

<b>TITOLO DOCUMENTO</b>	Manuale di Conservazione	
<b>TIPO DOCUMENTO</b>	Documento di supporto ai servizi - Manuale Operativo	
<b>EMESSO DA</b>	Telecom Italia Trust Technologies S.r.l.	
<b>AUTORE</b>	A.M. Fino, S. Rampazzo, A.P. Guarino	
<b>VERIFICATO</b>	C. Villani, E. Grechi, G. Allegrezza	
<b>APPROVATO</b>	L. Genovesi	
<b>DATA EMISSIONE</b>	<b>N. ALLEGATI</b>	<b>STATO</b>
22/10/2014	02	Rilasciato

# MANUALE DI CONSERVAZIONE

## Indice degli argomenti

<b>1</b>	<b>INFORMAZIONI GENERALI</b>	<b>6</b>
1.1	Scopo del Documento	6
1.2	Identificazione del Gestore del Servizio e del responsabile del manuale di conservazione	6
1.3	Dati identificativi dell'azienda	6
1.4	Storia delle Versioni del Manuale	7
1.5	Documenti collegati al Manuale	7
1.6	Riferimenti normativi	8
1.7	Standard	10
1.8	Glossario e acronimi	11
1.9	Soggetti che nel tempo hanno assunto il ruolo di responsabile del sistema di conservazione	14
<b>2</b>	<b>MODELLO ORGANIZZATIVO DELLA CONSERVAZIONE</b>	<b>15</b>
2.1	Organigramma	15
2.2	Ruoli e Responsabilità	15
<b>3</b>	<b>FIGURE RESPONSABILI NELL'AMBITO DEL SERVIZIO DI CONSERVAZIONE</b>	<b>19</b>
3.1	Responsabile del servizio di conservazione	19
3.2	Il Responsabile della funzione archivistica di conservazione	19
3.3	Responsabile del trattamento dei dati	19
3.4	Responsabile della sicurezza dei sistemi per la conservazione	20
3.5	Responsabile dei sistemi informativi per la conservazione	20
3.6	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	20
3.7	Deleghe	20
<b>4</b>	<b>STRUTTURA ORGANIZZATIVA SPECIFICA DEL SERVIZIO DI CONSERVAZIONE</b>	<b>21</b>
4.1	Produttore	21
4.2	Responsabile della conservazione	21
4.3	Utente	21
4.4	Attività e responsabilità del servizio di conservazione	22
4.4.1	<i>Attività relative al contratto con i Soggetti Produttori</i>	22
4.4.2	<i>Attività relative alla gestione dei sistemi informativi</i>	24

<b>5</b>	<b>RIFERIMENTI CONTRATTUALI</b>	<b>26</b>
<b>6</b>	<b>SISTEMA DI CONSERVAZIONE</b>	<b>27</b>
6.1	Descrizione generale del servizio	27
6.2	Informazione sulla rappresentazione	27
6.3	Oggetti sottoposti a conservazione	28
6.4	Documenti informatici e aggregazioni documentali informatiche	28
6.5	Unità documentaria	29
6.6	Formati	29
6.7	Apertura	31
6.8	Sicurezza	31
6.9	Portabilità	32
6.10	Funzionalità	32
6.11	Supporto allo sviluppo	32
6.12	Diffusione	32
6.13	Descrizioni Archivistiche speciali	33
6.14	Viewer	34
6.15	Informazione sulla rappresentazione sintattica	35
6.16	Informazione sulla rappresentazione semantica	35
6.17	Il pacchetto di versamento (SIP)	36
6.18	Il ruolo dei metadati nella conservazione	36
6.19	Il pacchetto di archiviazione (AIP)	41
6.20	Il pacchetto di distribuzione (DIP)	43
6.21	Gli stati del processo di conservazione	44
6.22	Le componenti del sistema di conservazione	47
6.23	Componenti principali	48
	<i>Front End:</i>	49
	<i>Back End:</i>	49
6.24	Layer Trust Services	49
6.25	Piattaforma di esercizio primario del servizio	50
6.26	Sistema di versamento (SV)	51
6.27	Sistema di gestione dati (SGD)	53
6.28	Copia del piano di conservazione	53
6.29	Sistema di memorizzazione (SM)	53

6.30	Sistema di accesso	54
6.31	Componenti software del sistema di conservazione	55
6.32	Servizi Erogati	56
6.33	Modalità di presa in carico dei pacchetti di versamento	56
	<i>Upload manuale</i>	56
	<i>Modalità SFTP</i>	57
	<i>A2A (Web Services)</i>	57
	<i>Modalità Custom</i>	57
6.34	Scalabilità sui volumi	57
6.35	Scalabilità sugli utenti	58
6.36	Sottosistema per la firma digitale e la marca temporale	58
<b>7</b>	<b>PROCESSO DI CONSERVAZIONE</b>	<b>60</b>
7.1	Il modello dati di riferimento: OAIS	60
7.2	Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico	61
7.3	Controlli preliminari	62
7.4	Costruzione del pacchetto di archiviazione	63
7.5	Conservazione del Pacchetto di Archiviazione (AIP)	63
<b>8</b>	<b>MODALITA' DI ATTIVAZIONE DI UN NUOVO SOGGETTO PRODUTTORE</b>	<b>64</b>
8.1	Il processo di provisioning	64
<b>9</b>	<b>MODALITA' DI ESIBIZIONE</b>	<b>66</b>
9.1	Pubblico ufficiale	67
<b>10</b>	<b>PIANO DI DISMISSIONE DEL SERVIZIO</b>	<b>68</b>
<b>11</b>	<b>SERVIZI DI MANUTENZIONE</b>	<b>69</b>
11.1	Approccio	69
11.2	Analisi d'impatto	69
11.3	Piano release	70
11.4	Modifiche design	70
11.5	Modifiche sorgenti e documentazione	70
11.6	Rilascio	70
11.7	Servizio di manutenzione evolutiva ed adeguativa	71
11.8	Pianificazione intervento	71
11.9	Sviluppo e rilascio	71

11.10	Manutenzione correttiva	72
<b>12</b>	<b>PRODUZIONE DI DUPLICATI E COPIE INFORMATICHE</b>	<b>74</b>
12.1	Selezione e scarto	75
<b>13</b>	<b>DISASTER RECOVERY</b>	<b>76</b>
<b>14</b>	<b>MONITORAGGI E CONTROLLI ACCETTAZIONE PDV</b>	<b>77</b>
14.1	Verifica l'integrità degli archivi	78
<b>15</b>	<b>MONITORAGGIO DEI SISTEMI</b>	<b>79</b>
<b>16</b>	<b>Movimentazioni massive di dati conservati</b>	<b>79</b>
16.1	Accettazione dati conservati da altri outsourcer.	80
16.2	Esportazione dati per fine contratto (non rinnovato)	80
16.3	Modalità di restituzione	80
16.4	Flusso di deprovisioning	80
<b>17</b>	<b>SERVIZI DI HELP DESK</b>	<b>82</b>
<b>18</b>	<b>LIVELLI DI SERVIZIO</b>	<b>83</b>
18.1	Disponibilità	83
18.2	Limiti di applicabilità dello SLA	83
<b>19</b>	<b>CONDIZIONI DI UTILIZZO DEL SERVIZIO DI CONSERVAZIONE</b>	<b>85</b>
19.1	Obblighi di TI Trust Technologies	85
19.2	Obblighi del Cliente	85
19.3	Limitazione ed esclusione delle responsabilità di TI Trust Technologies	85
19.4	Polizza assicurativa del Gestore del Servizio	86
19.4.1	<i>Compiti per la protezione dei dati e delle procedure informatiche</i>	87
<b>20</b>	<b>MODULISTICA DEL SERVIZIO</b>	<b>88</b>
20.1	Scheda di attivazione del servizio	88
20.2	Condizioni di Utilizzo del Servizio	88
20.3	Nomina di TI Trust Technologies quale Responsabile del servizio di Conservazione	88

## 1 INFORMAZIONI GENERALI

### 1.1 Scopo del Documento

Questo documento illustra le regole generali e le procedure seguite da Telecom Italia Trust Technologies S.r.l. (in breve TI.TT) nell'**erogazione del servizio di conservazione** del DPCM (Decreto del Presidente del Consiglio dei Ministri) del 3 Dicembre 2013, art.8.

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 originariamente analogici e informatici, trasferiti da Cliente Finale ad TI Trust Technologies;
- 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 Trust Technologies: <http://www.trusttechnologies.it>;
- Il manuale di conservazione è un documento informatico.

### 1.2 Identificazione del Gestore del Servizio e del responsabile del manuale di conservazione

La società TI Trust Technologies, con sede in Pomezia (RM) – S.S. 148 Pontina, km. 29,100 e CAP 00040 è una società del Gruppo Telecom Italia (Direzione e coordinamento di Telecom Italia S.p.A.) con unico socio Telecom Italia S.p.A.

Il responsabile del presente Manuale di conservazione è Cinzia Villani, responsabile della struttura operativa della società.

### 1.3 Dati identificativi dell'azienda

Denominazione sociale	Telecom Italia Trust Technologies S.r.l.
Indirizzo sede legale	S.S.148 Pontina, km. 29,100 00040 - Pomezia (RM)
Amministratore Delegato	Leopoldo Genovesi
n. P.IVA	04599340967
n. telefono ( centralino)	+3906911971

n.fax	+390691197331
Sito internet	www.trusttechnologies.it
Indirizzo Pec	TI.TT@ttpec.telecomitalia.it
Referente tecnico cui rivolgersi in caso di problemi tecnico operativi	CALL CENTER:
Indirizzo	S.S.148 Pontina, km. 29,100 00040 - Pomezia (RM)
n. telefono	800.28.75.24
indirizzo posta elettronica	<a href="mailto:clienti-ca@telecomitalia.it">clienti-ca@telecomitalia.it</a>

Tab.1

## 1.4 Storia delle Versioni del Manuale

Si riporta la storia delle modifiche apportate al manuale di conservazione.

DETTAGLIO REVISIONI				
VERSIONE	VARIAZIONI	DATA	AUTORE	APPROVAZIONE
10	CONSSOST.IT.POM0102287 00 - Manuale Operativo CS	25/02/2010	<b>F. Lappa, R. Pomarico, A. P. Guarino, E. Grechi, A.M. Fino</b>	Cinzia Villani
2.0	CERTSOS2.IT.DUMU11000	29/09/2011	<b>S. Bellio</b>	Cinzia Villani
3.0	EVOCAST.TT.POM014000.00	01/08/2014	<b>A.M. Fino, S. Rampazzo, A.P. Guarino</b>	Cinzia Villani

Tab.2

## 1.5 Documenti collegati al Manuale

Al presente manuale sono allegati i seguenti documenti:

DETTAGLIO COLLEGATI				
CODICE	DOCUMENTO	DATA	AUTORE	APPROVAZIONE
CURR_VR	EVOCAST.TT.ALMO14004 - Allegato Curricula Responsabili.docx	19/09/2014	<b>A.M. Fino, S. Rampazzo, A.P. Guarino</b>	Cinzia Villani

PSES_G	CAITPRIN.TT.QUPS11000 - Piano della Sicurezza Generale Erogazione Servizi TITT (Documento citato)	24/02/2011	<b>G.Tovo</b>	Cinzia Villani
PSES_C	CERTQUAL.TT.QUPS14000 - Piano della Sicurezza del Servizio di Conservazione (Documento citato)	23/09/2014	<b>E.Grechi, A.P.Guarino</b>	Cinzia Villani
REGI_FM	EVOCST.TT.ALMO14002 - Allegato Registro Formati e Metadati.docx	01/08/2014	<b>A.M. Fino, S. Rampazzo, A.P. Guarino</b>	Cinzia Villani

Tab.3

## 1.6 Riferimenti normativi

Si riporta un elenco dei principali riferimenti normativi in materia, in riferimento ai luoghi in cui sono conservati i documenti (art. 8 comma 2 lett. 1 DPCM 3 dicembre 2013)

<b>[DPCM 2012]</b>	<p><b>Decreto legislativo 30 giugno 2003 n. 196</b> e s.m.i. –, Codice in materia di protezione dei dati personali (legge delega n. 127/2001).</p> <ul style="list-style-type: none"> <li>– 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;</li> </ul> <p><b>Deliberazione Cnipa 21 Maggio 2009, n. 45</b> “Regole per il riconoscimento e la verifica del documento informatico.</p>
<b>DMEF 2014</b>	<p><b>Decreto del Ministero dell’Economia e delle Finanze 17 giugno 2014</b> Modalita' di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005.</p>
<b>CAD</b>	<p><b>Deliberazione Cnipa 19 febbraio 2004, n.11</b> Regole tecniche per la riproduzione e conservazione su supporto ottico idoneo a garantire la conformità dei documenti agli originali.</p> <p><b>Decreto Legislativo 7 marzo 2005, n. 82</b> e s.m.i. – – Codice dell’amministrazione digitale.</p>



<p><b>D.P.C.M. 3 Dicembre 2013</b></p>	<p><b>Decreto del Presidente del Consiglio dei Ministri del 3 Dicembre 2013</b> - 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. Il presente DPCM è entrato in vigore l'11 aprile 2014.</p> <p><b>Legge numero 244 del 24 dicembre 2007</b> , Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato ( legge finanziaria 2008).</p>
	<p><b>Decreto del Ministero dell'Economia e delle Finanze 3 aprile 2013 n. 55</b> Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'art. 1, commi da 209 a 213, della legge 24 dicembre 2007, n. 244.</p> <p><b>Circolare interpretativa 31 marzo 2014, n. 1 sul DM 55/2013.</b></p> <ul style="list-style-type: none"> <li>- 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;</li> <li>- 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.</li> </ul>
	<ul style="list-style-type: none"> <li>- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;</li> </ul>
	<ul style="list-style-type: none"> <li>- 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;</li> </ul>

 TELECOM ITALIA DIGITAL SOLUTIONS	<b>Manuale di Conservazione</b>	Codice: <b>EVOCST.TT.POM014000</b>	Revisione  00
		Stato: Rilasciato	


**Tab.4**

Le normative applicate al Bata Center della Certification Authority TI.T.T. sono la ISO/IEC 27001:2005 e la ISO/IEC 9001:2008. Inoltre, Telecom Italia ha ottenuto la certificazione autonoma di tutti i suoi Data Center (BS7799, divenuta in seguito ISO27001).

La normativa di riferimento varia a seconda della particolarità degli oggetti digitali.

## **1.7 Standard**

Così come richiesto dal DPCM 3 dicembre 2013 e, nello specifico dall'allegato 3, si riportano gli standard per la conservazione dei documenti informatici:

- 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.



Tutte le caratteristiche del servizio di Conservazione di TI Trust Technologies sono descritte nel presente Manuale Operativo.

Per ciascun Cliente, TI Trust Technologies compila e tiene aggiornata una Scheda di Attivazione del servizio nella quale sono indicate le caratteristiche specifiche che assume il servizio per il Cliente.

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

## 1.8 Glossario e acronimi

TERMINE	DEFINIZIONE
accesso	operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici
accreditamento	riconoscimento, da parte dell' <b>Agenzia per l'Italia digitale</b> , 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 supporto informatico di un documento analogico	dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico
autenticità	caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico
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' <b>Agenzia per l'Italia digitale</b> , 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 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' <b>Agenzia per l'Italia digitale</b> , il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, dall' <b>Agenzia per l'Italia digitale</b>

<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>copia analogica del documento informatico</b>	documento analogico avente contenuto identico a quello del documento informatico da cui è tratto
<b>copia di sicurezza</b>	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
<b>destinatario</b>	identifica il soggetto/sistema al quale il documento informatico è indirizzato
<b>esibizione</b>	operazione che consente di visualizzare un documento conservato e di ottenerne copia
<b>estratto per riassunto</b>	documento nel quale si attestano in maniera sintetica ma esaustiva fatti, stati o qualità desunti da dati o documenti in possesso di soggetti pubblici
<b>evidenza informatica</b>	una 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>formato</b>	modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
<b>funzione di hash</b>	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
<b>generazione automatica di documento informatico</b>	formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni
<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>immodificabilità</b>	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
<b>impronta</b>	la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di <i>hash</i>
<b>insieme minimo di metadati del documento informatico</b>	complesso dei metadati, la cui struttura è descritta nell'allegato 5 del presente decreto, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta
<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>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 presente decreto
<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>piano generale della sicurezza</b>	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
<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>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>registrazione informatica</b>	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
<b>riferimento 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>sistema di conservazione</b>	sistema di conservazione dei documenti informatici di cui all'articolo 44 del Codice

Tab.5

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>DIP:</b>	Dissemination Information Package (Pacchetto di distribuzione)
<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.
<b>VdC:</b>	volumi di conservazione

Tab.6

## 1.9 Soggetti che nel tempo hanno assunto il ruolo di responsabile del sistema di conservazione

Nella seguente tabella si citano i nominativi e i dati dei soggetti che nel tempo hanno assunto la responsabilità del sistema di conservazione.

Nominativo	Ruolo	Data inizio mandato	Data fine mandato
Ing. Giancarlo De Jacovo	Amministratore Delegato I.I. Telecom	25/02/2009	02/03/2009
Dott. Guido Allegrezza	Responsabile dei servizi Governance	02/03/2009	Mandato in vigore

Tab.7

## 2 MODELLO ORGANIZZATIVO DELLA CONSERVAZIONE

### 2.1 Organigramma

Responsabilità del conservatore TI TRUST TECHNOLOGIES

TI Trust Technologies, si configura come soggetto 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, pur prevedendo, il richiamato DPCM 3/12/2013, la possibilità di delegare, sotto la propria responsabilità, lo svolgimento del processo di conservazione o di parte di esso ad uno o più soggetti di specifica competenza ed esperienza in relazione alle attività ad essi delegate.

Secondo quanto stabilito dall'art. 6 co. 8 del DPCM 3 dicembre 2013 e, secondo quanto previsto dal Codice in materia di protezione dei dati personali, il conservatore TI TRUST TECHNOLOGIES assume il ruolo di responsabile del trattamento dei dati, come individuato da specifico atto scritto.

Tutte le persone coinvolte nel servizio di conservazione sono state incaricate al trattamento dei dati per l'attività di conservazione.

Nel contratto di affidamento del servizio di conservazione con il Produttore si riconosce a quest'ultimo la titolarità del trattamento dei dati contenuti nei documenti oggetto di conservazione in capo al Produttore

Si riporta l'organigramma della struttura organizzativa coinvolta nel servizio di conservazione:

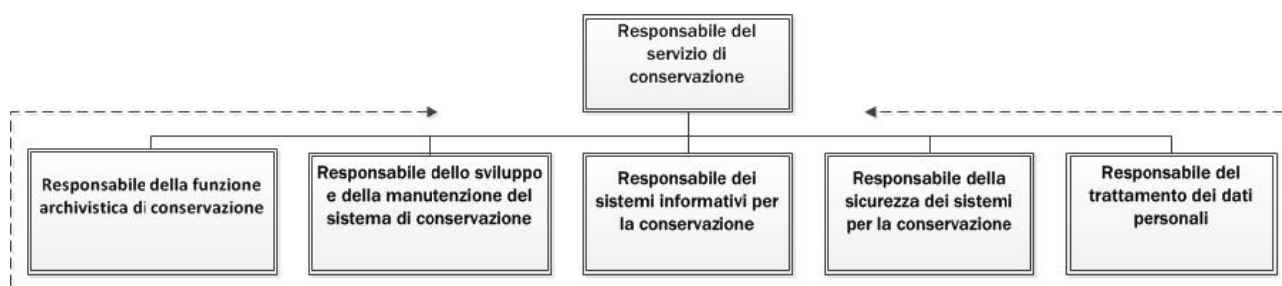


Fig.1

### 2.2 Ruoli e Responsabilità

Ruolo	Attività di competenza	Nominativo
Responsabile del servizio di conservazione	<p><b>Guido Allegrezza</b> in qualità di <b>responsabile del servizio di conservazione</b> 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</li> </ul>	<b>Guido Allegrezza</b>



	<p>conservazione in conformità alla normativa vigente;</p> <ul style="list-style-type: none"> <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 garantisce 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 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>	
<p>Responsabile della funzione archivistica di conservazione</p>	<p><b>Stefania Rampazzo</b> in qualità di <b>responsabile della funzione archivistica di conservazione</b> 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>- definizione del 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>- collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza;</li> <li>- supporto al responsabile del servizio di conservazione nell'acquisizione del pacchetto di versamento ed è presente nelle verifiche e controlli dell'autorità di competenza.</li> <li>- aggiornamento alle normative e formazione dell'organizzazione che segue il servizio di conservazione.</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</p>	<p><b>Stefania Rampazzo</b> <b>Contratto di consulenza della durata di tre anni, rinnovabile.</b></p>



	<p>archivistica di conservazione sono di seguito riportare:</p> <ul style="list-style-type: none"> <li>• Gestisce le modalità di trasferimento, esibizione e fruizione dei documenti informatici</li> <li>• Definizione delle informazioni sulla rappresentazione e delle informazioni sulla 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>• Il responsabile della funzione archivistica di conservazione si interfacerà con il soggetto produttore qualora sia necessario procedere allo scarto delle tipologie documentarie.</li> <li>• Avrà il compito di formare e aggiornare la struttura organizzativa coinvolta nel processo di conservazione</li> </ul>	
Responsabile del trattamento dei dati personali	<p><b>Cinzia Villani</b> in qualità di <b>responsabile del trattamento dei dati personali</b> espleta le seguenti attività:</p> <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>Cinzia Villani</b>
Responsabile della sicurezza dei sistemi per la conservazione	<p><b>Enrico Cavallo</b> in qualità di <b>responsabile della sicurezza dei sistemi per la conservazione</b> espleta le seguenti attività:</p> <ul style="list-style-type: none"> <li>- Rispetto e monitoraggio dei 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>	<b>Enrico Cavallo</b>
Responsabile dei sistemi informativi per la conservazione	<p><b>Francesca Mazzanti</b> in qualità di <b>responsabile dei sistemi informativi per la conservazione</b> espleta le seguenti attività:</p> <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>
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	<p><b>Elena Grechi</b> in qualità di <b>responsabile dello sviluppo e della manutenzione del sistema di conservazione</b> espleta le seguenti attività:</p> <ul style="list-style-type: none"> <li>- Coordina lo sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione;</li> </ul>	<b>Elena Grechi</b>

	<ul style="list-style-type: none"><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>- change management</li></ul>	
--	---	--

**Tab.8**

I curricula dei responsabili citati nella tabella sopradescritta sono oggetto del documento in allegato al presente manuale, con il codice [[CURR\\_VR](#)]

### 3 FIGURE RESPONSABILI NELL'AMBITO DEL SERVIZIO DI CONSERVAZIONE

Il presente documento elenca quali sono le figure professionali che compongono il gruppo di lavoro sulla conservazione dei documenti, al fine di garantire la corretta esecuzione del servizio, relativamente a tutte le problematiche tecnico/organizzative peculiari.

Tutte le procedure interne sono espletate sulla base dello standard mandatorio ISO27001 e ISO9001.

#### 3.1 Responsabile del servizio di conservazione

Il Responsabile del conservatore TI TRUST TECHNOLOGIES è Guido Allegrezza, Responsabile dei servizi di Governance e Conservazione. La sua nomina è stata formalizzata in data 01/03/2009. Tale nomina è stata controfirmata per accettazione dal responsabile nominato. I precedenti responsabili sono elencati al paragrafo 1.9.



**Il Servizio di Conservazione descritto nel presente Manuale di conservazione strutturato in modo tale da poter garantire l'esecuzione delle attività, affidate ad TI Trust Technologies, in qualità di Responsabile della Conservazione designato dal Produttore, come specificato successivamente.**

**TI Trust Technologies, nell'ambito del suo ruolo di conservatore e designato dal Produttore, non sottopone a nessun trattamento di verifica il contenuto dei documenti che le sono inviati per sottoporli al processo di Conservazione..**

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

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

Il responsabile della funzione archivistica del conservatore TI TRUST TECHNOLOGIES è Stefania Rampazzo. La sua nomina è stata formalizzata attraverso la stipula di un contratto di consulenza della durata di tre anni tra TI TRUST TECHNOLOGIES e IFIN Sistemi srl. La nomina decorre dal 01/10/2014.

#### 3.3 Responsabile del trattamento dei dati

Attualmente questo ruolo è ricoperto dalla dott.ssa Cinzia Villani. La nomina è stata formalizzata in forma scritta ed è stata controfirmata per accettazione dal responsabile designato. La nomina decorre dal 01/10/2014. Non ci sono precedenti responsabili.

### **3.4 Responsabile della sicurezza dei sistemi per la conservazione**

Il responsabile della sicurezza dei sistemi di conservazione del conservatore TI TRUST Technologies è Enrico Cavallo. La nomina è stata formalizzata e controfirmata per accettazione dal responsabile designato. La nomina decorre dal 01/10/2014.

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

Il responsabile dei sistemi informativi di conservazione del conservatore TI TRUST Technologies è Francesca Mazzanti. La nomina è stata formalizzata e controfirmata per accettazione dal responsabile designato. La nomina decorre dal 01/10/2014.

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.

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

Il **Responsabile dello sviluppo e della manutenzione del sistema di conservazione** è Elena Grechi. La nomina è stata formalizzata e controfirmata per accettazione dal responsabile designato. La nomina decorre dal 01/10/2014. 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 Legal Archive®. Il responsabile monitora e verifica le operazioni del sistema di conservazione. Inoltre il responsabile dello sviluppo monitora d'intesa con il responsabile del servizio di conservazione della sicurezza fisica e logica dell'impianto di IT Trust Technologies. 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.

### **3.7 Deleghe**

Al momento l'attività è espletata dai responsabili. Non sono state formalizzate deleghe di funzione.

## 4 STRUTTURA ORGANIZZATIVA SPECIFICA DEL SERVIZIO DI CONSERVAZIONE

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

### 4.1 Produttore

Il **Produttore (Cliente)**: il soggetto (persona fisica o giuridica, interna o esterna al sistema di conservazione) proprietario e responsabile, a tutti gli effetti, dei documenti che devono essere sottoposti al processo di Conservazione. Il Produttore è responsabile del contenuto del pacchetto di versamento (d'ora in poi SIP). Il responsabile di riferimento del Produttore è di norma il responsabile della gestione documentale.

.Nel contratto di affidamento del servizio di conservazione tra Produttore e conservatore si regoleranno i rapporti di servizio, la responsabilità delle parti e le condizioni economiche.

Il responsabile della funzione archivista del conservatore di TI TRUST TECHNOLOGIES avrà cura di definire con i soggetti responsabili interni all'ente Produttore, le tipologie degli oggetti da sottoporre al processo di conservazione. Le modalità di versamento verranno specificate nel documento "DESCRIZIONE DEL SERVIZIO", allegato al contratto di mandato di affidamento.

Il produttore mantiene la titolarità e la proprietà dei documenti versati al soggetto conservatore.

### 4.2 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 produttore e conservatore vengono definite le attività e le responsabilità affidate dall'ente produttore al conservatore TI TRUST TECHNOLOGIES.

### 4.3 Utente

Costituiscono le comunità di riferimento che interagiscono con il conservatore ai documenti 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.

## 4.4 Attività e responsabilità del servizio di conservazione

Riguardo alle principali attività del servizio di conservazione, si descrive di seguito la struttura organizzativa ne assume le responsabilità e le modalità di presa in carico.

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

L'attività del servizio di con presa in carico da TI.TT, viene espletata a seguito della sottoscrizione di un contratto per il servizio di conservazione con il soggetto produttore. TI.TT predispone la redazione del contratto attraverso l'area commerciale-amministrativa della società.

Il contratto consente l'avvio delle attività di attivazione del servizio. La responsabilità di tale sotto processo è del responsabile del trattamento dei dati personali, Cinzia Villani. Attraverso l'area del Provisioning, detto responsabile coordina e gestisce l'attivazione del servizio di conservazione per il Soggetto 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.

Questa attività il responsabile di area nella persona del Dott. Guido Allegrezza, il quale è coadiuvato dal responsabile del servizio archivistico, la Dott.ssa Stefania Rampazzo, che si interfaccia per la scelta sulle informazioni sulla rappresentazione con il Soggetto Produttore e, nello specifico, con un suo responsabile interno. Per maggiori dettagli afferenti al pacchetto di versamento si rimanda al manuale operativo di Legal Archive® cap. 18.

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

Il responsabile del servizio di conservazione, per i pacchetti accettati, provvede alla preparazione e alla gestione del pacchetto di archiviazione. Detto pacchetto viene così firmato e marcato digitalmente, così da poter essere fruito a chi ne farà richiesta, secondo la normativa vigente, come pacchetto di distribuzione. Le procedure operative sono poi dettagliate nel manuale operativo di Legal Archive® cap. 16.

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. Per maggiori dettagli sulla procedura operativa, si fa riferimento al manuale operativo Legal Archive® al cap. 19.

I processi di selezione e scarto sono sotto la gestione del responsabile del servizio, coadiuvato dal responsabile della funzione archivistica di conservazione. Essi sono descritti nel dettaglio nel paragrafo 11.1 del presente manuale.

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 gestione e la responsabilità di tali attività sono in carico al responsabile del trattamento dei dati, Cinzia Villani.

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 trattamento dei dati (Cinzia Villani)	Provisioning
Acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento.	Responsabile del servizio di conservazione (Guido Allegrezza), supporto del Responsabile della funzione archivistica di conservazione.	Controlli di processo e di sistema
Preparazione e gestione del pacchetto di archiviazione.	Responsabile del servizio di conservazione (Guido Allegrezza)	Controlli di processo e di sistema
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 (Guido Allegrezza)	Controlli di processo e di sistema
Scarto dei pacchetti di archiviazione.	Responsabile del servizio di conservazione (Guido Allegrezza), supporto del Responsabile della funzione archivistica di conservazione.	Controlli di processo e di sistema
Chiusura del servizio di conservazione (al termine di un contratto).	Responsabile del trattamento dei dati (Cinzia Villani)	Deprovisioning

**Tab.9**

#### 4.4.2 Attività relative alla gestione dei sistemi informativi

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

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

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 (Elena Grechi). Esso serve per garantire la leggibilità nel tempo dei documenti conservati ed evitare che l'obsolescenza dei sistemi possa pregiudicarne l'esibizione.

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

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

Attività	Responsabilità	Area di competenza
Conduzione e manutenzione del sistema di conservazione;	Responsabile dei sistemi informativi (Francesca Mazzanti)	Esercizio piattaforme applicative e sistemi
Monitoraggio del sistema di conservazione;	Responsabile dei sistemi informativi (Francesca Mazzanti)	Esercizio piattaforme applicative e sistemi
Change management;	Responsabile dello sviluppo e della manutenzione del sistema di conservazione (Elena Grechi)	Manutenzione e delivery



Verifica periodica di conformità a normativa e standard di riferimento	Responsabile della funzione archivistica di conservazione (Stefania Rampazzo)	Normative e standard
--	---	----------------------

**Tab.10**

## 5 RIFERIMENTI CONTRATTUALI

In questo capitolo vengono elencati i documenti relativi al contratto di affidamento del servizio di conservazione tra soggetto produttore e soggetto conservatore.

Il sistema di conservazione erogato da TI Trust Technologies è regolato dai seguenti documenti contrattuali:

- a. Contratto di affidamento del servizio di conservazione
- b. Schede per l'attivazione del servizio di conservazione
- c. Atti di nomina dei responsabili di area
- d. Atto di nomina responsabile al trattamento dei dati
- e. Manuale operativo Legal Archive

## 6 SISTEMA DI CONSERVAZIONE

### 6.1 Descrizione generale del servizio

La conservazione a norma è finalizzata all'estensione e al mantenimento della validità dei documenti conservati di cui ne garantisce nel tempo la fruibilità, l'inalterabilità e la validità ai fini legali.

Telecom Italia Trust Technologies fornisce il servizio di conservazione ai propri clienti eseguendo, in qualità di conservatore, le attività necessarie alla conservazione dei documenti inviati dal Soggetto Produttore, assumendo il ruolo di Responsabile della conservazione, su delega esplicita del Soggetto Produttore.

Le attività svolte da TI.TT nel ruolo di Responsabile del servizio di conservazione sono descritte nell'Art.7 comma 1 del DPCM 3 Dicembre 2013.

### 6.2 Informazione sulla rappresentazione

Lo standard OAIS prevede che, ad ogni oggetto portato in conservazione, vengano associate un insieme di informazioni (metadati) che ne permetta in futuro una facile reperibilità e 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.

È necessario, inoltre, ricordare che un sistema di conservazione che rispetti la normativa italiana, deve garantire il requisito di **leggibilità** degli oggetti dati conservati imposto dal comma 1 dell'art. 3 delle nuove regole tecniche e dal comma 1 dell'art. 44 del Codice dell'Amministrazione Digitale.

Per soddisfare questi requisiti, prima di versare un qualsiasi oggetto digitale nel sistema di conservazione, è necessario che il responsabile della conservazione, in accordo con il soggetto produttore, proceda a conservare tutte le informazioni sulla rappresentazione necessarie alla futura consultazione di tale oggetto.

Classifichiamo quindi le informazioni sulla rappresentazione in:

- **Strumenti per la leggibilità:** tipicamente legati al formato dell'oggetto conservato (Viewer).
- **Informazioni sulla rappresentazione sintattica:** tipicamente legate al formato dell'oggetto conservato (per esempio il documento di specifiche tecniche del formato del file).
- **Informazioni sulla rappresentazione semantica:** tipicamente legate alla descrizione archivistica dell'oggetto conservato (per esempio come leggere il contenuto di una fattura).

Per soddisfare l'eventuale necessità di una disponibilità immediata dell'oggetto conservato il sistema di conservazione deve avere almeno conservati gli strumenti per la leggibilità (visualizzatori) degli oggetti dati da conservare.

Le informazioni sulla rappresentazione, semantiche e sintattiche, e i visualizzatori potranno essere inglobate nel pacchetto di distribuzione assieme ai documenti richiesti garantendo così la piena leggibilità nel lunghissimo periodo del documento conservato.

Sarà compito del sistema di conservazione creare il pacchetto di distribuzione aggiungendo per ciascun file le corrette informazioni sulla rappresentazione ad esso correlate, e sarà compito del responsabile del servizio di conservazione configurare correttamente il software e mantenere aggiornate tali informazioni sulla rappresentazione.

### 6.3 Oggetti sottoposti a conservazione

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

### 6.4 Documenti informatici e aggregazioni documentali informatiche

Il Sistema di conservazione, gestito da TI Trust Technologies, conserva Documenti informatici, in particolare documenti amministrativi informatici, con i metadati ad essi associati e le loro aggregazioni documentali informatiche (aggregazioni), che includono i fascicoli informatici (fascicoli).

Tale modello riprende quello gerarchico di ordinamento di un Archivio, illustrato nella figura seguente, derivata dallo schema dello standard ISAD.

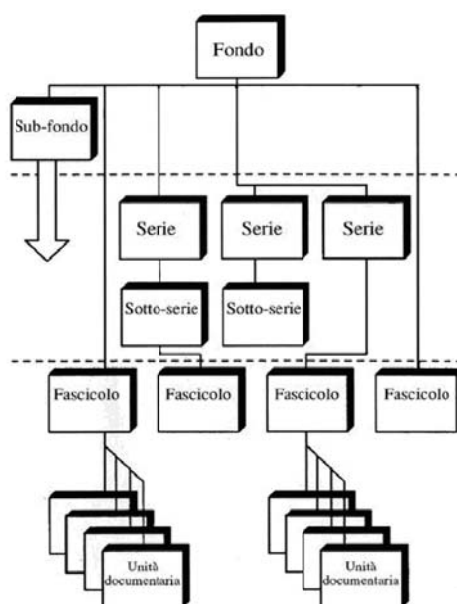


Fig.2

I documenti informatici e le loro aggregazioni di tipo Fascicolo sono trattati nel sistema nella forma di unità documentarie e fascicolo, specificamente descritte in questo documento, e sono inviati in conservazione sotto forma di pacchetti di versamento (SIP), che contengono anche i relativi metadati.

Il sistema gestisce gli oggetti sottoposti a conservazione distinti per ogni singolo soggetto produttore anche per singola struttura (generalmente corrispondenti alle Aree Organizzative Omogenee), consentendo di definire configurazioni e parametrizzazioni ad hoc per ogni Soggetto Produttore, in base agli accordi stipulati all'atto della sottoscrizione del servizio.

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 e l'eventuale articolazione in sottofascicoli. Inoltre è gestita la presenza di classificazioni, fascicoli e sottofascicoli secondari e collegamenti tra le diverse Unità archivistiche e documentarie presenti nel Sistema.

Le serie ed i fascicoli possono essere versati nel Sistema quando sono completi e dichiarati chiusi, descritte 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 possono essere 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 e i loro specifici metadati e articolazioni, sono indicate nell'allegato di servizio concordato con ogni soggetto produttore e riportate nelle funzionalità di amministrazione del Sistema.

## **6.5 Unità documentaria**

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 lo standard OAIS.

Con riferimento a quanto indicato nello standard ISO 23081-2, l'unità documentaria, rappresenta la più piccola "*unit of records*" individuabile e gestibile come una entità singola gestita nel Sistema, anche se al suo interno contiene elementi come ad esempio un messaggio di posta elettronica con i suoi allegati.

All'unità documentaria e agli elementi che la compongono sono associati set di metadati che li identificano e li descrivono.

Coerentemente con quanto sopra riportato l'unità documentaria è pertanto logicamente strutturata su tre livelli: unità documentaria, documento, File.

## **6.6 Formati**

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” [[REGI\\_FM](#)] in cui ogni Formato è corredato da Informazioni descrittive relative alla eventuale versione, e al Mimetype.

Con ogni Soggetto Produttore è concordato un elenco di formati ammessi, che individua i formati che il Sistema può accettare da ogni Produttore e per ogni tipologia documentaria gestita. L’elenco dei formati ammessi è riportato (e gestito) nelle funzionalità “Amministrazione strutture versanti” del Sistema ed è aggiornato continuamente in base alle esigenze del Produttore. Le modalità con cui si procede a tale aggiornamento sono concordate con ogni Produttore e riportate nell’allegato “Registro dei Formati” [[REGI\\_FM](#)].

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 a 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	MIME	Si	ISO/IEC DIS 29500:2008
ODF Open Document Format	OASIS	.ods, .odp, .odg, .odb	application/vnd.oasis.opendocument.text	Si	ISO/IEC 26300:2006; UNI CEI ISO/IEC 26300
XML Extensible Markup Language	W3C	.xml	application/xml text/xml	Si	
TXT	-	.txt	ASCII, UTF-8, UNICODE	Si	ISO 646, RFC 3629, ISO/IEC 10646
PEC ed EMAIL	-	.eml	MIME	No	RFC 2822/MIME

**Tab.11**

Le caratteristiche che sono state considerate nella scelta sono:

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

## 6.7 Apertura

Un formato si dice “aperto” quando è 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.

## 6.8 Sicurezza

La sicurezza di un formato dipende da due elementi: il grado di modificabilità del contenuto del file e la capacità di essere immune dall’inserimento di codice maligno. Nel sistema di conservazione a

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

norma di TI.TT i pacchetti di riversamento vengono sottoposti a scansione antivirus con verifica dei file e archivi compressi multilivello. Ogni file compresso è quindi controllato anche se si tratta di compressioni ripetute (tecnica utilizzata per evitare che l'antivirus controlli i file di un archivio compresso). Gli antivirus utilizzati sono costantemente aggiornati. L'invio dei file, inoltre, avviene attraverso linee controllate da firewall e Intrusion detector.

## 6.9 Portabilità

Per portabilità si intende la facilità con cui i formati possano essere usati su piattaforme diverse, sia dal punto di vista dell'hardware che del software, inteso come sistema operativo. 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.

## 6.10 Funzionalità

Per funzionalità si intende la 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.

Per questo criterio TI.TT ha scelto formati che consentono l'utilizzo di software che consentano diverse funzionalità. E' infatti 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.

## 6.11 Supporto allo sviluppo

E' 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.). Per rispettare questo criterio TI.TT ha scelto i formati di software house che permettano contratti di manutenzione e di seguire le varie versioni nel tempo.

## 6.12 Diffusione

La 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. La questione ha impatti sul fatto che un formato possa avere la disponibilità di più prodotti informatici idonei alla sua gestione e visualizzazione. TI.TT ha quindi scelto formati comuni, con una distribuzione capillare, consigliando ai propri clienti l'adozione degli stessi.



## 6.13 Descrizioni Archivistiche speciali

Lo standard OAIS prevede che, ad ogni oggetto 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 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, prima di versare un qualsiasi oggetto digitale nel sistema di conservazione è necessario che il responsabile del servizio di conservazione, in accordo con il soggetto produttore, proceda a conservare tutte le informazioni sulla rappresentazione necessarie alla consultazione di tale oggetto.

Classifichiamo quindi le informazioni sulla rappresentazione in:

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 dati da conservare.

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 della conservazione di conservare le tre tipologie di informazioni sulla rappresentazione.

Distinguiamo tre descrizioni archivistiche speciali:

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.

 <small>TELECOM ITALIA DIGITAL SOLUTIONS</small>	<b>Manuale di Conservazione</b>	Codice: <b>EVOCAST.TT.POM014000</b>	Revisione  00
		Stato: Rilasciato	

Le descrizioni archivistiche speciali sono descrizioni archivistiche i cui documenti conservati non hanno nessuna associazione con le informazioni sulla rappresentazione.

La prima deve essere obbligatoria, e oltre ai classici metadati *Dublin Core*, deve permettere di associare ad ogni documento conservato (eseguibile del visualizzatore) la versione del visualizzatore, la lingua del visualizzatore, il sistema operativo di riferimento (versione, bit, lingua).

Le operazioni per il suo versamento possono essere effettuate sia attraverso un pacchetto di versamento (file di metadati di tipo multi indice) che manualmente da interfaccia web.

Le descrizioni archivistiche per “Fascicolo Informazioni sulla rappresentazione” e per “Informazioni sulla rappresentazione” sono già presenti e non necessitano di ulteriori modifiche nelle loro definizioni. Esse potranno memorizzare le informazioni sulla rappresentazione sia di tipo sintattico che di tipo semantico, distinguendole tra di loro attraverso il metadato Dublin Core “Tipo”.

Dal punto di vista delle funzionalità invece si rende necessario tener presente i seguenti scenari:

- La conservazione di un nuovo “Viewer” per un Mime Type già associato ad un Software precedente deve andare in aggiunta.
- Sarà sempre possibile modificare il metadato “Data Fine” per un “Software” se non ci sono conservazioni successive alla “data fine” inserita.
- la modifica di un solo documento di un “fascicolo Informazioni sulla rappresentazione” – nel caso in cui cambiano le specifiche di un formato file - prevede la riconservazione dell’intero fascicolo, per cui dovrebbero essere creati gli automatismi che permettano l’interazione con l’utente per gestire questo caso.
- Va inoltre introdotta la possibilità di versare manualmente un fascicolo attraverso l’interfaccia web oppure un documento che va ad aggiungersi ad un fascicolo esistente.

Le descrizioni archivistiche speciali, sono di norma conservate per il SP titolare della licenza Legal Archive® ed ereditate da tutti gli altri SP. In generale l’ereditarietà delle Informazioni sulla rappresentazione si sviluppa come nel classico schema di ereditarietà:

Soggetto Produttore → Soggetto Produttore Padre → ... → Soggetto Produttore Padre → Soggetto Conservatore → Soggetto Conservatore Licenziatario.

## 6.14 Viewer

Il viewer associato ad un oggetto conservato (UID nel PdA) deve poter risalire alla seguente n-pla:

- formato (mime type);
- eventuale versione del formato;
- versione dello strumento di visualizzazione;
- lingua dello strumento di visualizzazione;
- versione del sistema operativo.

Visto che questa n-pla permette di avere diversi strumenti per uno stesso mime type, il sistema di conservazione deve permettere ad un responsabile del servizio di conservazione di impostare a livello di soggetto produttore e/o a livello di descrizione archivistica (di tipo Documento), quali

siano gli strumenti per la leggibilità di un formato da collegare all'atto della conservazione e all'atto dell'esibizione.

Tale associazione dovrà essere creata mediante un nuovo pannello da inserire nelle finestre: Soggetto Produttore e Descrizione archivistica. Questo pannello permette di selezionare la n-pla precedente descritta. Nel caso non sia definita nella descrizione archivistica, si procederà con il classico schema di ricerca gerarchica:

Soggetto Produttore → Soggetto Produttore Padre → ... → Soggetto Produttore Padre → Soggetto Conservatore → Soggetto Conservatore Licenziatario

All'inizio di ogni conservazione è indispensabile aggiungere un controllo che verifichi se esiste una sola n-pla per la DA che si sta conservando o per il SP che sta conservando.

## 6.15 Informazione sulla rappresentazione sintattica

Per quanto riguarda le informazioni sulla rappresentazione sintattica, essendo anche queste legate al mime type e alla relativa versione, si rende necessario fare in modo che ogni oggetto in un il pacchetto di archiviazione si riferisca ad uno o più UID/ID che permettano di risalire all'n-pla:

- formato (mime type)
- eventuale versione del formato

Queste informazioni non si distinguono a livello di descrizione archivistica o soggetto produttore in quanto sono le specifiche internazionali sul formato in oggetto.

## 6.16 Informazione sulla rappresentazione semantica

Per quanto riguarda le informazioni sulla rappresentazione semantica, essendo anche queste legate ad una particolare versione di una descrizione archivistica, si rende necessario fare in modo che ogni oggetto in un il pacchetto di archiviazione si riferisca ad uno o più UID/ID che permettano di risalire all'id della descrizione archivistica.

## 6.17 Il pacchetto di versamento (SIP)

Si tratta del pacchetto informativo inviato dal soggetto produttore al sistema di conservazione e oggetto dell'accordo stipulato in occasione del Contratto di servizio. Per maggiori informazioni afferenti alla descrizione delle diverse tipologie di pacchetti di versamento si rimanda al capitolo 18 del manuale operativo Legal Archive®

Il Contratto di servizio (v. modello OAI; submission agreement) è finalizzato alla definizione di tutte le componenti informative che il sistema di conservazione necessita per creare degli AIP (Archival Information Package) coerenti e bene strutturati.

Nel sistema di conservazione, sono accettati pacchetti di versamento che rispondono alle caratteristiche tecnologiche e informative previste nei rispettivi Contratti di servizio.

Un soggetto produttore può decidere, nella fase di negoziazione iniziale alla stipula del Contratto di servizio, di versare i SIP in maniera **automatizzata**, **semiautomatizzata** oppure **manuale**.

Nel caso di versamento manuale, il soggetto produttore può accedere all'interfaccia web del sistema la quale permette di inserire i metadati obbligatori, quelli opzionali, la classificazione che si riferisce allo strumento archivistico versato in fase di start-up del sistema.

Si possono anche prevedere, all'interno del Contratto di servizio, versamenti semiautomatizzati o totalmente automatizzati per alcune tipologie documentarie: ad esempio, nel caso dei mandati di pagamento, si può prevedere un versamento semestrale con l'attribuzione automatizzata ad un template di metadati prestabilito e alla classificazione. Ancora, un sistema di gestione documentale o un sistema di firma elettronica avanzata (FEA) potrebbe dialogare direttamente con i web services del sistema in modo tale che l'attribuzione di una determinata classifica sul documento permetta una sua automatica correlazione con gli altri documenti appartenenti al medesimo fascicolo digitale.

Il sistema supporta i pacchetti di versamento nel formato definito nell'allegato 5 delle nuove regole tecniche e nel formato CSV in tre varianti:

- formato CSV normale;
- formato CSV con indirizzamento di output;
- formato CSV con offset.

## 6.18 Il ruolo dei metadati nella conservazione

In base al modello dati descritto nei paragrafi precedenti, appare evidente che i metadati ricoprono un ruolo fondamentale per la comprensione, gestione e conservazione del pacchetto informativo. Letteralmente, la parola metadato significa dato sul dato, ossia dati che descrivono altri dati. Possono includere un'infinità di strumenti descrittivi della risorsa informativa, vanno da quelli tradizionali, in uso tuttora presso gli istituti di conservazione, a quelli più recenti per la descrizione delle risorse digitali.

Funzione primaria di questi dati strutturati è l'identificazione dell'oggetto digitale, ma anche il controllo dello stesso. In altre parole, i metadati tentano di creare una tassonomia delle risorse informative, non necessariamente esaustiva, ma che indica il tipo di relazioni intercorrente fra i vari attributi dei metadati e la strutturazione del modello cui tali dati fanno riferimento.

Come tale, un set omogeneo di metadati, dovrà possedere requisiti fondamentali, quali:

- una semantica, ossia tutte le informazioni opportune;
- una sintassi, che indica come strutturare le informazioni.

Una prima fonte autorevole di indicazioni sui requisiti dei metadati di un sistema ERMS (Electronic Resource Management System) è fornito dal MoReq<sup>2</sup> della Commissione Europea al cap. 12.

Pur nella consapevolezza che "non è possibile definire tutti i requisiti di metadati relativi a tutti i possibili tipi di implementazioni ERMS", il MoReq definisce, nel primo paragrafo, 24 requisiti generali per i metadati di un sistema archivistico e, nei paragrafi successivi, i cosiddetti "elementi di metadati" relativi ad ogni livello di gerarchia di archiviazione, prevedendo la definizione, da parte dell'utente, di ulteriori elementi di metadati. Anche il modello OAIIS costituisce una rappresentazione sufficientemente completa capace di fornire un modello funzionale per l'archiviazione e l'accesso e informativo per la gestione dei metadati descrittivi e conservativi (divenuto standard ISO 14721).

Una seconda fonte autorevole è lo standard *ISO23081-1: Records Management processes. Metadata for records. Principles*: fornisce alcune indicazioni generali per esempio sulla continuità di efficacia dei metadati rilevanti nella fase attiva anche per le successive fasi operative o sulla insufficienza degli altri set di metadati finora definiti nell'ambito del *Records Management* (come per esempio i metadati *Dublin Core*). L'importanza dello standard è anche quella di essere strettamente connesso all'ISO 15489 sul Record management e richiamarne di volta in volta i principi.

Lo standard richiama cinque tipologie di metadati che recano informazioni sicuramente in buona parte utilizzabili in fase descrittiva:

- dei documenti (ISAD<sup>3</sup>);
- delle regole, gli indirizzi le policies e altri requisiti per la formazione e gestione dei records;
- dei soggetti produttori (ISAAR<sup>4</sup>);
- delle attività e processi di lavoro (ISAAR);
- dei processi di "record management" (ISAD).

In base alle funzioni fin qui delineate, è possibile categorizzare a livello generale diverse tipologie di metadati:

1. metadati descrittivi: descrivono il creatore della risorsa, il titolo, il soggetto, e altri elementi utili per la ricerca e la localizzazione dell'oggetto;
2. metadati strutturali: si occupano di come un oggetto è strutturato;
3. metadati amministrativi: includono informazioni su come l'oggetto è stato prodotto e sugli aspetti della sua proprietà.

D'altra parte, i metadati non sono stati concepiti solo come identificatori e descrittivi della risorsa informativa, ma servono anche a tracciare come il documento interagisce con l'ambiente informativo circostante, le sue relazioni con gli altri oggetti informativi, le sue funzionalità.

Si può, quindi, ampliare la suddetta classificazione, aggiungendo:

<sup>2</sup> [http://ec.europa.eu/archival-policy/moreq/doc/moreq\\_it.pdf](http://ec.europa.eu/archival-policy/moreq/doc/moreq_it.pdf)

<sup>3</sup> [http://media.regesta.com/dm\\_0/ANAI/anaiCMS//ANAI/000/0111/ANAI.000.0111.0002.pdf](http://media.regesta.com/dm_0/ANAI/anaiCMS//ANAI/000/0111/ANAI.000.0111.0002.pdf)

<sup>4</sup> [http://media.regesta.com/dm\\_0/ANAI/anaiCMS//ANAI/000/0111/ANAI.000.0111.0001.pdf](http://media.regesta.com/dm_0/ANAI/anaiCMS//ANAI/000/0111/ANAI.000.0111.0001.pdf)

1. metadati tecnologici: quelli relativi alle funzionalità del sistema (come la documentazione sulle componenti HW e SW, informazioni sulle modalità di digitalizzazione, sull'autenticazione e sulla sicurezza);
2. metadati sull'utilizzo della risorsa informativa: ossia il livello e il tipo di utilizzo effettuato.
3. metadati per la conservazione: riguardano tutti gli elementi necessari per gestire la conservazione della risorsa informativa (ad esempio, informazioni sullo stato di conservazione fisica dei documenti, oppure la documentazione relativa alle strategie di conservazione);

Le risposte all'esigenza di identificare metadati sufficienti e necessari a descrivere e conservare una risorsa digitale nel tempo, sono state varie e molteplici, ed hanno portato alla compilazione di set di metadati standardizzati e condivisi a livello internazionale. Le categorie suddette non debbono, infatti, essere considerate come totalmente autonome le une dalle altre ma interagiscono fra di loro, intersecandosi in uno o più set di metadati.

Insieme alle componenti funzionali, nel paragrafo precedente, abbiamo visto che OAIS propone anche un modello di strutturazione delle informazioni finalizzato a descrivere gli oggetti digitali e i metadati ad essi associati, necessari per la conservazione di lungo periodo.

Adottando la terminologia OAIS sul sistema di conservazione possiamo affermare che: il sistema riceve in ingresso un Submission Information Package (SIP), la cui struttura informativa deve essere concordata con il soggetto produttore, ed avrà come fine ultimo la produzione di un Archival Information Package (AIP) che soddisfi i requisiti minimi definiti nell'ambito del progetto per l'archiviazione dei documenti.

Le componenti informative di un AIP sono molteplici, e si traducono in insiemi di metadati che devono essere associati univocamente ai documenti per consentirne la conservabilità. Di particolare rilievo, sul piano archivistico, sono le Content Information (CI) e le Preservation Description Information (PDI), parte delle quali potrà essere dedotta direttamente dal contenuto del SIP, parte invece sarà il frutto delle attività di riordino e descrizione.

Il modello OAIS, in virtù delle caratteristiche di generalità sulla cui base è concepito, **non definisce** uno specifico insieme di metadati, ma un modello, informativo e funzionale, che consente di adottare insiemi di metadati mirati di volta in volta all'ambito di riferimento. D'altro canto la comunità archivistica ha da tempo raggiunto un accordo su quali debbano essere gli elementi descrittivi che caratterizzano i complessi documentari, definendo lo standard ISAD (per la descrizione archivistica vera e propria) e ISAAR (per la descrizione del contesto di produzione).

A tali standard di carattere generale si sono nel tempo affiancati due schemi di metadati, EAD<sup>5</sup> (Encoded Archival Description) ed EAC<sup>6</sup> (Encoded Archival Context), che traducono in una codifica XML gli elementi descrittivi necessari a delineare un archivio, nelle sue componenti

---

<sup>5</sup> <http://www.loc.gov/ead/>

<sup>6</sup> <http://www.library.yale.edu/eac/>

archivistiche e documentarie, nelle relazioni essenziali interne all'archivio e relative al contesto amministrativo, giuridico, archivistico.

EAD, in particolare, consente di spingere la descrizione gerarchica di un complesso documentario fino a livello del fascicolo archivistico e, ove possibile, collegare ad esso la rappresentazione elettronica dei documenti digitali in esso contenuti (rif. elemento DAO).

A nostro avviso tali standard possono essere utilizzati come riferimento per rappresentare Content Information e Preservation Description Information del modello OAIS, e sono certamente preferibili alla definizione ex-novo di insiemi di metadati che comunque dovrebbero garantire la conformità ad ISAD e ISAAR.

Inoltre, per completare il quadro degli standard di riferimento per la caratterizzazione dei metadati dei documenti digitali, è importante fare riferimento a METS<sup>7</sup> (Metadata Encoding and Transmission Standard) come ad uno schema per la codifica dei metadati necessari alla gestione degli oggetti contenuti in un deposito digitale. La compatibilità di METS con il modello OAIS consente di immaginare il suo utilizzo in tutte le fasi del processo conservativo, e può includere metadati desunti da altri schemi legati a domini specifici, quali ad esempio EAD ed EAC per l'ambito archivistico.

L'impiego in forma integrata dei tre standard sopra citati può consentire la rappresentazione compiuta ed esaustiva, nel nostro modello di riferimento, di tutti i metadati necessari alla conservazione di documenti digitali.

---

<sup>7</sup> <http://www.loc.gov/standards/mets/>



Nel sistema di conservazione di TI Trust Technologies i metadati possono essere di vari tipi, in particolare vengono gestiti i seguenti tipi:

- Stringa;
- Numero;
- Data;
- Dizionario (insieme finito di valori);
- Hash (SHA256 del file);
- Universal UID (per collegare il documento ad un eventuale documentale presente nel SP);
- MIME Type (per poter poi associare un documento alle informazioni di rappresentazione);
- Document Type (per poter associare un documento di un fascicolo alla sua classe documentale);

Inoltre, per ogni metadato è possibile definire:

- Obbligatorietà;
- Univocità;
- Ricercabilità;
- Espressione regolare di validazione;
- Espressione di conversione (da stringa a intero oppure da stringa a data);
- Classificazione privacy: dato personale, sensibile, giudiziario, sanitario.

Inoltre, il sistema di conservazione è in grado di classificare i metadati versati in base alla gestione Privacy a cui sono soggetti. La classificazione permette di gestire i seguenti casi:

1. Dato generico;
2. Dato personale;
3. Dato sensibile;
4. Dato giudiziario.

Così come definito dall'art 22 del D. Lgs 196/2003 i dati sensibili e giudiziari (caso 3 e 4) vengono trattati con tecniche di cifratura dipendenti dal sistema di database utilizzato, e sono resi illeggibili anche a chi è autorizzato ad accedervi. L'identificazione dell'interessato da parte di un utente autorizzato, viene tracciato in appositi log del sistema e avviene in caso di necessità attraverso l'abilitazione di un pulsante.

La definizione di un metadato di tipo generico o personale (caso 1 e 2) fornisce la possibilità di essere comunque gestito con tecniche di cifratura se impostate nella configurazione della Descrizione Archivistica e fornisce anche la possibilità di tracciare l'utente che ha visualizzato il dato personale e i documenti ad esso associato.

Elenchiamo di seguito una tabella riepilogativa:



Tipo Dato	Cifratura	Tracciabilità
Dato Generico	opzionale	opzionale
Dato Personale	opzionale	obbligatoria
Dato Sensibile	obbligatoria	obbligatoria
Dato Giudiziario	obbligatoria	obbligatoria

Tab.12

## 6.19 Il pacchetto di archiviazione (AIP)

È l'elemento fondamentale del sistema di conservazione, 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, tale obiettivo viene raggiunto grazie all'aderenza al modello funzionale e al modello-dati previsto in OASIS.

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:

1. l'oggetto digitale possibilmente in un formato standard non proprietario;
  2. l'impronta del documento generata con funzione di hash;
  3. il riferimento temporale (rappresentato dalla marca temporale o altro riferimento temporale opponibile a terzi, come la segnatura di protocollo);
1. il set di metadati per la conservazione:
    - a. metadati identificativi (per esempio possono essere utilizzati i metadati dello standard ISAD);
    - b. metadati descrittivi (per esempio possono essere utilizzati i metadati dello standard ISAD);
    - c. metadati gestionali (UNI SinCRO);

 <small>TELECOM ITALIA DIGITAL SOLUTIONS</small>	<b>Manuale di Conservazione</b>	Codice: <b>EVOCAST.TT.POMO14000</b>	Revisione  00
		Stato: Rilasciato	

- d. metadati tecnologici (per esempio possono essere utilizzati i metadati dello standard METS);
2. 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;
3. 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.

Il sistema permette una perfetta *compliance* al modello OAIS, anche nel livello descrittivo adottato. Si assume, infatti, che il livello di descrizione minimo che garantisca una gestione efficace di tutti i dati e metadati necessari per la conservazione e che, al contempo, permettono 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 dalle 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 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. Il pacchetto, così formato, sarà pronto per essere versato nei Volumi di conservazione (VdC), previsti dalla normativa nazionale. Ogni VdC conterrà tutti gli AIP relativi ad

 TELECOM ITALIA DIGITAL SOLUTIONS	<b>Manuale di Conservazione</b>	Codice: <b>EVOCAST.TT.POMO14000</b>	Revisione  00
		Stato: Rilasciato	

un medesimo fascicolo digitale, le relazioni fra loro e l'AIP descrittivo del fascicolo stesso, nonché le relazioni fra il fascicolo e la struttura logica d'archivio. In tale maniera, si ritroveranno nello stesso VdC tutti gli elementi necessari e sufficienti per la corretta interpretazione del singolo AIP.

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.
- Per maggiori informazioni afferenti alla descrizione della struttura dati pacchetti di archiviazione s si rimanda al capitolo 16 del manuale operativo Legal Archive®

## **6.20 Il pacchetto di distribuzione (DIP)**

Nel modello OAIS, il pacchetto di distribuzione (DIP) è strutturato nel modello dati come il pacchetto di archiviazione (v. 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 l'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 re-impacchettati per un più fruibile utilizzo da parte dell'utente.

Un utente autorizzato di un soggetto produttore, quindi, 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 di TI Trust Technologies 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 possono essere associati ad una definizione archivistica in modo tale che, al momento della generazione dei pacchetti di distribuzione dei documenti 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 necessaria alla visualizzazione dei documenti del pacchetto.

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

- Per maggiori informazioni afferenti alla descrizione delle tipologie dei pacchetti di distribuzione si rimanda al capitolo 19 del manuale operativo Legal Archive®

## 6.21 Gli stati del processo di conservazione

Il sistema di conservazione definisce al proprio interno un insieme di processi che possono essere schedati in autonomia al fine di supportare il responsabile della conservazione nelle sue mansioni.

Un processo può risiedere in uno stato secondo la seguente tabella:

Valore	Descrizione
0-WAIT	In attesa di essere preso in carico da un nodo
1-RUN	In esecuzione
2-OK	Eseguito senza errori
3-SUSP	Sospeso da operatore
4-WARN	Eseguito con segnalazioni non bloccanti
5-ERR	Fermo in condizione di errore
6-SLP	Fermo in attesa di input da parte dell'utente
7-QED	Preso in carico da un nodo e accodato per l'esecuzione
8-ERRV	Errore durante la validazione dei dati
9-UDELE	Cancellato manualmente dall'utente
10-DELE	Cancellato da processo automatico

**Tab.13**

Il workflow degli stati è il seguente:

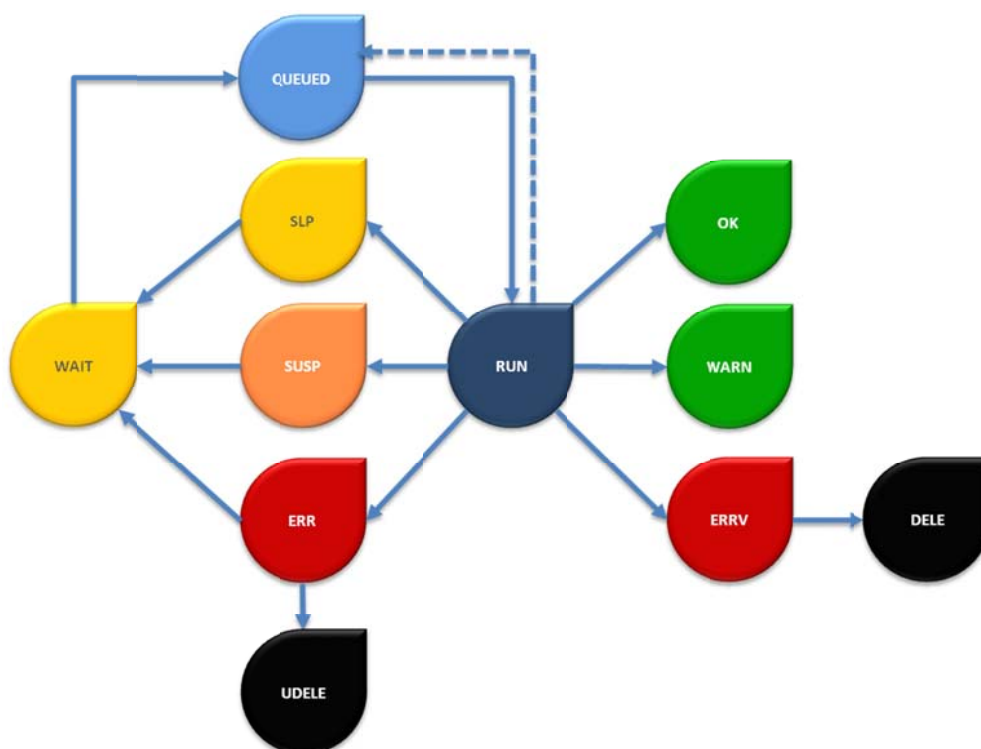


Fig.3

Esistono due processi di conservazione:

- 1) Il primo per i pacchetti di versamento provenienti da file system
- 2) Il secondo per i pacchetti di versamento provenienti da web services

Ognuno dei due processi, è costituito da 20 attività che vengono tracciate (stato, nodo esecutore, data inizio, data fine) e memorizzate nel database al fine di arricchire il processo di conservazione di tutte quelle informazioni descrittive di processo richieste dallo standard OAIS.

In particolare le 20 attività che vengono eseguite sono così definite:

CODICE ATTIVITA'	SISTEMA DI RIFERIMENTO	DESCRIZIONE
REQUISITI	Sistema di versamento	Viene verificato che: <ul style="list-style-type: none"> <li>- il soggetto produttore non sia bloccato;</li> <li>- non siano stati raggiunti i limiti di contratto;</li> <li>- sia definito almeno un certificato di firma;</li> <li>- sia definito un responsabile della conservazione per il soggetto produttore;</li> <li>- sia definito un account di marca temporale per la descrizione archivistica;</li> <li>- siano definite delle informazioni di rappresentazione valide;</li> </ul>
CREASOTTOPROCE SSI	Sistema di versamento	Per ogni SIP vengono creati dei sottoprocessi per migliorare le performance di conservazione
TRADUZIONEPdV	Sistema di versamento	Normalizzazione del file di metadati del pacchetto di versamento
CREATEMPDATA	Sistema di versamento	Caricamento nel database dei metadati del pacchetto di versamento
VALIDATEMPDATA	Sistema di versamento	Validazione dei metadati secondo le specifiche concordate con il soggetto produttore
CANCELLATEMPDATA	Sistema di versamento	Cancellazione delle tabelle temporanee create per la fase di validazione
CREAPdA	Sistema di versamento	Creazione del pacchetto di archiviazione
CREAFILEMETADATI	Sistema di versamento	Crea il file di metadati per il pacchetto di archiviazione
CREAIdC	Sistema di versamento	Crea l'indice di conservazione secondo lo standard UNI SINCRO
FIRMAIdC	Sistema di versamento	Firma l'indice di conservazione
MARCAIdC	Sistema di versamento	Marca l'indice di conservazione
MEMORIZZAPdA	Sistema di Gestione Dati	Memorizza nel database tutte le informazioni inerenti al pacchetto di archiviazione
COPIAPdA	Sistema di Memorizzazione	Copia i pacchetti di archiviazione nel repository di destinazione
VALIDAPdA	Sistema di Gestione Dati	Verifica che la copia sia andata a buon fine (controllo di hash)
COLLEGAIR	Sistema di Gestione Dati	Collega il pacchetto di archiviazione alle informazioni sulla rappresentazione
CANCELLAFILE	Sistema di Memorizzazione	Se previsto dalle impostazioni della descrizione archivistica cancella i file in input
ENCRYPTMETADATA	Sistema di Memorizzazione	Cripta i metadati con tipo di privacy impostato a giudiziario o sanitario
CREARdV	Sistema di versamento	Genera il rapporto di versamento

FIRMARdV	Sistema di versamento	Firma il rapporto di versamento
MARCARdV	Sistema di versamento	Marca il rapporto di versamento

Tab.14

## 6.22 Le componenti del sistema di conservazione

Il sistema di conservazione, così come richiesto dalla normativa, avendo come riferimento il modello dello standard OAIS (ISO 14721), cercando di ottimizzare il rapporto tra l'aderenza al modello teorico e le esigenze pratiche dei soggetti produttori. Una delle linee guida fondamentali della progettazione è stata quella di rendere il sistema flessibile dal punto di vista della definizione dei pacchetti sia di versamento che di accesso in modo da soddisfare pienamente le esigenze specifiche dei soggetti produttori e degli utenti.

Nel rispetto dello standard OAIS, il sistema è formato da 4 macro-componenti funzionali:

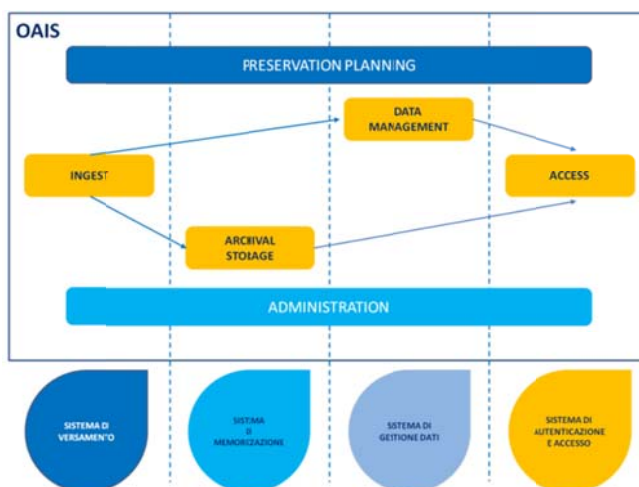
- 1) Sistema di Versamento (SV)
- 2) Sistema di Gestione Dati (SGD)
- 3) Sistema di Memorizzazione (SM)
- 4) Sistema di Autenticazione e Accesso (SAA)



Fig.4

Il sistema di conservazione, Legal Archive ha come obiettivo quello di interpretare nel modo più fedele possibile il modello OAIS traducendolo in un sistema reale. Nella Figura successiva si mostra come il sistema aderisce al modello OAIS, da notare come l'amministrazione e il *preservation planning* siano distribuite sui vari sistemi in quanto ognuno di essi metterà a disposizione una serie di funzionalità che ne consentiranno la configurazione (*preservation planning*) e la gestione (amministrazione).

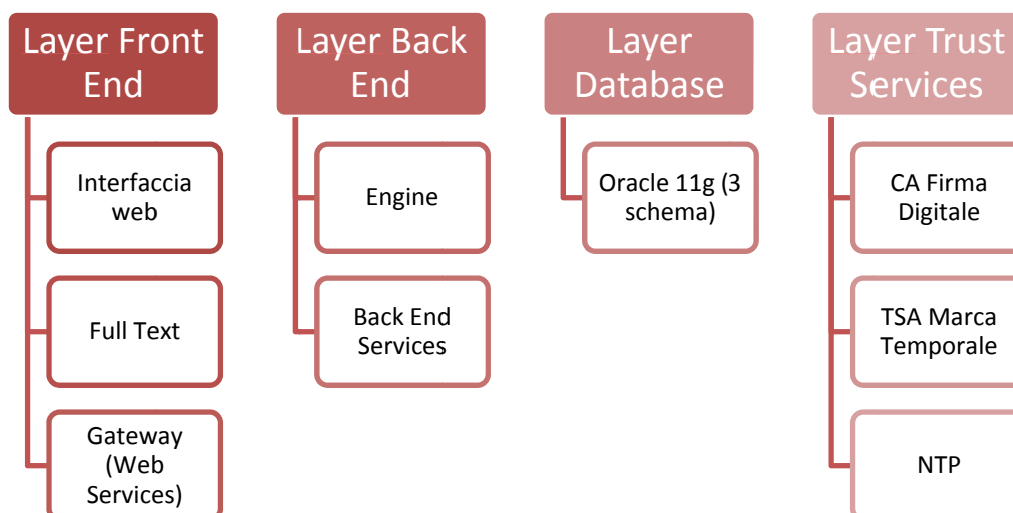




**Fig.5**

### 6.23 Componenti principali

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



**Fig.6**



## 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.

- **Full-text Engine:** è l'applicazione che abilita le funzionalità di full-text;
- **Web Services:** sono un insieme di servizi web che permettono, ad applicazioni di terze parti, di versare documenti nel sistema di conservazione o di interrogare lo stesso sullo stato di un documento;
- **File System:** è un sottoprocesso di Back End che permette di effettuare polling su folder per il versamento automatico dei documenti al sistema di conservazione.

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

## 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.

## 6.24 Layer Trust Services

TI Trust Technologies è un'azienda del Gruppo Telecom Italia che gestisce le risorse e le infrastrutture che il Gruppo utilizza per lo sviluppo e l'integrazione di soluzioni basate sulla certificazione dell'identità digitale e sulla gestione delle informazioni. TI Trust Technology è già:

- Certificatore Accreditato per il servizio di Firma Qualificata
- Gestore del servizio di Posta Elettronica Certificata;

TI Trust Technologies dispone anche dei servizi della propria TSA (Time Stamping Authority) per l'emissione delle marche temporali.

L'infrastruttura a chiave pubblica (PKI) di TI Trust Technologies, il cui elemento principale è rappresentato dalla Certification Authority (CA), consente un collegamento interno del sistema di conservazione con un *layer* che fornisce i servizi *Trust*, quali la firma dei pacchetti sottoposti a conservazione e la marcatura temporale.

Inoltre, TI Trust Technologies è dotata di piattaforma che eroga un servizio NTP (Network Time Protocol), per l'allineamento e il controllo del corretto sincronismo dei sistemi rispetto alla sorgente temporale (NTP), tramite l'utilizzo di una fonte esterna (Galileo Ferraris).

La sincronizzazione temporale dei sistemi gestiti da TI Trust Technologies per l'erogazione dei servizi di Certificazione 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.

I collegamenti fisici con il layer dei servizi trust avvengono tramite rete interna, nelle sale sistemi di TI Trust Technologies. La sala relativa alla piattaforma del sito di esercizio primario è dotata di un impianto di videocitofono utilizzato per mettere in comunicazione le persone che non fanno parte dell'organizzazione del Centro con il personale all'interno della sala stessa che è così in grado di vedere e riconoscere l'interlocutore esterno. La Sala Sistemi è inoltre collegata mediante videocitofono con la Guardiola per le eventuali comunicazioni di servizio.

In tutti i locali protetti sono installati sensori volumetrici che rilevano i tentativi di passaggio nelle zone immediatamente sottostanti il sensore stesso e/o possibili mascheramenti. Questi sensori sono attivati dal personale della guardiania nell'orario di chiusura del Centro.

I Data center di TI Trust Technologies sono conformi alle direttive del Gruppo, come riportato nel Piano della Sicurezza Generale dei Servizi Erogati da TI Trust Technologies e dal Piano della Sicurezza del Servizio di Conservazione [[PSES\\_G](#) e [PSES\\_C](#)]

I collegamenti applicativi sono ottenuti tramite una doppia configurazione (sia sugli applicativi di firma e marca temporale che su quelli della conservazione) con opportune autorizzazioni, sfruttando canali criptati (HTTPS) per la richiesta e l'invio delle firme e delle marche.

## 6.25 Piattaforma di esercizio primario del servizio

TI Trust Technologies ha scelto una soluzione applicativa denominata *Legal Archive*®, della società IFIN SISTEMI s.r.l.

La soluzione è stata implementata sia su una piattaforma di esercizio primario che su una piattaforma gemella, per la funzionalità di Disaster Recovery, che in condizioni normali funge da ambiente di collaudo, descritta nel Capitolo 14.

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

Per questo motivo, esistono 2 macchine gemelle di erogazione dei processi relativi al Front End e 2 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.

## 6.26 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 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 ricevuti.

Rispetto alla pluralità di situazioni documentarie possibili, il sistema si comporterà applicando le regole d'ingresso che saranno definite nell'accordo di servizio. Esattamente come avviene in un archivio di deposito tradizionale, le regole avranno lo scopo di stabilire:

- 1) le caratteristiche minime che la documentazione deve possedere per poter essere accettata in ingresso;
- 2) i tempi di versamento della documentazione dotata di tali caratteristiche;
- 3) le modalità di versamento;
- 4) 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 digitali 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 soggetto produttore.

Innanzitutto viene generata la cosiddetta "Descrizione del pacchetto" che consiste in una serie di informazioni descrittive (Descrizioni associate) che consentiranno l'accesso al documento da parte dell'utente. Infatti sulla base di queste descrizioni è possibile effettuare delle 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, oppure, si potrebbe consentire l'invio di formati di file non adatti alla conservazione;
- la verifica delle eventuali firme digitali apposte su di esso, comprensiva di convalida del certificato rispetto ad uno “store” locale ed alle liste di revoca on-line;
- l'eventuale verifica della presenza in archivio di un documento identico (i.e.: stessa impronta e/o metadati);
- 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) che può essere positivo o negativo. I documenti, per i quali l'esito della convalida è risultato positivo, possono quindi essere inseriti in un volume di conservazione.

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.

Un aspetto importante da sottolineare è che la fase relativa alla preparazione del Pacchetto di Versamento (SIP) e il seguente invio al sistema di conservazione può avvenire in molti modi essendo dipendente fortemente dalla situazione specifica del soggetto produttore; pertanto il sistema dispone di 3 modi per sottoporre un pacchetto di versamento:

- 1) **via web service**
- 2) **via file system**
- 3) **via interfaccia web attraverso una operazione manuale di upload dei documenti**

Riepilogando, quindi, il sistema di versamento mette a disposizione del soggetto produttore una serie di funzionalità (Modulo di Validazione) che gli consentono, se necessario, di completare la composizione dei pacchetti di versamento (SIP) prima del versamento vero e proprio, in particolare è possibile intervenire sui metadati descrittivi e sulle relazioni con il contesto archivistico laddove queste non fossero state correttamente impostate in fase di produzione dei singoli SIP.

Una volta che i pacchetti di versamento sono stati acquisiti questi vengono trasformati in pacchetti di archiviazione (AIP) e memorizzati nel Sistema di Memorizzazione; nella fase di generazione degli AIP vengono anche estratte le informazioni descrittive necessarie al funzionamento del Sistema di Gestione Dati a cui sono inviate anche tutte le informazioni di contesto eventualmente sottomesse dal soggetto produttore.

Poiché la conservazione è comunque funzionale a garantire la consultazione della documentazione nel tempo, il sistema consente, in qualunque fase del processo di conservazione, di reperire documenti e di esibirli all'interno del proprio contesto di appartenenza.

Le operazioni di accesso sono effettuate tramite l'apposito sistema, che grazie ai servizi messi a disposizione dal Sistema di Gestione Dati e dal Sistema di Memorizzazione è in grado di consentire

agli utenti abilitati di ricercare con varie modalità la documentazione conservata e di effettuare le azioni di:

- Download del singolo documento
- Esibizione: presentazione dei documenti conservati alle autorità competenti che ne facciano richiesta.

## 6.27 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 secondo canoni archivistici, offrendo funzionalità come la descrizione e il riordino, la selezione e scarto, la ricollocazione del materiale non digitale, ecc. 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.

## 6.28 Copia del piano di conservazione

Per la corretta formazione della struttura di archivio, TI Trust Technologies acquisisce gli strumenti archivistici del soggetto produttore (titolario di classificazione, Piano di conservazione, ecc.). L'aggiornamento del piano di conservazione memorizzato nel sistema di conservazione può essere demandato ad utenti dell'ente produttore.

## 6.29 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.

### **6.30 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 volume di conservazione) 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), assegnabili ad un gruppo tramite la definizione di "Profilo d'uso", attualmente sono poco più di 400. 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 uno o più descrizioni archivistiche, nonché è possibile assegnare visualizzazioni di singoli pulsanti e/o menù.



## 6.31 Componenti software del sistema di conservazione

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

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

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 certificati 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 di del prodotto 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 (Microsoft SQL 2012 oppure Oracle 11g) 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 Spring 3 realizzata attraverso l'uso di pagine web dinamiche costruite secondo il design pattern MVVM e la tecnologia Vaadin 7. Attraverso Front End gli utenti potranno accedere per configurare e monitorare il sistema.

La tecnologia Vaadin 7 è basata su Google Web Toolkit che garantisce la compatibilità con un larga parte degli attuali browser senza la necessità di installare ulteriori plug-in sul client.

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.

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.

- **Full-text Engine:** è l'applicazione che abilita le funzionalità di full-text.
- **Web Services:** sono un insieme di servizi web che permettono, ad applicazioni di terze parti, di versare documenti nel sistema di conservazione o di interrogare lo stesso sullo stato di un documento;
- **File System:** è un sottoprocesso di Back End che permette di effettuare polling su folder per il versamento automatico dei documenti al sistema di conservazione.

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

### 6.32 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.16

### 6.33 Modalità di presa in carico dei pacchetti di versamento

I pacchetti di versamento, descritti più avanti, possono raggiungere Il servizio di conservazione a norma di TI.TT in una delle seguenti modalità:

- 1) Upload manuale
- 2) SFTP (automatica)
- 3) Web Services (A2A)
- 4) Modalità Custom

#### Upload manuale

Avviene tramite l'autenticazione al sito di erogazione della Conservazione a Norma.



Una 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.

### 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 dei pacchetti di versamento nella folder SFTP dedicata, generando ed inviando lotti costituiti da un file di indice (xml o CSV), di cui saranno fornite le specifiche, e di una cartella contenente i documenti da porre in conservazione.

### 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 TI.TT. La modalità è detta Application To Application (A2A), in quanto un servizio applicativo viene messo

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.

### Modalità Custom

E' 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).

## 6.34 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.

### 6.35 Scalabilità sugli utenti

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 un maggior volume 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.

### 6.36 Sottosistema per la firma digitale e la marca temporale

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) del volume 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 ed eventualmente anche ad un Pubblico ufficiale (o ruolo equivalente), 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.

Il sistema di conservazione è in grado di applicare la firma digitale utilizzando certificati rilasciati da tutte le Certification Authority accreditate 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.

## 7 PROCESSO DI CONSERVAZIONE

Il sistema di conservazione riceve dei pacchetti di versamento 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 gli riguardano. Per maggiori informazioni afferenti al processo di conservazione si rimanda al manuale operativo Legal Archive®

### 7.1 Il modello dati di riferimento: OAIS

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

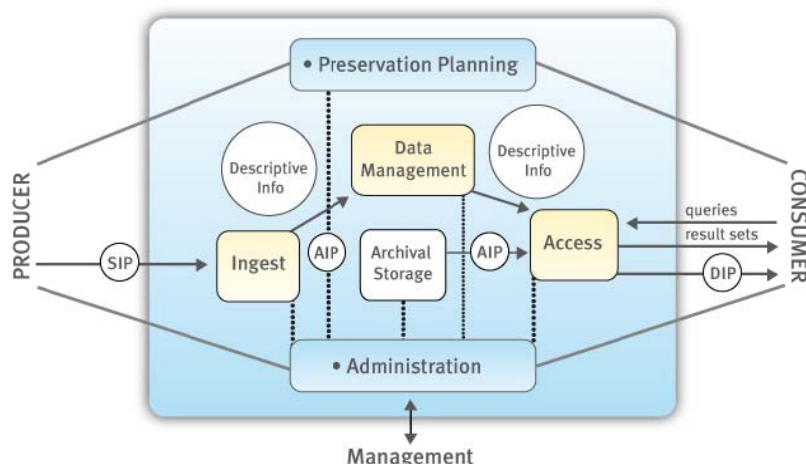


Fig.7

- 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.

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

Come accennato in precedenza, l'attività del servizio di con presa in carico da TI.TT, viene espletata a seguito della sottoscrizione di un contratto per il servizio di conservazione con il soggetto 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.

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) che può essere positivo o negativo. I documenti, per i quali l'esito della convalida è risultato positivo, possono quindi essere inseriti in un volume di conservazione.

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.

Per i soggetti che effettuano i versamenti tramite il protocollo SFTP, il rapporto di versamento viene copiato in una cartella apposita, visibile al solo Soggetto Produttore, il quale, attraverso una procedura automatica, ne riscontra la presenza e può effettuarne il download.

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

Per i soggetti che effettuano i versamenti tramite l'upload da web, il rapporto di versamento è a disposizione dalla stessa interfaccia web based, attraverso una pagina di ricerca che consente la visualizzazione e il download.

Per i soggetti che effettuano i versamenti tramite web services ricevono il rapporto di versamento attraverso un apposito comando dallo stesso applicativo che invia i documenti.

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

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

### 7.3 Controlli preliminari

Sui documenti informatici versati al sistema di conservazione, in base a quanto definito in fase di attivazione e configurazione del servizio, sono eseguite diverse serie di controlli di validazione della documentazione rispetto alle regole ed agli standard previsti dalle classi documentali di appartenenza.

Il processo di convalida riguarda almeno i seguenti aspetti:

- la verifica dell'integrità del documento memorizzato sul supporto rispetto all'impronta associata allo stesso;
- la verifica che il formato del dato sia coerente con quanto dichiarato nei suoi metadati;
- l'eventuale verifica della presenza di un documento identico (i.e.: stessa impronta e/o metadati).

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

In caso di esito negativo l'intero lotto è sospeso e viene immediatamente allertato il gruppo di competenza, sotto la responsabilità del Responsabile del servizio di conservazione, che procederà a contattare i referenti del soggetto produttore per definire, a seconda dei casi, le azioni da intraprendere.

Le casistiche relative al rifiuto di un pacchetto di versamento sono descritte nella Tabella n. del Capitolo 14 del presente manuale.

La comunicazione dell'anomalia è automaticamente gestita dal sistema attraverso due diverse modalità che si attivano entrambe per ogni evento.

La prima modalità è l'invio di una notifica informatica (*TRAP*) attraverso il protocollo SNMP (Simple Network Management Protocol) al sistema di monitoraggio di TI.TT. Detto sistema è nella visibilità del gruppo di esercizio piattaforme applicative e sistemi, sotto la responsabilità del Responsabile dei sistemi informativi.

La seconda modalità è una mail che il sistema invia direttamente alle persone di riferimento, opportunamente configurate sulla piattaforma all'atto dell'attivazione dello specifico Soggetto Produttore.

Le persone che riceveranno le mail di notifica sono il Responsabile del servizio di conservazione o i suoi delegati e il Responsabile dei sistemi informativi. E' possibile inserire anche un soggetto segnalato dal Soggetto Produttore, dietro richiesta esplicita, all'atto della compilazione della scheda di attivazione.

E' gestito un livello di gravità per dette notifiche di anomalie:

- Info (segnalazione dello stato di un processo);
- Warn (segnalazione di un'anomalia che non pregiudica il servizio);

- Error (condizione inaspettata che ha generato un'anomalia nel processo, i quale non si è concluso).
- Fatal (errore importante che causa un prematuro termine dell'esecuzione)

Tutte le notifiche e il tracciamento delle mail inviate sono riportate nei diversi file di log del sistema di conservazione.

Tutti i file di Log della piattaforma sono sottoposti a conservazione con cadenza mensile. Per ulteriori dettagli si rimanda al Piano della Sicurezza del Servizio di Conservazione [PSES\_C]

## 7.4 Costruzione del pacchetto di archiviazione

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

E' possibile separare i versamenti in diversi pacchetti di archiviazione (AIP) dividendo i lotti 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 lotto;
- Massimo 80mila documenti/file (allegati inclusi) per lotto;
- Massimo 5 MB per ogni file inviato (fino a 350 MB per invii tramite SFTP);

Una volta che la lottizzazione (chiusura del lotto 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.

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.

## 7.5 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 SIP o definite sul sistema di conservazione.



La conservazione si conclude con la firma digitale e la marcatura temporale dell'indice UNISincro e termina con la messa a disposizione del cliente di questa evidenza di avvenuta conservazione (indice P7M).

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

## 8 MODALITA' DI ATTIVAZIONE DI UN NUOVO SOGGETTO PRODUTTORE

### 8.1 Il processo di provisioning

L'attivazione di un nuovo cliente sulla piattaforma di Conservazione di TI.TT è composto da alcune fasi. Al soggetto produttore spettano le seguenti attività:

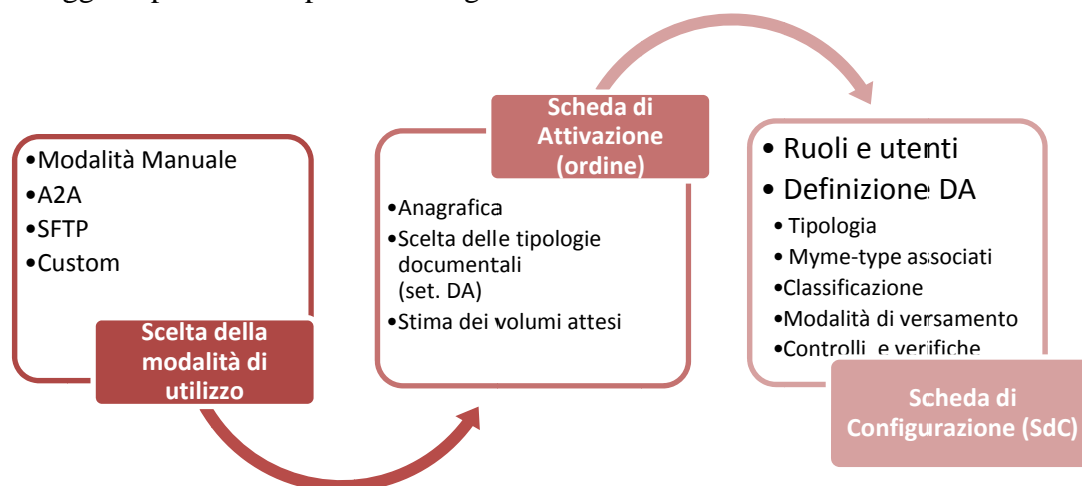


Fig.8

La scelta della modalità con la quale inviare i documenti informatici si effettua al momento della sottoscrizione del contratto di affidamento. E' possibile scegliere una modalità di invio dei documenti. Per la modalità A2A è necessario che il produttore crei presso la propria sede di invio, una interfaccia di colloquio con i *web services* che TI.TT mette a disposizione per la modalità A2A. Un documento aggiuntivo di specifiche tecniche guiderà il produttore (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 TI.TT.

La scelta della tipologia documentaria dipende dal tipo di documenti che il cliente intende conservare. La piattaforma di Conservazione a norma di TI.TT possiede una lista di tipologie documentarie con i relativi campi (metadati) per la ricerca dei documenti conservati. Queste tipologie documentarie sono descritte nel presente documento, al capitolo "Campi Specifici".

A seconda delle proprie esigenze, il produttore 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. 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 TI.TT 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.

## 9 MODALITA' DI ESIBIZIONE

Nei contratti standard non è previsto da parte del soggetto conservatore il rilascio di copie cartacee conformi agli originali digitali conservati, né l'Accesso diretto alla documentazione da parte di colui che, dovendo tutelare situazioni giuridicamente rilevanti, abbia presentato istanza di consultazione.

Pertanto, in merito all'esercizio del diritto d'accesso ai documenti conservati dal soggetto conservatore, questo si limita a fornire al soggetto produttore, su precisa richiesta di quest'ultimo e senza che su di esso debba gravare alcun particolare onere, il documento informatico conservato, qualora per un qualsiasi motivo il soggetto produttore stesso abbia deciso di non acquisirlo direttamente mediante le modalità delineate nel presente manuale. Permane in carico allo stesso soggetto produttore sia la responsabilità di valutare la fondatezza giuridica della domanda di accesso, sia l'onere di far pervenire il documento (o sua eventuale copia cartacea conforme) al soggetto richiedente la consultazione.

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 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.trustttechnologies.it>. Il collegamento avviene tramite connessione sicura SSL con certificato della Certification Authority TI. Trust Technologies.

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

A quel punto i produttori sono in grado di:

- Visualizzare direttamente i documenti informatici originali conservati da remoto
- Scaricare i documenti informatici conservati (duplicati) e i file di evidenza della conservazione (indice di conservazione Unisincro)
- Richiedere e scaricare i (DIP) da consegnare alle autorità competenti, in caso di necessità.
- Il soggetto produttore avrà cura di produrre una copia conforme richiedendo la presenza di un pubblico ufficiale.

In merito alla produzione delle copie sarà cura del produttore produrre le copie e richiedere, quando necessario, la presenza di un pubblico Ufficiale.

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.

## 9.1 Pubblico ufficiale

Qualora fosse richiesta la presenza di un pubblico ufficiale per l'attestazione di conformità all'originale di copie di documenti informatici originali, conservati dal sistema di conservazione, il produttore avrà cura di gestire tale scelta. Il conservatore rimanda la gestione di tale attività al soggetto produttore le cui modalità di intervento sono esplicitate nel contratto di affidamento. Il conservatore garantisce la messa a disposizione dell'originale informatico attraverso un DIP eventualmente firmato dal responsabile del servizio di conservazione.

## 10 PIANO DI DISMISSIONE DEL SERVIZIO

Per una corretta erogazione di un servizio di conservazione a norma che risponda alle caratteristiche richieste dallo standard 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*.

## 11 SERVIZI DI MANUTENZIONE

### 11.1 Approccio

Gli interventi di manutenzione, a qualunque tipologia appartengano, 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:

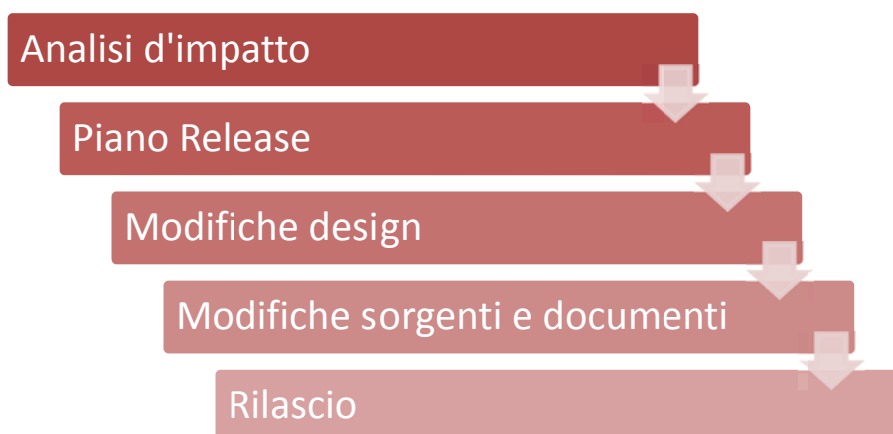


Fig.9

### 11.2 Analisi d'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.

### 11.3 Piano release

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.

### 11.4 Modifiche design

Attività:

- analisi della richiesta approvata ed eventuale revisione della struttura architeturale;
- 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.

### 11.5 Modifiche sorgenti e documentazione

Le principali attività 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.

### 11.6 Rilascio

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

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

## 11.7 Servizio di manutenzione evolutiva ed adeguativa

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.

Il processo operativo per la gestione degli interventi seguirà un modello iterativo incrementale suddiviso in due fasi descritte nei paragrafi seguenti:

- Pianificazione intervento;
- Sviluppo e rilascio.

## 11.8 Pianificazione Intervento

La pianificazione dell'intervento avverrà come segue:

- L'attivazione dell'intervento: l'intervento manutentivo viene sempre avviato in relazione ad una Richiesta di Sviluppo Modifiche (RSM) di manutenzione evolutiva proveniente dal Committente che comunicherà, via fax o e-mail, al Capo Progetto di TI Trust Technologies la richiesta di comprensiva dei requisiti e dei vincoli temporali ai quali deve sottostare l'intervento richiesto (affidamento). Il team di manutenzione di TI Trust Technologies, nel momento dell'attivazione dell'intervento, provvederà alla predisposizione di una Scheda di Intervento attraverso la quale le suddette richieste saranno formalizzate, corredate da informazioni utili al raggiungimento dell'obiettivo quali: data prevista di inizio attività; data richiesta per completamento fase di definizione; eventuali vincoli (ad esempio richieste utente di date di esercizio).
- Studio di evoluzione funzionale: il Responsabile del progetto, entro 5 giorni naturali consecutivi, analizza la richiesta e predispone il documento "Studio di evoluzione funzionale" comprendente l'analisi di fattibilità dell'intervento richiesto, le figure professionali da utilizzare, la pianificazione dello sviluppo, la tempificazione di svolgimento dell'intervento (e relativa data di rilascio) e la stima economica espressa come impegno in termini di giorni uomo per figura professionale. Lo Studio di evoluzione funzionale sarà sottoposto all'approvazione del responsabile del contratto del Committente.
- Affidamento: La realizzazione dell'intervento verrà affidata dal Committente attraverso una specifica richiesta di prestazione, a seguito dell'approvazione del suddetto "Studio di evoluzione funzionale" da parte del responsabile del contratto del Committente stesso.

## 11.9 Sviluppo e rilascio

Lo sviluppo ed il rilascio avverranno come segue:

- Definizione delle attività realizzative: il Responsabile del Servizio (RDS) di TI Trust Technologies, alla ricezione della richiesta di prestazione, provvede alla formulazione del documento di "Definizione delle attività realizzative" articolato in: definizione e pianificazioni; analisi; disegno; pianificazione delle attività.

- **Realizzazione:** Una volta approvato il documento di "Definizione delle attività realizzative, il piano di dettaglio correlato diventa esecutivo e il team di manutenzione prende in carico la gestione dell'intervento e diviene, quindi, responsabile del completamento dell'intervento; ove necessario, potrà contattare l'utente finale per richiedere ulteriori informazioni d'approfondimento sulla richiesta inviata. Il Responsabile del Servizio (RDS) sulla base del suddetto piano avvia le attività allocando le risorse e controllando la realizzazione fino alla consegna del prodotto secondo le scadenze pianificate.
- **Collaudo e Rilascio:** a conclusione delle attività realizzative, a seguito del test e del "collaudo di conformità" con esito positivo di punti realizzati.

## 11.10 Manutenzione correttiva

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.

La richiesta di azione correttiva (RAC) avverrà di norma attraverso la notifica formale via e-mail o fax al Capo Progetto di TI Trust Technologies da parte del Responsabile del contratto del Committente.

Il team di manutenzione prende in carico la gestione della Richiesta 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.

Il flusso operativo si articola attraverso i seguenti passi:

A fronte dell'attivazione, il team di manutenzione provvede alla fornitura di una prima risposta immediata con una prima soluzione temporanea (by-pass seguita dalla preparazione di una correzione puntuale - PTF (*Program Temporary Fix*) e dall'effettuazione del test di regressione e relativi collaudi di integrazione;

nella fase di presa in carico degli interventi viene svolta una attività di analisi volta a studiare l'impatto delle variazioni e le eventuali modifiche alla performance del sistema che ne derivano. Il responsabile di servizio/progetto di TI Trust Technologies effettua una prima valutazione e designa, sulla base delle competenze tecnico-funzionali necessarie, il responsabile dell'intervento e attiva il team di risorse in base agli *skill* necessari alla priorità dell'intervento richiesto ed alle disponibilità;



il passo successivo, la definizione dell'intervento, è volto a individuare e descrivere le esigenze funzionali e gli altri vincoli espressi dall'utente, nel caso di intervento originato da una richiesta da parte degli utenti del sistema, ovvero a individuare le necessità di adeguare le funzionalità del sistema alle variazioni del contesto tecnologico/funzionale. Si procede alla definizione della soluzione più idonea, all'individuazione degli oggetti da modificare e alla definizione dei casi di test, di integrazione e di sistema, che permettono di verificare il corretto ripristino della funzionalità: viene effettuata una attività di pianificazione che ha l'obiettivo di definire le operazioni da eseguire nell'ambito dell'intervento, le dipendenze tra di esse e la loro durata individuale ed in particolare ha ad oggetto la stima della dimensione dell'intervento, la stima dell'effort per eseguire l'intervento manutentivo ed i test di regressione ad esso associati (per ognuna delle figure professionali coinvolte), la stima della durata dell'intervento basata sulla precedente stima della quantità di lavoro necessaria;

una volta ottenuta l'approvazione del soggetto produttore, si passa alla fase successiva di attuazione/integrazione durante la quale vengono realizzate le modifiche necessarie al software applicativo e alla struttura della base dati; vengono eseguiti i casi di test unitario del software modificato/prodotto e vengono eseguiti i casi di test di integrazione e di sistema definiti nel corso della fase precedente. Le attività di aggiornamento del software sono accompagnate da altrettanti aggiornamenti della documentazione relativa rispetto alle modifiche effettuate. Il responsabile di servizio riceve notifica automatica dell'esito positivo delle attività di test; verifica i risultati delle attività eseguite e comunica al soggetto produttore la chiusura dell'intervento e la disponibilità per il rilascio nell'ambiente di esercizio;

si procede infine alle operazioni di collaudo di integrazione, per gli interventi che lo richiedano, ed al successivo rilascio in esercizio dell'applicazione.

Viene formalizzata la chiusura definitiva dell'intervento e registrata con l'apposito strumento di gestione interventi: la chiusura dell'intervento viene notificata al produttore e agli utenti secondo i canali di comunicazione concordati.

## 12 PRODUZIONE DI DUPLICATI E COPIE INFORMATICHE

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.

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.

Detta piattaforma, consente al Soggetto Produttore di effettuare sia la produzione di duplicati e copie informatiche che l'esibizione a norma dei documenti conservati, così come descritto nel Capitolo 9 di questo manuale.

Le credenziali serviranno per il collegamento al portale di conservazione, all'indirizzo <https://conservazione.trusttetchnologies.it>.

Il collegamento avviene tramite connessione sicura SSL con certificato della Certification Authority TI. Trust Technologies.

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

A quel punto i Soggetti Produttori sono in grado di:

- Visualizzare direttamente i documenti informatici originali conservati
- Scaricare i documenti informatici conservati (duplicati) e i file di evidenza della conservazione (indice di conservazione Unisincro)
- Richiedere e scaricare i (DIP) da consegnare alle autorità competenti, in caso di necessità.
- Produrre eventualmente una copia conforme richiedendo la presenza di un pubblico ufficiale.

La procedura per visualizzare i documenti 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, il Soggetto 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 il Soggetto 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.

Infine, ai fini del DPCM 3 dicembre 2013, allo scopo di garantire la leggibilità nel tempo dei documenti conservati nonostante l'obsolescenza dei sistemi e dei software che li hanno prodotti, TI.TT effettua copie conformi all'originale.

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, TI.TT provvederà a richiedere la presenza di un pubblico ufficiale per assolvere a tale obbligo.

## 12.1 Selezione e scarto

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 materiale dello scarto, a mantenere al proprio interno, ove richiesto, i metadati della documentazione fisicamente scartata.

Il sistema di conservazione produrrà quotidianamente un elenco degli AIP che ha superato il tempo di conservazione che sarà inviato al soggetto produttore. Una volta validato definitivamente l'elenco di scarto dal 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 sistema di conservazione, è quindi dotato di un processo di scarto che si occupa di controllare quotidianamente se esistono pacchetti di archiviazione che devono scartati. Alla presenza di uno o più pacchetti, il processo avvisa il Responsabile del servizio di conservazione, che avrà a disposizione una interfaccia che gli permetterà di decidere se scartare o meno i documenti.

In caso affermativo, 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 del volume, una nota che indica il fatto che il volume è stato sottoposto a processo di scarto includendo data e ora di esecuzione.

## 13 DISASTER RECOVERY

E' disponibile un sito di *Disaster Recovery*, nel Data Center Telecom Italia 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*.

## 14 MONITORAGGI E CONTROLLI ACCETTAZIONE PDV

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).

Tipo anomalia	Descrizione	Modalità di gestione
Mancata risposta al Versamento	È il caso in cui l'unità documentaria viene correttamente versata ma, per vari motivi, la risposta di avvenuta ricezione non perviene al produttore, che pertanto, erroneamente, lo reputa non versata.	Il soggetto produttore deve trasmettere nuovamente e il sistema di conservazione restituisce una risposta di esito negativo con l'indicazione che l'unità documentaria risulta già versata. Tale risposta deve essere usata dal produttore come attestazione di avvenuto versamento e l'unità documentaria deve risultare come versata.
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 caso più frequente è l'impossibilità temporanea di accedere alle CRL degli enti certificatori. In questi casi il sistema di conservazione dopo aver riprovato 10 volte, genera un messaggio di errore perché non riesce a completare le verifiche previste sulla validità della firma e il versamento viene quindi rifiutato impostando il processo in stato ERRV.	Il soggetto 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 soggetto 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.

**Tab.16**

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.

**Tab.17**

## **14.1 Verifica l'integrità degli archivi**

La funzionalità di verifica di integrità degli archivi, 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 in Legal Archive® come processo schedulabile, e può essere quindi pianificato a piacere da parte del responsabile del servizio di conservazione o di un suo delegato.

A ogni verifica effettuata viene generato un report in formato xml che può essere consultato da parte del responsabile del servizio di conservazione per attestare la corretta esecuzione della verifica o per diagnosticare eventuali anomalie.

## 15 MONITORAGGIO DEI SISTEMI

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 Certificazione e PEC 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.

## 16 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.

### **16.1 Accettazione dati conservati da altri outsourcer.**

TI.TT 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.

### **16.2 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.

### **16.3 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. TI.TT 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, TI.TT 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.

### **16.4 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.10

Il Soggetto Produttore con contratto in scadenza riceve tre mail di PEC (Posta Elettronica Certificata, oltre ad avvisi telefonici da parte del marketing. Alla scadenza del contratto, gli utenti interni del soggetto produttore, precedentemente abilitati all'accesso della piattaforma web all'atto della sottoscrizione del contratto, riceveranno anch'essi i tre avvisi via mail PEC e saranno invitati a collegarsi alla piattaforma web, tramite protocollo sicuro Https, per scaricarsi i DIP conservati.

Il Soggetto Produttore che non intende rinnovare il contratto per il servizio di conservazione è tenuto a verificare la coerenza dei dati consegnati entro i tempi prestabiliti.

TI.TT 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.

Infine, verrà disattivato l'account relativo al portale web e i dati saranno sottoposti a cancellazione.

In caso di volumi documentali di grandi dimensioni, di concorderà con il Soggetto Produttore la procedura di prelievo, presso il bunker di TI T.T., di adeguati supporti informatici in grado di contenere i dati conservati. Detti supporti verranno consegnati esclusivamente a personale autorizzato dal Soggetto Produttore. Le procedure verranno concordate all'inizio dell'attivazione del servizio (modalità di attivazione custom).

## 17 SERVIZI DI HELP DESK

Il servizio di conservazione di TI Trust Technologies beneficia di un'assistenza 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) servizio di informazioni su tematiche di natura commerciale: dal lunedì al venerdì dalle 9.00 alle 17.00, festivi esclusi;
- 2) servizio di assistenza ai clienti: dal lunedì al venerdì dalle 9:00 alle 17.00, festivi esclusi;
- 3) servizi di risoluzioni di inconvenienti: 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 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".

## 18 LIVELLI DI SERVIZIO

Di seguito viene descritta la tabella dei livelli di servizio garantiti, suddivisi per attività relativa al servizio di conservazione a norma di Telecom Italia Trust Technologies.

### 18.1 Disponibilità

ID	Attività	Livelli di servizio	% di applicazione
1	Lavorazione dei pacchetti di versamento ricevuti	Entro il giorno lavorativo successivo (festivi esclusi) dalla ricezione del pacchetto di versamento.	99,5% dei lotti ricevuti
2	Comunicazione eventuali anomalie nei lotti di documenti ricevuti (Per errori strettamente riguardanti il contenuto dei file ricevuti)	Entro il giorno lavorativo successivo (festivi esclusi) dalla ricezione del pacchetto di versamento.	99,5% dei lotti ricevuti
3	Invio ai clienti della segnalazione di errori che causano il blocco dell'elaborazione dei lotti da conservare.	Entro il giorno lavorativo successivo (festivi esclusi) dalla ricezione del pacchetto di versamento.	99,5% dei lotti ricevuti
4	Avvio rielaborazione dei lotti eventualmente impattati dall'anomalia.	Entro il giorno lavorativo successivo (festivi esclusi) dalla risoluzione anomalia (dalla data comunicazione al Cliente).	99,5% dei lotti ricevuti
5	Risoluzione malfunzionamenti del servizio di CS	Presenza in carico: entro 8 ore lavorative nei seguenti orari: dalle ore 9.00 alle ore 13.00 e dalle ore 14.00 alle ore 18 di ciascun giorno feriale.	N.A.
6	Disponibilità dei servizi di caricamento (upload) <ul style="list-style-type: none"> <li>Upload Manuale</li> <li>Modalità SFTP</li> <li>A2A (Web Services)</li> </ul> <p>N.B.: La disponibilità delle modalità Custom viene espressamente concordata con il Soggetto Produttore</p>	Entro il giorno lavorativo successivo (festivi esclusi) dalla segnalazione.	99,9% su base trimestrale
7	Disponibilità del servizio di consultazione ed esibizione dei documenti conservati (interfaccia Web).	Entro il giorno lavorativo successivo (festivi esclusi) dalla ricezione del pacchetto di versamento.	99% su base trimestrale

Tab.18

### 18.2 Limiti di applicabilità dello SLA

Qui di seguito sono riportate le condizioni in presenza delle quali, non saranno imputabili a TI Trust Technologies il verificarsi di eventuali disservizi:

- cause di Forza Maggiore e cioè eventi che, oggettivamente, impediscano al personale di TI Trust Technologies di intervenire per eseguire le attività poste dal Contratto a carico della stessa TI Trust Technologies (in via meramente esemplificativa e non esaustiva: scioperi e manifestazioni con blocco delle vie di comunicazione; incidenti stradali; guerre e atti di terrorismo; catastrofi naturali quali alluvioni, tempeste, uragani etc);

- interventi straordinari da effettuarsi con urgenza ad insindacabile giudizio di TI Trust Technologies per evitare pericoli alla sicurezza e/o stabilità e/o riservatezza e/o integrità dei dati e/o informazioni del Cliente. L'eventuale esecuzione di tali interventi sarà comunque comunicata al Cliente a mezzo e mail inviata all'indirizzo di posta elettronica indicato in fase d'ordine con preavviso anche inferiore alle 48 ore oppure contestualmente all'avvio delle operazioni in questione o comunque non appena possibile;
- indisponibilità o blocchi dell'Infrastruttura imputabili a:
  - errato utilizzo, errata configurazione o comandi di spegnimento, volontariamente o involontariamente eseguiti dal cliente;
  - anomalie e malfunzionamenti dei software applicativi/gestionali forniti da terze parti;
  - inadempimento o violazione del Contratto imputabile al Cliente;
  - anomalia o malfunzionamento del Servizio, ovvero loro mancata o ritardata rimozione o eliminazione imputabili ad inadempimento o violazione del Contratto da parte del Cliente ovvero ad un cattivo uso del Servizio da parte sua;
  - cause che determinano l'inaccessibilità, totale o parziale, dell'Infrastruttura dal Cliente imputabili a guasti nella rete internet esterna al perimetro di TI Trust Technologies e comunque fuori dal suo controllo (in via meramente esemplificativa guasti o problemi).

## 19 CONDIZIONI DI UTILIZZO DEL SERVIZIO DI CONSERVAZIONE

Questo capitolo definisce gli obblighi e le relative responsabilità che TI Trust Technologies ed il Cliente assumono nell'ambito del Servizio di Conservazione erogato da TI Trust Technologies in suo favore.

### 19.1 Obblighi di TI Trust Technologies

TI Trust Technologies, erogherà al Cliente il servizio di CS ex-lege dei predetti documenti informatici trasmessi dal Cliente nel rispetto della normativa applicabile ed assume i seguenti obblighi nei confronti del Cliente:

- a. archiviare i documenti informatici trasmessi dal Cliente sulla base dei dati ricevuti;
- b. apporre la propria firma digitale e la marca temporale all'evidenza informatica relativa al volume;
- c. garantire la restituzione, su richiesta o al termine del contratto di servizio, dei documenti conservati.

### 19.2 Obblighi del Cliente

Il Cliente assume gli obblighi seguenti:

- a) indicare la tipologia di documenti da sottoporre al processo di Conservazione a norma;
- b) individuare un Referente tecnico ed organizzativo per gli aspetti che riguardano le comunicazioni relative all'erogazione del servizio di Conservazione A Norma.
- c) mettere a disposizione di TI Trust Technologies i documenti da sottoporre al processo di Conservazione A norma in modo accurato e completo;
- d) adottare ogni e qualsiasi misura idonea a garantire la protezione e la sicurezza, fisica e logica, dei propri documenti, dati e/o informazioni ed in generale del proprio sistema informatico;
- e) alla scadenza del contratto di servizio, il Cliente avrà la responsabilità della custodia dei dati ricevuti, consegnati da TI Trust Technologies;
- f) garantire il corretto funzionamento delle proprie infrastrutture informatiche e di rete funzionali all'erogazione del servizio di Conservazione A Norma, ivi comprese quelle necessarie alla corretta operatività della Postazione di Firma;
- g) trasmettere i documenti da sottoporre al processo di Conservazione a norma attenendosi alle modalità indicate nel presente documento.

### 19.3 Limitazione ed esclusione delle responsabilità di TI Trust Technologies

TI Trust Technologies non sarà in alcun modo responsabile per quanto di seguito indicato:

- a) inadempimenti riconducibili a malfunzionamenti e/o disservizi delle infrastrutture del Cliente;

- b) salvo le ipotesi inderogabilmente previste dalla legge, in nessun altro caso, per nessun titolo e/o ragione, TI Trust Technologies potrà essere ritenuta responsabile nei confronti del Cliente, né nei confronti di altri soggetti, direttamente o indirettamente, connessi o collegati con il Cliente, per danni, diretti o indiretti, perdite di dati, violazione di diritti di terzi, ritardi, malfunzionamenti, interruzioni, totali o parziali, che si dovessero verificare nel corso dell'erogazione del servizio di Conservazione a norma, ove connessi, direttamente o indirettamente, o derivanti da:
- I. documenti trasmessi dal Cliente contenenti dati non accurati, non corretti, non completi, non integri o di scarsa qualità;
  - II. forza maggiore, caso fortuito o fatto di terzo;
  - III. situazioni oggettivamente al di fuori del controllo e delle possibilità di intervento di TI Trust Technologies, quali, in via meramente esemplificativa, la discontinuità/interruzione nell'erogazione dell'energia elettrica;
  - IV. mancato adempimento da parte del Cliente ad obblighi di legge.
- c) pretese e/o contestazioni avanzate nei confronti del Cliente da qualsivoglia soggetto e connesse all'emissione/formazione della documentazione oggetto del Servizio di Conservazione a norma, né sarà ad alcun titolo responsabile per il contenuto delle informazioni che saranno trasmesse attraverso lo stesso servizio.

#### 19.4 Polizza assicurativa del Gestore del Servizio

TI Trust Technologies è dotata di polizza assicurativa a copertura dei rischi dell'attività e dei danni causati a terzi, avente le seguenti caratteristiche:

Tipo di Risarcimento	Massimale annuo per sinistro, per attività informatiche	Massimale annuo, per sinistro, per conservazione documentale
<p>Risarcimento di danni patrimoniali cagionati a Terzi per:</p> <ul style="list-style-type: none"> <li>• fatto colposo e/o doloso dei dipendenti addetti all'attività per la quale è prestata l'assicurazione e dei quali il Gestore del Servizio debba rispondere ai sensi di legge;</li> <li>• atti dolosi di Terzi, commessi tramite intromissione nei sistemi informatici del Gestore del Servizio superando le misure di sicurezza logica e fisica predisposte;</li> <li>• inadempimenti o ritardi a seguito di danno materiale e diretto alle apparecchiature utilizzate per lo svolgimento dell'attività per la quale è prestata</li> </ul>	<p>€28.000.000,00 (ventottomilioni)</p>	<p>€5.000.000,00 (cinquemilioni)</p>

l'assicurazione.		
------------------	--	--

Tab.19

#### **19.4.1 Compiti per la protezione dei dati e delle procedure informatiche**

TI Trust Technologies è garante nei confronti del Cliente che lo ha nominato dell'applicazione delle misure necessarie per la sicurezza fisica, logica e ambientale dei dati e del sistema preposto alla loro conservazione, comprensivo della copie di sicurezza dei supporti di memorizzazione, al fine di proteggere le informazioni da possibili violazioni in termini di riservatezza, integrità e disponibilità delle informazioni.

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

TI Trust Technologies stabilisce attraverso un'analisi del rischio gli appropriati controlli di sicurezza delle informazioni da adottare.

## 20 MODULISTICA DEL SERVIZIO

### 20.1 Scheda di attivazione del servizio

La Scheda di attivazione del servizio costituisce il documento nel quale sono sintetizzati gli elementi peculiari del servizio attivato.

Essa integra il Manuale Operativo ed, essendo sottoscritta dal cliente, costituisce riferimento per gli impegni contrattuali fra le parti.

### 20.2 Condizioni di Utilizzo del Servizio

Le condizioni di utilizzo del servizio devono essere sottoscritte dal Cliente prima dell'attivazione del servizio.

### 20.3 Nomina di TI Trust Technologies quale Responsabile del servizio di Conservazione

La nomina di TI Trust Technologies quale responsabile del servizio di conservazione nell'ambito del servizio è contenuta all'interno delle condizioni di utilizzo del servizio, sottoscrivendo le quali, il Cliente effettua la nomina, accettata da TI Trust Technologies in automatico, all'attivazione del servizio.