



**Città  
metropolitana  
di Milano**

**Manuale per la gestione del protocollo informatico,  
dei flussi documentali e degli archivi  
della Città Metropolitana di Milano**

**Allegato n. 13**

**Manuale di conservazione interno**



Città  
metropolitana  
di Milano

## **Indice generale**

1. Scopo del documento .....	3
2. Definizioni .....	3
3. Normativa di riferimento .....	8
4. Oggetti della conservazione e tipologie documentarie .....	8
5. Struttura organizzativa dell'Ente per i processi di conservazione.....	9
6. Responsabile della conservazione .....	10
7. Il sistema di conservazione.....	11
8. Il processo di preparazione dei pacchetti di versamento (PdV).....	11
9. Il processo di conservazione.....	12
a. Definizione delle modalità di conservazione.....	13
b. Conservazione dei documenti e registrazione delle attività.....	13
c. Manutenzione del sistema di conservazione .....	13
10. Il processo di esibizione e di esportazione .....	13
11. Documentazione.....	14
12. Procedure di monitoraggio e verifica dei sistemi informativi interni all'Ente.....	14
13. Misure di Sicurezza.....	14
14. Allegati .....	15

## 1. Scopo del documento

Il presente Manuale della Conservazione è un documento interno della Città metropolitana di Milano che descrive le responsabilità e l'organizzazione logica e fisica del sistema di conservazione dei documenti digitali in particolare i soggetti che nel tempo ne hanno assunto la responsabilità, i processi attuati nell'ambito della conservazione, gli oggetti e le tipologie documentarie da destinare a conservazione.

Quanto descritto nel Manuale rappresenta dettagliatamente la struttura complessiva del processo di conservazione attivato dall'Ente in relazione al modello organizzativo, secondo quanto specificato al punto 6.

La Città metropolitana di Milano ha stabilito di realizzare i processi di conservazione digitale secondo il modello "in outsourcing", il quale prevede che il servizio di conservazione venga affidato parzialmente o totalmente dal Produttore ad uno o più Conservatori esterni, ossia a soggetti pubblici o privati accreditati ai sensi dell'art. 29 del D.Lgs. 82/2005 - Codice dell'amministrazione digitale.

Per il dettaglio delle tipologie documentarie degli oggetti sottoposti a conservazione l'Ente fa riferimento a quanto concordato e sottoscritto con il Conservatore accreditato, in forma di disciplinare tecnico.

Tale disciplinare è il prodotto di un lavoro congiunto tra i responsabili di riferimento dell'Ente (Produttore) ed il Conservatore accreditato.

## 2. Definizioni

Al fine di rendere esplicite le terminologie impiegate all'interno di questo manuale, si fa riferimento al glossario riportato nell'allegato 1 del D.P.C.M.13 dicembre 2013 sulla conservazione.

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
archivio	complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività
archivio informatico	archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico
area organizzativa omogenea	un insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445
attestazione di conformità delle copie per immagine su	dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico



supporto informatico di un documento analogico	
autenticità	caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico
base di dati	collezione di dati registrati e correlati tra loro
certificatore accreditato	soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, 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
Codice	decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni
codice eseguibile	insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici
conservatore accreditato	soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, dall'Agenzia per l'Italia digitale
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
Coordinatore della Gestione Documentale	responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 nei casi di amministrazioni che abbiano istituito più Aree Organizzative Omogenee
copia analogica del documento informatico	documento analogico avente contenuto identico a quello del documento informatico da cui è tratto
copia di sicurezza	copia di <i>backup</i> degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 delle presenti regole tecniche per il sistema di conservazione
destinatario	identifica il soggetto/sistema al quale il documento informatico è indirizzato
duplicazione dei documenti informatici	produzione di duplicati informatici
esibizione	operazione che consente di visualizzare un documento conservato e di ottenerne copia
estratto per riassunto	documento nel quale si attestano in maniera sintetica ma esaustiva fatti, stati o qualità desunti da dati o documenti in possesso di soggetti pubblici
evidenza informatica	una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica
fascicolo informatico	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



Città  
metropolitana  
di Milano

	Codice.
formato	modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
funzionalità aggiuntive	le ulteriori componenti del sistema di protocollo informatico necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni
Funzionalità interoperative	le componenti del sistema di protocollo informatico finalizzate a rispondere almeno ai requisiti di interconnessione di cui all'articolo 60 del D.P.R. 28 dicembre 2000, n. 445
funzionalità minima	la componente del sistema di protocollo informatico che rispetta i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445
funzione di <i>hash</i>	una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
generazione automatica di documento informatico	formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni
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
immodificabilità	Caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso
impronta	la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di <i>hash</i>
insieme minimo di metadati del documento informatico	complesso dei metadati, la cui struttura è descritta nell'allegato 5 del decreto, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta
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
manuale di gestione	strumento che descrive il sistema di gestione informatica dei documenti di cui all'articolo 5 delle regole tecniche del protocollo informatico ai sensi delle regole tecniche per il protocollo informatico D.P.C.M. 31 ottobre 2000 e successive modificazioni e integrazioni
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 decreto
pacchetto di archiviazione	pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del 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 della sicurezza del sistema di gestione informatica dei documenti	documento, che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi nell'ambito dell'organizzazione di appartenenza
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
piano generale della sicurezza	documento per la pianificazione delle attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza
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
registrazione informatica	insieme delle informazioni risultanti da transazioni informatiche o dalla presentazione in via telematica di dati attraverso moduli o formulari resi disponibili in vario modo all'utente
registro particolare	registro informatico di particolari tipologie di atti o documenti; nell'ambito della pubblica amministrazione è previsto ai sensi dell'articolo 53, comma 5 del D.P.R. 28 dicembre 2000, n. 445
registro di protocollo	registro informatico di atti e documenti in ingresso e in uscita che



Città  
metropolitana  
di Milano

	permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti
repertorio informatico	registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche con cui si formano altri atti e documenti o indici di atti e documenti secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica
responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi	dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione.
responsabile della conservazione	soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 delle regole tecniche del sistema di conservazione
responsabile del trattamento dei dati	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali
responsabile della sicurezza	soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza
riferimento temporale	informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento
Scarto	operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale
sistema di classificazione	strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata
sistema di conservazione	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
Staticità	Caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione
transazione informatica	particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche della base di dati
Testo unico	decreto del Presidente della Repubblica 28 dicembre 2000, n.445, e successive modificazioni
ufficio utente	riferito ad un'area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico
Utente	persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse
versamento agli archivi di stato	operazione con cui il responsabile della conservazione di un organo giudiziario o amministrativo dello Stato effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata



	ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali
--	--

### **3. Normativa di riferimento**

- D.P.R. 28 dicembre 2000 n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
- Il testo unico recepisce e riordina tutta la normativa precedente in tema di documentazione amministrativa ed istituisce e determina le funzioni del Responsabile della Gestione Documentale di un ente pubblico.
- D.Lgs. 7 marzo 2005 n. 82 - Codice dell'amministrazione digitale (CAD)
- Il codice costituisce un corpo organico di disposizioni che presiede all'uso dell'informatica come strumento di comunicazione tra Pubblica Amministrazione e cittadini.
- D.P.C.M. 22 febbraio 2013 - Regole tecniche sulle firme elettroniche
- Il decreto definisce le regole in materia di generazione, apposizione e verifica delle firme elettroniche avanzate e digitali.
- D.P.C.M. 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione
- Il decreto definisce le caratteristiche, gli oggetti, le responsabilità, le modalità di esibizione del contenuto connesse ad un sistema di conservazione.
- D.P.C.M. 3 dicembre 2013 - Regole tecniche sul protocollo informatico
- Il decreto definisce le regole tecniche, i criteri e le specifiche delle informazioni previste nelle operazioni di registrazione e segnatura di protocollo, nonché gli adeguamenti a cui sono sottoposte le Pubbliche Amministrazioni in tema di protocollo informatico.
- D.P.C.M. 13 novembre 2014 - Regole tecniche sul documento informatico
- Il decreto regola la formazione, la copia, la duplicazione, la riproduzione e la validazione temporale dei documenti informatici.
- Regolamento UE 679/2916 - Regolamento generale sulla protezione dei dati personali

### **4. Oggetti della conservazione e tipologie documentarie**

Sono oggetti del sistema di conservazione:

- i documenti informatici e i documenti amministrativi informatici prodotti e acquisiti dall'Ente, con i metadati ad essi associati e descritti nella documentazione sottoscritta tra Ente e Conservatore;
- i fascicoli informatici ovvero le aggregazioni documentali informatiche con i metadati ad essi associati e descritti nella documentazione sottoscritta tra Ente e Conservatore, contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che appartengono al fascicolo o all'aggregazione documentale.

Essi sono trattati dal sistema di conservazione in pacchetti informativi che si distinguono in:

- **pacchetti di versamento;**
- **pacchetti di archiviazione;**
- **pacchetti di distribuzione.**

Le tipologie documentali oggetto di conservazione sono individuate dal Responsabile della gestione documentale in collaborazione con il Responsabile della Conservazione.

Per ogni tipologia documentale sono definite le caratteristiche necessarie e qualificanti all'identificazione e al trattamento dei singoli documenti durante il loro intero ciclo di vita.

L'elenco delle tipologie documentarie che l'Ente invia in conservazione, sono indicate nell'allegato 1 del presente documento.

In caso di variazione o integrazione delle tipologie documentarie in uso, sarà cura del Responsabile della Conservazione dell'ente in accordo con il Responsabile della gestione documentale avviare opportuni contatti con il Conservatore Accreditato al fine di adeguare i flussi informativi.

### **5. Struttura organizzativa dell'Ente per i processi di conservazione**

L'iter procedurale del processo di conservazione viene descritto nel presente capitolo e nei successivi in forma schematica, individuando i ruoli coinvolti, le competenze e le responsabilità necessarie a garantirne il regolare svolgimento.

I ruoli previsti nel processo di conservazione sono i seguenti:

Ruolo	Descrizione
Produttore	Ai sensi dell'art. 6 delle regole tecniche sulla conservazione, 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. Tale figura si identifica con il responsabile della gestione documentale.
Responsabile della gestione documentale	È il soggetto (dirigente o funzionario), responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi (art. 61 D.P.R. 28 Dicembre 2000 n. 445). È anche responsabile della produzione del pacchetto di versamento (art. 6 comma 3 - D.P.C.M. 3 Dicembre 2013 sulla conservazione).
Responsabile della Conservazione	Il Responsabile della Conservazione è il soggetto cui fa capo la responsabilità di verifica del corretto svolgimento del processo di conservazione. Si distingue il responsabile della conservazione interno dell'ente dal responsabile esterno individuato quale Delegato di servizi di Conservazione (Conservatore accreditato).
Delegato di servizi di conservazione	E' il soggetto delegato dal Responsabile della conservazione allo svolgimento di attività correlate ai processi di conservazione a norma dei documenti informatici, le cui mansioni e responsabilità sono chiaramente formalizzate tramite atto amministrativo.
Utente	Ai sensi dell'art. 6 delle regole tecniche sulla conservazione, è la 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.

## 6. Responsabile della conservazione

Il Responsabile della Conservazione definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.

Ai sensi dell'art. 7 delle regole tecniche sulla conservazione, il Responsabile della Conservazione:

- definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente;
- gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
- genera il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
- genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
- effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
- assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
- al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;
- provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
- adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12(*delle regole tecniche*);
- assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
- assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
- provvede, per gli organi giudiziari e amministrativi dello Stato, al versamento dei documenti conservati all'archivio centrale dello Stato e agli archivi di Stato secondo quanto previsto dalle norme vigenti;
- predispone il manuale di conservazione di cui all'art. 8 (*delle regole tecniche*) e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Il Responsabile della conservazione può delegare in tutto o in parte lo svolgimento del processo di conservazione ad uno o più soggetti esterni. La delega è formalizzata esplicitando chiaramente il contenuto della stessa ed in particolare le specifiche funzioni e competenze affidate al delegato. La delega prevede per il soggetto esterno anche la nomina del responsabile del trattamento dei dati personali ai sensi della normativa vigente.

La Città Metropolitana di Milano ha individuato un responsabile interno della conservazione e più responsabili esterni per il servizio di conservazione. Nell'allegato 5 si riportano le informazioni relative ai soggetti esterni delegati allo svolgimento di attività inerenti il processo di conservazione, con la descrizione delle loro funzioni e degli ambiti oggetto della delega stessa.

### **7. Il sistema di conservazione**

Il sistema di conservazione garantisce l'autenticità, l'integrità, l'affidabilità, la leggibilità e la reperibilità degli oggetti conservati dal momento della loro presa in carico dal Produttore, fino all'eventuale scarto indipendentemente dall'evolversi del contesto tecnologico e organizzativo. Il Città metropolitana intende avvalersi di un conservatore accreditato esterno per la conservazione delle tipologie documentarie descritte nell'allegato 1.

I riferimenti del conservatore accreditato, incaricato dall'Ente per lo svolgimento delle attività di conservazione, sono indicati nell'allegato 6.

### **8. Il processo di preparazione dei pacchetti di versamento (PdV)**

La produzione dei pacchetti di versamento sarà effettuata mediante il sistema di protocollo informatico in essere presso l'Ente. I riferimenti della software house sono riportati nell'allegato 5.

Il Produttore e il Responsabile della conservazione definiscono le modalità di trasmissione dei documenti al sistema di conservazione.

## 9. Il processo di conservazione

I documenti informatici trattati dall'Ente e formati ai sensi dell'art. 3 c. 1 del D.P.C.M. 13 novembre 2014 possono, secondo necessità, essere memorizzati in un sistema di gestione informatica dei documenti idoneo a garantire le caratteristiche di immutabilità e integrità degli stessi.

Nell'allegato 1 sono riportate le singole tipologie documentarie ed il sistema nel quale sono conservate. Il processo di versamento nel sistema di conservazione, nel dettaglio, ai sensi dell'articolo 9 delle Regole tecniche, prevede:

- l'acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico;
- la verifica che il pacchetto di versamento e gli oggetti contenuti siano coerenti con le modalità previste dal manuale di conservazione;
- il rifiuto del pacchetto di versamento, nel caso in cui le verifiche di cui alla lettera b) abbiano evidenziato delle anomalie;
- la generazione, anche in modo automatico, del rapporto di versamento relativo ad uno o più pacchetti di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo universale coordinato (UTC), e una o più impronte, calcolate sull'intero contenuto del pacchetto di versamento, secondo le modalità descritte nel manuale di conservazione del conservatore accreditato;
- l'eventuale sottoscrizione del rapporto di versamento con la firma digitale o firma elettronica qualificata apposta dal delegato del servizio di conservazione, ove prevista nel manuale di conservazione;
- la preparazione, la sottoscrizione con firma digitale o firma elettronica qualificata del delegato del servizio di conservazione e la gestione del pacchetto di archiviazione sulla base delle specifiche della struttura dati contenute nell'allegato 4 e secondo le modalità riportate nel manuale della conservazione del conservatore accreditato;
- la preparazione e la sottoscrizione con firma digitale o firma elettronica qualificata, ove prevista nel manuale di conservazione, del pacchetto di distribuzione ai fini dell'esibizione richiesta dall'utente;
- ai fini della interoperabilità tra sistemi di conservazione, la produzione dei pacchetti di distribuzione coincidenti con i pacchetti di archiviazione;
- la produzione di duplicati informatici o di copie informatiche effettuati su richiesta degli utenti in conformità a quanto previsto dalle regole tecniche in materia di formazione del documento informatico;
- la produzione delle copie informatiche al fine di adeguare il formato di cui all'art. 11, in conformità a quanto previsto dalle regole tecniche in materia di formazione del documento informatico;
- lo scarto del pacchetto di archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dalla norma, dandone informativa al produttore, previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo rilasciata al produttore secondo quanto previsto dalla normativa vigente in materia.

L'iter procedurale del processo di conservazione viene di seguito descritto in forma schematica, individuando i ruoli coinvolti, le competenze e le responsabilità necessarie a garantirne il regolare svolgimento.

Si rimanda agli allegati dal 5 al 9 per i dettagli organizzativi e tecnologici relativi ai processi di conservazione specifici per la varie categorie documentali.

### ***a. Definizione delle modalità di conservazione***

Il Produttore e il Responsabile della conservazione:

- individuano le tipologie di documenti che dovranno essere trattate dal sistema di conservazione;
- definiscono i set di metadati per ciascuna tipologia documentale;
- stabiliscono la periodicità di invio dei documenti in conservazione;
- determinano i criteri di formazione dei volumi di conservazione;
- fissano gli specifici tempi di conservazione.

Il Responsabile della conservazione, inoltre, verifica le caratteristiche e i requisiti del sistema di conservazione in funzione delle tipologie dei documenti da conservare e della normativa di riferimento.

### ***b. Conservazione dei documenti e registrazione delle attività***

Il Responsabile della conservazione o il soggetto specificamente delegato conclude la procedura di conservazione dei documenti firmandoli digitalmente e associando una marca temporale al file di chiusura, contenente le impronte dei documenti informatici da conservare.

Il Responsabile della conservazione o il soggetto specificamente delegato tiene traccia delle attività inerenti la conservazione dei documenti, memorizzando, al termine di ogni procedura i seguenti dati:

- codice univoco del volume di documenti;
- tipologia di documento archiviato;
- estremi identificativi del lotto di documenti conservati;
- estremi identificativi del responsabile della conservazione;
- estremi identificativi delle persone eventualmente delegate dal responsabile della conservazione.

### ***c. Manutenzione del sistema di conservazione***

Il Responsabile della conservazione o il soggetto specificamente delegato garantisce la disponibilità dei documenti conservati, garantendo:

- l'attuazione di tutte le azioni necessarie per garantire la piena funzionalità del sistema di conservazione;
- il corretto funzionamento dei sistemi e dei supporti di memorizzazione;
- il mantenimento dei software e dei dispositivi hardware necessari alla consultazione dei supporti di memorizzazione;
- lo svolgimento di tutte le attività necessarie per impedire l'obsolescenza dei formati in uso.

## ***10. Il processo di esibizione e di esportazione***

La procedura di esibizione è anch'essa un'applicazione attivata dal Responsabile della conservazione o un suo delegato.

La procedura di esibizione del documento permette, a partire da una funzione di ricerca nel sistema di conservazione, di estrarre dal sistema stesso un documento (o un insieme di documenti), di cui sia completata la procedura di conservazione.

La procedura si articola sinteticamente in:

- ricerca

- estrazione
- esibizione vera e propria

La fase di ricerca si compie nella composizione di un criterio di ricerca tramite il quale è individuato, nel catalogo, il flusso cui il documento appartiene.

La fase di estrazione ricava, dal flusso estratto dall'archivio, lo specifico documento/record di interesse.

Tale procedura di esibizione deve permettere la leggibilità in qualunque momento del documento ricercato presso il sistema di conservazione e deve poter essere disponibile (eventualmente su richiesta) su supporto cartaceo.

L'accesso alla documentazione è regolata e garantita attraverso un sistema di gestione delle autorizzazioni e credenziali, che permetta l'accesso al sistema di conservazione solo ed esclusivamente alle persone autorizzate, mediante gli adeguati profili.

Per quanto riguarda la descrizione tecnologica dettagliata, delle modalità di esibizione e/o esportazione dei documenti, si rimanda alla documentazione tecnica del Conservatore Accreditato a cui è stato affidato il servizio di conservazione.

### **11. Documentazione**

In base a quanto indicato nell'allegato 4, si procederà all'aggiornamento delle informazioni contenute nel presente Manuale.

È compito dei soggetti nominati vigilare sullo stato di aggiornamento della documentazione e procedere all'aggiornamento con cadenza almeno semestrale.

Il responsabile della conservazione procede a comunicare al Conservatore accreditato scelto, eventuali variazioni relative alle tipologie documentarie oggetto di conservazione.

### **12. Procedure di monitoraggio e verifica dei sistemi informativi interni all'Ente**

La Città metropolitana di Milano, nell'ambito della conservazione, gestisce e regola gli aspetti inerenti alla sicurezza dei sistemi informativi dell'Ente, all'interno dei quali vengono prodotti e gestiti i documenti informatici.

Si riporta di seguito il contesto normativo di riferimento:

**Amministratori di sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008)**

Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008

**Regolamento Generale sulla Protezione dei Dati Personali**  
(Regolamento UE 679/2016)

### **13. Misure di Sicurezza**

La Città metropolitana di Milano verifica che il conservatore scelto sia tra i soggetti accreditati da AGID, secondo le specifiche norme e circolari di riferimento (all'art. 44-bis del D.lgs. 7 Marzo 2005 n. 82, DPCM 3 Dicembre 2013, Circolare AGID n. 65 10 Aprile 2014), e che possieda quindi i requisiti previsti per la conservazione dei documenti informatici.

#### **14. Allegati**

- Allegato 1 - Elenco delle tipologie documentarie sottoposte a conservazione
- Allegato 2 - Fascicolo documentale
- Allegato 3 - Soggetti esterni incaricati che intercorrono nel processo di conservazione
- Allegato 4 - Responsabile della Conservazione interno all'Ente
- Allegato 5 - Manuale di conservazione Telecom Italia Trust Technologies S.r.l.
- Allegato 6 - Descrizione del servizio TRUST LEGAL SPACE Telecom Italia Trust Technologies S.r.l.
- Allegato 7 - Manuale del versamento in modalità SFTP Telecom Italia Trust Technologies S.r.l.
- Allegato 8 - Conservazione a Norma Manuale Utente Telecom Italia Trust Technologies S.r.l.
- Allegato 9 - Manuale di conservazione Unimatica S.p.A.

## ALLEGATO 1

Elenco delle tipologie documentarie sottoposte a conservazione( Fase di attuazione operativa)

Tipologia documentale	Conservatore	Periodicità di invio in conservazione	Note
Registro giornaliero di protocollo	Telecom Italia Trust Technologies S.r.l.	giornaliera	
Fattura elettronica attiva	Telecom Italia Trust Technologies S.r.l.	mensile	
Fattura elettronica passiva	Telecom Italia Trust Technologies S.r.l.	mensile	
Contratto	Telecom Italia Trust Technologies S.r.l.	mensile	
Atto amministrativo	Telecom Italia Trust Technologies S.r.l.	mensile	Atti dirigenziali Atti del Sindaco metropolitano Delibere del Consiglio metropolitano Delibere della Conferenza metropolitana
Documento informatico	Telecom Italia Trust Technologies S.r.l.		
Documento generico	Telecom Italia Trust Technologies S.r.l.		
Ordinativo di pagamento e incasso (Mandati di pagamento e Reversali d'incasso)	Unimatica S.p.A.	giornaliera	

## **ALLEGATO 2**

Fascicolo informatico o aggregazione documentale informatica, informazioni minime (da implementare)

<b>Informazione</b>	<b>Definizione</b>
<b>Identificativo</b>	Identificativo univoco e persistente è una sequenza di caratteri alfanumerici associata in modo univoco e permanente al fascicolo o aggregazione documentale informatica in modo da consentire l'identificazione.
<b>Amministrazione Titolare</b>	Amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo
<b>Amministrazioni partecipanti</b>	Amministrazioni che partecipano all'iter del procedimento
<b>Responsabile del procedimento</b>	Responsabile del procedimento
<b>Oggetto</b>	Oggetto, metadato funzionale a riassumere brevemente il contenuto del documento o comunque a chiarirne la natura.
<b>Documento</b>	Elenco degli identificativi dei documenti contenuti nel fascicolo che ne consentono la reperibilità

### ALLEGATO 3

Soggetti esterni incaricati che intercorrono nel processo di conservazione

Nome Incaricato	Ruolo	Compito
<b>Telecom Italia Trust Technologies S.r.l.</b> (TI.TT) S. R.148 Pontina, km. 29,100 00071 - Pomezia (RM) P.IVA 04599340967	Conservatore 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)	Eroga il servizio di conservazione digitale
<b>UNIMATICA S.p.A</b> Via Cristoforo Colombo, 21 - 40131 Bologna P.IVA 02098391200	Conservatore 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)	Eroga il servizio di conservazione digitale degli ordinativi di pagamento e incasso nell'ambito dell'affidamento del servizio di tesoreria
<b>NTT DATA Italia S.p.A</b> Viale Cassala 14/a - 20143 Milano P.IVA n. 07988320011	Produttore sistema di protocollo informatico e gestione documentale DocsPA	Garantire il buon funzionamento del software e l'aggiornamento delle funzioni dello stesso, manutenzione evolutiva e correttiva.

#### **ALLEGATO 4**

Responsabile della Conservazione interno all'Ente

Periodo	Soggetto	Qualifica	Estremi atto di nomina
Dal 2017 ad oggi	Novellini Domenico	Responsabile Servizio Intranet, protezione dati e progetti innovativi	Decreto del Sindaco metropolitano R.G. n. 156/2017

# 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: <ol style="list-style-type: none"> <li>1. Cap. 1 - Scopo del documento: precisazione relative alle modalità di commercializzazione dei servizi, degli aspetti contrattuali e dei ruoli;</li> <li>2. Par. 3.1 - Normativa di riferimento: Revisione e integrazione delle fonti normative;</li> <li>3. Cap. 4 - Ruoli e responsabilità: sintesi e chiarimenti sui ruoli; modifica del Responsabile del servizio di Conservazione;</li> <li>4. Cap. 5 - Struttura organizzativa per il SERVIZIO : precisazioni in merito alle nomine per il trattamento dei dati e sull'organizzazione;</li> <li>5. Cap. 6 - Oggetti sottoposti a conservazione: precisazioni in merito alle modalità di conservazione</li> <li>6. Cap. 7 - Il processo di conservazione: precisazioni e miglioramento della descrizione del processo.</li> <li>7. Par. 7.1- Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico: migliorata la rappresentazione delle modalità</li> <li>8. Par. 7.2 - Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti: migliorata la descrizione delle verifiche effettuate</li> <li>9. Par. 7.6 - Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione.: Migliorata la descrizione delle attività effettuate</li> <li>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</li> <li>11. Par. 7.9.1 - Deprovisioning del SERVIZIO: Precisazione sui termini dell'attività e sugli obblighi di accesso</li> <li>12. Par. 8.1.1 - Sistema di versamento (SV).e Par. 8.1.4 - Sistema di accesso: Eliminate alcune tabelle di dettaglio ridondanti</li> <li>13. Par. 8.4 - Procedure di gestione e di evoluzione: Eliminazione di alcune informazioni ridondanti</li> <li>14. Per. 9.3 - SLA e soluzioni adottate in caso di anomalie: Ridefinizione ed aggiornamento degli SLA</li> </ol>	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: <ol style="list-style-type: none"> <li>1. Cap. 1 - Scopo del documento: Aggiornamento della qualifica di Conservatore Accreditato; Riferimenti del Conservatore</li> <li>2. Par.2.2- Acronimi: Inserimento acronimi per nuovi formati trattati;</li> <li>3. Par. 3.1 - Normativa di riferimento: Inserimento riferimento alla normativa GDPR (Regolamento UE 2016/679);</li> <li>4. Cap. 4 - Ruoli e responsabilità: Aggiornamento ruoli (Responsabile sicurezza e Responsabile Trattamento Dati);</li> <li>5. Par. 6.1 - Oggetti conservati: inserimento nuovi formati ;</li> <li>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;</li> <li>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;</li> <li>8. Par. 8.2 - Componenti tecnologiche: aggiornamento delle informazioni relative ad elementi infrastrutturali</li> </ol>	25/05/2018

	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
06	<ol style="list-style-type: none"><li>1. Aggiornamento dati identificativi (par. 1.1) e struttura organizzativa (par. 1.2) del Conservatore</li><li>2. Correzione di refusi e riferimenti nel testo</li><li>3. Modifica definizione di 'sicurezza' (cap. 2)</li><li>4. Aggiornamento della tabella n. Tabella 9 - Formati ammessi per la conservazione</li><li>5. Revisione terminologia par. 7.9</li></ol>	08/11/2018

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

## Indice degli argomenti

<b>1</b>	<b>Scopo del documento .....</b>	<b>6</b>
1.1	Dati identificativi del conservatore .....	7
1.2	Struttura organizzativa del conservatore .....	8
<b>2</b>	<b>Terminologia (Glossario, Acronimi) .....</b>	<b>8</b>
2.1	Glossario.....	8
2.2	Acronimi.....	13
<b>3</b>	<b>Normativa e standard di riferimento .....</b>	<b>14</b>
3.1	Normativa di riferimento .....	14
3.2	Standard di riferimento .....	14
<b>4</b>	<b>Ruoli e responsabilità .....</b>	<b>15</b>
<b>5</b>	<b>Struttura organizzativa per il SERVIZIO .....</b>	<b>19</b>
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
<b>6</b>	<b>Oggetti sottoposti a conservazione .....</b>	<b>22</b>
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
<b>7</b>	<b>Il processo di conservazione .....</b>	<b>30</b>
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
<b>8</b>	<b>Il sistema di conservazione.....</b>	<b>36</b>
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
<b>9</b>	<b>Monitoraggi e controlli.....</b>	<b>45</b>
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
<b>10</b>	<b>Assistenza al Cliente.....</b>	<b>47</b>
<b>11</b>	<b>Protezione dei dati personali .....</b>	<b>48</b>

## 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](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 Leopoldo Genovesi (responsabile ad interim della funzione Operations).

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	<a href="http://www.trusttechnologies.it">www.trusttechnologies.it</a>
Indirizzo Pec	TI.TT@tpec.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:

- **Marketing & Sales** (attività di commercializzazione del portafoglio di offerta) a sua volta articolata in Service & Solution Sales (commercializzazione dei servizi e delle soluzioni a portafoglio) e Customized Sales (commercializzazione di servizi personalizzati);
- **Business Development** (sviluppo e 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 (conduzione operativa dei sistemi, provisioning, Service Management).

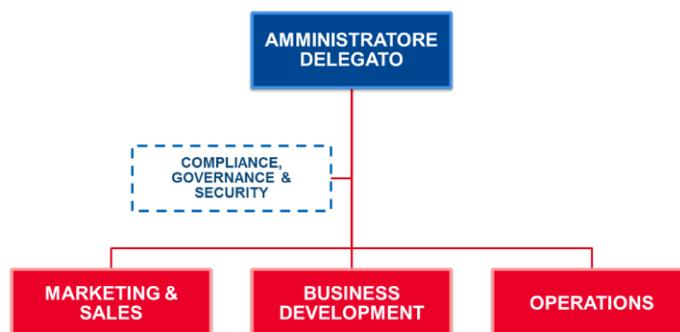


Figura 1 - Organigramma

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
<b>accesso</b>	Operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici.
<b>accreditamento</b>	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.
<b>affidabilità</b>	Caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico.
<b>aggregazione documentale informatica</b>	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.
<b>allegato</b>	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.

<b>annesso</b>	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.
<b>apertura</b>	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.
<b>application server</b>	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).
<b>archivio</b>	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.
<b>attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico</b>	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.
<b>autenticità</b>	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.
<b>certificatore accreditato</b>	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.
<b>ciclo di gestione</b>	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.
<b>classificazione</b>	Attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati.
<b>cluster</b>	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.
<b>Codice</b>	Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni.
<b>comunità di riferimento</b>	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].
<b>Conservatore accreditato</b>	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.
<b>conservazione</b>	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.
<b>contenuto informativo</b>	Insieme delle informazioni che costituisce l'obiettivo originario della conservazione. È composto dall'Oggetto-dati e dalle Informazioni di rappresentazione [da OAIS].
<b>data center</b>	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.
<b>diffusione</b>	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.
<b>disaster recovery</b>	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.
<b>esibizione</b>	Operazione che consente di visualizzare un documento conservato e di ottenerne copia.
<b>evidenza informatica</b>	Sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.
<b>fascicolo informatico</b>	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.
<b>file di indice</b>	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.
<b>formato</b>	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
<b>funzionalità</b>	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.
<b>funzione di hash</b>	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.
<b>identificativo univoco</b>	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.
<b>impronta</b>	Sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash.
<b>informazioni descrittive</b>	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.
<b>informazioni sulla conservazione (PDI)</b>	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].
<b>informazioni sulla rappresentazione</b>	Informazioni che associano un Oggetto-dati a concetti più significativi.
<b>informazioni sull'impacchettamento</b>	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.
<b>integrità</b>	Insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato.
<b>interoperabilità</b>	Capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi.
<b>leggibilità</b>	Insieme delle caratteristiche in base alle quali le informazioni contenute nei

	documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti.
<b>log di sistema</b>	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.
<b>manuale di conservazione</b>	Strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 delle regole tecniche del sistema di conservazione.
<b>marca temporale</b>	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.
<b>memorizzazione</b>	Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici.
<b>metadati</b>	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.
<b>pacchetto di archiviazione</b>	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.
<b>pacchetto di distribuzione</b>	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta.
<b>pacchetto di versamento</b>	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione.
<b>pacchetto informativo</b>	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.
<b>piano della sicurezza del sistema di conservazione</b>	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.
<b>piano di conservazione</b>	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.
<b>portabilità</b>	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.
<b>presa in carico</b>	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione.
<b>processo di conservazione</b>	Insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 10 delle regole tecniche del sistema di conservazione.
<b>produttore</b>	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.
<b>rapporto di versamento</b>	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema

	di conservazione dei pacchetti di versamento inviati dal produttore.
<b>responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi</b>	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.
<b>responsabile della conservazione</b>	Soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 delle regole tecniche del sistema di conservazione.
<b>responsabile del trattamento dei dati</b>	Persona fisica, persona giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.
<b>responsabile della sicurezza</b>	Soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza.
<b>referimento temporale</b>	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.
<b>scarto</b>	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale.
<b>serie</b>	Unità Archivistiche o Unità Documentarie ordinate secondo un sistema di classificazione o conservati insieme perché: <ul style="list-style-type: none"> <li>- sono il risultato di un medesimo processo di sedimentazione o archiviazione o di una medesima attività;</li> <li>- appartengono ad una specifica tipologia documentaria;</li> <li>- a ragione di qualche altra relazione derivante dalle modalità della loro produzione, acquisizione o uso.</li> </ul> (fonte: ISAD).
<b>sicurezza</b>	La sicurezza di un formato dipende da due elementi: il grado di modificabilità del contenuto del file e la capacità di essere immune dall'inserimento di codice maligno. Nel sistema di conservazione a norma di TI.TT i pacchetti di versamento vengono sottoposti a scansione antivirus con verifica dei file e archivi compressi multilivello. Ogni file compresso è quindi controllato anche se si tratta di compressioni ripetute (tecnica utilizzata per evitare che l'antivirus controlli i file di un archivio compresso). Gli antivirus utilizzati sono costantemente aggiornati. L'invio dei file, inoltre, avviene attraverso linee controllate da firewall e Intrusion detector.
<b>sistema di classificazione</b>	Strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata.
<b>sistema di conservazione</b>	Sistema di conservazione dei documenti informatici di cui all'articolo 44 del Codice.
<b>sistema di gestione informatica dei documenti</b>	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.
<b>Soggetto produttore o Titolare</b>	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.
<b>supporto allo sviluppo</b>	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.).
<b>Testo unico</b>	Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni.
<b>Unità archivistica</b>	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].
<b>Unità documentaria:</b>	Aggregato logico costituito da uno più Documenti che sono considerati come un tutto unico. Costituisce l'unità elementare in cui è composto l'archivio.
<b>Versamento:</b>	Azione di trasferimento di SIP dal Produttore al Sistema di conservazione.
<b>utente</b>	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
<b>AgID:</b>	Agenzia per l'Italia digitale
<b>AIP:</b>	Archival Information package (Pacchetto di archiviazione)
<b>CA:</b>	Certification Authority
<b>CAD:</b>	Codice dell'amministrazione digitale
<b>CRL:</b>	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
<b>DICOM</b>	Digital Imaging and Communications in Medicine
<b>DIP:</b>	Dissemination Information Package (Pacchetto di distribuzione)
<b>HL7</b>	Health Level 7
<b>HSM:</b>	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
<b>ISO:</b>	International organization for Standardization
<b>IR:</b>	Informazioni sulla rappresentazione
<b>IRse:</b>	Informazioni sulla rappresentazione semantiche
<b>IRSI:</b>	Informazioni sulla rappresentazione sintattiche
<b>OAIS:</b>	Open archival information system.
<b>PDI:</b>	Preservation description information (informazioni sulla conservazione).
<b>PEC:</b>	Posta Elettronica Certificata.
<b>SIP:</b>	Submission Information Package (Pacchetto di versamento).
<b>SMTP:</b>	Simple Mail Transfer Protocol (SMTP) è il protocollo standard per la trasmissione via internet di e-mail.
<b>TSA:</b>	Time Stamping Authority, è il soggetto che eroga la marca temporale.
<b>UNI SinCRO:</b>	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, comma 3, 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 sono descritte nel presente Manuale di Conservazione e nella documentazione richiamata al capitolo 1.**

**Per ciascun Cliente, TI.TT 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 a TI.TT. Lo stesso avverrà per ogni successiva modifica o integrazione della scheda.**

[Torna al sommario](#)

## 4 Ruoli e responsabilità



**Il SERVIZIO descritto nel presente Manuale di Conservazione è strutturato in modo tale da poter garantire l'esecuzione delle attività affidate a TI.TT, in qualità di 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.TT 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.TT, 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
<b>Responsabile del servizio di conservazione</b>	<p>Il Responsabile del servizio di conservazione espleta le seguenti funzioni:</p> <ul style="list-style-type: none"> <li>- Definisce e attua politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione;</li> <li>- Definisce le caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente;</li> <li>- Verifica la corretta erogazione del servizio di conservazione all'ente produttore;</li> <li>- 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)</li> </ul> <p>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 e dell'erogazione del servizio ai soggetti produttori. Il responsabile del servizio di conservazione genera il rapporto di versamento.</p> <p>Il responsabile del servizio di conservazione appone la firma digitale e la marca temporale sul pacchetto di archiviazione. Il</p>	<p><b>Giantommaso Lafavia</b></p>

	<p>responsabile del servizio di conservazione garantisce l'esibizione del pacchetto di distribuzione qualora la comunità di riferimento lo richiedesse.</p> <p>Il responsabile del servizio di conservazione sottoscrive i pacchetti di distribuzione.</p>	
<b>Responsabile della sicurezza dei sistemi per la conservazione</b>	<p>Il Responsabile della sicurezza dei sistemi per la conservazione espleta le seguenti attività</p> <ul style="list-style-type: none"> <li>- Rispetta e monitora i requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza;</li> <li>- Segnala eventuali difformità al Responsabile del servizio di conservazione e individua e pianifica le necessarie azioni correttive.</li> </ul>	<p><b>Massimiliano Medros</b></p>
<b>Responsabile della funzione archivistica di conservazione</b>	<p>Il Responsabile della funzione archivistica di conservazione espleta le seguenti funzioni:</p> <ul style="list-style-type: none"> <li>- 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;</li> <li>- Definisce il set di metadati di conservazione dei documenti e dei fascicoli informatici; questa attività sarà espletata con il supporto del soggetto produttore</li> <li>- Monitora il processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione;</li> <li>- 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;</li> <li>- Supporta il responsabile del servizio di conservazione nell'acquisizione del pacchetto di versamento ed è presente nelle verifiche e controlli dell'autorità di competenza.</li> <li>- Si occupa dell'aggiornamento alle normative e della formazione dell'organizzazione.</li> </ul> <p>Il responsabile della funzione archivistica di conservazione opera a stretto contatto con il responsabile del servizio di conservazione.</p> <p>Le principali mansioni affidate al responsabile della funzione archivistica di conservazione sono di seguito riportate:</p> <ul style="list-style-type: none"> <li>- Gestisce le modalità di trasferimento, esibizione e fruizione dei documenti informatici</li> <li>- Definisce le informazioni sulla rappresentazione e sulle informazioni della conservazione. Questa attività sarà espletata con il supporto del soggetto produttore.</li> <li>- Coadiuvare il responsabile del servizio di conservazione nelle procedure di chiusura del pacchetto di archiviazione</li> <li>- Si interfaccia con il soggetto produttore qualora sia necessario procedere allo scarto delle tipologie documentarie.</li> <li>- Forma e aggiornare la struttura organizzativa coinvolta nel processo di conservazione.</li> </ul>	<p><b>Stefania Rampazzo</b> <b>(contratto di consulenza della durata di tre anni, rinnovabile)</b></p>

<b>Responsabile del trattamento dei dati personali</b>	Il Responsabile del trattamento dei dati personali: <ul style="list-style-type: none"> <li>- Garantisce il rispetto delle vigenti disposizioni in materia di trattamento dei dati personali;</li> <li>- 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;</li> <li>- Coordina l'attivazione del servizio di conservazione a seguito della sottoscrizione di un contratto;</li> <li>- Coordina le attività di chiusura del servizio al termine del contratto.</li> </ul>	<b>Giantommaso Lafavia</b>
<b>Responsabile dei sistemi informativi per la conservazione</b>	Il Responsabile dei sistemi informativi per la conservazione espleta le seguenti attività <ul style="list-style-type: none"> <li>- Gestisce l'esercizio delle componenti hardware e software del sistema di conservazione;</li> <li>- Monitora il mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore;</li> <li>- Segnala eventuali difformità degli SLA al Responsabile del servizio di conservazione e individua e pianifica le necessarie azioni correttive;</li> <li>- Pianifica lo sviluppo delle infrastrutture tecnologiche del sistema di conservazione;</li> <li>- Controlla e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.</li> </ul>	<b>Francesca Mazzanti</b>
<b>Responsabile dello sviluppo e della manutenzione del sistema di conservazione</b>	Il Responsabile dello sviluppo e della manutenzione del sistema di conservazione espleta le seguenti attività <ul style="list-style-type: none"> <li>- Coordina lo sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione;</li> <li>- Pianifica e monitora progetti di sviluppo del sistema di conservazione;</li> <li>- Monitora gli SLA relativi alla manutenzione del sistema di conservazione;</li> <li>- 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;</li> <li>- Gestisce inoltre lo sviluppo di siti web e portali connessi al servizio di conservazione;</li> <li>- Coordina le attività di change management.</li> </ul>	<b>Marco Donatone</b>

**Tabella 6 - Ruoli e Responsabilità**
**Responsabile del servizio di conservazione**

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

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

**Il Responsabile della sicurezza dei sistemi per la conservazione**

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

### **Il Responsabile della funzione archivistica di conservazione**

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'attuale Responsabile.

### **Il Responsabile dei sistemi informativi per la conservazione**

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

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

### **Il Responsabile dello sviluppo e della manutenzione del sistema di conservazione**

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

[Torna al sommario](#)

## **5 Struttura organizzativa per il SERVIZIO**

### **5.1 Organigramma**

TI.TT si configura come conservatore che svolge attività di conservazione, che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia. Secondo quanto stabilito 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'articolazione organizzativa preposta all'erogazione del SERVIZIO:

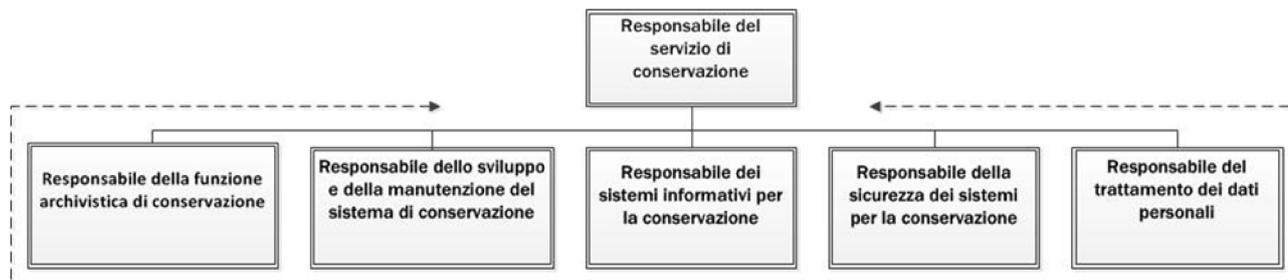


Figura 2 - Articolazione organizzativa per l'erogazione del SERVIZIO

[Torna al sommario](#)

## 5.2 Strutture organizzative

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

È individuato il Responsabile del Servizio di Conservazione e non sono previste attività delegate a terzi.

(rif. art. 6 del DPCM 3 dicembre 2013).

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

[Torna al sommario](#)

### 5.2.1 Attività relative al contratto con i Soggetti Produttori

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

Il perfezionamento del contratto consente l'attivazione del SERVIZIO, 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 di 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	Infrastructure & Document Management
Acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento.	Responsabile del servizio di conservazione, supporto del Responsabile della funzione archivistica di conservazione	Infrastructure & Document Management
Preparazione e gestione del pacchetto di archiviazione.	Responsabile del servizio di conservazione	Infrastructure & Document Management
Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta.	Responsabile del servizio di conservazione	Infrastructure & Document Management
Scarto dei pacchetti di archiviazione.	Responsabile del servizio di conservazione, supporto del Responsabile della funzione archivistica di conservazione, previa autorizzazione da parte del soggetto produttore	Infrastructure & Document Management
Chiusura del servizio di conservazione (al termine di un contratto).	Responsabile del servizio di conservazione Coordinatore attività di delivery	Infrastructure & Document Management

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

[Torna al sommario](#)

## 5.2.2 Attività relative alla gestione dei sistemi informativi

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

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

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

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

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

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

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

[Torna al sommario](#)

## 6 Oggetti sottoposti a conservazione

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

[Torna al sommario](#)

### 6.1 Oggetti conservati

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

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 parametrizzazioni 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 <sup>1</sup>	Adobe Systems <a href="http://www.adobe.com/">http://www.adobe.com/</a>	.pdf	application/pdf	Si	ISO 32000-1 (PDF); ISO 19005-1:2005 (vers. PDF 1.4); ISO 19005-2:2011 (vers. PDF 1.7)
TIFF	Aldus Corporation (acquisita Adobe)	.tif	image/tiff	No	ISO 12639 (TIFF/IT); ISO 12234 (TIFF/EP)
JPG e JPEG 2000	Joint Photographic Experts Group	.jpg, .jpeg, .jp2 (JPEG 2000)	image/jpeg	Si	ISO/IEC 10918:1 (JPG); ISO/IEC 15444-1 (JPEG 2000)
Office Open XML (OOXML)	Microsoft	.docx, .xlsx, .pptx	application/vnd.openxmlformats-officedocument.*	Si	ISO/IEC DIS 29500:2008
ODF Open Document Format	OASIS	.ods, .odp, .odg, .odb	application/vnd.oasis.opendocument.text	Si	ISO/IEC 26300:2006; UNI CEI ISO/IEC 26300
XML Extensible Markup Language	W3C	.xml	application/xml text/xml	Si	
TXT	-	.txt	ASCII, UTF-8, UNICODE	Si	ISO 646, RFC 3629, ISO/IEC 10646
PEC ed EMAIL	-	.eml	message/RFC822	No	RFC 2822/MIME
HL7	Health Level 7	.pdf; .cda;	application/(.pdf;	SI	HL7 Implementation Guide for CDA® Release 2 -

<sup>1</sup> Il PDF/A è stato sviluppato con l'obiettivo specifico di rendere possibile la conservazione.

		.p7m;	p7m; cda)		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.TTII. Il produttore può scegliere, al momento dell'attivazione del servizio fra le opzioni disponibili per il trasferimento dei pacchetti di versamento descritte secondo le modalità e protocolli riportati nel Documento di Descrizione del Servizio.

In questo sistema di conservazione possono essere trasferiti pacchetti di versamento conformi a quanto previsto dalle 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 trasferito 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:

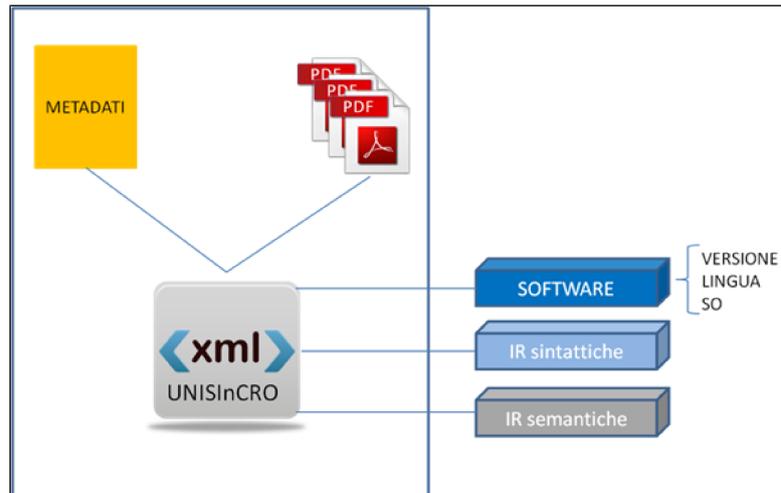


Figura 3 - Pacchetto di archiviazione (AIP)

### 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'obiettivo originario della conservazione e dalle relative informazioni sulla conservazione. In un contesto OAIS il pacchetto di archiviazione deve 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.

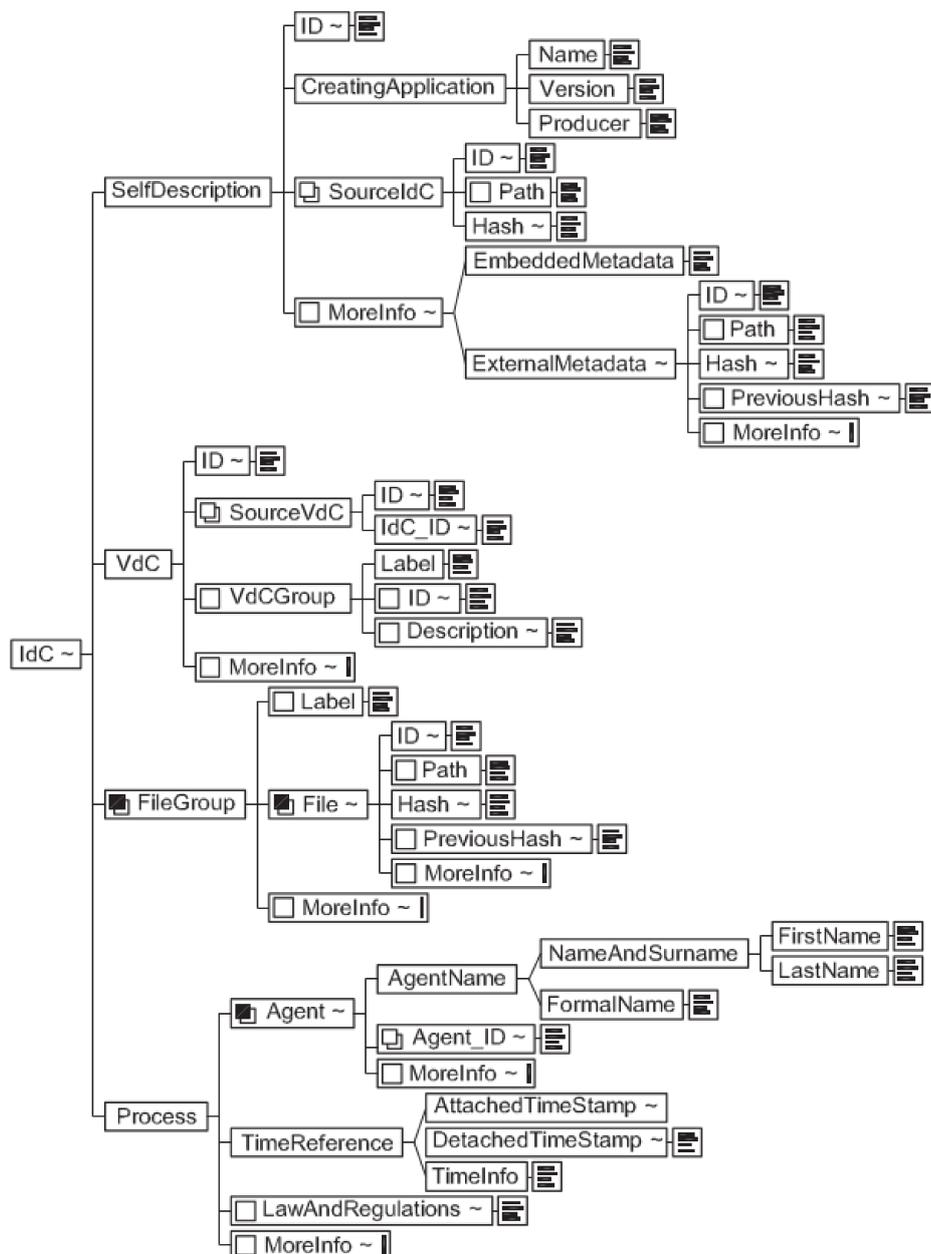


Figura 4: struttura dell'indice del pacchetto di archiviazione

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="MetadataItem">
<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 <sup>2</sup> (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 Transfer Protocol) criptato punto-punto con la piattaforma del cliente e autorizzato dai firewall e dall'intero *layer* di sicurezza. Il Cliente ottiene le credenziali di autenticazione e può accedere dalla piattaforma tramite un set predefinito di IP statici. In modalità automatica si può quindi procedere all'upload dei pacchetti di versamento nella folder SFTP dedicata, costituiti da un file di indice e di una cartella contenente i documenti da porre in conservazione
- 3) **Web Services (A2A):** con credenziali personalizzate e accesso consentito dal *layer* di sicurezza, il Cliente può raggiungere i *web services* di conservazione esposti da TI.TT. La modalità è detta Application To Application (A2A). L'applicazione del Cliente, dopo l'autenticazione, potrà utilizzare le chiamate per eseguire tutte le operazioni previste dalla conservazione.
- 4) **DICOM:** consente l'acquisizione di immagini DICOM utilizzando procedure standard Storage/Storage Commitment e Query/Retrieve DICOM 3.0;
- 5) **HI7:** consente l'acquisizione di documenti utilizzando il messaggio standard HI7 (ver. 2.6 o successive) "MDM T10";
- 6) **Modalità Custom:** relativa a clienti che richiedono una progettazione puntuale delle esigenze, con metadati personalizzati e aggiuntivi rispetto allo standard, oppure modalità di invio dei documenti da conservare ibridi o comunque diversi da quelli standard (gli standard sono l'Upload Manuale, l'SFTP e l'A2A).

[Torna al sommario](#)

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

Il sistema esegue per i 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.

<sup>2</sup> 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 all'attivazione del servizio.

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

[Torna al sommario](#)

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

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

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

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

Tutti i rapporti di versamento sono conservati insieme ai documenti informatici sottoposti al processo di 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.trusttechnologies.it>. Il collegamento avviene tramite connessione sicura SSL con certificato della Certification Authority TI.TT.

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

A quel punto i produttori sono in grado di:

- Visualizzare direttamente i documenti informatici originali conservati da remoto;
- Scaricare i documenti informatici conservati (duplicati) e i file di evidenza della conservazione (indice di conservazione Uni SinCRO);
- Richiedere e scaricare i (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<sup>3</sup>.

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

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

A quel punto i soggetti produttori sono in grado di:

- Visualizzare direttamente i documenti informatici originali conservati
- Scaricare i documenti informatici conservati (duplicati) e i file di evidenza della conservazione (indice di conservazione Unisincro)

<sup>3</sup> Il collegamento avviene tramite connessione sicura SSL con certificato della Certification Authority TI.TT

- 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 la copia 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 del 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.



**Le operazioni di generazione e scarico dei DIP devono essere completate entro 60 giorni dalla scadenza del contratto, trascorsi i quali TI.TT procederà loro alla cancellazione definitiva, 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 esplicito 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.

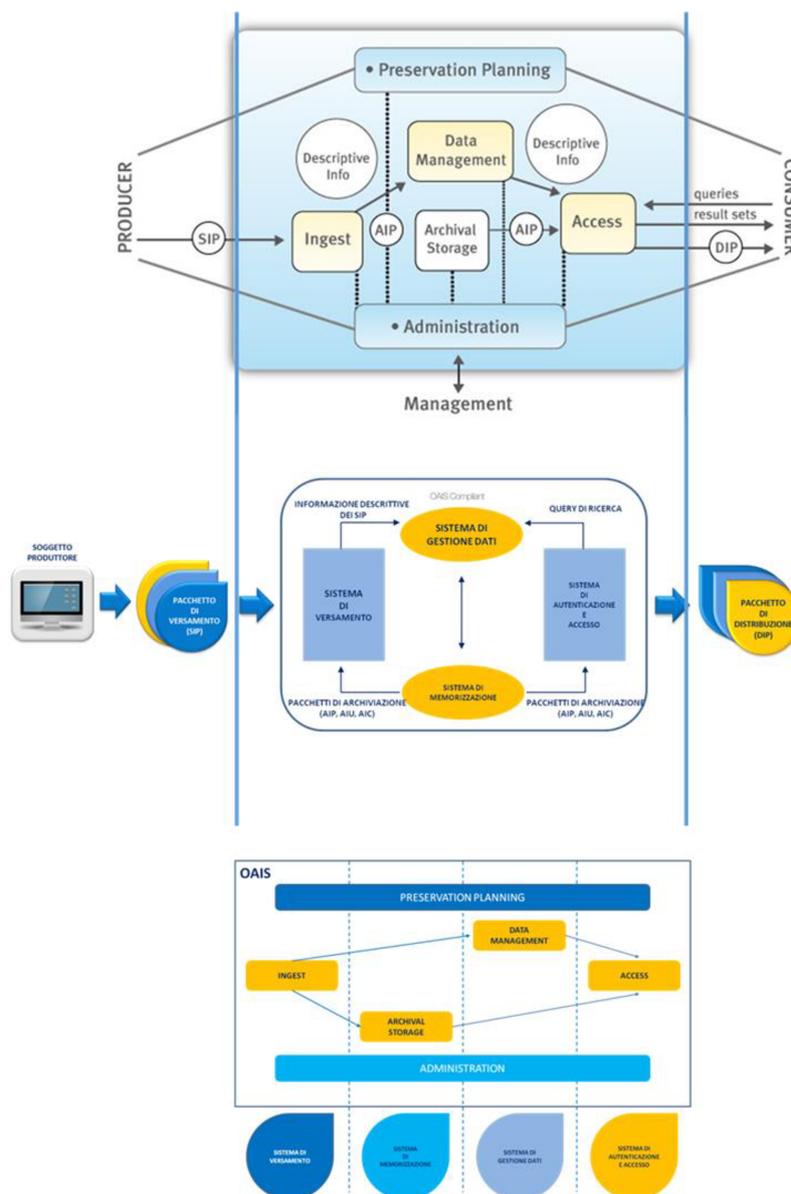


Figura 5 - Sistema di conservazione e conformità al modello OAIS

[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 ricerche 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 restrittivi standard di sicurezza:

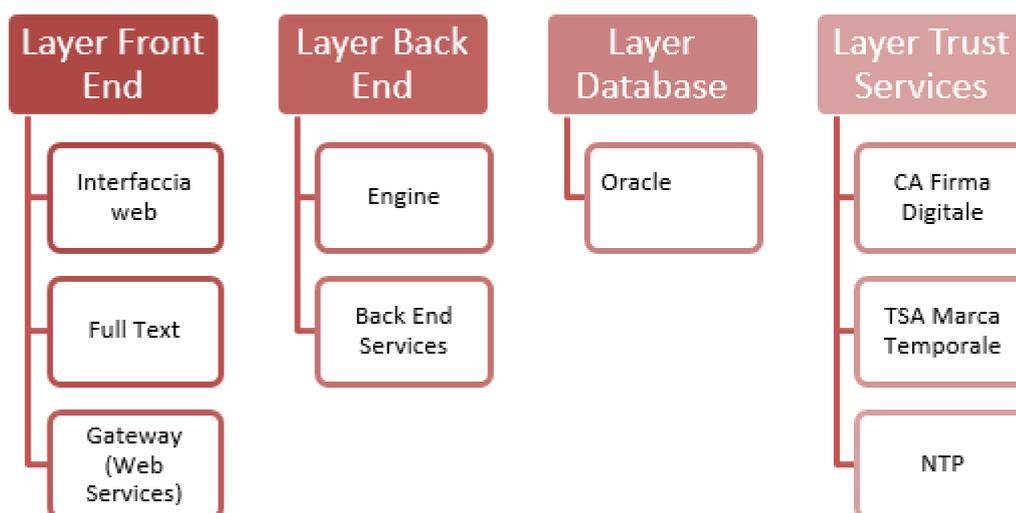


Figura 6 - Componenti core del sistema di conservazione

[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 dei volumi di documenti da conservare, permettendo di reagire tempestivamente alle nuove esigenze del cliente.

[Torna al sommario](#)

## 8.2.1 Servizi Erogati

Sottodominio	Descrizione
<a href="https://cons-coll.trusttechnologies.it">https://cons-coll.trusttechnologies.it</a>	Sito di esibizione e upload manuale - Ambiente di Collaudo

<a href="https://wscons-coll.trusttechnologies.it">https://wscons-coll.trusttechnologies.it</a>	Web Services di upload automatizzato di Collaudo (utilizzabile solo da indirizzi abilitati e da utenti con user e password)
<a href="https://conservazione.trusttechnologies.it">https://conservazione.trusttechnologies.it</a>	Sito di esibizione e upload manuale - Ambiente di Produzione
<a href="https://wsconservazione.trusttechnologies.it">https://wsconservazione.trusttechnologies.it</a>	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)
<a href="https://cons-datisensibili-coll.trusttechnologies.it/asap_arc/">https://cons-datisensibili-coll.trusttechnologies.it/asap_arc/</a>	Sito di esibizione - Ambiente di Collaudo (per il trattamento di documenti contenenti dati sensibili)
<a href="https://cons-datisensibili.trusttechnologies.it/asap_arc/">https://cons-datisensibili.trusttechnologies.it/asap_arc/</a>	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 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 schedata, 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 architettuale;
- 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 modifiche sorgenti sono:

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

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

- Livello di manutenzione (Maintenance 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:

<b>File System</b>	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.
<b>Database</b>	Si effettua la restore tramite le funzioni standard di Oracle dal sito primario o dal sito secondario (nel caso di indisponibilità del DB primario)
<b>Area SFTP/Upload</b>	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 schedabile, 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 <sup>4</sup>
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;
- 2) Assistenza ai clienti: dal lunedì al venerdì dalle 9:00 alle 18.00, festivi esclusi;

<sup>4</sup> 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.

3) Segnalazione di inconvenienti (apertura ticket di lavorazione): 24 ore su 24, 7 giorni su 7.

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

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

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

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

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

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

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

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

[Torna al sommario](#)

## 11 Protezione dei dati personali

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

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

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

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

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

- TI.TT conserva nel proprio Registro dei Trattamenti le informazioni previste dal GDPR e relative al servizio contrattualizzato con l'azienda cliente. La registrazione sarà mantenuta anche successivamente alla data di cessazione del servizio contrattualizzato;
- Nel caso TI.TT rilevi violazioni dei dati personali nell'ambito dei trattamenti previsti dal SERVIZIO (c.d. "data breach") e svolti per conto del Cliente Finale, TI.TT gliene darà tempestiva segnalazione;
- Ove applicabile in relazione al SERVIZIO, nel rispetto dei contratti in corso e delle normative in vigore, TI.TT fornirà al Titolare il supporto per permettere l'esercizio degli ulteriori diritti previsti dal GDPR da parte delle persone fisiche interessate;

- I servizi erogati al Titolare in virtù dei contratti in corso sono stati acquisiti da terze parti soggette a stringenti vincoli contrattuali o sviluppati da TI.TT secondo metodologie già conformi al principio della *privacy by design* e *by default*. In particolare, tramite l'applicazione del processo di *risk analysis* e l'adozione di policy interne di sicurezza e compliance Privacy, TI.TT ha definito ed applica adeguate misure di sicurezza per la protezione dei dati personali trattati nelle proprie piattaforme. Ad esse si aggiungono, ove applicabile e in relazione al SERVIZIO, le misure di sicurezza specifiche per rispondere alle esigenze del Titolare e previste dai contratti in corso. L'elenco delle misure definite da TI.TT per la protezione dei dati personali è pubblicato sul sito di TI.TT all'indirizzo : <https://www.trusttechnologies.it/download/legale-e-privacy/> ;
- In caso di nuovi servizi o di interventi sui servizi caratterizzati da un rischio significativo per i diritti e le libertà delle persone fisiche TI.TT effettua il Privacy Impact Assessment (PIA);
- TI.TT effettua i trattamenti dei dati personali in infrastrutture collocate sul territorio italiano. Nei casi previsti da accordi con il Titolare si applicano le garanzie previste dal GDPR per il trasferimento extra-EU, previa autorizzazione del Titolare;
- TI.TT fornirà supporto per lo svolgimento delle attività di verifica dei trattamenti che svolge in qualità di responsabile, previo accordo che stabilisca le modalità e i corrispettivi;
- I riferimenti del Data Protection Officer del Gruppo TIM sono i seguenti:  
recapito: Data Protection Officer, via Gaetano Negri, 1 - 20123 Milano  
indirizzo email: [dpo.trusttechnologies@telecomitalia.it](mailto: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](#)

## **Descrizione del servizio**

### **TRUST LEGAL SPACE**

#### **DESCRIZIONE DEL SERVIZIO**

**VERSIONI DEL DOCUMENTO**

Revisione	Descrizione delle modifiche	Emissione
00	Redazione	16/06/2014
01	Revisione : c.3 – revisione ; c.5 – revisione ; c.6 – integrazione dati UNISinCRO ; c.7 e c.8	26/06/2014
02	c.6 - integrazione	15/11/2014
03	c. 2.5 – rettifica ; c. 8.2.1 - integrazione	28/11/2014
04	c. 5.2.1 - revisione	26/06/2015
05	c. 8.11 – Integrazione esempi DA	09/09/2015
06	c.2,5 – Aggiornamento modalità di Scarto	25/11/2015
07	c. 8.11 – Integrazione esempi DA	26/07/2016
08	c. 5 - revisione	23/02/2016
09	c. 5 - revisione	07/03/2016
10	Revisione Capitoli: c.5.1 Campi Minimi ; c.5.1.2 Tipologie Descrizioni Archivistiche ; c.6.1 viewer	15/09/2016
11	C.5 Inserimento nuove DA (Determina)	22/09/2016
12	Revisione DA	06/10/2016
13	Inserimento DA inerenti ai Libri Contabili	20/10/2016
14	Inserimento DA inerenti agli Ordini PA/Privati ed F23/F24	19/12/2016
15	Modifiche DA	10/04/2017
16	Inserimento DA inerenti ai Cedolini	20/09/2017

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

## Indice degli argomenti

<b>1</b>	<b>Scopo del documento .....</b>	<b>6</b>
1.1	Definizioni.....	6
1.2	Riferimenti .....	7
<b>2</b>	<b>La Conservazione .....</b>	<b>7</b>
2.1	Normativa di riferimento .....	8
2.2	Standard di riferimento.....	8
	<i>Internazionali:</i> .....	8
	<i>Nazionali:</i> .....	9
2.3	Descrizione del processo di conservazione.....	9
	<i>2.3.1 Versamento degli oggetti digitali .....</i>	<i>10</i>
	<i>2.3.1.1 Upload manuale .....</i>	<i>11</i>
	<i>2.3.1.2 Modalità SFTP.....</i>	<i>11</i>
	<i>2.3.1.3 A2A (Web Services) .....</i>	<i>11</i>
	<i>2.3.2 Costruzione del pacchetto di archiviazione.....</i>	<i>12</i>
	<i>2.3.3 Controlli preliminari.....</i>	<i>13</i>
	<i>2.3.4 Conservazione del pacchetto di archiviazione (AIP).....</i>	<i>13</i>
	<i>2.3.5 Verifica dell'integrità .....</i>	<i>13</i>
2.4	Utilizzo dei dati conservati.....	13
	<i>2.4.1 Il processo di esibizione .....</i>	<i>14</i>
2.5	Scarto dei documenti (Retention) .....	14
<b>3</b>	<b>La soluzione di TI Trust Technologies .....</b>	<b>15</b>
3.1	Architettura funzionale .....	15
	<i>3.1.1 Componenti principali.....</i>	<i>15</i>
	<i>3.1.1.1 Front End:.....</i>	<i>16</i>
	<i>3.1.1.2 Back End:.....</i>	<i>16</i>
	<i>3.1.2 Servizi Erogati .....</i>	<i>17</i>
<b>4</b>	<b>Modalità di utilizzo del servizio .....</b>	<b>17</b>
4.1	Modalità Manuale.....	18
	<i>4.1.1 Operazioni preliminari.....</i>	<i>18</i>
	<i>4.1.2 Descrizione Flusso .....</i>	<i>18</i>
4.2	Flusso A2A.....	18
	<i>4.2.1 Operazioni Preliminari .....</i>	<i>18</i>
	<i>4.2.2 Descrizione Flusso .....</i>	<i>19</i>
4.3	Modalità SFTP .....	19
	<i>4.3.1 Operazioni Preliminari .....</i>	<i>19</i>
	<i>4.3.2 Descrizione Flusso .....</i>	<i>19</i>
4.4	Modalità Custom .....	20

<b>5</b>	<b>Descrizioni Archivistiche (Set Standard)</b>	<b>20</b>
5.1	Dettagli di conservazione (Campi Minimi)	21
5.1.1	Metadati minimi (comuni a tutte le DA)	21
5.2	Tipologie Descrizioni Archivistiche (DA)	22
	Metadati di profilo archivistico (opzionale)	22
	Metadati di profilo archivistico 2 (opzionale)	22
5.2.1	Tipologia documentaria: Documento Informatico	23
5.2.2	Tipologia documentaria: Documento Amministrativo Informatico (PA)	23
5.2.3	Tipologia documentaria: Registro Unico delle Fatture	24
5.2.4	Tipologia documentaria: Registro IVA (PA)	24
5.2.5	Tipologia documentaria: Delibera CDA	25
5.2.6	Tipologia documentaria: Fatture Elettroniche Attive (Privati)	26
5.2.7	Tipologia documentaria: Fatture Elettroniche Attive (PA)	26
5.2.8	Tipologia documentaria: Fatture Elettroniche Passive (PA)	27
5.2.9	Tipologia documentaria: Fatture Elettroniche Passive (Privati)	28
5.2.10	Tipologia documentaria: Libro Giornale (Privati)	28
5.2.11	Tipologia documentaria: Documento di Trasporto	29
5.2.12	Tipologia documentaria: Libro Magazzino (Privati)	29
5.2.13	Tipologia documentaria: Verbalì Esame Universitario	30
5.2.14	Tipologia documentaria: Contratti	30
5.2.15	Tipologia documentaria: Contabili di sportello	31
5.2.16	Tipologia documentaria: Registro Giornaliero di Protocollo	31
5.2.17	Tipologia documentaria: Determina	32
5.2.18	Tipologia documentaria: PEC	33
5.2.19	Tipologia documentaria: Libri Contabili	34
5.2.19.1	Tipologia documentaria: Libro Cespiti Privati	34
5.2.19.2	Tipologia documentaria: Libro Inventari (privati)	34
5.2.19.3	Tipologia documentaria: Libro Mastro (privati)	35
5.2.19.4	Tipologia documentaria: Registro IVA (privati)	36
5.2.19.5	Tipologia documentaria: Libro unico del Lavoro	36
5.2.20	Tipologia documentaria: Ricevute F24 e F23 Privati	37
5.2.21	Tipologia documentaria: Ricevute F24 e F23 PA	37
5.2.22	Tipologia documentaria: Ordini Privati	38
5.2.23	Tipologia documentaria: Ordini PA	39
5.2.23.1	Tipologia documentaria: Mandati di pagamento	39
5.2.23.2	Tipologia documentaria: Ordini di riscossione / Reversali di incasso	39
5.2.23.3	Tipologia documentaria: Ordine diretto d'acquisto PA tramite MEPA	40
5.2.24	Tipologia documentaria: Cedolini	41
5.2.25	Tipo documento: DA Custom	42

<b>6</b>	<b>Definizione degli oggetti “conservabili”</b> .....	<b>42</b>
6.1	I formati dei documenti sottoposti a conservazione .....	43
<b>7</b>	<b>Modalità di attivazione di un nuovo cliente</b> .....	<b>44</b>
7.1	Il processo di provisioning.....	44
<b>8</b>	<b>Movimentazioni massive di dati conservati</b> .....	<b>45</b>
8.1	Accettazione dati conservati da altri outsourcer .....	45
8.1.1	<i>Per i dati conservati dopo il 13 aprile 2014</i> .....	45
8.1.2	<i>Per i dati conservati prima del 13 aprile 2014</i> .....	45
8.2	Esportazione dati per fine contratto (non rinnovato).....	46
8.2.1	<i>Modalità di restituzione</i> .....	46
8.2.2	<i>Flusso di deprovisioning</i> .....	46
8.2.3	<i>Modalità di restituzione di casi particolari</i> .....	47

## 1 Scopo del documento

Il presente documento descrive la piattaforma di Telecom Italia Trust Technologies s.r.l. (in seguito T.I.T.T.) per la conservazione a norma rispondente alla nuova normativa espressa nel D.P.C.M (Decreto del Presidente del Consiglio dei Ministri) del 3 dicembre 2013 e successive modificazioni.

### 1.1 Definizioni

Nell'ambito del documento saranno utilizzati gli acronimi e le definizioni riportate nel seguito.

A2A	Application to Application, modalità di interfaccia fra applicazioni software
AIP RDV	Creazione di pacchetti di archiviazione / Rapporti di versamento
CA	Autorità di Certificazione: prestatore di servizi di certificazione, la società ITT
CDP	CRL Distribution Point, la URI internet che punta all'oggetto binario CRL presente all'interno di un server di disseminazione. Per l'accesso di norma è usato il protocollo LDAP. Il CDP viene inserito all'interno di ogni certificato dalla CA.
CRL	Lista dei Certificati Revocati: la lista firmata digitalmente, tenuta e aggiornata dal certificatore, dei certificati che hanno perduto temporaneamente (sospesi) o definitivamente (revocati) la propria validità, in anticipo rispetto alla scadenza prevista.
DA	Descrizione Archivistica: l'insieme di informazioni, procedure, specifiche, dati, ecc... che determinano ed identificano un particolare gruppo di documenti appartenenti ad un solo SP
DIP	Pacchetto di distribuzione
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer (HTTPS): canale di comunicazione criptato tra il client e il server attraverso uno scambio di certificati; una volta stabilito questo canale al suo interno viene utilizzato il protocollo diverso (solitamente http) per la comunicazione.
LDAP	Lightweight Directory Access Protocol: protocollo utilizzato per la gestione degli accessi al registro dei certificati e l'effettuazione di operazioni di prelievo di certificati e liste di revoca e sospensione.
P	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 amministrazioni pubbliche, tale figura si identifica con il responsabile della gestione documentale.
PIN	Codice personale di accesso alle chiavi custodite su HSM dispositivi sicuri di firma.
RA	Ente adibito all'attività di registrazione delle anagrafiche del titolare e di richiesta dei certificati.
SIP	Pacchetto di Versamento
SOAP	Simple Object Access Protocol. È un protocollo leggero per lo scambio di messaggi tra componenti software.
SP	Soggetto Produttore: l'ente, la famiglia o la persona che ha posto in essere, accumulato e/o conservato la documentazione nello svolgimento della propria attività personale o istituzionale. Non va confuso con il soggetto che ha
SSL	Protocollo standard per la trasmissione sicura dei dati su internet

XML	EXtensible Markup Language. È un metalinguaggio di markup, ovvero un linguaggio marcatore che definisce un meccanismo sintattico che consente di estendere o controllare il significato di altri linguaggi marcatori.
VPN	Virtual Private Network
VIP	Virtual IP

**Tab.1 - Acronimi**

## 1.2 Riferimenti

[NORM]	<a href="http://www.gazzettaufficiale.it/eli/id/2014/03/12/14A02098/sg">http://www.gazzettaufficiale.it/eli/id/2014/03/12/14A02098/sg</a>
[SCATT]	EVOCAST01.IT.DPDP14000.01- Allegato Scheda Di Attivazione – Conservazione a Norma.pdf
[SCCONF]	EVOCAST01.IT.DPDP14001.00- Allegato Scheda Di Configurazione – Conservazione a Norma.pdf
[MUINT]	Specifiche di alimentazione e versamento SFTP e A2A

**Tab.2 – Riferimenti**

## 2 La Conservazione

La conservazione è un processo finalizzato all'estensione e al mantenimento della validità dei documenti informatici conservati, di cui ne garantisce nel tempo la fruibilità, l'integrità, la leggibilità, l'affidabilità, l'autenticità e reperibilità. A causa della mole di informazioni, controlli ed attività previste per il rispetto della normativa si consiglia di utilizzare il servizio di conservazione come implementazione alle modalità di gestione documentale già in essere presso il cliente.

Salvo che, attraverso un'offerta custom, l'abilitazione dei flussi input/output può essere attivata per un massimo di tre utenti per ogni soggetto produttore.

Il sistema di conservazione riceve i pacchetti di versamento, li verifica e produce un rapporto di versamento, nel caso in cui si riscontrassero errori il sistema produce un rifiuto del pacchetto di versamento; eseguiti i controlli il sistema li trasforma in pacchetti di archiviazione e produce pacchetti di distribuzione al richiedente, rispondendo a tutti i requisiti che la normativa vigente pone per l'esibizione dei documenti informatici, arricchendo le informazioni che accompagnano i dati conservati e tracciando tutte le attività riguardanti.

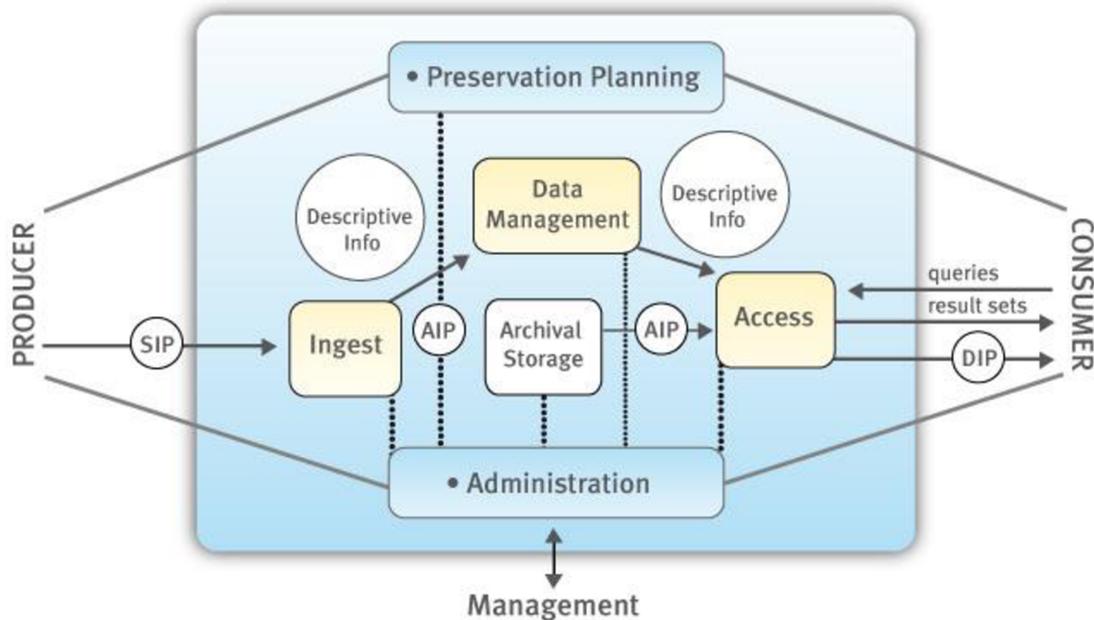


Fig.1

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. (Glossario DPCM 3 dicembre 2013).

Il Management è gestito dal conservatore accreditato (TI Trust Technologies srl) che trasforma i pacchetti di versamento in pacchetti di archiviazione (AIP).

I delegati del cliente (Consumer) possono procedere all'esibizione ai fini legali dei documenti conservati richiedendo la generazione di pacchetti di distribuzione al conservatore.

## 2.1 Normativa di riferimento

Il sistema di conservazione di T.I.T.T. rispetta la normativa espressa nel Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013, pubblicato in Gazzetta Ufficiale n.59 del 12-3-2014 - Suppl. Ordinario n. 20 [NORM]. Si richiama anche il Decreto del Ministero dell'Economia e delle Finanze 17 giugno 2014 per la conservazione dei documenti informatici fiscali.

Nel Dpcm sopraindicato sono indicati gli standard da adottare per la conservazione e la gestione archivistica degli oggetti digitali.

## 2.2 Standard di riferimento

Il sistema di conservazione di T.I.T.T. rispetta i seguenti standard e le specifiche tecniche di riferimento.

### Internazionali:

- Dublin Core: ISO 15386 The metadata element set
- OAIS: sistema informativo aperto per l'archiviazione ISO 14721:2002 Open Archival Information System ETSI TS 101 533-1 V1.1.1 (2011-05) 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 V1.1.1 (2011-05) 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.

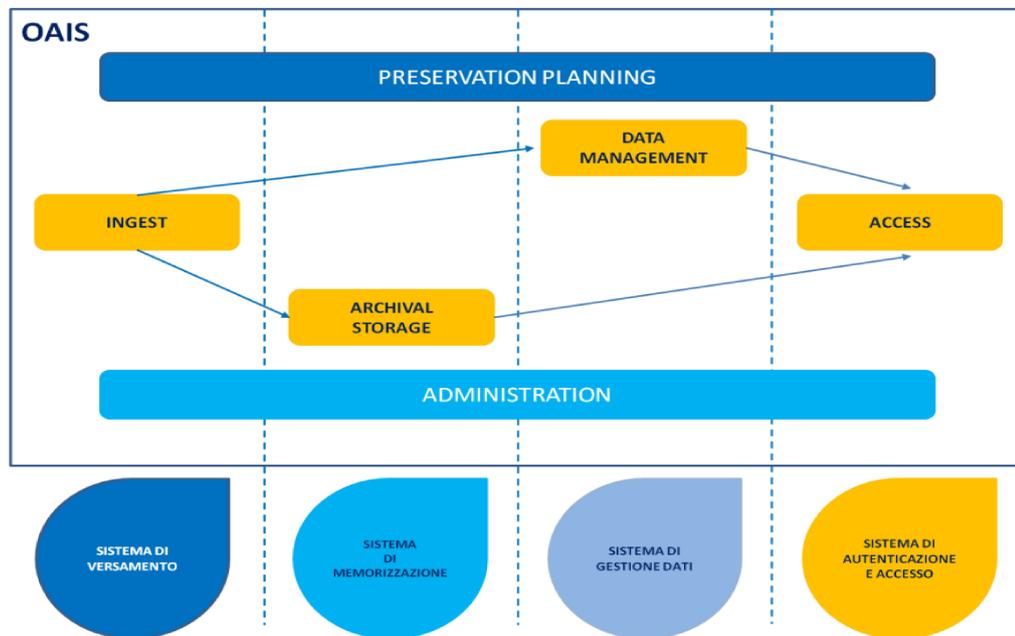


Fig.2 – Flusso Archivistico OAIS std.

### Nazionali:

- UniSInCRO: UNI 11386 Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali

## 2.3 Descrizione del processo di conservazione

Il sistema di conservazione riceve dei pacchetti di versamento, li trasforma in pacchetti di archiviazione e produce pacchetti di distribuzione, rispondendo a tutti i requisiti che la normativa pone per l'esibizione dei documenti informatici, arricchendo le informazioni che accompagnano i dati conservati e tracciando tutte le attività che li riguardano.

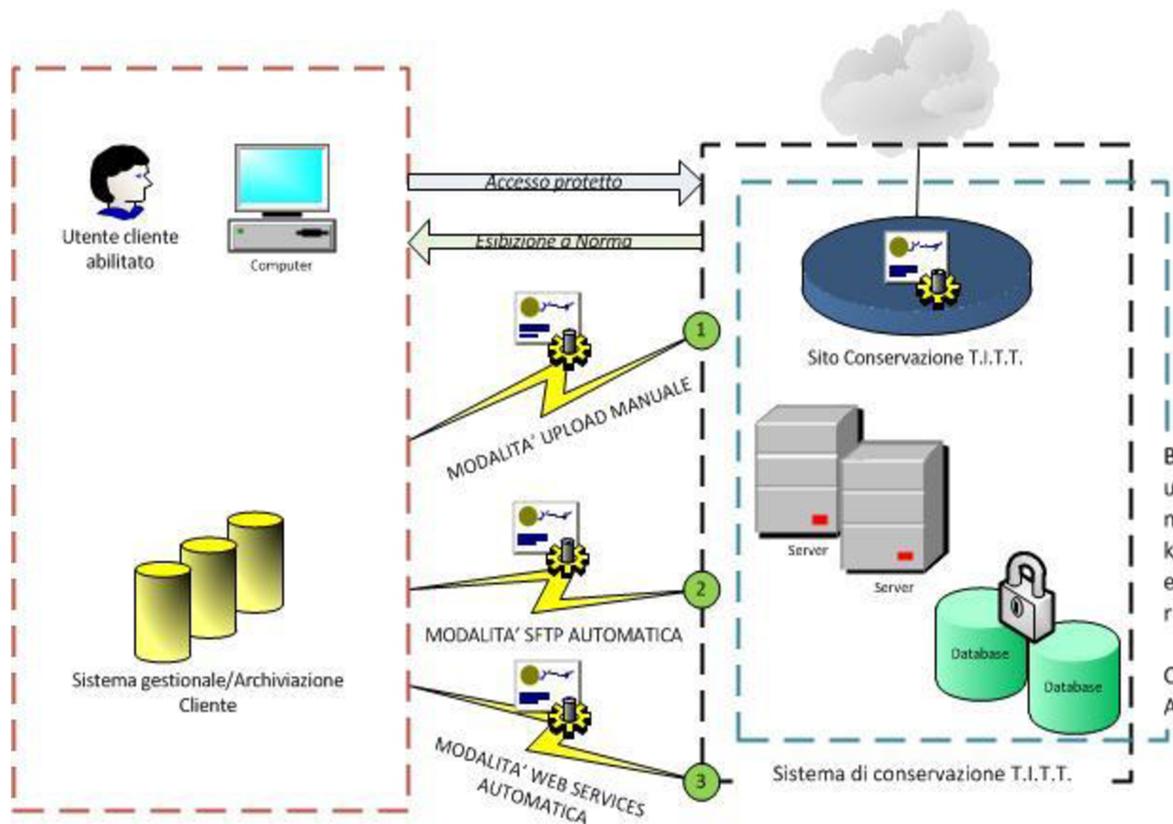


Fig.3

L'immagine riportata di seguito descrive la procedura di generazione dei pacchetti di archiviazione che il sistema di conservazione di T.I. Trust Technologies ha implementato, adottando gli standard di riferimento della normativa vigente.

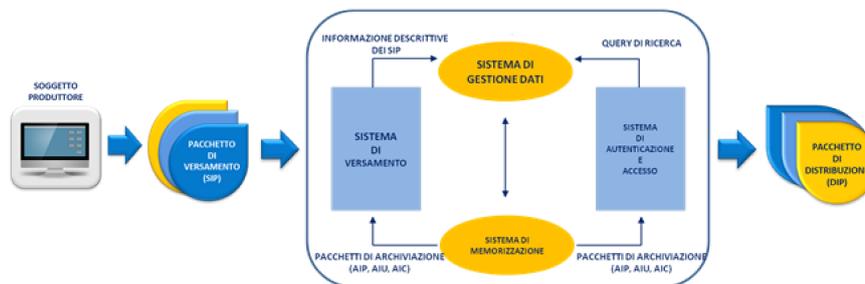


Fig.4

### 2.3.1 Versamento degli oggetti digitali

I pacchetti di versamento, descritti più avanti, possono raggiungere il servizio di conservazione di T.I.T.T. in una delle seguenti modalità:

1. Upload manuale da WEB;
2. SFTP (automatica);
3. A2A - Web Services (automatica).

 Trust Technologies	Codice: EVOCAST01.TT.DPMU14001.16
Descrizione del servizio TRUST LEGAL SPACE	Stato: Rilasciato

### 2.3.1.1 Upload manuale

---

Avviene tramite l'autenticazione al sito di erogazione della conservazione.

Un' apposita Web-App, presentata in seguito, consente agli utenti, autorizzati dal Cliente e profilati sulla piattaforma, di accedere e caricare uno ad uno i file da conservare, inserendo di volta in volta i metadati che serviranno a ricercare i dati conservati e ad effettuarne l'esibizione.

### 2.3.1.2 Modalità SFTP

---

È costituita da un collegamento SFTP (Secure File Transfert Protocol). Esso è un collegamento 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 potrà quindi procedere all'upload sia dei pacchetti di versamento nella folder SFTP dedicata, generando ed inviando pacchetti informativi costituiti da un file di indice (txt,xml o csv), di cui saranno fornite le specifiche, sia di una cartella contenente i documenti da porre in conservazione.

È consigliabile creare dei pacchetti zip piccoli, piuttosto che uno molto grande in modo da ridurre l'impatto negativo in caso di brusca interruzione durante il trasferimento per problemi di connessione.

In ogni caso gli scarti vanno nella cartella unzip\_error dell'area sftp a disposizione.

Esiste un processo che scompatta il file zip per poterlo sottomettere in conservazione.

Il processo è un trigger che è configurato per scattare ogni tot ore/minuti e prende in carico i files zip presenti nella cartella sftp.

Il trigger, quando scatta, prende in carico i files zip; va evitato di lasciare nella cartella sftp dei file aperti in scrittura in formato zip poiché risulterebbero corrotti.

Di conseguenza durante la fase di upload si può nominare il file con estensione .zip.tmp e solamente a scrittura terminata va eseguito il rename in .zip, poiché questo deve essere lo stato dell'upload terminato con esito positivo.

E' fondamentale che venga impostata questa policy onde evitare che il trigger prenda in carico il file prima del termine del trasferimento e di conseguenza lo scarti.

Questa funzionalità standard è tipicamente inclusa per i client sftp.

### 2.3.1.3 A2A (Web Services)

---

Con credenziali personalizzate e accesso consentito dal layer di sicurezza ad un set predefinito di IP statici riservati al Cliente è possibile raggiungere i web services di conservazione esposti da T.I.T.T.

L'applicazione del Cliente, dopo l'autenticazione, potrà utilizzare le chiamate di cui saranno fornite le specifiche per eseguire tutte le operazioni previste dalla conservazione.

### 2.3.2 Costruzione del pacchetto di archiviazione

Una volta a disposizione i file presso la piattaforma di T.I.T.T., il processo di conservazione può avere inizio.

E' possibile separare i versamenti in diversi pacchetti di archiviazione (AIP) dividendo i pacchetti 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 VIP, è richiesto il rispetto delle seguenti configurazioni:

- Massimo 4 GB di documenti conservati per pacchetto di archiviazione;
- Massimo 80mila documenti/file (allegati inclusi) per pacchetto di archiviazione;
- Massimo 5 MB per ogni file inviato (fino a 350 MB per invii tramite SFTP);
- NON saranno considerati accettabili invii "millesimati", ossia sporadici invii massivi di piccoli o piccolissimi pacchetti di versamento. Il Soggetto Produttore (SP) potrà invece scegliere una periodicità di upload definita in modo da ottimizzare e standardizzare i processi e i pacchetti di archiviazione.

Una volta che la conservazione (chiusura del pacchetto di archiviazione e avvio del processo di conservazione) 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.

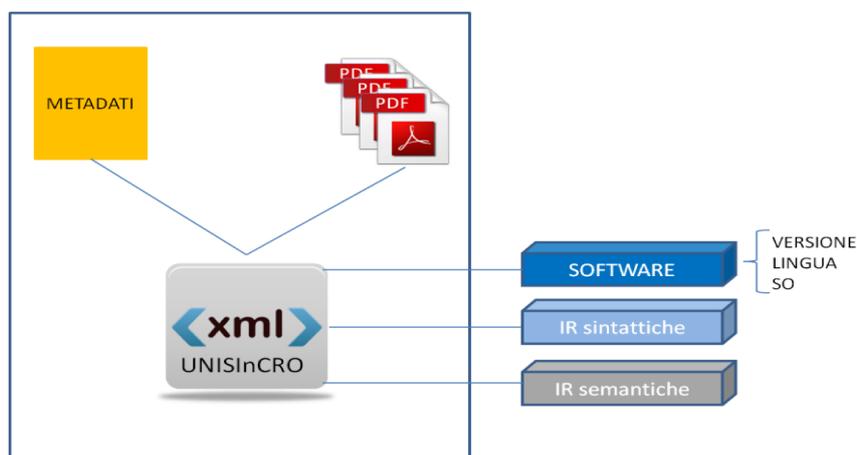


Fig.5 – Struttura AIP (pacchetto di archiviazione) UNISinCRO

I metadati associati ai file da conservare sono concordati prima dell'esercizio del servizio tra il Cliente e T.I.T.T. 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.

 Trust Technologies	Codice: EVOCAST01.TT.DPMU14001.16
Descrizione del servizio TRUST LEGAL SPACE	Stato: Rilasciato

### 2.3.3 Controlli preliminari

Di default, su ogni documento informatico versato al sistema di conservazione è eseguita una serie di controlli e verifiche di validazione rispetto alle regole ed agli standard previsti dalle tipologie documentarie di appartenenza.

Il processo di convalida riguarda almeno i seguenti aspetti:

- la verifica dell'integrità del documento memorizzato sul supporto rispetto all'impronta associata allo stesso;
- la verifica che il formato del dato sia coerente con quanto dichiarato nei suoi metadati;
- la verifica della presenza di un documento identico già caricato a sistema (i.e.: stessa impronta e/o 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 (SIP). In caso di esito negativo l'intero pacchetto è sospeso e viene immediatamente allertato il gruppo di competenza, che procederà a contattare i referenti del soggetto produttore per definire, a seconda dei casi, le azioni da intraprendere.

### 2.3.4 Conservazione del pacchetto di archiviazione (AIP)

La struttura utilizzata nella costruzione degli AIP fa riferimento alla norma UNI 11386:2010 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 contenete tutte le informazioni inviate dal SP 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)

### 2.3.5 Verifica dell'integrità

Nei controlli preliminari, durante la conservazione e periodicamente sui sistemi di conservazione, la funzionalità di verifica, permette di garantire l'integrità e l'inalterabilità del documento nel tempo, confrontando l'impronta attuale con quella contenuta nell'Indice del pacchetto di conservazione e fornita a suo tempo nel SIP dal Soggetto Produttore.

Tale funzionalità assolve i requisiti di verifica periodica della leggibilità dei documenti, come enunciati dalla normativa vigente. Opzionalmente, questa funzione può includere la verifica dell'integrità e della firma digitale apposta al relativo file indice (indice di Conservazione). In qualsiasi momento a seguito di una ricerca, è possibile effettuare una verifica sul singolo file o insieme di file.

## 2.4 Utilizzo dei dati conservati

Sono di seguito descritte le modalità di esibizione ed esportazione dei dati per richieste in ambito legale. Più avanti nel documento è descritta anche la procedura di deprovisioning e la relativa esportazione dei dati per fine contratto (non rinnovato).

 Trust Technologies	Codice: EVOCAST01.TT.DPMU14001.16
Descrizione del servizio TRUST LEGAL SPACE	Stato: Rilasciato

## 2.4.1 Il processo di esibizione

L'esibizione è una procedura da svolgersi in ottemperanza di quanto previsto dall'ultimo comma dell'art. 2220 del Codice Civile, ribadito nell'Art. 10 del D.P.C.M. del 3 dicembre 2013.

Essa consiste nel permettere la fruibilità, con mezzi idonei, i documenti informatici conservati a norma. L'Articolo 10 del D.P.C.M. del 3 dicembre 2013 ribadisce le norme vigenti e specifica che ai fini dell'esibizione il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, al documento informatico conservato, attraverso la produzione di un pacchetto di distribuzione (DIP) selettiva secondo le modalità descritte nel manuale di conservazione. Il pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta

Il sistema di conservazione di T.I.T.T. consente l'esibizione in modo da richiedere, generare e 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 Cliente, in fase di attivazione del servizio segnala al provisioning di T.I.T.T., su apposita documentazione correlata dagli allegati autorizzativi e di identificazione, i propri delegati alla visualizzazione e al download dei file 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.

A quel punto i delegati del cliente sono in grado di:

- Visualizzare i documenti conservati da remoto
- Scaricare i documenti conservati e i file di evidenza della conservazione
- Richiedere e scaricare dei pacchetti di distribuzione da consegnare all'istante.

Nel pacchetto 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.

## 2.5 Scarto dei documenti (Retention)

I tempi di conservazione per ciascuna tipologia documentaria sono riportati nel piano di conservazione di ciascuna amministrazione pubblica. Lo scarto è consentito dal d.lgs 22 gennaio 2004, 42.

Raggiunta la soglia di retention, il responsabile del servizio di conservazione (interno al soggetto conservatore) contatterà il Responsabile della gestione documentale e, o ove nominato, il Responsabile della Conservazione presso il Cliente per comunicargli che il documento ha cessato la funzione giuridico amministrativa e che può essere scartato, previa autorizzazione dal Ministero.

Nel caso in cui si tratti di un soggetto produttore privato il conservatore gli comunicherà quali documenti informatici hanno superato i tempi di conservazione come previsto da codice civile art.2220.

L'indicazione del periodo di retention, nell'apposita sezione della scheda di configurazione del servizio, non sostituisce né svincola il cliente dagli obblighi previsti dalla legge e lo scarto si applica solo quando il periodo di retention rientra nella durata del contratto. Nel caso in cui il contratto giunga a conclusione prima del termine della retention di tutti i dati conservati, i dati rimanenti saranno riconsegnati al cliente come previsto dalle procedure di deprovisioning.

L'amministrazione archivistica italiana, nel quadro della disciplina dettata dal Codice dei beni culturali e del paesaggio (d.lgs 42/2004) cura la tutela, la conservazione e la valorizzazione degli archivi attraverso gli archivi di stato e le soprintendenze archivistiche. L'art. 68 del DPR 445/2000 prevede che ogni amministrazione pubblica (vale solo per le PA) debba dotarsi di un piano di conservazione degli archivi

	<b>Codice:</b> EVOCAST01.TT.DPMU14001.16
<b>Descrizione del servizio</b> TRUST LEGAL SPACE	<b>Stato:</b> Rilasciato

integrato con il sistema di classificazione, per la definizione dei criteri di organizzazione dell'archivio. Il piano di conservazione è strettamente connesso con il piano di classificazione.

La finalità del piano di conservazione è quella di elencare tipologie di serie e di documenti che possono essere eliminati con una certa automaticità, onde rendere agile il flusso della documentazione.

La Legislazione archivistica (artt. 23-27 del DPR 1409/1963) in materia di conservazione recepiti ed integrati dall'art. 41, comma 1-3 del codice dei beni culturali e del paesaggio) dispone che gli organi giudiziari e amministrativi, centrali e periferici dello Stato una volta effettuate le operazioni di scarto versano all'Archivi di Stato i documenti relativi ad affari esauriti da oltre 30 anni, Decreto legge 83/2014 art.12.

In merito allo scarto archivistico è opportuno che il conservatore ricordi al soggetto Produttore (PA) che per tale intervento, deve ottenere l'autorizzazione allo scarto da parte del Ministero per i beni e le attività culturali ai sensi dell'art. 21 comma 1 lett. d del Codice dei beni culturali e del paesaggio, d.Lgs 22 gennaio 2004, n. 42. Nessun versamento può essere effettuato all'Archivio di Stato competente per territorio o alle separate sezioni di archivio se non sono state effettuate le operazioni di scarto, secondo quanto previsto dall'art. 41, comma 3 del Decreto Legislativo 22 gennaio 2004, n. 42. Per gli archivi statali lo scarto è approvato dalle commissioni di sorveglianza, come stabilito dall'art. 6 comma 2 del DPR 37/2001.

Le soprintendenze archivistiche regionali esercitano invece la vigilanza e rilasciano l'autorizzazione allo scarto sugli archivi non statali esistenti nella rispettiva regione e su quelli privati dichiarati di notevole interesse storico.

La richiesta di autorizzazione allo scarto è a carico del soggetto produttore. I documenti informatici, di cui è prescritta per legge o per regolamento la conservazione, possono essere archiviati per le esigenze correnti anche con modalità cartacee, ma devono essere conservati in modo permanente con modalità digitali. Si riconoscono esplicitamente i poteri di controllo del Ministero dei Beni culturali.

Il soggetto conservatore è la persona che operativamente eseguirà la procedura di scarto, ma solo a seguito di una autorizzazione scritta rilasciata da parte del soggetto produttore.

## 3 La soluzione di TI Trust Technologies

### 3.1 Architettura funzionale

La struttura della piattaforma di conservazione si compone di moduli e nodi ad alto livello di integrazione ed espansione.

Tutti i servizi di conservazione a norma, dalla presa in carico dei pacchetti di versamento alla generazione dei pacchetti di distribuzione e l'esibizione dei documenti è erogata in alta affidabilità e disaster recovery.

#### 3.1.1 Componenti principali

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

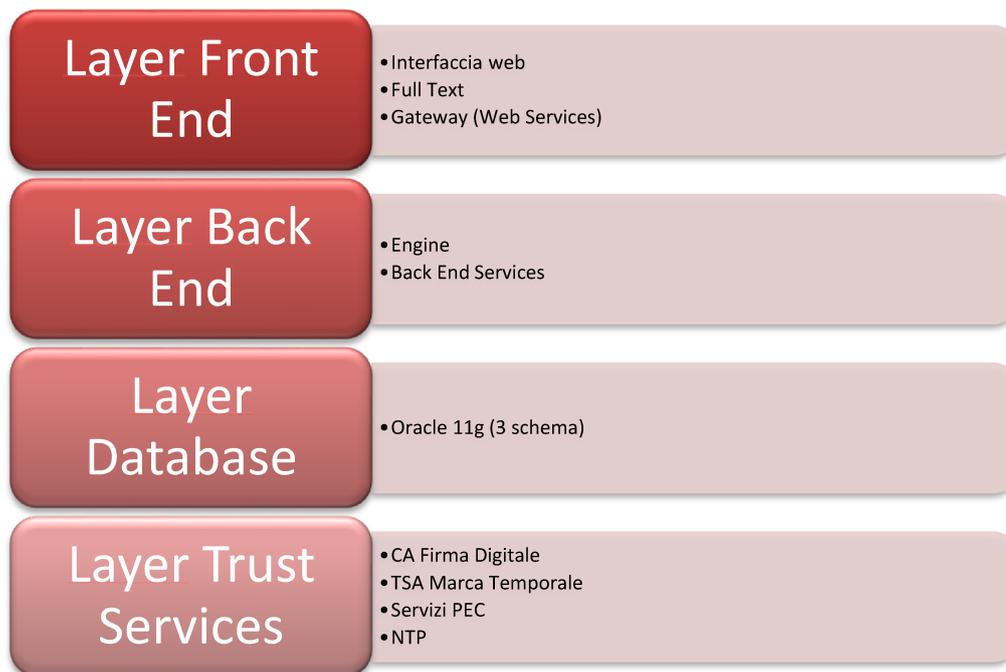


Fig.6 – Architettura funzionale

### 3.1.1.1 Front End:

---

L' Interfaccia Web è erogata protetta ed espone i servizi di consultazione, esibizione e download.

Di seguito la lista dei browser dichiarati compatibili:

- Android 2.3 o superiore
- Google Chrome 23 o superiore
- Internet Explorer 9 o superiore
- iOS 5 o superiore
- Mozilla Firefox 17 o superiore
- Opera 12 o superiore
- Safari 6 o superiore.

### 3.1.1.2 Back End:

---

I Back End Services rappresentano il core della logica applicativa e l'interfaccia verso le basi dati (Oracle 11g) 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.

### 3.1.2 Servizi Erogati

Sottodominio	Descrizione
<a href="https://cons-coll.trusttechnologies.it">https://cons-coll.trusttechnologies.it</a>	Sito di esibizione e upload manuale - Ambiente di Collaudo
<a href="https://wscons-coll.trusttechnologies.it">https://wscons-coll.trusttechnologies.it</a>	Web Services di upload automatizzato di Collaudo (utilizzabile solo da indirizzi abilitati e da utenti con user e password)
<a href="https://conservazione.trusttechnologies.it">https://conservazione.trusttechnologies.it</a>	Sito di esibizione e upload manuale - Ambiente di Produzione
<a href="https://wsconservazione.trusttechnologies.it">https://wsconservazione.trusttechnologies.it</a>	Web Services di upload automatizzato di Produzione (utilizzabile solo da indirizzi abilitati e da utenti con user e password)
<a href="sftp://consftp.ittelecom.it">sftp://consftp.ittelecom.it</a>	Siti di SFTP per upload misto (manuale e/o automatizzato)

Tab.3 - Servizi

## 4 Modalità di utilizzo del servizio

Il servizio di Conservazione erogato da Telecom Italia Trust Technologies (T.I.T.T.), offre diverse modalità di utilizzo ed ognuna di esse dispone di profili, strumenti e utility adatti alle diverse possibili esigenze dei Soggetti Produttori.

- **Modalità Manuale**
  - ❖ Utente Avanzato
    - **Input:** Web-In - Caricamento manuale dei singoli documenti e dei relativi metadati tramite Web-App
    - **Output:** Web-Usr - Ricerca, Esibizione e Download tramite Web-App
- **Flusso A2A**
  - ❖ Utente WS
    - **Input:** WS-In - Invio dei pacchetti di versamento tramite chiamate SOAP
    - **Output:** Ws-Get - Esibizione e Download documenti tramite chiamate SOAP
  - ❖ Utente Base
    - **Output :** Web-Usr - Ricerca, Esibizione e Download tramite Web-App
- **Modalità SFTP**
  - ❖ Utente SFTP
    - **Input:** SFTP-In - Caricamento lotti via SFTP
    - **Evidenze:** SFTP-Get - Download dell'evidenza di avvenuta conservazione tramite SFTP
  - ❖ Utente Base
    - **Output:** Web-Usr - Ricerca, Esibizione e Download tramite Web-App
- **Modalità Custom**
  - ❖ Possibilità di personalizzare o modificare le Descrizioni Archivistiche di default fino ad un massimo di 3 campi di metadati per ogni DA attivata.
  - ❖ Possibilità di scegliere tra l'upload WS-In, fino a 3 utenti WS, e quello SFTP-In.

 Trust Technologies	Codice: EVOCAST01.TT.DPMU14001.16
Descrizione del servizio TRUST LEGAL SPACE	Stato: Rilasciato

- ❖ Possibilità di richiedere l'attivazione di fino a 3 utenti base anche se si dispone già della modalità WS-Get offerta dall'Utente WS.

## 4.1 Modalità Manuale

Dedicato a volumi modesti, è interamente gestito da operatori del Cliente (più raramente da un Soggetto Produttore delegato) e si avvale di un set di utenze web, personali e non cedibili, con privilegi di caricamento, ricerca, esibizione e download.

### 4.1.1 Operazioni preliminari

Il Cliente potrà scegliere le Descrizioni Archivistiche dal set di default e compilare la relativa scheda di configurazione. Indicando la modalità di utilizzo prescelta in fase di attivazione, tramite la medesima scheda potrà richiedere la profilazione di fino a 3 utenze web di tipo "Utente Avanzato".

T.I.T.T. effettuerà le operazioni di provisioning e fornirà le credenziali di accesso ai titolari richiesti che potranno immediatamente procedere alla login e ai caricamenti manuali

### 4.1.2 Descrizione Flusso

L'utente esegue il login ed accede all'interfaccia di caricamento. Avvia una nuova istanza di caricamento e procede all'upload dei documenti popolando di volta in volta la form di caricamento dei metadati.

Confermando i dati inseriti si avvia il caricamento che inizia con i controlli preliminari e si conclude con la notifica dell'esito dell'elaborazione nella home page dell'utente.

I documenti conservati possono essere ricercati, esibiti o scaricati generando dei pacchetti di distribuzione come descritto nel manuale dedicato.

## 4.2 Flusso A2A

Dedicato a Soggetti Produttori, normalmente collegati direttamente (o tramite connettori ad hoc) ai siti documentali del cliente, di grandi dimensioni che necessitano di un flusso affidabile e ad un alto livello di automazione.

Viene fornito un manuale dettagliato di tutte le chiamate SOAP disponibili. A discrezione del cliente è possibile eseguire tramite protocollo SOAP tutte le operazioni previste dalla conservazione o parte di esse. Le operazioni di ricerca, esibizione e download possono essere eseguite anche richiedendo la configurazione di utenti di tipo base (massimo 3) delegati alle attività disponibili tramite interfaccia web.

### 4.2.1 Operazioni Preliminari

Il Cliente potrà scegliere le Descrizioni Archivistiche dal set di default e compilare la relativa scheda di configurazione. Indicando la modalità di utilizzo prescelta in fase di attivazione, tramite la medesima scheda, potrà richiedere la profilazione di fino a 3 utenze WS e 3 utenti web di tipo "base"

T.I.T.T. effettuerà le operazioni di provisioning e fornirà le credenziali di accesso al referente tecnico del cliente e/o al soggetto produttore indicato nella scheda di attivazione. Contestualmente il Soggetto Produttore potrà integrare in un suo client o nel sito documentale del Cliente le chiamate WS che intende implementare.

Con le credenziali saranno forniti anche gli Alias\_SP e gli Alias\_DA assegnati alle attivazioni richieste e necessari a comporre le chiamate di servizio.

 Trust Technologies	Codice: EVOCAST01.TT.DPMU14001.16
Descrizione del servizio TRUST LEGAL SPACE	Stato: Rilasciato

## 4.2.2 Descrizione Flusso

Il/i Server-Client del Soggetto Produttore (precedentemente censiti ed autorizzati) eseguono tutte le chiamate di push, get, action e request descritte nel manuale dedicato.

Il sistema di conservazione risponde come previsto dalle singole chiamate ricevute.

A fine upload, viene sempre prodotto un rapporto di versamento. A fine conservazione è possibile scaricare l'evidenza con un'apposita chiamata. Sono disponibili chiamate WS dedicate anche a verifiche massive, come l'elenco delle DA attivate, dei metadati associati ad una determinata DA, ecc...

## 4.3 Modalità SFTP

Si tratta di un flusso in cui l'upload dei lotti o dei pacchetti di versamento avviene tramite SFTP in un'area dedicata, messa a disposizione del Soggetto Produttore. Può essere utilizzato sia per gestire grandi che piccoli volumi e non è necessariamente collegato ad un connettore/sito documentale.

### 4.3.1 Operazioni Preliminari

Il Cliente potrà scegliere le Descrizioni Archivistiche dal set di default e compilare la relativa scheda di configurazione. Indicando la modalità di utilizzo prescelta in fase di attivazione e tramite la medesima scheda, dovrà censire i server di provenienza delle chiamate SFTP e potrà richiedere la profilazione di fino a 3 utenze web di tipo "Utente Base".

T.I.T.T. effettuerà le operazioni di provisioning, fornirà le credenziali di accesso ai titolari richiesti e fornirà le informazioni necessarie a stabilire la connessione SFTP al referente tecnico del cliente e/o al soggetto produttore indicato nella scheda di attivazione. Contestualmente il Soggetto Produttore potrà integrare in un suo client o nel sito documentale del Cliente le procedure di generazione ed invio dei pacchetti di versamento a T.I.T.T.

### 4.3.2 Descrizione Flusso

Il/i Server-Client del Soggetto Produttore (precedentemente censiti ed autorizzati) generano ed depositano i pacchetti di versamento nell'area SFTP dedicata (root: /home/public/Alias\_SP/Alias\_DA/).

Il Cliente dovrà inviare al server della conservazione dei file in formato **zip**, contenuti un file **indice** (ad esempio, con estensione .csv) e **i file da conservare**. Il file indice conterrà i metadati della DA di appartenenza, separati dal carattere pipe (|), come nell'esempio seguente:

Contenuto del file index.txt:

```
b3b155bde9a1905f13a1f8af91c087e1570479ababababba769cb7ce848c3f84|nomefiledaconservare.pdf|metadato2|metadato3|metadato4|...
```

**E' molto importante che l'ordine dei valori sia relativo all'ordine dei metadati della DA, come specificato negli esempi dell'Allegato A di questo documento.**

Il sistema di conservazione provvederà al versamento vero e proprio, ai controlli e alla generazione dei pacchetti di archiviazione. A conservazione ultimata sarà possibile scaricare il file di evidenza dall'area SFTP.

Gli utenti potranno eseguire le login all'interfaccia web per le attività di ricerca, esibizione e download.

## 4.4 Modalità Custom

Estende la modalità "A2A" consentendo di avere DA custom e di sostituire le chiamate SOAP con l'upload tramite SFTP.

## 5 Descrizioni Archivistiche (Set Standard)

Ogni DA è definita dalle seguenti informazioni:

- il set di metadati (Tipologia di Documento dal set standard)
- modalità di utilizzo del servizio (versamento)
- tempi (cadenza di caricamento)
- tipo di verifiche da fare:
  - sugli oggetti della conservazione (mime type e validità firme)
  - sui metadati
- informazioni della rappresentazione
  - campi ricerca
  - viewer
  - versione del viewer
  - sistema operativo
  - lingua
  - mime-type associati
- il contesto
- informazioni di provenienza
- informazioni di identificazione
- informazioni di integrità
- 
- Tutte queste informazioni vanno concordate preventivamente con il soggetto produttore e riportate nella scheda di configurazione del servizio al fine di cominciare le operazioni di configurazione sul sistema. L'offerta standard consente di richiedere una DA, ma è possibile richiederne di aggiuntive.

Per consentire il mantenimento di informazioni aggiuntive, non necessarie ai fini della conservazione, non incluse tra i metadati presentati, ma che il cliente desidera conservare, è possibile inviare dei file accessori come allegati dei documenti sottoposti a conservazione. In questa modalità il documento conservato sarà ricercabile attraverso i suoi metadati e sarà sempre corredato dai suoi allegati completi.

## 5.1 Dettagli di conservazione (Campi Minimi)

In accordo agli standard citati, si riportano di seguito i metadati obbligatori e comuni a tutte le Descrizioni Archivistiche (DA) ai fini della conservazione.

### 5.1.1 Metadati minimi (comuni a tutte le DA)

Si tratta dei metadati necessari ed indispensabili a garantire nel tempo l'inalterabilità, la fruibilità e la validità dell'oggetto digitale conservato del DPCM 3 dicembre 2013. Si ricorda che oltre alle informazioni sulla conservazione riportate nell'allegato 5 del DPCM 3 dicembre 2013, i documenti informatico fiscali devono contenere altresì i metadati indicati nell'art. 3 DM 17 giugno 2014.

Metadato	Descrizione	Formato
<b>Hash</b>	Impronta del documento	Hash
<b>Nome_Documento</b>	Nome del Documento conservato nel sistema del SP	Stringa
<b>Contesto</b>	Piano di Classificazione (Nei casi in cui è previsto. Indicare il titolo e classe, e il numero di fascicolo cui appartiene l'unità documentaria. È possibile valorizzare solo la Classifica e non i campi descrittivi del Fascicolo nel caso l'Unità documentaria sia stata solo classificata e non fascicolata. (Si ricorda che la classificazione è un'operazione necessaria richiesta dalla norma DPR 445/2000).	Stringa
<b>UID_Documento</b>	ID del Documento nel sistema del SP	Stringa
<b>Data di chiusura</b>	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immutabile.	dd/MM/yyyy
<b>Versione</b>	Versione del Documento	Numero intero
<b>Destinatario</b>	Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico il (codice fiscale)	Stringa
<b>Soggetto produttore</b>	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico	Stringa
<b>Oggetto</b>	Metadato funzionale a riassumere brevemente il contenuto del documento	Stringa

Al fine di garantire la possibilità di cercare uno specifico documento durante l'esibizione in sede legale, alcuni di questi campi sono disponibili nelle form di ricerca sull'interfaccia web dedicata.

Oltre ai metadati minimi, necessari alla conservazione, T.I.T.T. consente di caricare sul sistema di conservazione un certo numero di metadati aggiuntivi che possano aiutare i clienti a ricercare ed esibire i dati conservati. Il primo passo necessario ad utilizzare al meglio questa estensione del servizio di conservazione parte dalla scelta della corretta Descrizione Archivistica (DA) da associare al flusso di input in fase di definizione.

Ad ogni DA corrisponde un set di metadati che potranno/dovranno essere caricati sul sistema contestualmente alle conservazioni. Allo stesso modo, alcune informazioni saranno invece stabilite a priori ed andranno a compilare tutti quei campi che nella tabella precedente riportano la provenienza "Definito sul sistema di conservazione".

Si tratta in sostanza di identificare il **tipo di documento** che si intende portare in conservazione e di associarlo alla DA più prossima alle esigenze del cliente definendone al contempo i mime-type che saranno utilizzati.

Informazioni aggiuntive, documentazione a corredo e tutto quanto non definito nella DA può essere inserito in file che saranno allegati ai documenti sottoposti a conservazione. Per i file allegati è sufficiente indicarne il nome e l'HASH nella chiamata o nella sezione di indice dedicata.

## 5.2 Tipologie Descrizioni Archivistiche (DA)

I metadati riportati nella colonna "Nome\_Campo" delle Descrizioni Archivistiche (DA) integrano sempre i metadati minimi, indicati nella tabella precedente e che devono essere forniti dal Soggetto Produttore, contestualmente al versamento.

IMPORTANTE:

**L'Offerta Standard copre solamente la configurazione di Descrizioni Archivistiche (DA) tra quelle indicate nel seguito**

**E' possibile definire delle Descrizioni Archivistiche (DA) Custom con ulteriori Nomi Campi (Metadati). Per questo tipo di esigenza è necessaria un'analisi a progetto prima dell'offerta.**

L'insieme minimo dei metadati del documento informatico e del documento amministrativo informatico sono indicati agli articoli 9, 21 del DPCM sul protocollo informatico, 3.12.2013; il DPR 445/2000 artt. 53-55-56 e il DPCM 3.12.2013, allegato 5.

### Metadati di profilo archivistico (opzionale)

*La tabella andrà compilata con i metadati richiesti solo per i documenti afferenti al fascicolo informatico di procedimento amministrativo. In questo caso il fascicolo informatico è creato e gestito secondo le disposizioni dell'articolo 41 del Codice dell'amministrazione digitale (DLgs. 82/2005 e s.m.i.).*

N°	Metadato	Descrizione	Formato	Obb.	Ric.
1	Titolo		(in numero romano)	SI	SI
2	Classe		(in numero arabo)	SI	SI
3	Tipologia Documentaria			SI	SI
4	ID Fascicolo/ repertorio	Identificativo del fascicolo		SI	SI
5	Oggetto	Oggetto del procedimento	Oggetto del fascicolo	SI	SI
6	Elenco documenti	Elenco documenti afferenti il fascicolo		SI	
7	Responsabile del procedimento	Responsabile del procedimento amministrativo		SI	
8	Amministrazioni partecipanti	Amministrazioni partecipanti al procedimento		SI	
9	Anno di apertura	Anno di apertura del fascicolo		SI	SI
10	Anno di chiusura	Anno di chiusura del fascicolo		SI	SI

### Metadati di profilo archivistico 2 (opzionale)

*La tabella andrà compilata per tutti gli altri tipi di documenti afferenti esclusivamente a fascicoli per attività e per affare. Le informazioni fanno riferimento alla segnatura archivistica. Inoltre, si ricorda che il fascicolo di affare conserva i documenti relativi ad una competenza non procedimentalizzata, per la quale non segue un provvedimento finale.*

N°	Metadato	Descrizione	Formato	Obb.	Ric.
1	AnnoDiApertura	Anno di apertura del fascicolo		SI	SI
2	Titolo		(in numero romano)	SI	SI
3	Classe		(in numero arabo)	SI	SI
4	IDFascicolo	Identificativo del fascicolo		SI	SI

**N.B.: Ciascun metadato di ogni singola DA è contrassegnato come obbligatorio o meno nella colonna corrispondente, in ogni caso è possibile concordare caso per caso obbligatorietà anche diverse da quelle esemplificate in tabella, oltre ad eventuali altri metadati aggiuntivi.**

**Il concetto vale anche per la ricercabilità dei metadati indicati per ciascuna tipologia documentaria; la decisione in merito a quali metadati rendere ricercabili o meno rimarrà in capo al Conservatore. Quelli indicati come ricercabili devono considerarsi a titolo esemplificativo.**

**Si ricorda che ogni procedimento amministrativo deve avere un responsabile (UOR e RPA; L.241/90).**

**Nel caso si decida di avviare la fascicolazione, dovrà esserci una fase di progettazione precedente al versamento.**

### 5.2.1 Tipologia documentaria: Documento Informatico

N°	Metadato	Descrizione	Formato	Obb	Ric
1	Hash	Impronta del documento	Hash	SI	
2	Nome_Documento	Nome del Documento conservato nel sistema del SP	Stringa	SI	SI
3	UID_Documento	ID del Documento nel sistema del SP	Stringa	SI	SI
4	Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immodificabile.	dd/MM/yyyy	SI	SI
5	Versione	Versione del Documento	Numero intero	SI	
6	Destinatario	Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico (codice fiscale)	Stringa	SI	SI
7	Soggetto produttore	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico	Stringa	SI	SI
8	Oggetto	Metadato funzionale a riassumere brevemente il contenuto del documento (es. tipologia documentaria)	Stringa	SI	SI

### 5.2.2 Tipologia documentaria: Documento Amministrativo Informatico (PA)

N°	Metadato	Descrizione	Formato	Obb	Ric
1	Hash	Impronta del documento	Hash	SI	
2	Nome_Documento	Nome del Documento conservato nel sistema del SP	Stringa	SI	SI
3	UID_Documento	ID del Documento nel sistema del SP	Stringa	SI	SI
4	Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immodificabile.	dd/MM/yyyy	SI	SI
5	Versione	Versione del Documento	Numero intero	SI	
6	Destinatario	Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico (codice fiscale) <b>[NOTA. Tale metadato andrà compilato solo nei casi in cui è richiesto, per gli altri documenti che non lo prevedono (Es. fattura passiva) dovrà essere sostituito dal corrispondente "Mittente"]</b>	Stringa	SI	SI
7	Soggetto produttore	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico	Stringa	SI	SI
8	Oggetto	Metadato funzionale a riassumere brevemente il contenuto del documento (es. tipologia documentaria)	Stringa	SI	SI
9	Mittente	Soggetto che ha autorità e competenza ad inviare il documento	Stringa	NO	
10	DataProtDocumento	Data del protocollo	dd/MM/yyyy	NO	
11	IdentificativoDocRicevuto	Protocollo del documento ricevuto (se disponibile)	Stringa	NO	
12	CodiceIPA	Codice identificativo IPA	Stringa	SI	SI
13	CodiceAOO	Codice identificativo dell'AOO	Stringa	SI	SI
14	CodiceRegistro	Codice identificativo del registro	Stringa	SI	SI
15	RGD	Responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico	Stringa	NO	

### 5.2.3 Tipologia documentaria: Registro Unico delle Fatture

N°	Metadato	Descrizione	Formato	Obb	Ric
1	Hash	Impronta del documento	Hash	SI	
2	Nome_Documento	Nome del Documento conservato nel sistema del SP	Stringa	SI	SI
3	UID_Documento	ID del Documento nel sistema del SP	Stringa	SI	SI
4	Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immodificabile.	dd/MM/yyyy	SI	SI
5	Versione	Versione del Documento	Numero intero	SI	
6	Destinatario	Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico (codice fiscale)	Stringa	SI	SI
7	Soggetto produttore	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico	Stringa	SI	SI
8	Oggetto	Metadato funzionale a riassumere brevemente il contenuto del documento (es. tipologia documentaria)	Stringa	SI	SI
9	Numero	Numero progressivo attribuito al registro unico delle fatture	Numero intero	SI	SI
10	Anno	Anno del registro unico delle fatture	yyyy	SI	SI
11	Data	Data di creazione del registro	dd/MM/yyyy	SI	SI
12	NumeroIniziale	Numero della prima registrazione sul registro unico delle fatture	Numero intero	NO	
13	NumeroFinale	Numero dell'ultima registrazione sul registro unico delle fatture	Numero intero	NO	
14	DataInizioRegistrazioni	Data della prima registrazione sul registro unico delle fatture	dd/MM/yyyy	NO	
15	DataFineRegistrazioni	Data dell'ultima registrazione sul registro unico delle fatture	dd/MM/yyyy	NO	
16	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 il responsabile della gestione documentale.	Stringa	SI	
17	Mittente	Nome, Cognome, Codice Fiscale. Soggetto che ha l'autorità a inviare il documento (se richiesto)	Stringa	SI	
18	CodiceIdentificativoAmministrazione	Codice IPA	Stringa	NO	
19	CodiceIdentificativoAOO	Codice AOO	Stringa	SI	
20	CodiceIdentificativoRegistro	Codice identificativo del registro	Stringa	SI	
21	Identificazione del conservatore	Telecom Italia Trust Technologies	Stringa	NO	

### 5.2.4 Tipologia documentaria: Registro IVA (PA)

N°	Metadato	Descrizione	Formato	Obb	Ric
1	Hash	Impronta del documento	Hash	SI	
2	Nome_Documento	Nome del Documento conservato nel sistema del SP	Stringa	SI	SI
3	UID_Documento	ID del Documento nel sistema del SP	Stringa	SI	SI
4	Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immodificabile.	dd/MM/yyyy	SI	SI
5	Versione	Versione del Documento	Numero intero	SI	

6	Destinatario	Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico (codice fiscale)	Stringa	SI	SI
7	Soggetto produttore	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico	Stringa	SI	SI
8	Oggetto	Metadato funzionale a riassumere brevemente il contenuto del documento (es. tipologia documentaria)	Stringa	SI	SI
9	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 il responsabile della gestione documentale.	Stringa	SI	
10	Repertorio	Numerazione continua e progressiva per anno del registro	Stringa	SI	SI
11	Anno	Anno di competenza fiscale	yyyy	SI	SI
12	Data	Data di creazione del registro	dd/MM/yyyy	SI	SI
13	Numero prima registrazione		Stringa	NO	
14	Numero ultima registrazione		Stringa	NO	
15	Identificazione del conservatore	Telecom Italia Trust Technologies	Stringa	NO	

### 5.2.5 Tipologia documentaria: Delibera CDA

N°	Metadato	Descrizione	Formato	Obb	Ric
1	Hash	Impronta del documento	Hash	SI	
2	Nome_Documento	Nome del Documento conservato nel sistema del SP	Stringa	SI	SI
3	UID_Documento	ID del Documento nel sistema del SP	Stringa	SI	SI
4	Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immutabile.	dd/MM/yyyy	SI	SI
5	Versione	Versione del Documento	Numero intero	SI	
6	Destinatario	Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico	Stringa	SI	SI
7	Soggetto produttore	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico	Stringa	SI	SI
8	Oggetto	Metadato funzionale a riassumere brevemente il contenuto del documento (es. tipologia documentaria)	Stringa	SI	SI
9	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 il responsabile della gestione documentale.	Stringa	SI	SI
10	Anno	Coincide con l'anno della data di deliberazione	yyyy	SI	SI
11	Membri del CDA	Elenco nominativi dei membri CDA	Stringa	NO	
12	Numero di repertorio	Coincide con il numero di registrazione della deliberazione nello specifico repertorio	Stringa	SI	
13	Repertorio	Indicare il registro di repertorio di riferimento	Stringa	SI	
14	CodiceUOR (unità operativa responsabile)	Nei casi in cui è previsto	Stringa	NO	
15	CodiceIdentificativoAOO	Nei casi in cui sia previsto	Stringa	SI	
16	ResponsabileGestioneDocumentale	Responsabile della gestione documentale o Responsabile del servizio per la tenuta del protocollo informatico.	Stringa	SI	
17	Responsabile del procedimento	Responsabile del procedimento amministrativo	Stringa	NO	
18	Identificazione del conservatore	Telecom Italia Trust Technologies	Stringa	NO	

### 5.2.6 Tipologia documentaria: Fatture Elettroniche Attive (Privati)

N°	Metadato	Descrizione	Formato	Obb	Ric
1	Hash	Impronta del documento	Hash	SI	
2	Nome_Documento	Nome del Documento conservato nel sistema del SP	Stringa	SI	SI
3	UID_Documento	ID del Documento nel sistema del SP	Stringa	SI	SI
4	Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immodificabile.	dd/MM/yyyy	SI	SI
5	Versione	Versione del Documento	Numero intero	SI	
6	Destinatario	Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico (codice fiscale)	Stringa	SI	SI
7	Soggetto produttore	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico	Stringa	SI	SI
8	Oggetto	Metadato funzionale a riassumere brevemente il contenuto del documento (es. la tipologia documentaria)	Stringa	SI	SI
9	NumeroFattura	Numero della fattura	Stringa	SI	SI
10	Produttore	Responsabile del versamento - Generalità	Stringa	NO	
11	Mittente	(Nei casi in cui sia previsto)	Stringa	SI	SI
12	Identificazione del conservatore	Telecom Italia Trust Technologies	Stringa	NO	
13	AnnoFiscale	Anno di competenza fiscale	yyyy	SI	SI
14	Data Emissione	Data di emissione della fattura attiva	dd/MM/yyyy	SI	SI
15	Registro/Sezionale	Codice identificativo univoco per la struttura versante del registro in cui la fattura è registrata	Stringa		SI

### 5.2.7 Tipologia documentaria: Fatture Elettroniche Attive (PA)

N°	Metadato	Descrizione	Formato	Obb	Ric
1	Hash	Impronta del documento	Hash	SI	
2	Nome_Documento	Nome del Documento conservato nel sistema del SP	Stringa	SI	SI
3	UID_Documento	ID del Documento nel sistema del SP	Stringa	SI	SI
4	Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immodificabile.	dd/MM/yyyy	SI	SI
5	Versione	Versione del Documento	Numero intero	SI	
6	Destinatario	Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico (codice fiscale)	Stringa	SI	SI
7	Soggetto produttore	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico	Stringa	SI	SI
8	Oggetto	Metadato funzionale a riassumere brevemente il contenuto del documento (es. tipologia documentaria)	Stringa	SI	SI
9	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 il responsabile della gestione documentale.	Stringa	SI	
10	Mittente	Indicazione del mittente della fattura (indicare il nome, cognome, codice fiscale, P.IVA) [NOTA. In caso di fatture attive basterà il destinatario]	Stringa	SI	SI
11	AnnoFiscale	Anno di competenza fiscale	yyyy	SI	SI

12	DataEmissione	Data di emissione della fattura (coincide con la data del documento)	dd/MM/yyyy	SI	SI
13	RegistroSezionale	Codice identificativo univoco per la struttura versante del registro in cui la fattura è registrata	Stringa	SI	SI
14	IdentificativoSDI	Numero attribuito dal Sistema di Interscambio al file ricevuto	Stringa	SI	SI
15	NumeroDocumento	Numero della fattura	Stringa	SI	SI
16	NomeFile	Nome attribuito al file secondo le regole riportate su Disciplinare Tecnico	Stringa	SI	SI
17	DataOraRicezione	Data e ora in cui il file è stato ricevuto dal Sistema di Interscambio	dd/MM/yyyy/ HH:MM	SI	SI
18	DataOraConsegna	Data e ora in cui il file è stato consegnato dal Sistema di Interscambio	dd/MM/yyyy HH:MM	SI	SI
19	IndiceFascicolo	Identificativo del fascicolo	Stringa	NO	NO
20	Identificazione conservatore	del Telecom Italia Trust Technologies	Stringa	NO	

### 5.2.8 Tipologia documentaria: Fatture Elettroniche Passive (PA)

N°	Metadato	Descrizione	Formato	Obb	Ric
1	Hash	Impronta del documento	Hash	SI	
2	Nome_Documento	Nome del Documento conservato nel sistema del SP	Stringa	SI	SI
3	UID_Documento	ID del Documento nel sistema del SP	Stringa	SI	SI
4	Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso imm modificabile.	dd/MM/yyyy	SI	SI
5	Versione	Versione del Documento	Numero intero	SI	
6	Destinatario	Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico è. [NOTA. Anche se è un metadato obbligatorio, dato che si tratta di fatture passive, <b>non deve essere inserito</b> ]	Stringa		
7	Soggetto produttore	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico	Stringa	SI	SI
8	Oggetto	Metadato funzionale a riassumere brevemente il contenuto del documento (es. la tipologia documentaria)	Stringa	SI	SI
9	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 il responsabile della gestione documentale.	Stringa	SI	
10	Mittente	Indicazione del mittente della fattura (indicare il nome, cognome, codice fiscale, P.IVA)	Stringa	SI	SI
11	Anno	Anno di registrazione	yyyy	SI	SI
12	DataEmissione	Data di emissione della fattura	dd/MM/yyyy	SI	SI
13	RegistroSezionale	Codice del registro/sezionale/bollato IVA di pertinenza	Stringa	SI	SI
14	AOO	Area Organizzativa Omogenea	Stringa	SI	
15	UOR	Unità Operativa Responsabile	Stringa	NO	
16	ResponsabileProcedimento	Nominativo del Responsabile del procedimento	Stringa	NO	
17	NumeroRUF	Codice di registrazione della fattura nel Registro unico delle fatture	Stringa	SI	
18	DataRegistrazioneRUF	Data di registrazione nel Registro unico delle fatture	dd/MM/yyyy	SI	SI
19	CIG	Codice identificativo di gara	Stringa	NO	
20	CUP	Codice unico di Progetto in caso di fatture relative a opere pubbliche, interventi di manutenzione straordinaria	Stringa	NO	
21	Identificazione del conservatore	Telecom Italia Trust Technologies	Stringa	NO	

### 5.2.9 Tipologia documentaria: Fatture Elettroniche Passive (Privati)

N°	Metadato	Descrizione	Formato	Obb	Ric
1	Hash	Impronta del documento	Hash	SI	
2	Nome_Documento	Nome del Documento conservato nel sistema del SP	Stringa	SI	SI
3	UID_Documento	ID del Documento nel sistema del SP	Stringa	SI	SI
4	Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immodificabile.	dd/MM/yyyy	SI	SI
5	Versione	Versione del Documento	Numero intero	SI	
6	Destinatario	Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico <b>[NOTA. Anche se è un metadato obbligatorio, dato che si tratta di fatture passive, non deve essere inserito]</b>	Stringa		
7	Soggetto produttore	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico	Stringa	SI	SI
8	Oggetto	Metadato funzionale a riassumere brevemente il contenuto del documento (esempio: tipologia documentaria)	Stringa	SI	SI
9	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 il responsabile della gestione documentale.	Stringa	SI	
10	Mittente	Indicazione del mittente della fattura (indicare il nome, cognome, codice fiscale, P.IVA)	Stringa	SI	SI
11	AnnoFiscale	Anno fiscale di registrazione nel registro IVA	yyyy	SI	SI
12	DataRegistrazioneIVA	Data di registrazione della fattura nel registro IVA	dd/MM/yyyy	SI	SI
13	DataEmissione	Data di emissione della fattura o del documento contabile equivalente (art. 42 DL 66/2014)	dd/MM/yyyy	SI	
14	RegistroSezionale	Codice del registro/sezionale/bollato IVA di pertinenza	Stringa	SI	
15	Identificazione conservatore del	Telecom Italia Trust Technologies	Stringa	NO	

### 5.2.10 Tipologia documentaria: Libro Giornale (Privati)

N°	Metadato	Descrizione	Formato	Obb	Ric
1	Hash	Impronta del documento	Hash	SI	
2	Nome_Documento	Nome del Documento conservato nel sistema del SP	Stringa	SI	SI
3	UID_Documento	ID del Documento nel sistema del SP	Stringa	SI	SI
4	Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immodificabile.	dd/MM/yyyy	SI	SI
5	Versione	Versione del Documento	Numero intero	SI	
6	Destinatario	Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico (codice fiscale)	Stringa	SI	SI
7	Soggetto produttore	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico	Stringa	SI	SI
8	Oggetto	Metadato funzionale a riassumere brevemente il contenuto del documento (es. tipologia documentaria)	Stringa	SI	SI
9	Produttore	Responsabile del versamento - Generalità	Stringa	SI	
10	Mittente	(nei casi in cui sia previsto)	Stringa	NO	
11	Identificazione del conservatore	Telecom Italia Trust Technologies	Stringa	NO	
12	AnnoFiscale	Anno di competenza fiscale	yyyy	SI	SI

13	Data Emissione	Data di inizio emissione del Libro Giornale	dd/MM/yyyy	NO	SI
14	Data termine Emissione	Data di fine emissione del Libro Giornale	dd/MM/yyyy	NO	

### 5.2.11 Tipologia documentaria: Documento di Trasporto

N°	Metadato	Descrizione	Formato	Obb	Ric
1	Hash	Impronta del documento	Hash	SI	
2	Nome_Documento	Nome del Documento conservato nel sistema del SP	Stringa	SI	SI
3	UID_Documento	ID del Documento nel sistema del SP	Stringa	SI	SI
4	Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immutabile.	dd/MM/yyyy	SI	SI
5	Versione	Versione del Documento	Numero intero	SI	
6	Destinatario	Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico (codice fiscale)	Stringa	SI	SI
7	Soggetto produttore	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico	Stringa	SI	SI
8	Oggetto	Metadato funzionale a riassumere brevemente il contenuto del documento (es. tipologia documentaria)	Stringa	SI	SI
9	Produttore	Responsabile del versamento - Generalità	Stringa	NO	
10	Mittente	(Nei casi in cui sia previsto)	Stringa	NO	
11	Identificazione del conservatore	Telecom Italia Trust Technologies	Stringa	NO	
12	Vettore		Stringa	SI	
13	AnnoFiscale	Anno di competenza fiscale	yyyy	SI	SI
14	Tipologia documentaria	Documento di trasporto,	Stringa	NO	
15	Codice Fiscale	codice fiscale, P.IVA	Stringa	SI	

### 5.2.12 Tipologia documentaria: Libro Magazzino (Privati)

N°	Metadato	Descrizione	Formato	Obb	Ric
1	Hash	Impronta del documento	Hash	SI	
2	Nome_Documento	Nome del Documento conservato nel sistema del SP	Stringa	SI	SI
3	UID_Documento	ID del Documento nel sistema del SP	Stringa	SI	SI
4	Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immutabile.	dd/MM/yyyy	SI	SI
5	Versione	Versione del Documento	Numero intero	SI	
6	Destinatario	Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico <b>[NOTA. Anche se è un metadato obbligatorio, dato che in questo caso non esiste, non deve essere inserito]</b>			
7	Soggetto produttore	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico	Stringa	SI	SI
8	Oggetto	Metadato funzionale a riassumere brevemente il contenuto del documento (es. tipologia documentaria)	Stringa	SI	SI
9	Produttore	Responsabile del versamento - Generalità	Stringa	NO	
10	Mittente	(Nei casi in cui sia previsto)	Stringa	NO	
11	Identificazione del conservatore	Telecom Italia Trust Technologies	Stringa	NO	

12	AnnoFiscale	Anno fiscale di riferimento	yyyy	SI	SI
13	Mese	Mese di riferimento	Stringa	SI	SI
14	DataPrimaRegistrazione		dd/MM/yyyy	SI	SI
15	DataUltimaRegistrazione		dd/MM/yyyy	SI	SI
16	DataDiCarico		dd/MM/yyyy	SI	SI

### 5.2.13 Tipologia documentaria: Verbali Esame Universitario

N°	Metadato	Descrizione	Formato	Obb	Ric
1	Hash	Impronta del documento	Hash	SI	
2	Nome_Documento	Nome del Documento conservato nel sistema del SP	Stringa	SI	SI
3	UID_Documento	ID del Documento nel sistema del SP	Stringa	SI	SI
4	Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso imm modificabile.	dd/MM/yyyy	SI	SI
5	Versione	Versione del Documento	Numero intero	SI	
6	Destinatario	Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico (codice fiscale)	Stringa	SI	SI
7	Soggetto produttore	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico	Stringa	SI	SI
8	Oggetto	Metadato funzionale a riassumere brevemente il contenuto del documento (es. tipologia documentaria)	Stringa	SI	SI
9	Area	Facoltà o Area (Codice o Nome)	Stringa	SI	SI
10	Cod_Corso	Codice del corso di studio	Stringa	NO	
11	Cod_Ins	Codice Insegnamento	Stringa	NO	
12	Cod_Esame	Identificativo del singolo esame	Stringa	NO	
13	Cod_Appello	Identificativo del singolo appello	Stringa	NO	

### 5.2.14 Tipologia documentaria: Contratti

N°	Metadato	Descrizione	Formato	Obb	Ric
1	Hash	Impronta del documento	Hash	SI	
2	Nome_Documento	Nome del Documento conservato nel sistema del SP	Stringa	SI	SI
3	UID_Documento	ID del Documento nel sistema del SP	Stringa	SI	SI
4	Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso imm modificabile.	dd/MM/yyyy	SI	SI
5	Versione	Versione del Documento	Numero intero	SI	
6	Destinatario	Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico (codice fiscale)	Stringa	SI	SI
7	Soggetto produttore	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico	Stringa	SI	SI
8	Oggetto	Metadato funzionale a riassumere brevemente il contenuto del documento (es. tipologia documentaria)	Stringa	SI	SI
9	Data del Documento	Data del Documento	dd/MM/yyyy	SI	SI

10	Data_Contabile	Data contabile	dd/MM/yyyy	SI	SI
11	Cod_BU	Dipartimento, ente o settore	Stringa	SI	SI
12	Cod_Archivio	Rif. Archivio del Cliente	Stringa	NO	
13	Tipo_Documento	Rif. Archivio del Cliente	Stringa	NO	
14	Oggetto_Doc	secondo l'esigenza	Stringa	NO	
15	Cod_Rapporto	Rif. Archivio del Cliente	Stringa	SI	SI
16	Cod_SottoRapp	secondo l'esigenza	Stringa	NO	
17	Cod_Cliente	Rif. Archivio del Cliente	Stringa	NO	
18	Cod_Promotore	Rif. Archivio del Cliente	Stringa	NO	
19	Cod_Fornitore	Rif. Archivio del Cliente	Stringa	NO	

### 5.2.15 Tipologia documentaria: Contabili di sportello

N°	Metadato	Descrizione	Formato	Obb	Ric
1	Hash	Impronta del documento	Hash	SI	
2	Nome_Documento	Nome del Documento conservato nel sistema del SP	Stringa	SI	SI
3	UID_Documento	ID del Documento nel sistema del SP	Stringa	SI	SI
4	Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immodificabile.	dd/MM/yyyy	SI	SI
5	Versione	Versione del Documento	Numero intero	SI	
6	Destinatario	Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico (codice fiscale)	Stringa	SI	SI
7	Soggetto produttore	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico	Stringa	SI	SI
8	Oggetto	Metadato funzionale a riassumere brevemente il contenuto del documento (es. tipologia documentaria)	Stringa	SI	SI
9	Data_Contabile	Data contabile dell'operazione	dd/MM/yyyy	SI	SI
10	ABI_BANCA_OP	ABI banca da cui è stata fatta l'operazione	Stringa	SI	
11	Cod_Operazione	Codice/Tipo Operazione	Stringa	SI	SI
12	Stato_Doc	Stato del documento	Stringa	NO	
13	Cod_Rapporto	Rapporto sul quale è stata fatta l'operazione	Stringa	SI	
14	Tipo_Rapporto	Tipo rapporto	Stringa	NO	
15	CF_PIVA_CL	Codice fiscale di chi firma	Stringa	SI	SI
16	Cod_Filiale_Rapp	Filiale a cui appartiene il rapporto	Stringa	NO	
17	NDG_Cliente	NDG del cliente	Stringa	NO	
18	Postazione_Op	Applicazione/postazione operazione	Stringa	NO	
19	Matricola_Op	Matricola operatore	Stringa	NO	

### 5.2.16 Tipologia documentaria: Registro Giornaliero di Protocollo

N°	Metadato	Descrizione	Formato	Obb	Ric
1	Hash	Impronta del documento	Hash	SI	
2	Nome_Documento	Nome del Documento conservato nel sistema del SP	Stringa	SI	SI
3	UID_Documento	ID del Documento nel sistema del SP	Stringa	SI	SI
4	Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immodificabile.	dd/MM/yyyy	SI	SI

5	Versione	Versione del Documento	Numero intero	SI	
6	Destinatario	Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico (codice fiscale)	Stringa	SI	SI
7	Soggetto produttore	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico	Stringa	SI	SI
8	Oggetto	Metadato funzionale a riassumere brevemente il contenuto del documento (es. tipologia documentaria)	Stringa	SI	SI
9	Cod_IPA	Identificativo dell'amministrazione	Stringa	SI	SI
10	Amministrazione	Denominazione amministrazione	Stringa	SI	SI
11	Cod_AOO	Area organizzativa omogenea	Stringa	SI	SI
12	Responsabile	Responsabile della gestione documentale o Responsabile del servizio per la tenuta del protocollo informatico - Nome, Cognome, Codice fiscale	Stringa	SI	
13	Numero	Numero progressivo del registro	Numero intero	SI	SI
14	Anno	Anno del registro giornaliero di protocollo	Numero intero	SI	SI
15	Soggetto produttore2	Operatore che ha prodotto il Registro - Nome, Cognome, Codice fiscale	Stringa	NO	NO
16	Numero registrazione prima	Numero della prima registrazione effettuata sul registro	Numero intero	NO	NO
17	Numero registrazione ultima	Numero dell'ultima registrazione effettuata sul registro	Numero intero	NO	NO
18	Data registrazione prima	Data della prima registrazione effettuata sul registro	dd/MM/yyyy	NO	NO
19	Data registrazione ultima	Data dell'ultima registrazione effettuata sul registro	dd/MM/yyyy	NO	NO
20	Codice registro	Codice identificativo del registro	Stringa	NO	NO

Rif. Istruzioni per il registro giornaliero di protocollo di AgID - PRODUZIONE E CONSERVAZIONE DEL REGISTRO GIORNALIERO DI PROTOCOLLO - documento di marzo 2015

[http://www.agid.gov.it/sites/default/files/documenti\\_indirizzo/istruzioni\\_per\\_la\\_produzione\\_e\\_conservazione\\_registro\\_giornaliero\\_di\\_protocollo.pdf](http://www.agid.gov.it/sites/default/files/documenti_indirizzo/istruzioni_per_la_produzione_e_conservazione_registro_giornaliero_di_protocollo.pdf)

## 5.2.17 Tipologia documentaria: Determina

N°	Metadato	Descrizione	Formato	Obb	Ric
1	Hash	Impronta del documento	Hash	SI	
2	Nome_Documento	Nome del Documento conservato nel sistema del SP	Stringa	SI	SI
3	UID_Documento	ID del Documento nel sistema del SP	Stringa	SI	SI
4	Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immutabile.	dd/MM/yyyy	SI	SI
5	Versione	Versione del Documento	Numero intero	SI	
6	Destinatario	Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico (codice fiscale)	Stringa	SI	SI
7	Soggetto produttore	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico	Stringa	SI	SI
8	Oggetto	Metadato funzionale a riassumere brevemente il contenuto del documento (es. tipologia documentaria)	Stringa	SI	SI

9	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 il responsabile della gestione documentale.	Stringa	SI	
10	Anno	Anno di repertorio	yyyy	SI	
11	Numero	Numero intero (numero di registrazione nel repertorio)	Stringa	SI	SI
12	Data	Data della determinazione	dd/MM/yyyy	SI	SI
13	Autore	Autore del documento: nome e cognome del Dirigente o responsabile firmatario (nel caso di delega indicare il soggetto delegante per conto del quale il firmatario opera)	Stringa	SI	SI
14	CodiceUOR (unità operativa responsabile)	Nei casi in cui è previsto		NO	
15	CodiceIdentificativoAOO	Nei casi in cui sia previsto		SI	
16	Responsabile procedimento del	Responsabile del procedimento amministrativo		NO	
17	Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immutabile.	dd/MM/yyyy	SI	
18	Identificazione conservatore del	Telecom Italia Trust Technologies	Stringa	NO	
19	FirmatarioEnte	Nome del firmatario della determina per conto dell'ente	Stringa	NO	
20	RuoloFirmatario	Ruolo o qualifica del firmatario della determinazione (può essere specificato eventuale funzione di delega)	Stringa	NO	

## 5.2.18 Tipologia documentaria: PEC

N°	Metadato	Descrizione	Formato	Obb	Ric
1	Hash	Impronta del documento	Hash	SI	
2	Nome_Documento	Nome del Documento conservato nel sistema del SP	Stringa	SI	SI
3	UID_Documento	ID del Documento nel sistema del SP	Stringa	SI	SI
4	Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immutabile. <b>[NOTA. Anche se questo metadato è obbligatorio, poiché in questo caso coincide con la data del messaggio PEC, non deve essere valorizzato]</b>			
5	Destinatario	Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico (codice fiscale)	Stringa	SI	SI
6	Soggetto produttore	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico	Stringa	SI	SI
7	Oggetto	Metadato funzionale a riassumere brevemente il contenuto del documento : campo oggetto del messaggio PEC	Stringa	SI	SI
8	Message_ID	Il codice identificativo univoco dei messaggi correlati generati (ricevute, errori, ecc.) (Message-ID cfr. 6.3 delle Regole Tecniche PEC - Allegato al DM 2 novembre 2005)	STRING	NO	
9	Data	Data del messaggio PEC	dd/MM/yyyy	SI	SI
10	ConsegnatoA	Solo per ricevute di consegna ricevute : indica il destinatario a cui è stato consegnato il messaggio PEC spedito.	STRING	NO	
11	mailbox	Casella di posta elettronica a cui è afferente il messaggio PEC (mittente per messaggi spediti o destinataria per messaggi ricevuti)	STRING	NO	
12	Tipo_Messaggio	Tipologia del messaggio PEC (Busta di Trasporto, Ricevuta, Avviso)	STRING	NO	
13	Mittente	Indirizzo email del mittente del messaggio PEC	STRING	NO	SI
14	RIFMSGID	Il codice identificativo univoco assegnato al messaggio originale (X-Riferimento-Message-ID cfr. 6.3 delle Regole Tecniche PEC - Allegato al DM 2 novembre 2005)	STRING	NO	SI

15	Destinatari	Indirizzo email del/i destinatario/i del messaggio PEC	STRING	NO	SI
----	-------------	--	--------	----	----

## 5.2.19 Tipologia documentaria: Libri Contabili

Di seguito vengono descritte le tipologie documentarie dei Libri Contabili.

### 5.2.19.1 Tipologia documentaria: Libro Cespiti Privati

N°	Metadato	Descrizione	Formato	Obb	Ric
1	Hash	Impronta del documento	Hash	SI	
2	Nome_Documento	Nome del Documento conservato nel sistema del SP	Stringa	SI	SI
3	UID_Documento	ID del Documento nel sistema del SP	Stringa	SI	SI
4	Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immodificabile.	dd/MM/yyyy	SI	SI
5	Versione	Versione del Documento	Numero intero	SI	
6	Destinatario	Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico	Stringa	SI	SI
7	Soggetto produttore	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico	Stringa	SI	SI
8	Oggetto	Metadato funzionale a riassumere brevemente il contenuto del documento (es. tipologia documentaria)	Stringa	SI	SI
9	Produttore	Responsabile del versamento - Generalità	Stringa	SI	
10	Mittente	(Nei casi in cui sia previsto)	Stringa	NO	
11	Identificazione del soggetto conservatore	Telecom Italia Trust Technologies	Stringa	SI	
12	AnnoFiscale	Anno di competenza fiscale	AAAA	SI	SI
13	Data Emissione	Data di inizio emissione del Libro cespiti. A titolo di esempio: 01/01/2012	dd/MM/yyyy	NO	
14	Data termine Emissione	Data di fine emissione del Libro cespiti. A titolo di esempio: 31/12/2012	dd/MM/yyyy	NO	
15	ProgressivoInizio	Numero prima pagina	Numero intero	NO	
16	ProgressivoFine	Numero ultima pagina	Numero intero	NO	

### 5.2.19.2 Tipologia documentaria: Libro Inventari (privati)

N°	Metadato	Descrizione	Formato	Obb	Ric
1	Hash	Impronta del documento	Hash	SI	
2	Nome_Documento	Nome del Documento conservato nel sistema del SP	Stringa	SI	SI
3	UID_Documento	ID del Documento nel sistema del SP	Stringa	SI	SI
4	Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immodificabile.	dd/MM/yyyy	SI	SI
5	Versione	Versione del Documento	Numero intero	SI	
6	Destinatario	Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico <b>[NOTA. Anche se è un metadato obbligatorio, dato che in questo caso non esiste, non deve essere inserito]</b>			

7	Soggetto produttore	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico	Stringa	SI	SI
8	Oggetto	Metadato funzionale a riassumere brevemente il contenuto del documento (es. tipologia documentaria)	Stringa	SI	SI
9	Produttore	Responsabile del versamento - Generalità	Stringa	SI	
10	Mittente	(Nei casi in cui sia previsto) <b>[NOTA. Poiché in questo caso il mittente coincide con il Soggetto Produttore questo metadato può non essere inserito]</b>	Stringa	NO	
11	Identificazione del soggetto conservatore	Telecom Italia Trust Technologies	Stringa	SI	
12	AnnoFiscale	Anno di competenza fiscale	aaaa	SI	
13	Data Emissione	Data di inizio emissione del Libro inventari. A titolo di esempio: 2012-01-01	dd/MM/yyyy	NO	
14	Data termine Emissione	Data di fine emissione del Libro inventari. A titolo di esempio: 2012-12-31	dd/MM/yyyy	NO	
15	ProgressivoInizio	Numero prima pagina	Numero intero	NO	
16	ProgressivoFine	Numero ultima pagina	Numero intero	NO	

**NOTA.** Nel caso questa DA debba essere utilizzata da una PA andranno considerati anche i metadati di profilo archivistico

### 5.2.19.3 Tipologia documentaria: Libro Mastro (privati)

N°	Metadato	Descrizione	Formato	Obb	Ric
1	Hash	Impronta del documento	Hash	SI	
2	Nome_Documento	Nome del Documento conservato nel sistema del SP	Stringa	SI	SI
3	UID_Documento	ID del Documento nel sistema del SP	Stringa	SI	SI
4	Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immodificabile.	dd/MM/yyyy	SI	SI
5	Versione	Versione del Documento	Numero intero	SI	
6	Destinatario	Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico	Stringa	SI	SI
7	Soggetto produttore	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico	Stringa	SI	SI
8	Oggetto	Metadato funzionale a riassumere brevemente il contenuto del documento (es. tipologia documentaria)	Stringa	SI	SI
9	Produttore	Responsabile del versamento - Generalità	Stringa	SI	
10	Mittente	(Nei casi in cui sia previsto)	Stringa	NO	
11	Identificazione del soggetto conservatore	Telecom Italia Trust Technologies	Stringa	SI	
12	DataDocumento	Coincide con le data emissione	dd/MM/yyyy	SI	
13	AnnoFiscale	Anno di competenza fiscale	aaaa	SI	
14	Data Emissione	Data di inizio emissione del Libro Mastro. A titolo di esempio: 2012-01-01	dd/MM/yyyy	NO	
15	Data termine Emissione	Data di fine emissione del Libro Mastro. A titolo di esempio: 2012-12-31	dd/MM/yyyy	NO	
16	ProgressivoInizio	Numero della prima pagina	Numero intero	SI	
17	ProgressivoFine	Numero dell'ultima pagina	Numero intero	SI	

**NOTA.** Nel caso questa DA debba essere utilizzata da una PA andranno considerati anche i metadati di profilo archivistico

### 5.2.19.4 Tipologia documentaria: Registro IVA (privati)

N°	Metadato	Descrizione	Formato	Obb	Ric
1	Hash	Impronta del documento	Hash	SI	
2	Nome_Documento	Nome del Documento conservato nel sistema del SP	Stringa	SI	SI
3	UID_Documento	ID del Documento nel sistema del SP	Stringa	SI	SI
4	Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immodificabile.	dd/MM/yyyy	SI	SI
5	Versione	Versione del Documento	Numero intero	SI	
6	Destinatario	Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico (codice fiscale)	Stringa	SI	SI
7	Soggetto produttore	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico	Stringa	SI	SI
8	Oggetto	Metadato funzionale a riassumere brevemente il contenuto del documento (Es. Tipologia documentaria)	Stringa	SI	SI
9	Produttore	Responsabile del versamento - Generalità	Stringa	SI	
10	Mittente	(Nei casi in cui sia previsto)	Stringa	NO	
11	Identificazione del soggetto conservatore	Telecom Italia Trust Technologies	Stringa	SI	
12	Anno	Anno di competenza fiscale	AAAA	SI	
13	Data	Data di emissione	dd/MM/yyyy	NO	
14	Data termine Emissione	Data di fine emissione del Registro IVA A titolo di esempio: 2012-12-31	dd/MM/yyyy	NO	
15	Numero registrazione prima		Stringa	NO	
16	Numero registrazione ultima		Stringa	NO	

**NOTA.** Nel caso questa DA debba essere utilizzata da una PA andranno considerati anche i metadati di profilo archivistico

### 5.2.19.5 Tipologia documentaria: Libro unico del Lavoro

N°	Metadato	Descrizione	Formato	Obb	Ric
1	Hash	Impronta del documento	Hash	SI	
2	Nome_Documento	Nome del Documento conservato nel sistema del SP	Stringa	SI	SI
3	UID_Documento	ID del Documento nel sistema del SP	Stringa	SI	SI
4	Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immodificabile.	dd/MM/yyyy	SI	SI
5	Versione	Versione del Documento	Numero intero	SI	
6	Destinatario	Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico	Stringa	SI	SI
7	Soggetto produttore	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico	Stringa	SI	SI
8	Oggetto	Metadato funzionale a riassumere brevemente il contenuto del documento (es. Tipologia documentaria)	Stringa	SI	SI
9	AnnoRetribuzione	Anno a cui si riferisce la retribuzione	Anno (AAAA)	SI	SI
10	MeseRetribuzione	Mese a cui si riferisce la retribuzione	Stringa	SI	SI

11	Produttore	Responsabile del versamento - Generalità	Stringa	SI	
12	Mittente	Nome, Cognome, Codice Fiscale/P.IVA. Soggetto che ha l'autorità a inviare il documento (in questo caso la società che fa le buste paga).	Stringa	NO	
13	Data di nascita	Data di nascita del dipendente	AAAA/MM/GG	NO	
14	Matricola	Matricola del dipendente	Stringa	NO	SI
15	Numero	Numero di registrazione del cedolino nel relativo registro	Numero	SI	
16	CodiceIdentificativoRegistro	Denominazione o codice del registro in cui sono registrati i cedolini stipendiali	Stringa	SI	
17	Identificazione conservatore del	Telecom Italia Trust Technologies	Stringa	SI	

## 5.2.20 Tipologia documentaria: Ricevute F24 e F23 Privati

N°	Metadato	Descrizione	Formato	Obb	Ric
1	Hash	Impronta del documento	Hash	SI	
2	Nome_Documento	Nome del Documento conservato nel sistema del SP	Stringa	SI	SI
3	UID_Documento	ID del Documento nel sistema del SP	Stringa	SI	SI
4	Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immutabile.	dd/MM/yyyy	SI	SI
5	Versione	Versione del Documento	Numero intero	SI	
6	Destinatario	Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico	Stringa	SI	SI
7	Soggetto produttore	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico	Stringa	SI	SI
8	Oggetto	Metadato funzionale a riassumere brevemente il contenuto del documento (es. tipologia documentaria)	Stringa	SI	SI
9	Produttore	Responsabile del versamento - Generalità	Stringa	SI	
10	Mittente	Indicazione del mittente della fattura (indicare il nome, cognome, codice fiscale, P.IVA) (Nei casi in cui sia previsto)	Stringa	SI	
11	AnnoFiscale	Anno di competenza fiscale	AAAA	SI	
12	Data Emissione	Data di emissione della ricevuta	dd/MM/yyyy	SI	
13	NumeroDocumento	Numero della ricevuta	Stringa	NO	
14	NumeroModello	Numero identificativo progressivo del Modello F24 cui si rifà la ricevuta	Stringa	NO	
15	AnnoDiCompetenza	Anno di competenza del Modello F24/F23 cui si rifà la ricevuta	Stringa	NO	
16	MeseDiCompetenza	Mese di competenza del Modello F24/f23 cui si rifà la ricevuta	Stringa	NO	
17	Conservatore	Il soggetto sul quale ricade la responsabilità della conservazione e valorizzazione dell'archivio del complesso archivistico descritto.	Stringa	NO	

## 5.2.21 Tipologia documentaria: Ricevute F24 e F23 PA

N°	Metadato	Descrizione	Formato	Obb	Ric
1	Hash	Impronta del documento	Hash	SI	
2	Nome_Documento	Nome del Documento conservato nel sistema del SP	Stringa	SI	SI
3	UID_Documento	ID del Documento nel sistema del SP	Stringa	SI	SI
4	Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immutabile.	dd/MM/yyyy	SI	SI

5	Versione	Versione del Documento	Numero intero	SI	
6	Destinatario	Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico	Stringa	SI	SI
7	Soggetto produttore	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico	Stringa	SI	SI
8	Oggetto	Metadato funzionale a riassumere brevemente il contenuto del documento (es. Tipologia documentaria)	Stringa	SI	SI
9	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 il responsabile della gestione documentale.	Stringa	SI	
10	Mittente	Indicazione del mittente della fattura (indicare il nome, cognome, codice fiscale, P.IVA) (Nei casi in cui sia previsto)	Stringa	NO	
11	AnnoFiscale	Anno di competenza fiscale	AAAA	SI	
12	Data Emissione	Data emissione della ricevuta	dd/MM/yyyy	NO	
13	NumeroDocumento	Numero della ricevuta	Stringa	NO	
14	NumeroModello	Numero identificativo progressivo del Modello F24 cui si rifà la ricevuta	Stringa	NO	
15	AnnoDiCompetenza	Anno di competenza del Modello F24 cui si rifà la ricevuta	Stringa	NO	
16	MeseDiCompetenza	Mese di competenza del Modello F24 cui si rifà la ricevuta	Stringa	NO	
17	CodiceUOR (unità operativa responsabile)	Nei casi in cui è previsto	Stringa	NO	
18	CodicIdentificativoAOO	Nei casi in cui sia previsto	Stringa	SI	
19	ResponsabileProcedimentoAmministrativo	Responsabile del procedimento amministrativo	Stringa	NO	
20	Conservatore	Il soggetto sul quale ricade la responsabilità della conservazione e valorizzazione dell'archivio del complesso archivistico descritto.	Stringa	NO	

## 5.2.2 Tipologia documentaria: Ordini Privati

N°	Metadato	Descrizione	Formato	Obb	Ric
1	Hash	Impronta del documento	Hash	SI	
2	Nome_Documento	Nome del Documento conservato nel sistema del SP	Stringa	SI	SI
3	UID_Documento	ID del Documento nel sistema del SP	Stringa	SI	SI
4	Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immutabile.	dd/MM/yyyy	SI	SI
5	Versione	Versione del Documento	Numero intero	SI	
6	Destinatario	Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico	Stringa	SI	SI
7	Soggetto produttore	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico	Stringa	SI	SI
8	Oggetto	Metadato funzionale a riassumere brevemente il contenuto del documento (es. Tipologia documentaria)	Stringa	SI	SI
9	Produttore	Responsabile del versamento - Generalità	Stringa	SI	
10	Mittente	Indicazione del mittente della fattura (indicare il nome, cognome, codice fiscale, P.IVA) (Nei casi in cui sia previsto)	Stringa	SI	
11	AnnoFiscale	Anno di competenza fiscale	AAAA	SI	
12	DataEmissione	Data di emissione del documento	dd/MM/yyyy	SI	
13	NumeroDocumento	Numero dell'ordine	Stringa		

14	Conservatore	Il soggetto sul quale ricade la responsabilità della conservazione e valorizzazione dell'archivio del complesso archivistico descritto.	Stringa	NO	
----	--------------	---	---------	----	--

### 5.2.23 Tipologia documentaria: Ordini PA

Di seguito vengono descritte le tipologie documentarie degli ordini per la Pubblica Amministrazione

#### 5.2.23.1 Tipologia documentaria: Mandati di pagamento

N°	Metadato	Descrizione	Formato	Obb	Ric
1	Hash	Impronta del documento	Hash	SI	
2	Nome_Documento	Nome del Documento conservato nel sistema del SP	Stringa	SI	SI
3	UID_Documento	ID del Documento nel sistema del SP	Stringa	SI	SI
4	Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immutabile.	dd/MM/yyyy	SI	SI
5	Versione	Versione del Documento	Numero intero	SI	
6	Destinatario	Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico	Stringa	SI	SI
7	Soggetto produttore	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico	Stringa	SI	SI
8	Oggetto	Metadato funzionale a riassumere brevemente il contenuto del documento (es. tipologia documentaria)	Stringa	SI	SI
9	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 il responsabile della gestione documentale.	Stringa	SI	
10	Mittente	Indicazione del mittente (indicare il nome, cognome, codice fiscale, P.IVA) (Nei casi in cui sia previsto)	Stringa		
11	AnnoFiscale	Anno di competenza fiscale	AAAA	SI	
12	Data	Data del mandato di pagamento	AA/MM/GG	SI	
13	Repertorio	Indicare il registro di repertorio di riferimento	Stringa	SI	
14	Autore	Autore del documento: nome e cognome del Dirigente o responsabile firmatario (nel caso di delega indicare il soggetto delegante per conto del quale il firmatario opera).	Stringa	NO	
15	CodiceUOR (unità operativa responsabile)	Nei casi in cui è previsto	Stringa	NO	
16	CodiceIdentificativoAOO	Nei casi in cui sia previsto	Stringa	SI	
17	ResponsabileProcedimentoAmministrativo	Responsabile del procedimento amministrativo	Nome; alfanumerico 40 caratteri;	NO	
18	Conservatore	Il soggetto sul quale ricade la responsabilità della conservazione e valorizzazione dell'archivio del complesso archivistico descritto.	Stringa	NO	

#### 5.2.23.2 Tipologia documentaria: Ordini di riscossione / Reversali di incasso

N°	Metadato	Descrizione	Formato	Obb	Ric
1	Hash	Impronta del documento	Hash	SI	

2	Nome_Documento	Nome del Documento conservato nel sistema del SP	Stringa	SI	SI
3	UID_Documento	ID del Documento nel sistema del SP	Stringa	SI	SI
4	Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immodificabile.	dd/MM/yyyy	SI	SI
5	Versione	Versione del Documento	Numero intero	SI	
6	Destinatario	Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico	Stringa	SI	SI
7	Soggetto produttore	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico	Stringa	SI	SI
8	Oggetto	Metadato funzionale a riassumere brevemente il contenuto del documento (es. Tipologia documentaria)	Stringa	SI	SI
9	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 il responsabile della gestione documentale.	Stringa	SI	
10	Mittente	Indicazione del mittente della fattura (indicare il nome, cognome, codice fiscale, P.IVA) (Nei casi in cui sia previsto)	Stringa		
11	AnnoFiscale	Anno di competenza fiscale	AAAA	SI	
12	Data	Data del reversale	AA/MM/GG	SI	
13	Repertorio	Indicare il registro di repertorio di riferimento	Stringa	SI	
14	Autore	Autore del documento: nome e cognome del Dirigente o responsabile firmatario (nel caso di delega indicare il soggetto delegante per conto del quale il firmatario opera). Informazione obbligatoria nel caso sia disponibile.	Stringa	NO	
15	CodiceUOR (unità operativa responsabile)	Nei casi in cui è previsto	Stringa	NO	
16	CodiceIdentificativoAOO	Nei casi in cui sia previsto	Stringa	SI	
17	ResponsabileProcedimentoAmministrativo	Responsabile del procedimento amministrativo	Nome: alfanumerico 40 caratteri;	NO	
18	Conservatore	Il soggetto sul quale ricade la responsabilità della conservazione e valorizzazione dell'archivio del complesso archivistico descritto.	Stringa	NO	

### 5.2.23.3 Tipologia documentaria: Ordine diretto d'acquisto PA tramite MEPA

N°	Metadato	Descrizione	Formato	Obb	Ric
1	Hash	Impronta del documento	Hash	SI	
2	Nome_Documento	Nome del Documento conservato nel sistema del SP	Stringa	SI	SI
3	UID_Documento	ID del Documento nel sistema del SP	Stringa	SI	SI
4	Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immodificabile.	dd/MM/yyyy	SI	SI
5	Versione	Versione del Documento	Numero intero	SI	
6	Destinatario	Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico	Stringa	SI	SI
7	Soggetto produttore	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico	Stringa	SI	SI
8	Oggetto	Metadato funzionale a riassumere brevemente il contenuto del documento (es. Tipologia documentaria)	Stringa	SI	SI

9	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 il responsabile della gestione documentale.	Stringa	SI	
10	Mittente	Indicazione del mittente della fattura (indicare il nome, cognome, codice fiscale, P.IVA) (Nei casi in cui sia previsto)	Stringa		
11	AnnoFiscale	Anno di competenza fiscale	AAAA	SI	
12	Data	Data creazione ordine	AA/MM/GG	SI	
13	CodiceUOR (unità operativa responsabile)	Nei casi in cui è previsto	Stringa	NO	
14	CodiceIdentificativoAOO	Nei casi in cui sia previsto	Stringa	SI	
15	CIG	Codice identificativo di gara	Stringa		
16	CUP	Codice unico di Progetto	Stringa		
17	ResponsabileProcedimentoAmministrativo	Responsabile del procedimento amministrativo	Stringa	NO	
18	Conservatore	Il soggetto sul quale ricade la responsabilità della conservazione e valorizzazione dell'archivio del complesso archivistico descritto.	Stringa	NO	

## 5.2.24 Tipologia documentaria: Cedolini

N°	Metadato	Descrizione	Formato	Obb	Ric
1	Hash	Impronta del documento	Hash	SI	
2	Contesto	Piano di Classificazione (Nei casi in cui è previsto. Indicare il titolo e classe, e il numero di fascicolo cui appartiene l'unità documentaria. È possibile valorizzare solo la Classifica e non i campi descrittivi del Fascicolo nel caso l'Unità documentaria sia stata solo classificata e non fascicolata. (Si ricorda che la classificazione è un'operazione necessaria richiesta dalla norma DPR 445/2000 ).	Stringa	NO	NO
3	UID_Documento	ID del Documento nel sistema del SP	Stringa	SI	SI
4	Data di chiusura	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso imm modificabile.	dd/MM/yyyy	SI	SI
5	Soggetto produttore	Il soggetto che ha l'autorità e la competenza a produrre il documento informatico	Stringa	SI	
6	DataDocumento	Data di inserimento	dd/MM/yyyy	SI	SI
7	Oggetto	Metadato funzionale a riassumere brevemente il contenuto del documento (es. Tipologia documentaria)	Stringa	SI	SI
8	Mese	Mese di riferimento a seconda del Tipo Doc.	Numero intero	NO	SI
9	Anno	Anno di riferimento a seconda del Tipo Doc.	yyyy	SI	SI
10	Matricola	Numero di matricola del cedolino	Numero intero	SI	SI
11	Ruolo	(secondo l'esigenza: Assegni di ricerca, Titolari di assegno di ricerca, Docenti a contratto, Collaboratori, Compensi imponibili ruoli esenti NO DETR, Professori a contratto, Dirigenti a tempo indet., Dirigenti a contratto, Eredi, Lettore di madre lingua t.indet., Non docenti comandati in ingresso, PTA T.I. ex- INPDAP, Addetti ufficio stampa INPGI t. ind., Non docenti a tempo det. Ex-INPDAP, Personale T.A. CPDEL ENPAS, Non docenti a tempo det. INPS, Personale non docente CPDEL, Professori Associati, Professore Straord. a tempo determinato, Professori Ordinari, Professionisti, Personale no adempimenti, Ricercatori Legge 240/10 - t.det., Ricercatori a tempo det., Ricercatori Universitari t.i., Supplenti Docenti (soggetti a contrib.))	Stringa	SI	SI
12	Nome Cognome	Generalità del dipendente	Stringa	SI	SI
13	Cod. Fiscale Dipendente	Codice fiscale del dipendente	Stringa	SI	SI

14	Tipo Documento	Retribuzione e compensi	Stringa	SI	SI
15	Cod. Archivio	Rif. Archivio del Cliente	Stringa	NO	SI
16	DataInvioConservazione	Data invio al sistema di conservazione	dd/MM/yyyy	SI	SI

### 5.2.25 Tipo documento: DA Custom

Ogni offerta standard include la scelta di una tipologia documentaria tra quelle sopra riportate.

Ogni Cliente è libero di chiedere l'integrazione di tale offerta con l'opzione di disporre di più DA o richiedendo la creazione di una DA Custom personalizzata. In questo caso tutta l'offerta è considerata custom e richiederà quindi la richiesta di fattibilità al gruppo competente ed almeno un incontro tecnico per la definizione dei dettagli richiesti.

## 6 Definizione degli oggetti "conservabili"

Ai fini della conservazione sono stati identificati formati che possano garantire la leggibilità e la reperibilità del documento informatico nel suo ciclo di vita.

La scelta tra i formati è stata effettuata seguendo le disposizioni della normativa relativa al DPCM 3 dicembre 2013 sulle regole tecniche in materia di sistema di conservazione, pubblicato in GU n.59 del 12-3-2014 - Suppl. Ordinario n. 20, con riferimento particolare all'allegato sui formati.

Le **caratteristiche** che sono state considerate nella scelta sono:

#### 1. Apertura

- Conforme a specifiche pubbliche, cioè disponibili a chiunque abbia interesse ad utilizzare quel formato.
- Gli organismi di standardizzazione internazionali considerati dalla normativa sono ISO e ETSI.

#### 2. Sicurezza

- La capacità di essere immune dall'inserimento di codice maligno.

#### 3. Portabilità

- La facilità con cui i formati possano essere usati su piattaforme diverse, sia dal punto di vista dell'hardware che del software
  - per esportare i propri dati presso un altro outsourcer qualora, alla fine del contratto, non intenda rinnovarlo.
  - per poter importare i dati di un nuovo cliente provenienti da un altro outsourcer che utilizzi gli standard descritti dalla normativa

#### 4. Funzionalità

- La possibilità da parte di un formato di essere gestito da prodotti informatici, che prevedono una varietà di funzioni per la formazione e gestione del documento informatico.

#### 5. Supporto allo sviluppo

- Mettono a disposizione le risorse necessarie alla manutenzione e sviluppo del formato e i prodotti informatici che lo gestiscono
- Formati di software house che permettano contratti di manutenzione e di seguire le varie versioni nel tempo.

#### 6. Diffusione

- È l'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

## 6.1 I formati dei documenti sottoposti a conservazione

Al fine di garantire nel tempo la leggibilità dei documenti conservati è indispensabile che ad ognuno di essi siano associate le informazioni di rappresentazione corrette. Nella soluzione adottata da Trust Technologies, oltre a indicare il mime-type corrispondente all'oggetto conservato, il Soggetto Produttore deve fornire un viewer che lo supporti.

Il viewer sarà conservato al pari degli altri documenti inviati dal SP e verrà inserito nei pacchetti di distribuzione, eventualmente richiesti, al fine di fornire al cliente tutti gli strumenti necessari in sede di esibizione del dato conservato. Nella scheda di configurazione del servizio è richiesto, quindi, di indicare i formati dei documenti che si intendono conservare e il viewer che dovrà essergli associato.

Per venire incontro alle esigenze dei suoi clienti, indicando uno o più formati di quelli riportati nella tabella seguente e selezionando la casella "default" nella sezione viewer, il Soggetto Produttore incarica e delega Trust Technologies di scaricare e conservare per suo nome e conto i viewer corrispondenti, come indicato nella tabella riportata qui sotto.

Tipo di Documento	Estensione	MIME-TYPE
<b>Text</b>	.txt	text/plain
<b>XML</b>	.xml	application/xml; text/xml
<b>Portable Document Format</b>	.pdf	application/pdf
<b>E-Mail Message or PEC</b>	.eml	message/rfc822
<b>TIFF</b>	.tif , .tiff	image/tiff
<b>JPG</b>	.jpg, .jpeg	image/jpeg
<b>P7M</b>	.p7m	p7m

Nel caso in cui il Soggetto Produttore non fornisca il viewer indicato o invii in conservazione formati (mime-type) non supportati, l'elaborazione incorrerà in un errore di validazione e l'intero lotto sarà rimosso automaticamente. Contestualmente saranno allertati i tecnici di TI-TT che provvederanno a contattare il riferimento tecnico del Cliente per decidere sul da farsi.

Il cliente potrà:

- inviare il viewer corretto e poi risottomettere le elaborazioni precedentemente andate in errore
- fornire una liberatoria che sarà conservata al posto delle informazioni di rappresentazione e che sarà poi allegata ai DIP corrispondenti.

## 7 Modalità di attivazione di un nuovo cliente

### 7.1 Il processo di provisioning

L'attivazione di un nuovo cliente sulla piattaforma di Conservazione a norma di T.I.T.T. è composto da alcune fasi. Al cliente spettano le seguenti attività:



Fig.8

La scelta della tipologia con la quale inviare i documenti si effettua al momento della sottoscrizione del contratto. E' possibile scegliere una modalità di invio dei documenti. Per la modalità A2A è necessario che il cliente crei presso la propria sede di invio, una interfaccia di colloquio con i web services che T.I.T.T. mette a disposizione per la modalità A2A. Un documento aggiuntivo di specifiche tecniche guiderà il cliente (o una ditta specializzata alla quale il cliente vorrà affidarsi) nella costruzione dell'interfaccia. Ogni modalità scelta è soggetta ad una sessione di test di invio coordinata da T.I.T.T.

La scelta della tipologia documentale dipende dal tipo di documenti che il cliente intende conservare. La piattaforma di Conservazione a norma di T.I.T.T. possiede una lista di tipologie (es. fatture, registri IVA, distinte bancarie, verbali di esami, ecc..) con i relativi campi (metadati) per la ricerca dei documenti conservati. Queste tipologie sono descritte nel presente documento, al capitolo "Campi Specifici".

A seconda delle proprie esigenze, il cliente sceglierà la Descrizione Archivistica (DA) con i relativi metadati che ritiene più utile. Una volta scelta la DA con i metadati, essa non potrà essere modificata né scambiata con altra se vi è stata anche una sola conservazione. Occorrerà richiedere una nuova DA per una nuova tipologia documentale (da richiedere alla parte commerciale e non tecnica, poiché il contratto standard prevede una sola DA).

La Scheda Di Attivazione è lo strumento che darà il via alle operazioni di configurazione del nuovo cliente nel sistema di Conservazione a norma. Nella sua compilazione ci sono campi obbligatori e altri facoltativi. In ogni caso, per agevolare il cliente nella raccolta dei dati, la scheda è corredata da un manuale di istruzioni per la compilazione.

La Scheda di Attivazione, debitamente compilata, deve essere inviata al provisioning di T.I.T.T. tramite posta (cartaceo firmato) e anticipata via fax ai recapiti che verranno forniti dalla parte commerciale. Il provisioning risponderà contattando il referente tecnico indicato nella scheda di attivazione e fornendo il giusto supporto alla compilazione della scheda di configurazione del servizio.

## 8 Movimentazioni massive di dati conservati

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 lo standard 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 soggetto conservatore ad un altro o da un conservatore ad un utente autorizzato, è sempre obbligatorio l'uso di 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, è necessario utilizzare supporti criptati.

### 8.1 Accettazione dati conservati da altri outsourcer

T.I.T.T. è in grado di importare dati di altri outsourcer qualora dette informazioni, precedentemente soggette a conservazione a norma, rispettino alcune caratteristiche. La verifica di dette caratteristiche è preventiva rispetto all'accettazione dei dati conservati da migrare.

I contratti avranno pertanto una componente di valutazione preventiva della fattispecie.

#### 8.1.1 Per i dati conservati dopo il 13 aprile 2014

Per i dati provenienti dai nuovi outsourcer (che rientrano nel comma 1 dell'Art.14 del Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013), si richiede il rispetto della normativa citata, pertanto:

- i file conservati dovranno essere esclusivamente di estensione prevista nell'allegato n.2 "Formati"
- devono essere forniti i metadati che accompagnano i pacchetti di conservazione, con struttura rispondente alle specifiche tecniche degli allegati al D.P.C.M. del 3 dicembre 2013;
- In merito ai documenti fiscali informatici si richiama anche l'art. 3 DM 17 giugno 2014.
- devono essere forniti i software licenziati dal cliente con i quali è possibile visualizzare tutti i formati dei file conservati;
- il file delle evidenze XML deve rispettare le specifiche tecniche del D.P.C.M. del 3 dicembre 2013;
- tutte le firme e le marche temporali devono essere a norma;
- devono essere forniti dei pacchetti conservati per effettuare dei test di verifica.

#### 8.1.2 Per i dati conservati prima del 13 aprile 2014

Per i dati provenienti da outsourcer con sistemi già esistenti (che rientrano nel comma 2 dell'Art.14 del Decreto del Presidente del Consiglio dei Ministri del 3 Dicembre 2013), si richiede il rispetto della deliberazione CNIPA n. 11/2004, pertanto:

- i file conservati dovranno escludere la possibilità di contenere macro istruzioni (vedi i file .doc e .xls);
- devono essere forniti i software licenziati dal cliente con i quali è possibile visualizzare tutti i formati dei file conservati;
- devono essere forniti dei pacchetti conservati per effettuare dei test di verifica.

## 8.2 Esportazione dati per fine contratto (non rinnovato)

Di seguito viene tracciato l'iter procedurale del de-provisioning, cioè della sequenza temporale relativa alle azioni da effettuare al termine naturale dei contratti con i clienti, qualora tali contratti non vengano rinnovati.

### 8.2.1 Modalità di restituzione

Il produttore aveva già nominato gli utenti abilitati all'accesso della piattaforma web, all'atto della sottoscrizione del contratto.

Tali utenti sono invitati tramite 3 avvisi via mail a collegarsi alla piattaforma web per generare e scaricare i DIP contenenti tutti i documenti conservati.

L'ex cliente è tenuto a verificare la coerenza dei dati consegnati entro i tempi prestabiliti. T.I.T.T. fornirà supporto telefonico in orario di ufficio, per eventuali problemi. Gli utenti avranno a disposizione un manuale, scaricabile direttamente dal portale web, che descrive tutte le attività da espletare per queste operazioni.

In alternativa, per volumi di grandi dimensioni, T.I.T.T. restituirà le conservazioni all'ex-cliente o ai delegati autorizzati con apposita lettera firmata, previa consultazione con il Responsabile dei Dati del Soggetto Produttore, su appositi supporti.

Infine, verrà disattivato l'account relativo al portale web e i dati verranno cancellati.

### 8.2.2 Flusso di deprovisioning

La procedura di Deprovisioning è articolata in 2 fasi, come descritto dalla seguente figura:



(\*)

Primo avviso di scaricarsi i dati attraverso la piattaforma web (mail PEC). La piattaforma è dotata di un manuale operativo per la descrizione delle attività da effettuare;

(\*\*)

Secondo avviso di scaricarsi i dati attraverso la piattaforma web (mail PEC);

(\*\*\*)

Terzo ed ultimo avviso di scaricarsi i dati attraverso la piattaforma web (mail PEC);

Fig.9

### 8.2.3 Modalità di restituzione di casi particolari

In caso di clienti con mole di dati conservati che non consentono il download da web, si concorda con il Soggetto Produttore un supporto digitale adeguato con il quale quest'ultimo potrà accogliere i dati.

In questi casi, il Soggetto Produttore si procurerà il supporto digitale concordato e si recherà presso il bunker della Certification Authority di Telecom Italia Trust Technologies s.r.l., Strada Statale Pontina Km. 29,100, 00040, Pomezia (Roma), e presiederà alle operazioni di copia dei dati conservati, firmando apposita l'lettera di consegna.

# **Manuale del versamento in modalità SFTP**

## **MANUALE DEL VERSAMENTO SFTP**

**VERSIONI DEL DOCUMENTO**

Revisione	Descrizione delle modifiche	Emissione
01	Redazione	28/10/2016
02	Rapporti di Versamento	23/11/2016
03	Verifiche su RDV	25/11/2016
04	Revisione documento	02/02/2017

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

## Indice degli argomenti

<b>Manuale del versamento in modalità SFTP .....</b>	<b>1</b>
<b>Indice degli argomenti .....</b>	<b>3</b>
<b>1 Scopo del documento .....</b>	<b>4</b>
1.1 Definizioni.....	4
<b>2 Spazio SFTP .....</b>	<b>5</b>
<b>3 Struttura del PdV.....</b>	<b>6</b>
3.1 Nome file del Pacchetto Di Versamento (PdV) .....	6
3.2 Struttura del file ZIP .....	6
3.3 Struttura del file index.txt.....	6
3.3.1 Inserimento di allegati correlati al documento conservato. ....	8
<b>4 Rapporto di Versamento .....</b>	<b>9</b>
4.1 Struttura dell'Area SFTP .....	9
4.2 Verifica del versamento sul sistema di Conservazione .....	11

## 1 Scopo del documento

Il presente documento descrive la procedura operativa per il versamento mediante la modalità SFTP verso la piattaforma di Telecom Italia Trust Technologies s.r.l. (in seguito T.I.T.T.) per la conservazione a norma rispondente alla nuova normativa espressa nel D.P.C.M (Decreto del Presidente del Consiglio dei Ministri) del 3 Dicembre 2013 e successive modificazioni.

### 1.1 Definizioni

Nell'ambito del documento saranno utilizzati gli acronimi e le definizioni riportate nel seguito.

<i>PdV</i>	Pacchetto di Versamento
<i>SFTP</i>	Secure File Transport Protocol
<i>DA</i>	Descrizione Archivistica
<i>FS</i>	File System
<i>RdV</i>	Rapporto di Versamento
<i>PID</i>	Process Identification Number

Tab.1 - Acronimi

## 2 Spazio SFTP

In fase di delivery viene creata una struttura di directory dedicata al Soggetto Produttore (area pubblica, ad esempio: /NomeCliente/public); in essa il Cliente può depositare i PdV da inviare in conservazione e prelevare i relativi Rapporti di Versamento generati dal sistema di Conservazione.

Il cliente accedendo sul server SFTP mediante le proprie credenziali, si trova automaticamente posizionato su una porzione di FS ad esso esclusivamente dedicato (area public).

**All'interno di quest'area (/NomeCliente/public/) l'utenza assegnata al Cliente è autorizzata a leggere, scrivere e cancellare files o directory.**

Su tale porzione di FS il Cliente ha a disposizione delle directory predefinite, con nomenclatura correlata alle descrizioni archivistiche (DA) attivate, nelle quali deve essere depositato il PdV in formato .zip.

Ad esempio il PdV .zip contenente i documenti da conservare mediante la DA "**Registro Giornaliero di Protocollo**" deve essere collocato nella directory **registroprotocollo** presente nella propria area SFTP.

All'interno della directory pubblica è quindi presente per ciascuna DA una apposita directory in cui caricare il PdV.

Ad esempio:

/ NomeCliente/public/fatture

/ NomeCliente/public/registroprotocollo

All'interno di ciascuna directory avente il nome della DA viene creata una ulteriore directory denominata 'notifiche' contenente l'esito delle elaborazioni.

Ad esempio:

/fatture/notifiche

/registroprotocollo/notifiche

### 3 Struttura del PdV

Viene di seguito descritta la struttura del file zip con cui inviare metadati e dei documenti da mandare in conservazione.

Il mancato rispetto delle regole di seguito descritte può determinare il rigetto del PdV con relativo RdV negativo.

#### 3.1 Nome file del Pacchetto Di Versamento (PdV)

Il file del PdV deve essere in formato zip e deve avere la seguente nomenclatura: **NomeCliente-DA-Progressivo-dataora.zip**

Esempio di un PdV per la DA Registro Giornaliero di Protocollo:

NomeCliente = Acme

DA = registroprotocollo

Progressivo = 0001 (numero progressivo)

dataora = 280720161400

**Nome del file compresso.**

**NomeZIP: Acme-registroprotocollo-0001-280720161400.zip**

#### 3.2 Struttura del file ZIP

La struttura del file zip, una volta decompresso sui sistemi (procedura a cura di TITT) deve essere composta da una directory contenente al suo interno il file **index.txt** ed una sottodirectory **FILES** contenente tutti i file da inviare in conservazione.

La struttura directory del pacchetto zip decompresso deve essere del tipo:

NomeCliente-DA-Progressivo-dataora/index.txt

NomeCliente-DA-Progressivo-dataora/FILES/[file1, file2, file3, ecc.]

Esempio:

**Acme-registroprotocollo-0001-280720161400/index.txt**

**Acme-registroprotocollo-0001-280720161400/FILES/file1**

**Acme-registroprotocollo-0001-280720161400/FILES/file2**

**Acme-registroprotocollo-0001-280720161400/FILES/file3**

....

#### 3.3 Struttura del file index.txt

Viene di seguito descritta la struttura del tracciato di metadati, da includere nel file zip, con cui identificare i documenti e correlare i rispettivi metadati per inviarli in conservazione.

Il file indice (**index.txt**), generato in formato testo, deve contenere su ogni singola riga solo ed esclusivamente le informazioni (metadati) di un singolo file presente nel PdV. Non devono essere presenti righe duplicate e il numero delle righe deve corrispondere al numero di documenti presenti nel PdV.

Su ogni riga deve essere riportato il nome file (comprensivo della sottodirectory es.: registroprotocollo /NomeFile) seguito dalla lista dei metadati riportati secondo lo specifico ordine stabilito nella corrispondente DA.

Ad esempio, considerando la seguente struttura directory del pacchetto zip decompresso:

NomeCliente-DA-Progressivo-dataora/index.txt

NomeCliente-DA-Progressivo-dataora/FILES/[file1, file2, file3, ecc.]

il file indice conterrà nella prima riga:

**FILES/file1|metadato1|metadato2|metadato3|metadato4 ....**

**FILES/file2|metadato1|metadato2|metadato3|metadato4 ....**

**FILES/file3|metadato1|metadato2|metadato3|metadato4 ....**

....

Ogni valore del metadato deve essere separato dal carattere "|" (Pipe).

Qualora il metadato non sia stato definito come obbligatorio, può all'occorrenza non essere inserito, lasciando vuoto il relativo valore, ma inserendo comunque il carattere "|" di separazione:

Esempio.

Se il metadato n.3 non è obbligatorio e si decide di non inserirlo si avranno due pipe ||:

FILES/file1|metadato1|metadato2||metadato4

**NOTA:** I campi dei Metadati da inserire nel file Index.txt devono tassativamente essere inseriti nell'ordine descritto nella relativa Descrizione Archivistica come nell'esempio riportato di seguito. Il metadato (nell'es. UID\_documento) che identifica il documento deve essere sempre univoco all'interno del medesimo Soggetto Produttore.

N°	Metadato	Formato	Obbl
1	Hash	Hash	SI
2	Nome_Documento	Stringa	SI
3	Contesto	Stringa	SI
4	UID_Documento	Stringa	SI
5	Data di chiusura	dd/MM/yyyy	SI
6	Versione	Numero intero	SI

Hash	Nome_Documento	Contesto	UID_Documento	Data di chiusura	Versione
BB4F664D2240895C7732CC6146D17D3410CBA370A4ABB003BBA2D89C60821D5E	file1	AB24001	2431	28/07/2016	1

Esempio della prima riga del file Index.txt

FILES/file1|BB4F664D2240895C7732CC6146D17D3410CBA370A4ABB003BBA2D89C60821D5E|file1|AB24001|2431|28/07/2016|1

### 3.3.1 Inserimento di allegati correlati al documento conservato.

Qualora si desideri collegare uno o più allegati al documento inviato in conservazione, è necessario inserire, nella linea immediatamente successiva alla linea in cui sono definiti i metadati del documento da conservare, il carattere “+” seguito dal path ed il nome dell'allegato; si deve utilizzare una singola riga per ogni allegato.

La sintassi è quella dell'esempio di seguito riportato:

```
FILES/file1|BB4F664D2240895C7732CC6146D17D3410CBA370A4ABB003BBA2D89C60821D5E|file  
1|AB24001|2431|28/07/2016|1
```

```
+FILES/file1_allegato1
```

```
+FILES/file1_allegato2
```

```
+FILES/file1_allegato3
```

```
FILES/file2|BB4F664D2240895C7732KK6146D17D3410EFA370A4ABB003BBA2D89C60821D5E|file  
2|AB24101|2531|28/07/2016|1
```

```
+FILES/file2_allegato1
```

*È importante precisare che i documenti allegati NON sono direttamente ricercabili, possono essere recuperati esclusivamente tramite la ricerca del documento conservato cui sono correlati.*

## 4 Rapporto di Versamento

I Rapporti di Versamento (RdV) sono la raccolta, normalizzata, dei metadati forniti in fase di upload degli oggetti sottoposti a conservazione nel PdV.

La presenza del rapporto di versamento indica che i controlli preliminari sono stati eseguiti e che la conservazione dei documenti è in corso (nel caso di esito positivo) oppure è stata rigettata (caso negativo).

### I rapporti di Versamento sono sempre firmati in formato PKCS#7 (estensione .p7m).

*L'estensione del file P7M identifica un file firmato digitalmente. Quando un file viene firmato digitalmente l'estensione p7m sarà aggiunta al nome del file dopo l'estensione già presente.*

**NOTA:** *E' bene che i Soggetti Produttori verifichino, tramite il rapporto di versamento, che quanto inviato nel PdV sia stato correttamente preso in carico dal sistema per essere versato nel sistema di conservazione.*

Il nome del file del RdV riporta anche il PID (negli esempi 20325 oppure 22358) che identifica il Processo di elaborazione che ha preso in carico il PdV.

### 4.1 Struttura dell'Area SFTP

All'interno della directory avente il nome della DA associata al PdV inviato, viene creata una directory denominata '**notifiche**' contenente i rapporti di versamento.

Ad esempio:

/fatture/**notifiche**

/registroprotocollo/**notifiche**

Per ciascun PdV, viene ulteriormente creata una apposita directory, avente il nome del file compresso inviato, in cui viene depositato dal sistema, al termine dei controlli preliminari, il relativo RdV in formato xml.

Viene depositato in questa directory anche:

- il file di indice contenente nel nome l'esito della conservazione (ok oppure ko) ed il PID
- il file .xsd che definisce lo schema del file xml che costituisce il RdV

**NOTA:** *Durante la fase di elaborazione il sistema rinomina temporaneamente il file indice in **index.txt.inp\_(PID)**, per poi rinominare definitivamente al termine dell'elaborazione il file con l'esito in **index.txt.ok\_(PID)** oppure **index.txt.ko\_(PID)**.*

Nel caso di RdV con esito positivo:

**Esempio.**

/registroprotocollo/notifiche/**Acme-registroprotocollo-0001-280720161400/rapporto\_di\_versamento\_20325.xml.p7m**

/registroprotocollo/notifiche/**Acme-registroprotocollo-0001-280720161400/rapporto\_di\_versamento\_20325.xsd**

/registroprotocollo/notifiche/**Acme-registroprotocollo-0001-280720161400/index.txt.ok\_20325**

Il contenuto di un rapporto di versamento con esito positivo sarà del tipo:

```
<?xml version="1.0" ?>
<Documenti UID="20325" UTC="03-11-2016 11:51:42 UTC(+0000)"
HASH_PDV="A3051FA00D1ADFCE6CA4EBAD1E04720552B862C1AC694691AA2E24E5F0138E4C" schemaVersion="1.1">
  <documento UID="406528B528E00249E05354150D0A576D">
    <versione>1.0</versione>
    <file fileName="testfileIDX00" UID="406528B528E10249E05354150D0A576D"
hash="45A2BCE0E04D07D793EF3F5E29DD29605D872CD0ABEA2916CA991B3C4B1B6CAA"></file>
    <metadato chiave="Data" valore="29-11-2015"></metadato>
    <metadato chiave="stringa1" valore="0000"></metadato>
    <metadato chiave="stringa2" valore="c3-0000"></metadato>
    <metadato chiave="stringa3" valore="c3-test"></metadato>
    <metadato chiave="stringa4" valore="c5"></metadato>
    <metadato chiave="stringa5" valore="19c0b0a5-72e6-43e6-bfdc-92afe36c4c8a"></metadato>
    <metadato chiave="stringa6" valore="e26d100b-6359-4e14-a604-34cc61dbc849"></metadato>
    <metadato chiave="stringa7" valore="e0067f9e-adac-4e27-8aff-5feb04ac2f87"></metadato>
    <metadato chiave="stringa8" valore="b753e6c8-4042-4ed9-8953-24f5857ecae8"></metadato>
    <metadato chiave="stringa9" valore="77798db1-3ac5-4024-9300-8a69aa5ca3a5"></metadato>
    <metadato chiave="stringa10" valore="b6c8dbbf-af12-4544-a8f2-58757ae6e197"></metadato>
    <metadato chiave="stringa11" valore="51f296d4-87be-4d60-b134-cff41594024c"></metadato>
    <metadato chiave="stringa12" valore="41841097-0dcf-4c74-b991-9c6d387ff434"></metadato>
    <metadato chiave="stringa13" valore="693c6adb-135f-47a1-af4e-1d30d2b2b021"></metadato>
    <metadato chiave="stringa14" valore="a1456242-e4d6-4f4c-a50d-d449287edb0e"></metadato>
    <metadato chiave="stringa15" valore="7130049e-ec3e-4101-a00e-a9004b5c78b8"></metadato>
    <metadato chiave="stringa16" valore="30a8a05f-d8a1-4d26-8e7a-7454b9fa5677"></metadato>
  </documento>
</documento UID="406528B528E20249E05354150D0A576D">
  <versione>1.0</versione>
  <file fileName="testfileIDX01" UID="406528B528E30249E05354150D0A576D"
```

Il tag HASH\_PDV corrisponde allo SHA-256 calcolato sul file indice dei metadati ed è presente solamente nel rapporto del pacchetto di versamento. Viene solamente utilizzato dal sistema per identificare il rapporto di versamento; non è rilevante ai fini dell'integrazione con il servizio di Conservazione.

Il tag HASH invece viene utilizzato per garantire e verificare la corretta integrità del file versato.

Nel caso di RdV con esito negativo invece:

### Esempio.

```
/registroprotocollo/notifiche/Acme-registroprotocollo-0001-280720161400/rapporto_di_versamento_22358.xml.p7m
/registroprotocollo/notifiche/Acme-registroprotocollo-0001-280720161400/rapporto_di_versamento_22358.xsd
/registroprotocollo/notifiche/Acme-registroprotocollo-0001-280720161400/index.txt.ko_22358
```

Il contenuto del rapporto di versamento con esito negativo sarà del tipo:

```
<?xml version="1.0" ?>
- <Documenti UID="22358" UTC="23-11-2016 14:30:08 UTC(+0000)"
HASH_PDV="842F5DCBB2DEFA597CAFF7F6ADF6C7A6F55172AD27509706E52FDA5F627C3276" schemaVersion="1.1">
- <errori>
  <errore>Errore durante la validazione documenti per il processo con id 22358 File: [/NFS_DATA/TEMP/TestIndice/Mauro_03112016/files/testfileIDX00] non
esiste.</errore>
</errori>
</Documenti>
```

## 4.2 Verifica del versamento sul sistema di Conservazione

Il PdV è composto da un file di testo `index.txt` e dai files da inviare in conservazione; una volta depositato il file indice nell'area SFTP viene attivato il processo che effettua i controlli formali e di congruità tra il file indice, i metadati ed i documenti inseriti nel PdV.

Terminato il processo di verifica, viene creato il RdV: `rapporto_di_versamento_20325.xml.p7m` oppure `rapporto_di_versamento_22358.xml.p7m`.

Terminata la elaborazione del PdV il file Indice `index.txt` viene rinominato in:

- `index.txt.ok_PID` in caso di esito positivo e quindi conservazione correttamente eseguita , oppure
- `index.txt.ko_PID` in caso di esito negativo e quindi conservazione non eseguita.

Nei due esempi precedenti: `index.txt.ok_20325` oppure `index.txt.ko_22358`.

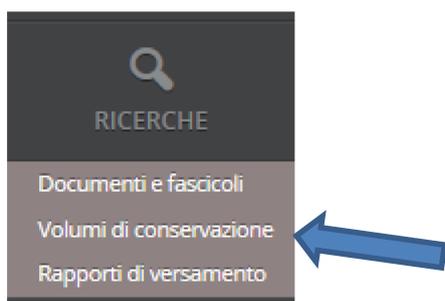
Entrambi i tipi di file contengono nel nome file l'identificativo del PID, ovvero il processo con cui il sistema ha preso in carico il PdV (PID **20325** e PID **22358**).

Con il PID il Soggetto Produttore è in grado di verificare nel dettaglio se il processo di conservazione del PdV inviato si sia concluso.

Per verificare che la conservazione si sia conclusa con successo ed i documenti siano disponibili sul sistema, l'utente abilitato dal Soggetto Produttore all'esibizione, deve accedere al sistema di conservazione (<https://conservazione.trusttechnologies.it>) e, mediante il PID, effettuare la ricerca del volume ad esso associato.

Di seguito i passi da seguire per effettuare questa verifica.

Accedere al sistema di conservazione <https://conservazione.trusttechnologies.it> e selezionare il menu Ricerche → Volumi di conservazione



Inserire nel campo PID il PID del processo del RdV e cliccare su Cerca.

**Lo Stato “Conservato” è l'evidenza che il PdV è stato correttamente conservato.**

## Volumi di conservazione

Forma di ricerca per i volumi di conservazione:

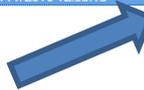
PID:  ID. Volume:  Soggetto Produttore:

Descrizione Archivistica [-]:  Stato:

Cerca

PID	ID. Volume	Desc. Arc.	Dimensione [MB]	Data Marca	Stato
20325	0000000000000358	crea-indice	97.66	03/11/2016 12:53:13	Conservato

Apri



Se la ricerca con PID non restituisce alcun esito significa che il processo di conservazione non si è ancora concluso.

# Conservazione a Norma

## Manuale Utente

<MANUALE UTENTE>



## Indice degli argomenti

<b>1</b>	<b>Descrizione del sistema di conservazione.....</b>	<b>4</b>
	<i>Internazionali:.....</i>	<i>4</i>
	<i>Nazionali:4</i>	
1.1	Definizione delle DA.....	4
1.2	Utilizzo dei dati conservati.....	5
	1.2.1 <i>Il processo di esibizione .....</i>	<i>5</i>
	1.2.2 <i>Esportazione dati per richieste in ambito legale.....</i>	<i>5</i>
1.3	Supporto.....	6
<b>2</b>	<b>Istruzioni Operative .....</b>	<b>7</b>
2.1	Login.....	7
	2.1.1 <i>Recupero credenziali.....</i>	<i>7</i>
	2.1.2 <i>Impostazioni .....</i>	<i>8</i>
2.2	Ricerca, Esibizione e Download .....	8
	2.2.1 <i>Documenti e fascicoli.....</i>	<i>8</i>
	2.2.2 <i>Creazione di un Pacchetto di Distribuzione (DIP) .....</i>	<i>12</i>
	2.2.3 <i>Volumi di conservazione .....</i>	<i>13</i>
	2.2.4 <i>Rapporti di versamento .....</i>	<i>14</i>
2.3	Utente Avanzato e Upload .....	15
	2.3.1 <i>Upload manuale .....</i>	<i>16</i>

## 1 Descrizione del sistema di conservazione

Il sistema di conservazione a norma di T.I.T.T. rispetta i seguenti standard:

### Internazionali:

- OAIS: ISO 14721 Open Archival Information System
- Dublin Core: ISO 15386 The metadata element set

### Nazionali:

- UniSInCRO: UNI 11386 Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali

L' Interfaccia Web-User è un'applicazione J2EE che, attraverso l'accesso in modalità protetta (protocollo https porta 443 con certificato SSL), consente di procedere con le attività di esibizione e download previste dalla normativa.

Di seguito la lista dei browser dichiarati compatibili:

- 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.

Esistono anche dei Web Services che permettono, ad applicazioni di terze parti, di versare documenti nel sistema di conservazione o di interrogare lo stesso sullo stato di un documento.

### 1.1 Definizione delle DA

Ogni soggetto produttore sceglie i tipi di documento che intende conservare e, ereditandone le caratteristiche di default, dispone di un proprio set di Descrizioni Archivistiche (DA).

Ogni DA è caratterizzata dalle seguenti informazioni, che devono essere concordate preventivamente con il soggetto produttore e riportate nell'apposita scheda di attivazione :

- il set di metadati (in relazione al tipo di documento selezionato dal set di metadati standard)
- modalità di versamento (scegliendo uno dei flussi presentati)
- informazioni sull'uso e la rappresentazione dei dati conservati (mime-type utilizzati, viewer associati, classificazione dei documenti, modalità di accesso ai documenti)
- periodicità di upload (giornaliera, settimanale, mensile, trimestrale o custom)
- tipo di verifiche da fare:
  - sugli oggetti della conservazione (mime type e validità firme)
  - sui metadati (obbligatorietà, dimensione, set predefinito)

Per evitare la perdita di informazioni aggiuntive (non necessarie ai fini della conservazione), che il cliente desidera conservare, è possibile inviare dei file accessori come allegati dei documenti sottoposti a conservazione. In questa modalità il documento conservato sarà ricercabile attraverso i suoi metadati e sarà sempre corredato dai suoi allegati completi.

## 1.2 Utilizzo dei dati conservati

### 1.2.1 Il processo di esibizione

L'esibizione è un atto da svolgersi in ottemperanza di quanto previsto dall'ultimo comma dell'art. 2220 del Codice Civile, ribadito nell'Art. 10 del D.P.C.M. del 3 Dicembre 2013.

Essa consiste nel rendere leggibili, con mezzi messi idonei, tutte le scritture e i documenti conservati a norma.

L'Articolo 10 del D.P.C.M. del 3 Dicembre 2013 ribadisce le norme vigenti e specifica che ai fini dell'esibizione il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, al documento informatico conservato, attraverso la produzione di un pacchetto di distribuzione (DIP) selettiva secondo le modalità descritte nel manuale di conservazione.

Il sistema di conservazione di T.I.T.T. consente l'esibizione in modo da visualizzare e scaricare i DIP conservati, 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.

### 1.2.2 Esportazione dati per richieste in ambito legale

Il sistema di conservazione di T.I.T.T. consente l'esibizione ai fini legati dei pacchetti di distribuzione (DIP) e i documenti conservati, completi di file di evidenza della conservazione. Tale file è fondamentale per testimoniare l'avvenuta conservazione dei documenti secondo le norme vigenti.

In concreto, il processo di esibizione viene gestito attraverso un'interfaccia web, raggiungibile tramite browser utilizzando credenziali personali non cedibili.

Il Cliente, in fase di attivazione del servizio segnala al provisioning di T.I.T.T., su apposita documentazione correlata dagli allegati autorizzativi e di identificazione, i propri delegati alla visualizzazione e al download dei file ai fini dell'esibizione.

A quel punto i delegati del cliente sono in grado di:

- Visualizzare i documenti conservati da remoto
- Scaricare i documenti conservati e i file di evidenza della conservazione
- Richiedere e scaricare dei pacchetti di distribuzione da consegnare alle autorità, in caso di contenzioso

Nel pacchetto è compreso anche il necessario per la rappresentazione (es. 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 e l'effettiva validità del certificato di firma al momento dell'apposizione stessa.

Tale procedura, non potendo essere effettuata stampando l'evidenza firmata della conservazione, deve necessariamente prevedere un supporto informatico. Essa può pertanto essere espletata in almeno 2 modi:

1. Attraverso un pc collegato alla rete Internet che, tramite le credenziali di accesso del delegato del cliente, possa accedere al portale della conservazione per scaricare i documenti completi di file di evidenza (con le impronta, firma e marca);
2. Attraverso un file contenente i documenti completi di file di evidenza (con le impronte, firma e marca); nel caso in cui id DIP debba essere spostato dalla sede del Produttore, i dati devono essere criptati (ISO/IEC 27001:2005).

Di seguito lo schema temporale di attivazione degli utenti abilitati alle consultazioni via web. Si ricorda che il sistema di conservazione non è un archivio digitale, pertanto gli accessi devono essere limitati alle operazioni di esibizione a norma dei documenti conservati e non per la visualizzazione per altri scopi (ad esempio, avere una copia del documento). In tutti gli altri casi si dovrà usare un sistema di gestione documentale.

Comunicazione al Produttore (Cliente) > Provisioning T.I.T.T. dei nominativi delegati all'accesso al Portale della Conservazione (scheda attivazione in allegato)

Comunicazione delle credenziali agli utenti (delegati del produttore)

Accesso dei delegati al Portale (utenti) della Conservazione davanti agli inquirenti o creazione del CD con l'ISO attraverso il portale.

### 1.3 Supporto

In caso di errori, malfunzionamenti o dubbi sugli esiti ricevuti dall'interfaccia web è possibile aprire una segnalazione inviando una mail a [CRPresidio\\_CA@telecomitalia.it](mailto:CRPresidio_CA@telecomitalia.it) o telefonando al numero verde **800.28.75.24**.

Per velocizzare l'identificazione e l'evasione delle vostre richieste, oltre al vostro nome e all'eventuale username, indicate sempre il nome del Cliente o del Soggetto Produttore, il servizio (Conservazione a Norma) o l'indirizzo dell'applicazione web a cui vi siete collegati e la tipologia del problema riscontrato.

Es. [**Oggetto:** Conservazione a Norma, Cliente1 SPA, user123, Errore in fase di esibizione]

Nel testo del messaggio potrete riportare il messaggio di errore e la descrizione del contesto in cui si è verificato. Eventuali screenshot possono essere inviati come allegato.

 Trust Technologies	Codice: EVOCAST01.IT.DPMU14000.04
Conservazione a Norma - Manuale Utente	Stato: Rilasciato

## 2 Istruzioni Operative

L'Utente delegato dal Cliente, dal Soggetto Produttore o dal proprietario dei dati conservati, può mettere in pratica tutte le azioni previste sui dati conservati utilizzando l'interfaccia web di T.I.T.T. [<https://conservazione.trusttechnologies.it>].

### 2.1 Login

Accedere all'indirizzo di erogazione del servizio ed inserire le proprie credenziali



# Conservazione Documentale

Questo sito utilizza esclusivamente cookie tecnici per garantire le proprie funzioni.  
Per visionare la policy sulla privacy completa [clicca qui](#).

BENVENUTO Legal Archive

Username  Password

[Password dimenticata](#)

#### 2.1.1 Recupero credenziali

Nel caso in cui non si disponesse della password di accesso è possibile recuperare le credenziali utilizzando l'apposito link "[Password dimenticata](#)".



# Conservazione Documentale

Questo sito utilizza esclusivamente cookie tecnici per garantire le proprie funzioni.  
Per visionare la policy sulla privacy completa [clicca qui](#).

BENVENUTO Legal Archive

Username  Password

[Password dimenticata](#)

Indirizzo Email

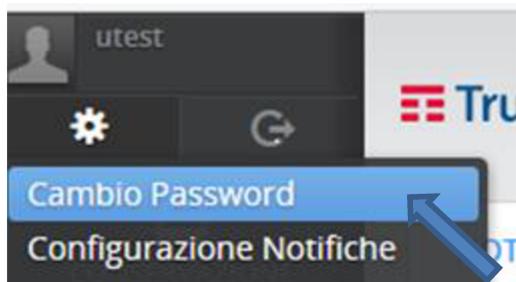
Verrà resettata la password dell'utente associato alla mail inserita e verrà inviata una mail con le istruzioni per accedere nuovamente al sistema.

Inserendo la username e l'indirizzo mail fornito in fase di configurazione del servizio si riceverà un messaggio contenente le istruzioni per effettuare l'accesso.

Nel caso in cui il problema persista, l'utenza risulti bloccata o scaduta, o non si riceva la mail di accesso: è possibile aprire una segnalazione di verifica scrivendo a [CRPresidio\\_CA@telecomitalia.it](mailto:CRPresidio_CA@telecomitalia.it).

## 2.1.2 Impostazioni

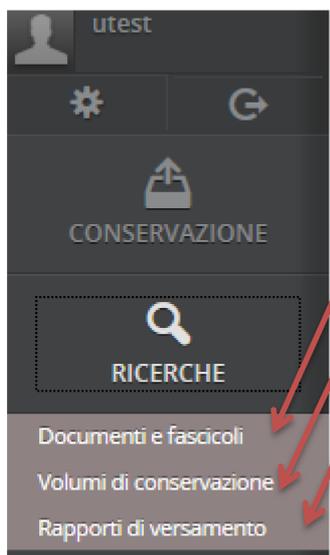
Eseguito il log in, cliccando sul tasto "Impostazioni" , sarà possibile modificare la password di accesso.



## 2.2 Ricerca, Esibizione e Download

### 2.2.1 Documenti e fascicoli

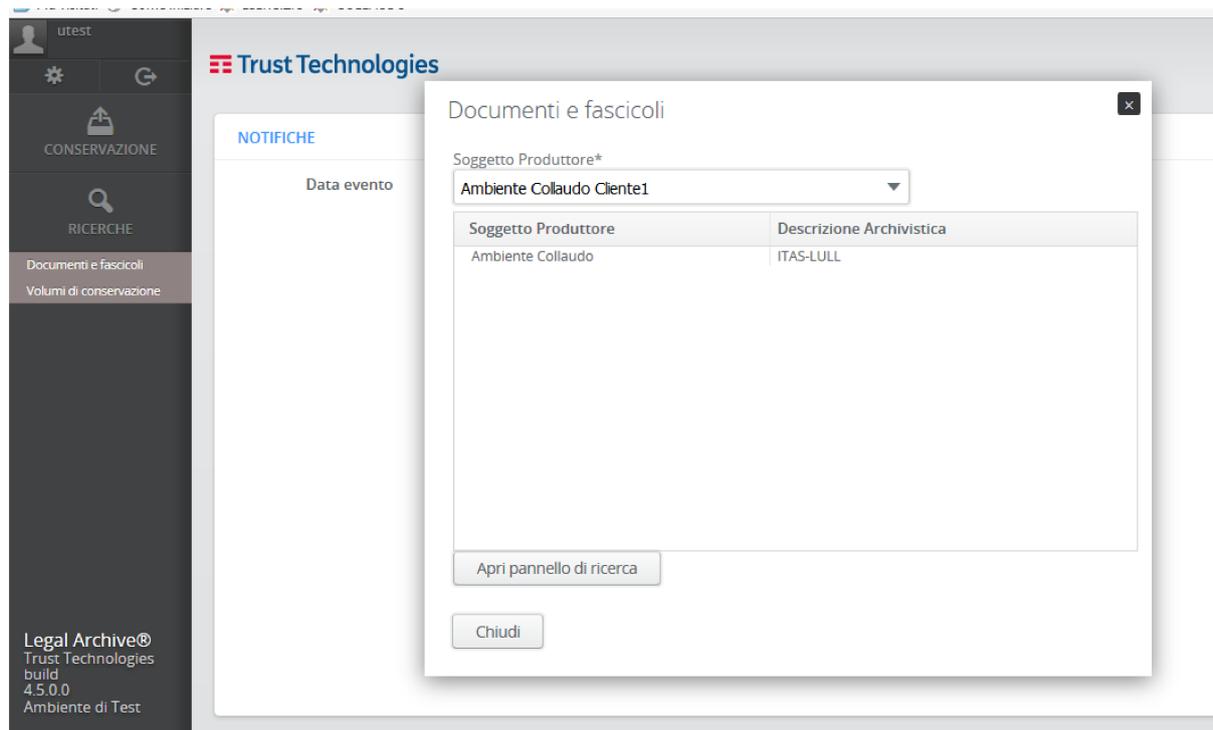
Accedendo con la propria utenza personale, si potranno ricercare i documenti conservati e assegnati ai Soggetti Produttori per i quali si è delegati, a seconda del proprio ruolo.



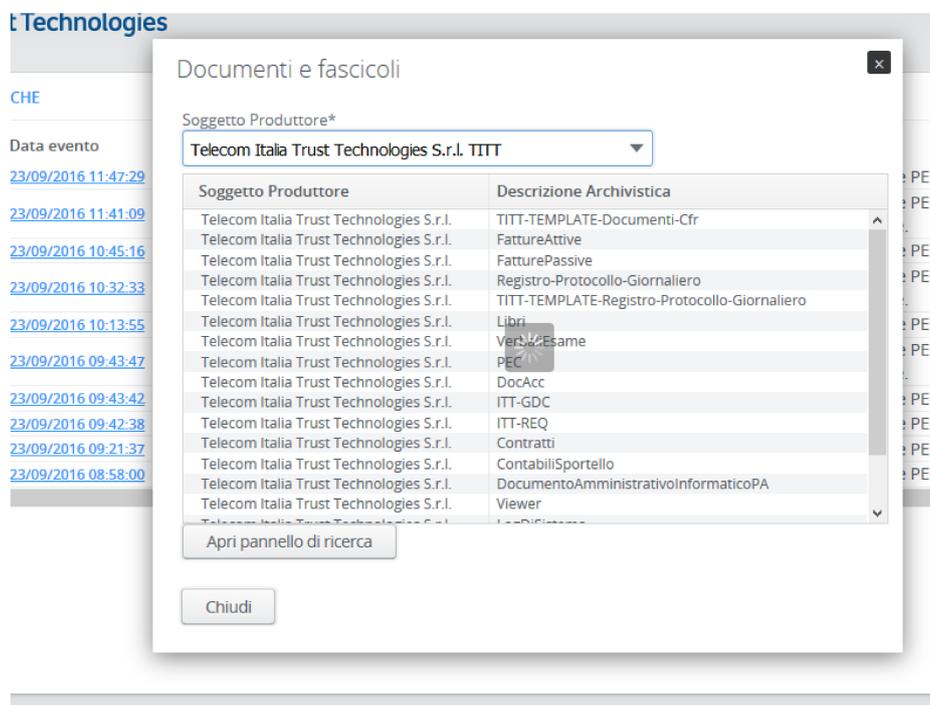
Gli oggetti ricercabili sono di 3 tipi:

- I documenti conservati
- Gli interi volumi (lotti) inviati in conservazione
- I rapporti (o verbali) di versamento [RdV]

Per procedere all'esibizione, selezionare dal menù di sinistra [RICERCHE] → "Documenti e fascicoli"; si aprirà una pagina in cui andrà definito l'ambito della ricerca stessa selezionando uno dei Soggetti Produttori (SP) per i quali si dispone dei privilegi di visualizzazione e la Descrizione Archivistica (DA) per la quale si necessita di eseguire la ricerca.



È possibile selezionare una specifica associazione SP/DA (Soggetto Produttore/Descrizione Archivistica, da selezionare solo se si hanno più soggetti produttori e/o più tipologie documentali conservate) oppure eseguire una ricerca sulle varie DA dello stesso Soggetto Produttore; in quest'ultimo caso saranno utilizzati solo i campi comuni alle varie Descrizioni Archivistiche.



Cliccando su "Apri pannello di ricerca" verrà restituita una finestra con un wizard per arrivare ad ottenere i pacchetti per l'esibizione a norma.

Il primo passo sarà inserire opportunamente i Filtri per ricercare i documenti conservati.



- **Se si vuole scaricare l'evidenza della conservazione per effettuare l'esibizione a norma:** cliccare sul link **"Scarica indice firmato"**. L'operazione consentirà di salvare in locale (su un supporto a scelta) il file "Indice\_00000000000000000000000000000001.xml.p7m" che consente la verifica della conservazione (fig)
- **Se si vuole scaricare il file conservato:** cliccare sulla tab Files e poi scegliere il link **"Download"** oppure **"Preview"** rispettivamente per scaricare in locale o visualizzare il file conservato.
- **Se si vogliono conoscere le informazioni della conservazione (quando è stato conservato il documento, le informazioni sulla firma digitale e sulla marca temporale, ecc.):** cliccare sulla tab IdC e leggere le informazioni della conservazione.

### Dettaglio

Tipo Descrizione Archivistica: Unita' documentaria

Volume: 00000000000000000000000000000001

UID: 1F257B687A1348C1E0540021283C3670

[Scarica Indice firmato](#) [Scarica Indice](#) [Scarica informazioni rappr.](#)

Metadati	Files	IdC
----------	-------	-----

Verifica impronta

Files

Nome file	Mime Type	Azione
112287-1-RegistroProtocollo20150827.PDF	application/pdf	<a href="#">Download</a> <a href="#">Preview</a>

### Dettaglio

Tipo Descrizione Archivistica: Unita' documentaria

Volume: 00000000000000000000000000000001

UID: 1F257B687A1348C1E0540021283C3670

[Scarica Indice firmato](#) [Scarica Indice](#) [Scarica informazioni rappr.](#)

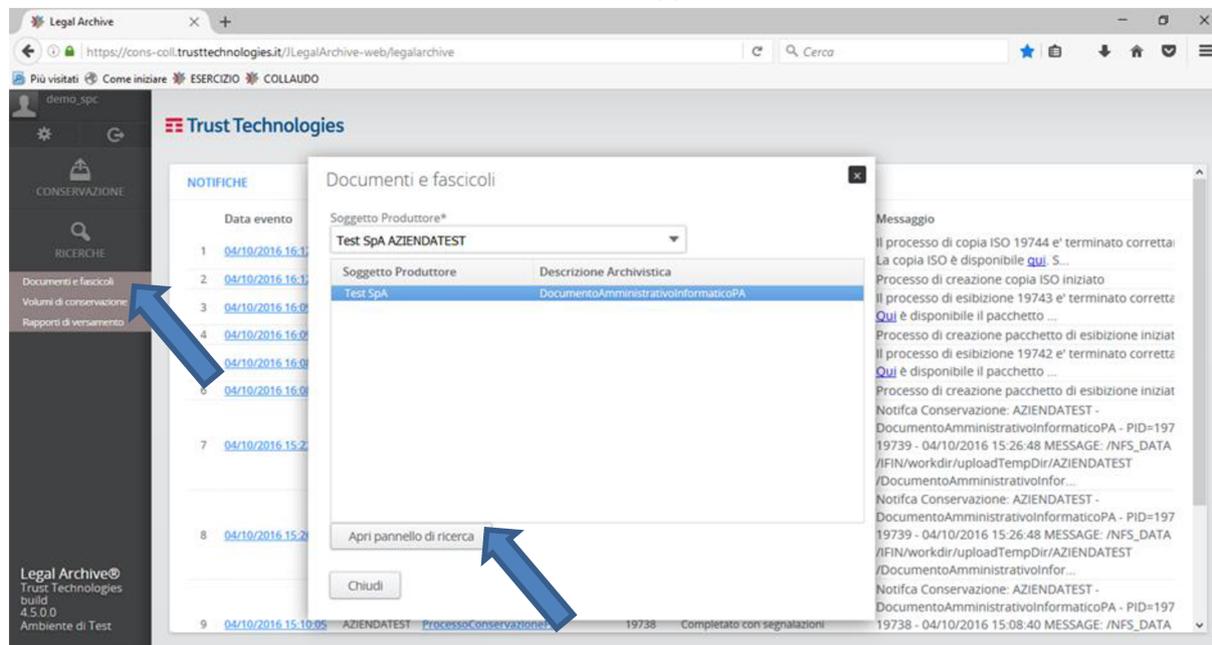
Metadati	Files	IdC
----------	-------	-----

Evidenza Indice\_00000000000000000000000000000001.xml.p7m

Info	Valore
ID Volume	00000000000000000000000000000001
Nome file	Indice_00000000000000000000000000000001.xml.p7m
Data scadenza	Fri Sep 07 11:25:11 CEST 2035
Data firma	Mon Sep 07 11:25:02 CEST 2015
Numero seriale firma	199786
Issuer certificato firma	CN=TI Trust Technologies CA 1,OU=Servizi di certificazione,O=Telecom Italia Trust Technologies S.r.l.,C=IT
Data marca	07-09-2015 09:25:11 UTC(+0000)
Numero seriale marca	13613205
TSA marca	CN=TI Trust Technologies Time Stamp Authority,OU=Servizi di certificazione,O=Telecom Italia Trust Technolog

## 2.2.2 Creazione di un Pacchetto di Distribuzione (DIP)

Selezionare Documenti e Fascicoli → selezionare il soggetto produttore



Effettuare la ricerca esempio ricerca per Data

Apri pannello di ricerca

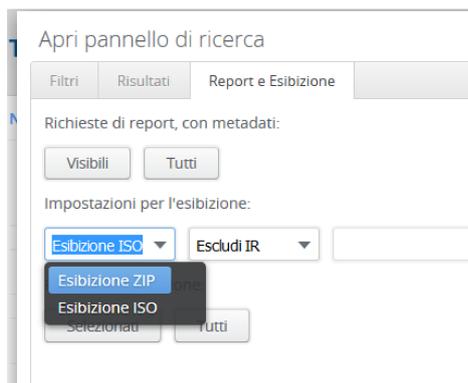
Filtri	Risultati	Report e Esibizione
<input type="text" value="FileName"/> <input type="text" value="CodiceRegistro"/> <input type="text" value="Destinatario"/> <input type="text" value="RSA"/> <input type="text" value="Hash"/>	<input type="text" value="CodiceA00"/> <input type="text" value="Data di chiusura min"/> <input type="text" value="Nome_Documento"/> <input type="text" value="Soggetto Produttore"/> <input type="text" value="ID Volume"/>	<input type="text" value="CodiceIPA"/> <input type="text" value="Data di chiusura max"/> <input type="text" value="Oggetto"/> <input type="text" value="UID_Documento"/> <input type="text" value="UID"/>
<input type="button" value="Cerca"/>		

Selezionare i file con cui creare il Pacchetto di distribuzione e selezionare il TAB “Report e Esibizione”

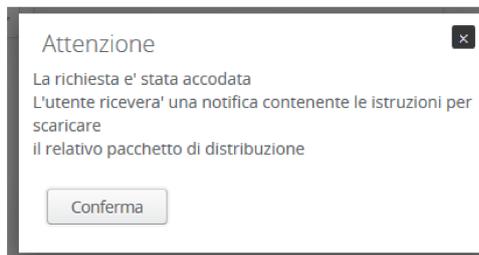
Apri pannello di ricerca

File Name	CodiceA00	CodiceIPA	CodiceRegistro	Data di chiusura	Destinatario	Nome_Documento	Oggetto
lista file	codA0014	codIPA14	FileTest01_Pdv4A29686DA	03/10/2016	destSPC	FileTest01_Pdv4.txt	testS
lista file	codA0024	codIPA24	FileTest02_Pdv4A29686DA	03/10/2016	destSPC	FileTest02_Pdv4.txt	testS
lista file	codA0034	codIPA34	FileTest03_Pdv4A29686DA	03/10/2016	destSPC	FileTest03_Pdv4.txt	testS
lista file	CODAO04	CODIPA4	FileTest4_WEB4A29686DA	04/10/2016	destSPC	FileTest4_WEB.txt	test
lista file	CODAO01	CODIPA1	FileTest01_WEB4A29686DA	04/10/2016	destSPC	FileTest01_WEB.txt	testW

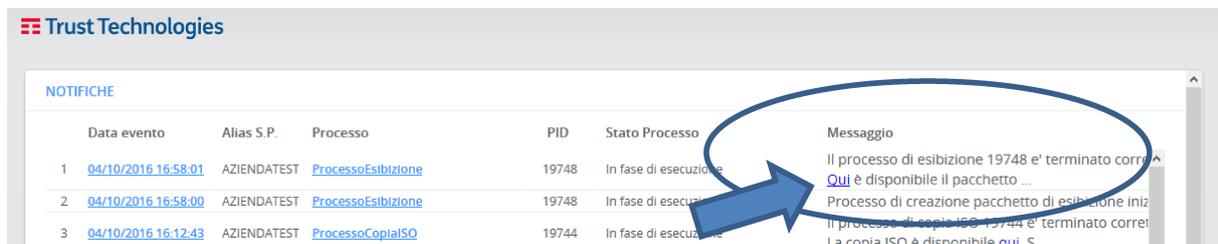
Selezionare il tipo di Esibizione “ Esibizione ZIP “ per creare il DIP in formato ZIP o “Esibizione ISO” se si vuole creare una ISO Per supporto CD/DVD



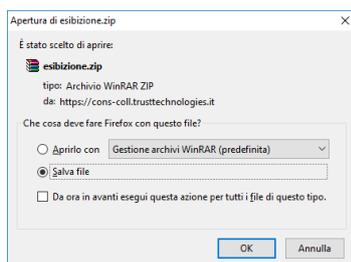
Apparirà una schermata che Avvisa che il processo per il DIP è stata avviata



A processo ultimato comparirà nella Dashboard la notifica e il link per poter scaricare il DIP



Cliccando su "Qui" si potrà scaricare il DIP



### 2.2.3 Volumi di conservazione

Oltre alla necessità di esibizione a norma potrebbe essere necessario il download di interi lotti precedentemente conservati. Il caso d'uso previsto, in questo frangente, sono le operazioni di de-provisioning o riversamenti massivi da un soggetto conservatore ad un altro.

Selezionando la funzionalità [RICERCHE] → "Volumi di conservazione"





Questa voce di menu non è in dotazione a tutti gli utenti, ma solo ai Soggetti Produttori che hanno la necessità di controllare che il pacchetto sia stato effettivamente versato nel sistema di conservazione. Utili soprattutto per verifiche interne all'eventuale flusso A2A, i "Verbali di Versamento" sono la raccolta, normalizzata, dei metadati forniti in fase di upload degli oggetti sottoposti a conservazione.

Non sostituiscono l'evidenza di avvenuta conservazione, ma comprovano la presa in carico, con esito positivo, dei dati sottoposti a conservazione.

La conservazione a norma, infatti, non è un processo sincrono; i dati caricati con il versamento subiscono vari controlli e lavorazioni e l'intero flusso è sempre monitorato, verificato e finalizzato con firma dal responsabile della conservazione o dai suoi delegati

La presenza del rapporto (o verbale) di versamento indica che i controlli preliminari sono stati eseguiti con esito positivo e che la conservazione dei documenti è in corso.

## 2.3 Utente Avanzato e Upload

L'Utente "Avanzato" differisce dall'utente "Base" per la possibilità di effettuare upload manuali semplicemente accedendo alla Web-App di conservazione.

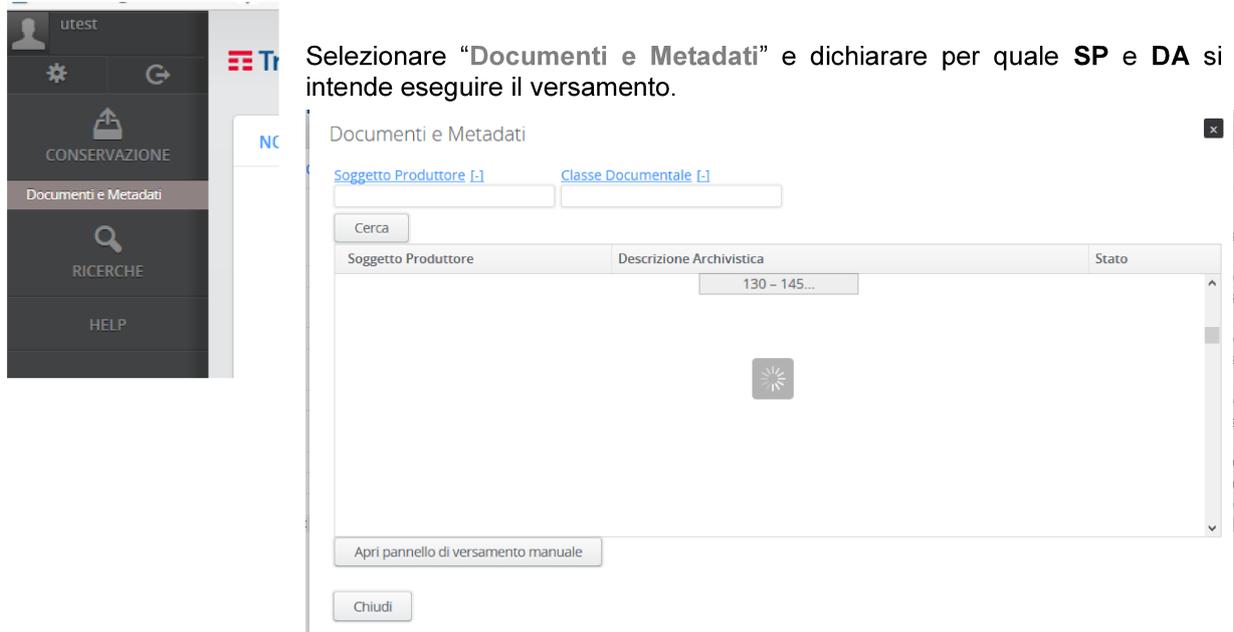
La scelta sul tipo di utenza da attivare è fatta in fase di provisioning e configurazione e dipende dalla modalità di utilizzo del servizio definita al momento della richiesta di attivazione del servizio stesso.

La funzionalità di upload tramite Web-App è dedicata ad utenti delegati dal Soggetto Produttore che dovranno essere opportunamente censiti dal gruppo di provisioning di Trust Technologies.

Le utenze web sono personali e non cedibili. Gli upload esterni, escludendo quindi i versamenti massivi eseguiti dal conservatore stesso (ad esempio in fase di migrazione dei dati), possono avvenire solo versando i singoli documenti a nome del Soggetto Produttore da cui si è stati delegati e in ogni Descrizione Archivistica a lui associata.

### 2.3.1 Upload manuale

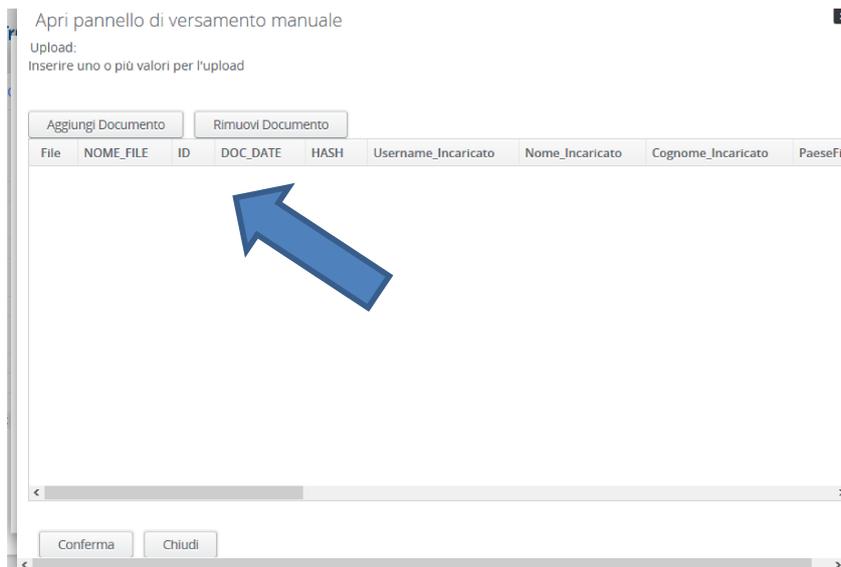
Eseguire il log in all'indirizzo [<https://conservazione.trusttechnologies.it>] e attivare la funzionalità di **versamento** dal menù di sinistra.



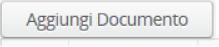
Selezionare “Documenti e Metadati” e dichiarare per quale **SP** e **DA** si intende eseguire il versamento.

The screenshot shows a sidebar menu on the left with the following items: 'utest', 'CONSERVAZIONE', 'Documenti e Metadati' (highlighted), 'RICERCHE', and 'HELP'. The main content area is titled 'Documenti e Metadati' and contains two dropdown menus for 'Soggetto Produttore [-]' and 'Classe Documentale [-]', a 'Cerca' button, and a table with columns 'Soggetto Produttore', 'Descrizione Archivistica', and 'Stato'. The table shows a single entry with '130 - 145...' in the 'Descrizione Archivistica' column. Below the table is a button 'Apri pannello di versamento manuale' and a 'Chiudi' button.

Utilizzare il tasto  per procedere.



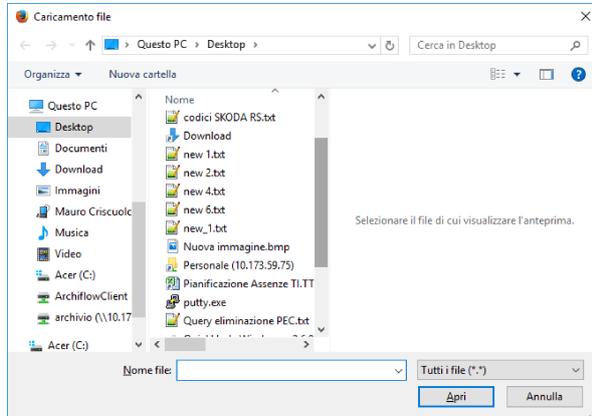
The screenshot shows a dialog box titled 'Apri pannello di versamento manuale'. It contains an 'Upload:' section with the instruction 'Inserire uno o più valori per l'upload'. Below this are two buttons: 'Aggiungi Documento' and 'Rimuovi Documento'. A table with the following columns is visible: 'File', 'NOME\_FILE', 'ID', 'DOC\_DATE', 'HASH', 'Username\_Incaricato', 'Nome\_Incaricato', 'Cognome\_Incaricato', and 'PaeseFile'. A blue arrow points to the 'Aggiungi Documento' button. At the bottom of the dialog are 'Conferma' and 'Chiudi' buttons.

Selezionare 

Nella pagina seguente sarà possibile caricare tutti i documenti da porre in conservazione compilando di volta in volta i metadati corrispondenti a ciascun documento.

Seleziona Documento

Cliccare su **Seleziona Documento** Si aprirà esplora risorse del Vostro PC e Selezionare il documento che si vuole carica sul sistema di conservazione



Compilare i Campi METADATI i campi con “\*” sono Obbligatori

**Carica Documento**

File

Seleziona Documento

Aggiungi Allegato	File Allegati	Rimuovi Allegato

Metadati

NOME_FILE	ID *	DOC_DATE *	HASH
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Username_Incaricato	Nome_Incaricato	Cognome_Incaricato	PaeseFiscale_Incaricato
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
CF_Incaricato	Username_Titolare	Nome_Titolare	Cognome_Titolare
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
PaeseFiscale_Titolare	CF_Titolare	Stato_Richiesta	Profilo
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Supporto	Data_Creazione	Data_Modifica	
<input type="text"/>	<input type="text"/>	<input type="text"/>	

Conferma Annulla

Confermi

Terminati gli upload, premere su **Confermi** per inoltrare il volume e concludere il versamento.