantiene la titolarità e la proprietà dei documenti versati al conservatore.

Torna al sommario

Utente

Costituisce la comunità di riferimento che interagisce con il conservatore per acquisire le informazioni di interesse nei limiti previsti dalla legge. Tali informazioni vengono fornite dal sistema di conservazione secondo le modalità previste all'art. 10 del DPCM 3 dicembre 2013.

Torna al sommario

Responsabile della conservazione

L’art. 7 del DPCM 3 dicembre 2013 definisce le responsabilità del responsabile di conservazione. Nel contratto di affidamento del servizio di conservazione, sottoscritto tra soggetto produttore e il conservatore, vengono definite le attività e le responsabilità affidate dall’ente produttore, all’interno del quale si definirà la figura del responsabile della conservazione, al conservatore TI Trust Technologies, all’ interno del quale verrà nominata la figura del **Responsabile del servizio di conservazione**.

Lo svolgimento del processo di conservazione richiede la collaborazione e l’interazione fra 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 dell’attività elencate all’art. 7 comma 1 delle Regole tecniche del sistema di conservazione. In qualità di responsabile del servizio di conservazione si occupa inoltre delle politiche complessive del sistema di conservazione. E’ responsabile inoltre delle specifiche del sistema di conservazione sulla base della normativa vigente	**Giantommaso Lafavia**

	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.	
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 conservazione	Il Responsabile della funzione archivistica di conservazione espleta le seguenti funzioni: - 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	**Stefania Rampazzo** **(contratto di consulenza della durata d tre anni, rinnovabile)**

	- 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 conservazione	Il Responsabile dei sistemi informativi per la conservazione espleta le seguenti attività - Gestisce l'esercizio delle componenti hardware e software del sistema di 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.	**Francesca Mazzanti**
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 Sicruezza, 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

Il responsabile della funzione archivistica del conservatore TI.TT è Stefania Rampazzo. La sua nomina è stata formalizzata attraverso la stipula di un contratto di consulenza della durata di tre anni tra TI.TT e IFIN Sistemi srl. La nomina decorre dal 22/10/2014.

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 operazione 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 di conservazione

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 dall'art. 6 co. 8 del DPCM 3 dicembre 2013 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'organigramma della struttura organizzativa coinvolta nel servizio di conservazione:

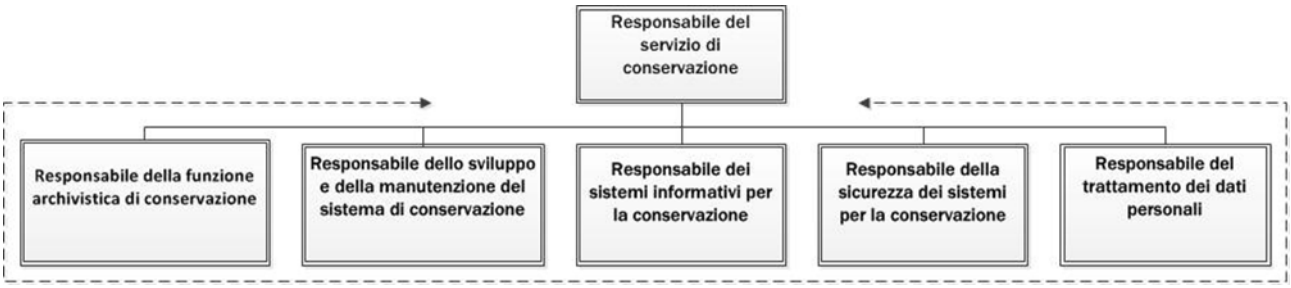


Figura 2 - Organigramma della struttura organizzativa coinvolta nel servizio di conservazione

Torna al sommario

5.2 Strutture organizzative

Collocazione della struttura dedicata alle attività di Conservazione secondo quanto descritto nell'art. 6 del DPCM 3 dicembre 2013.

Riguardo alle principali attività del servizio di conservazione, si descrive di seguito la struttura 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'attività del servizio di conservazione e presa in carico 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 Sales e Operations (commerciale e provisioning del SERVIZIO) della società.

Il perfezionamento del contratto consente l'attivazione del servizio, curato dall'area *Provisioning*,

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 i conformità alla normativa e agli standard di riferimento, da parte del responsabile del servizio di conservazione, coadiuvato dal responsabile del servizio archivistico.

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.

Per quanto concerne il processo di **esibizione** e di **produzione copie e duplicati**, esso è a carico del responsabile del servizio. Egli garantirà il documento informatico originale alla comunità di riferimento e la produzione di duplicati e copie informatiche su richiesta del Soggetto Produttore e delle autorità competenti.

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

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	Infrastrutture, Delivery e Assurance
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	Infrastrutture, Delivery e Assurance
Preparazione e gestione del pacchetto di archiviazione.	Responsabile del servizio di conservazione	Infrastrutture, Delivery e Assurance
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	Infrastrutture, Delivery e Assurance
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	Infrastrutture, Delivery e Assurance
Chiusura del servizio di conservazione (al termine di un contratto).	Responsabile del servizio di conservazione Coordinatore attività di delivery	Infrastrutture, Delivery e Assurance

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 di conservazione, 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 Trust Technologies 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 TITT 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	Infrastrutture, Delivery e Assurance
Monitoraggio del sistema di conservazione;	Responsabile dei sistemi informativi	Infrastrutture, Delivery e Assurance
Change management;	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Infrastrutture, Delivery e Assurance
Verifica periodica di conformità a normativa e standard di riferimento	Responsabile della funzione archivistica di conservazione	Infrastrutture, Delivery e Assurance

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).

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 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.

Il sistema di conservazione utilizza come formati di conservazione quelli elencati al punto 5 dell'Allegato 5 alle Regole tecniche e, inoltre, è in grado di gestire, su richiesta del soggetto produttore, anche formati non compresi nel suddetto elenco ma che il soggetto produttore utilizza nei propri sistemi e che ritiene di dover conservare.

Tutti i formati gestiti 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.

Il sistema identifica i formati al momento della ricezione del SIP mediante l'analisi dei *magic number* o del contenuto del file, in modo tale da consentire l'individuazione dello specifico *mimetype.* L'informazione sul formato è parte dei metadati dei componenti dell'unità documentaria e costituisce un elemento delle informazioni sulla rappresentazione.

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	MIME	Si	ISO/IEC DIS 29500:2008
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	MIME	No	RFC 2822/MIME

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

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

Le caratteristiche che sono state considerate nella scelta sono (v. capitolo 2.1 per le definizioni):

1. apertura
2. sicurezza
3. portabilità
4. funzionalità
5. supporto allo sviluppo
6. diffusione

Per quanto concerne il criterio della funzionalità, TI.TT ha scelto formati che consentono l'utilizzo di *software* che mettono a disposizione diverse funzionalità, poiché ritiene importante che un software sia versatile e permetta all'utente finale di svolgere diverse attività. Questo concetto è strettamente legato alla durata del formato nel tempo.

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, imposto dal comma 1 dell'art. 3 delle nuove regole tecniche, 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 (SIP)

Si tratta del pacchetto informativo inviato dal produttore al sistema di conservazione, utilizzando gli strumenti e le modalità messi a disposizione da TI.TTIl 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 regole tecniche: esso supporta SIP eventualmente accompagnati da IR nel formato definito nell’allegato 5 delle nuove regole tecniche e nel formato CSV.

La fase relativa alla preparazione del pacchetto di versamento (SIP) e il conseguente invio al sistema di conservazione può 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 (AIP).

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

Ci si è attenuti all’allegato 5 del DPCM del 3 dicembre 2013 recante le regole tecniche per il sistema di conservazione. In aggiunta ai metadati previsti dal DPCM suddetto, 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 (AIP)

Il pacchetto di archiviazione (AIP) 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 l'AIP 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 all'AIP 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 SIP 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 AIP 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 (AIP). Lo schema seguente mostra sinteticamente come sarà costruito l'AIP:

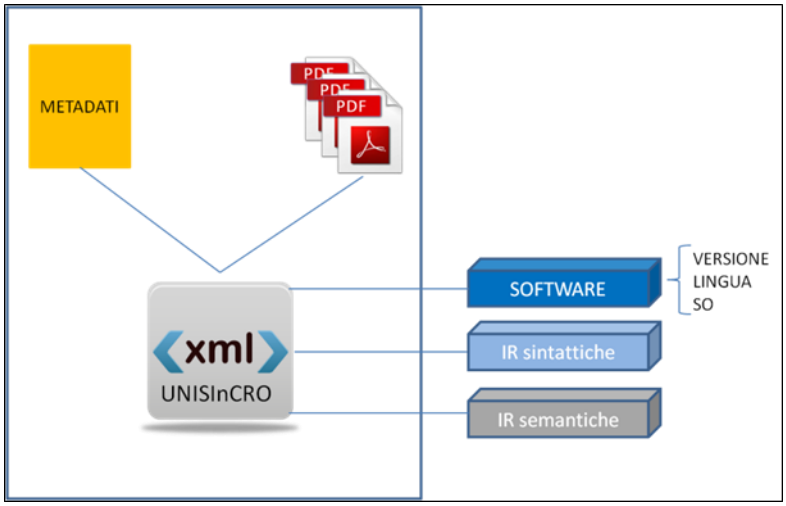


Figura 3 - Pacchetto di archiviazione (AIP)

Schema dell'AIP 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'obbiettivo 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.

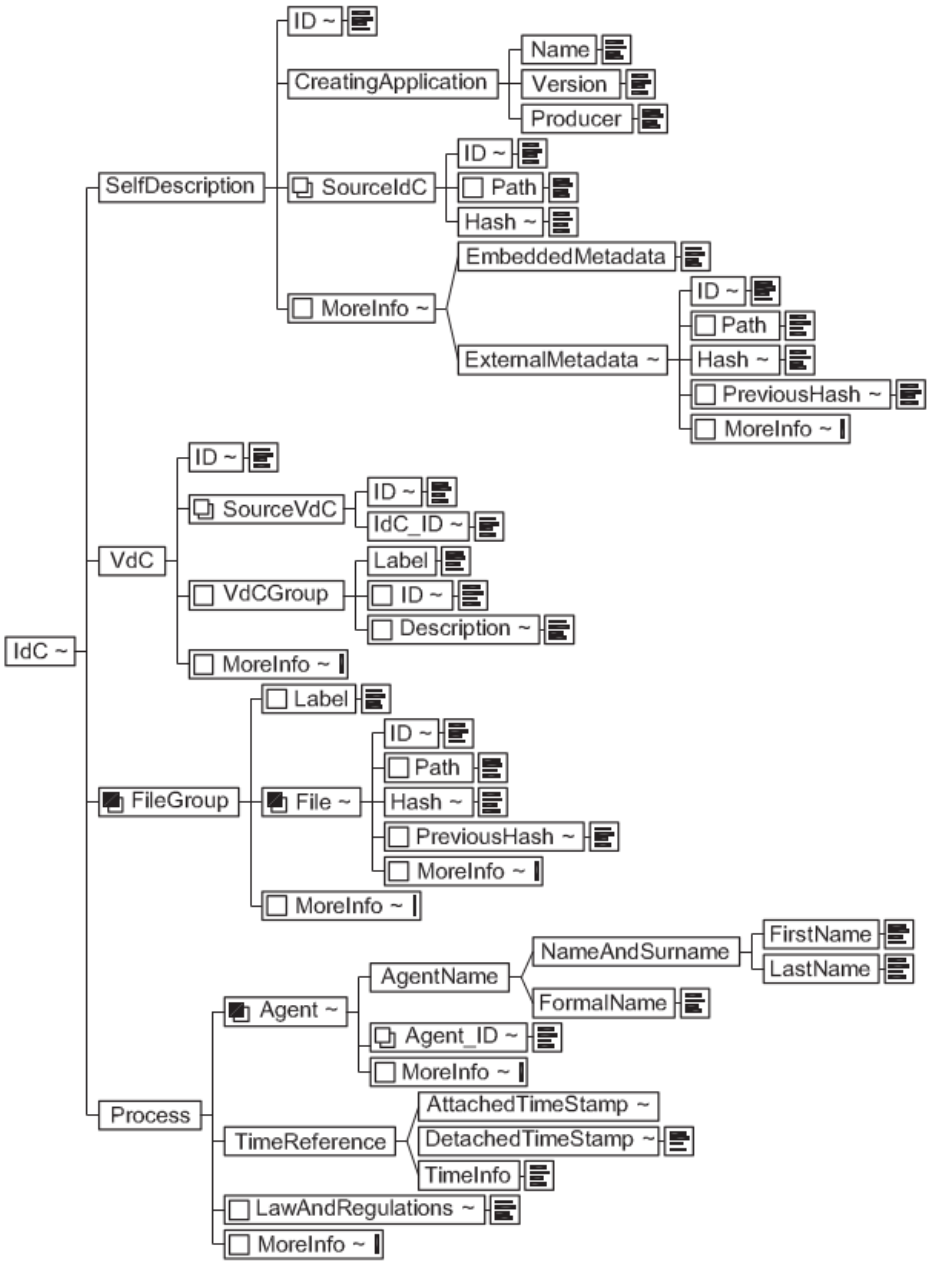


Figura 4: struttura dell'indice del pacchetto di archiviazione

Nella specificazione delle varie strutture dell'indice del pacchetto di archiviazione, l'elemento "ExtraInfo" presente può essere oggetto di ulteriori specificazioni e deve essere inteso come una sorta di "plug-in" per strutture di metadati specialistiche.

Si riporta di seguito la struttura dati del pacchetto di archiviazione completa delle strutture collegate ai diversi elementi "MoreInfo" previsti dallo standard SInCRO.

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema elementFormDefault="qualified" attributeFormDefault="qualified" xmlns:dp="http://www.ifin.it/docpa"
xmlns:xs="http://www.w3.org/2001/XMLSchema" targetNamespace="http://www.ifin.it/docpa">
  <xs:element name="MetadataComponent" type="dp:MetadataComponentType" />

  <xs:complexType name="MetadataComponentType">
    <xs:sequence>
                    <xs:element name="MetadataItem" type="dp:MetadataItemType" minOccurs="0"
maxOccurs="unbounded"/>
```

```
                <xs:element name="MetadataComponent" type="dp:MetadataComponentType" minOccurs="0"
maxOccurs="unbounded"/>
      </xs:sequence>
      <xs:attribute name="type" type="xs:string" use="required" />
      <xs:attribute name="id" type="xs:unsignedByte" use="required" />
   </xs:complexType>

   <xs:complexType name="MetadataItemType">
      <xs:simpleContent>
         <xs:extension base="xs:string">
            <xs:attribute name="type" type="xs:string" use="required" />
            <xs:attribute name="id" type="xs:string" use="required" />
         </xs:extension>
      </xs:simpleContent>
   </xs:complexType>

</xs:schema>
```

Torna al sommario

6.4 Il pacchetto di distribuzione (DIP)

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

In questo caso, un DIP può anche non coincidere con un AIP 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 AIP (negando ad esempio l'accesso ad una parte di esso). Può anche verificarsi il caso di DIP che sono il frutto di più AIP 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 DIP. 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 DIP 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 6).

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)
5) **DICOM**: consente l'acquisizione di immagini DICOM utilizzando procedure standard Storage/Storage Commitment e Query/Retrieve DICOM 3.0;
6) **HI7**: consente l'acquisizione di documenti utilizzando il messaggio standard HI7 (ver. 2.6 o successive) "MDM T10";
7) **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 SIP 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.

[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

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 email 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 al' 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 AIP.

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 l

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 SIP viene sottoposto ai controlli di validazione descritti nel paragrafo 7.2, Qualora il SIP 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.

E' possibile separare i versamenti in diversi pacchetti di archiviazione (AIP) 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 AIP (al fine di supportare il formato ISO);
- Massimo 80mila documenti/file (allegati inclusi) per AIP (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 degli AIP 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 UNISincro generato nel corso del processo di conservazione e contenente tutte le informazioni inviate dal SIP o definite sul sistema di conservazione.

La conservazione si conclude con la firma digitale e la marca temporale dell'indice UNISincro 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 (AIP) conservati, gli , utenti con profilo di esibizione o ricerca possono effettuare ricerche e ottenere pacchetti di distribuzione (DIP).

Il DIP, coincidente con l'AIP, contiene

- tutti gli elementi presenti nell'AIP;
- i documenti dell'AIP 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 DIP 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 DIP, completi di file di evidenza della conservazione e delle informazioni di rappresentazione. Inoltre, nei DIP 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 Trust Technologies.

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 (DIP) 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 DIP) 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.

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

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 Unisincro)
- Richiedere e scaricare i DIP da consegnare alle autorità competenti, in caso di necessità.

La procedura per visualizzare i documenti informatici conservati è semplice e intuitiva. E' 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 responsabile del servizio di conservazione una copia, 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 (DIP) 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

L'art. 9 comma 2, lett. k del DPCM 3 dicembre 2013 stabilisce che deve essere effettuato lo scarto dal sistema di conservazione, alla scadenza dei termini di conservazione previsti dalla norma, dandone informativa al soggetto produttore.

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.

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 degli AIP 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 degli AIP, una nota che indica il fatto che l'AIP è stato sottoposto a processo di scarto includendo data e ora di esecuzione.

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 DIP 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 il riversamento dei DIP 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 accreditato, 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.

7.9.1 Deprovisioning del SERVIZIO

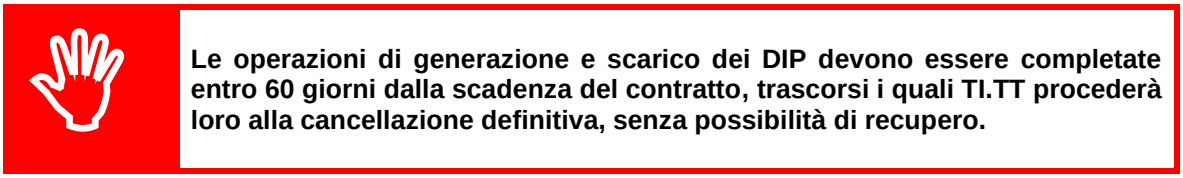
Di seguito viene tracciato l'iter procedurale del *de-provisioning,* cioè le azioni da effettuare alla scadenza dei contratti con i clienti, qualora non vengano rinnovati.

I referenti indicati dal Cliente in fase di attivazione, riceveranno 3 avvisi via email che li invitano a collegarsi alla piattaforma web dedicata alla generazione e allo scarico dei DIP 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 DIP 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: OAIS Open Archival Information System esplicato nella gestione di tre differenti tipologie di pacchetti informativi:

- Il pacchetto di versamento (SIP): 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 (AIP): uno o più SIP sono trasformati in pacchetto di archiviazione per la conservazione. L'AIP ha un insieme completo di informazioni sulla conservazione che si aggiungono al file di metadati.
- Il pacchetto di distribuzione (DIP): il documento digitale o l'insieme dei documenti digitali, corredati da tutti o da parte dei metadati previsti nell'AIP, 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.

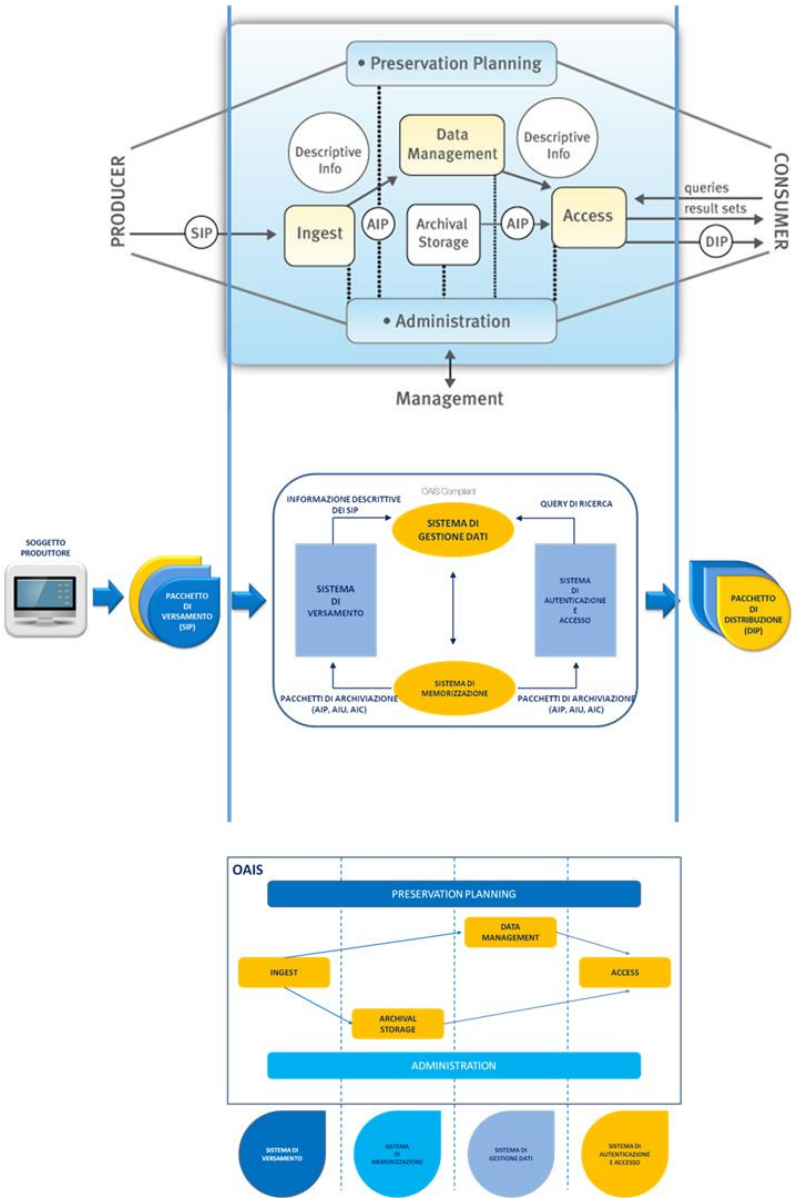


Figura 5 - Sistema di conservazione e conformità al modello OAIS

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 SIP 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 icerche ed è a partire da queste descrizioni che verranno costruiti i *Dissemination Information Package* (DIP) 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 (rapporto di versamento). I documenti informatici, per i quali l'esito della convalida è risultato positivo, possono quindi essere inseriti in un AIP.

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 degli AIP, è in grado di rispondere alla richiesta; l'utente una volta individuato il documento desiderato (o i documenti, o addirittura un intero fascicolo o AIP) potrà inoltrare una richiesta di accesso ai dati, questa genererà la richiesta al modulo di Generazione DIP il quale interagendo sia con il Sistema di Gestione Dati che con il Sistema di Memorizzazione recupererà le informazioni necessarie (AIP e informazioni descrittive) per produrre il Dissemination Information Package (DIP) corrispondente alla richiesta.

Inoltre, il sistema consente anche ricerche trasversali tra tipologie documentali differenti.

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) degli AIP 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:

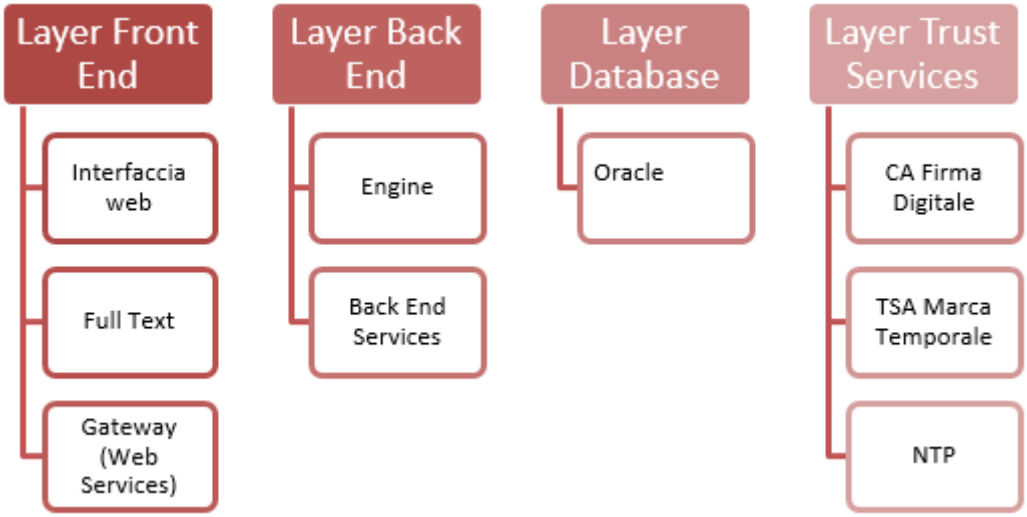


Figura 6 - Componenti core del sistema di conservazione

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 soggette 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. E' 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:

- Android 2.3 o superiore.
- Google Chrome 23 o superiore.
- Internet Explorer 8 o superiore.
- iOS 5 o superiore.
- Mozilla Firefox 17 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 del 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://cons-coll.trusttechnologies.it	Sito di esibizione e upload manuale - Ambiente di Collaudo

https://wscons-coll.trusttechnologies.it	Web Services di upload automatizzato di Collaudo (utilizzabile solo da indirizzi abilitati e da utenti con user e password)
https://conservazione.trusttechnologies.it	Sito di esibizione e upload manuale - Ambiente di Produzione
https://wsconservazione.trusttechnologies.it	Web Services di upload automatizzato di Produzione (utilizzabile solo da indirizzi abilitati e da utenti con user e password)
sftp://consftp.ittelecom.it	Siti di SFTP per upload misto (manuale e/o automatizzato)
https://cons-datisensibili-coll.trusttechnologies.it/asap_arc/	Sito di esibizione - Ambiente di Collaudo (per il trattamento di documenti contenenti dati sensibili)
https://cons-datisensibili.trusttechnologies.it/asap_arc/	Sito di esibizione - Ambiente di Produzione (per il trattamento di documenti contenenti dati sensibili)

Tabella 10 - Servizi Erogati

Torna al sommario

8.2.1.1 Scalabilità sui volumi

La conservazione dei documenti, rispetto ai volumi, è soggetto 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 di conservazione 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.

E' 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:

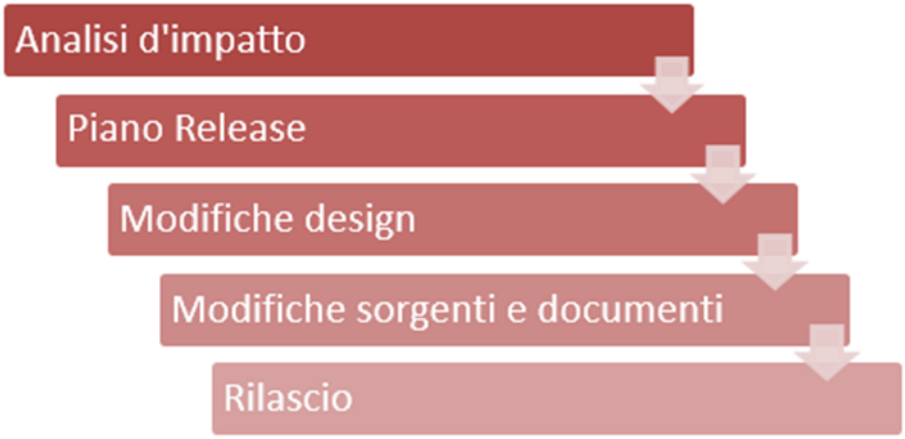


Figura 7 - Processi di sviluppo e manutenzione

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 Trust Technologies 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. (Regole tecniche: art. 8, comma 2 lettera h).

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 SIP.

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
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;

[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.

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 di Conservazione, esclusivamente per la finalità relativa all'erogazione del Servizio. 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 di Conservazione 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 di Conservazione (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 email: 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