Manuale della
Conservazione Digitale

TESI SpA Registered office: Via Mendicità Istruita, 24 – 12042 Bra (CN) - Headquarters: Via Savigliano, 48 - 12062 Roreto di Cherasco (CN)
Phone +39 0172 476301 - Fax +39 0172 476399 - www.tesisquare.com - info@tesisquare.com
Tax Code and VAT no. 02448510046 – Cuneo Chamber of Commerce - Economic and Administrative Register no. 177331
Share Capital € 750,000 fully vested

EMISSIONE DEL DOCUMENTO

AZIONE	DATA	NOMINATIVO	FUNZIONE
Redazione	12/06/2018	Chiara T. Quaranta	*Responsabile della funzione archivistica di Conservazione*
		Antonella Vota	*Consultant*
		Rossella Gullane	*PM and Planner*
Verifica	15/06/2018	Claudio Rossero	*Responsabile sicurezza dei sistemi per la Conservazione*
	18/06/2018	Marco Segato	*Responsabile UG Digital*
	19/06/2018	Stefano Galati	*Responsabile sistemi informativi per la Conservazione*
Approvazione	20/06/2018	Giuseppe Crivello	*Responsabile del servizio di Conservazione*

REGISTRO DELLE VERSIONI

N° VERSIONE	DATA EMISSIONE	MODIFICHE APPORTATE
1.0	12/02/2016	Prima Redazione
1.1	20/05/2016	Integrazione a seguito di segnalazioni Agid
1.2	15/09/2017	Variazione responsabile Sicurezza dei sistemi per la conservazione
2.0	26/02/2018	Aggiornamento normative e integrazioni a seguito di revisione procedure interne Aggiunto par. 7.8.1 Comunità di riferimento
2.1	28/03/2018	Inserimento cap. 7.12 Cessazione Contratto Aggiornamento fig. 14-15 per recepimento nuovo framework piattaforma Tesi E-integration Aggiornamento fig. 27 per arricchimento schema topologico sistema di conservazione Aggiornamento cap. 6.2 per integrazione gestione "singolo versamento" Aggiornamento cap. 8.3 per inserimento riferimenti a DR in Tesisquare® Aggiornamento intero documento per affinamento ed eliminazione ridondanze con Piano della Sicurezza
2.2	20/06/2018	Aggiornamento, a valle delle segnalazioni Audit per certificazione, dei cap. 6.2; 7.3; 7.4; 7.5 e 7.6 per esplicitazione composizione PDV per tutte le casistiche ammissibili di caricamento degli oggetti da conservare Aggiornamento cap. 6.1 per inserimento riferimento a documento elenco metadati standard Aggiornamento cap. 7.5 per approfondimento regole di sicurezza del canale di comunicazione tra Tesi e-Integration ed il SdC Aggiornamento normative 2018 Aggiornamento fig.10 per rendere maggiormente esplicito il perimetro del Sistema di Conservazione nell'infrastruttura e-Integration

Sommario

TESI SpA Registered office: Via Mendicità Istruita, 24 – 12042 Bra (CN) - Headquarters: Via Savigliano, 48 - 12062 Roreto di Cherasco (CN)
Phone +39 0172 476301 - Fax +39 0172 476399 - www.tesisquare.com - info@tesisquare.com
Tax Code and VAT no. 02448510046 – Cuneo Chamber of Commerce - Economic and Administrative Register no. 177331
Share Capital € 750,000 fully vested

1. SCOPO E AMBITO DEL DOCUMENTO

Tesisquare® è impegnata dal 1995 nell'ideazione e nella messa a punto di soluzioni IT in grado di migliorare e integrare i processi di business grazie a un'attenta analisi dell'evoluzione tecnologica, dei cambiamenti e delle richieste del mercato nazionale e internazionale.
Dal 2011 Tesisquare® ha messo a punto soluzioni innovative nell'ambito dell'archiviazione e della conservazione digitale, offrendo ai suoi clienti sistemi di interscambio dei dati, di postalizzazione e di storage in linea con le prescrizioni normative italiane ed europee, e con i principali standard internazionali del settore.
Il presente Manuale della Conservazione Digitale dei documenti è redatto e sottoscritto dalla società Tesisquare® in qualità di Conservatore accreditato della società Cliente ed è adottato ai sensi del DPCM 3 dicembre 2013 ("Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005"), art.8. e ha lo scopo di:

- Descrivere dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dai medesimi;
- Illustrare il modello di funzionamento e le procedure che compongono il processo di conservazione;
- Descrivere le architetture e le infrastrutture utilizzate;
- Descrivere le misure di sicurezza adottate e ogni altra informazione utile alla gestione e al monitoraggio nel tempo del funzionamento del sistema di conservazione;

Tale documento viene utilizzato come riferimento per il mantenimento, l'aggiornamento e lo sviluppo del Sistema di conservazione della società e, inoltre, fa riferimento alle procedure di gestione della sicurezza e della privacy adottate all'interno dell'azienda.

Il presente Manuale della Conservazione è collegato ai documenti riportati nella successiva tabella, che entrano più nel dettaglio dei diversi aspetti del Sistema di Conservazione e costituiscono parti integranti e sostanziali del Manuale della Conservazione.

DOCUMENTI COLLEGATI	
Scheda Servizio Cliente - Specificità del Contratto	È il disciplinare tecnico che contiene le specifiche forniture del servizio di Conservazione (SPECIFICITÀ DEL CONTRATTO) per i produttori dei documenti. È parte integrante del contratto di servizi sottoscritto tra le parti e del Manuale di Conservazione, redatto dal Conservatore sulla base delle informazioni condivise con il produttore dei documenti (Cliente), contenente i requisiti essenziali del Servizio, le relative specifiche tecnico-funzionali e procedurali per le varie fase del sevizio (attivazione, versamento, conservazione, post-produzione, distribuzione) oltre ai livelli di Servizio (SLA); tale documento è redatto in fase di analisi, prima del primo processo di Conservazione. Ogni variazione delle modalità di erogazione del Servizio, dovuta a richieste del Cliente o a evoluzioni del Sistema di Conservazione, comporta la necessità di aggiornare la Scheda Servizio Cliente – Specificità del Contratto.
Piano per la Sicurezza	È il documento aziendale che analizza il contesto in cui l'azienda opera riportando i fattori interni ed esterni che lo influenzano ed evidenzia le principali criticità legate alla gestione della sicurezza delle informazioni gestite

[Torna al Sommario](#)

Il presente manuale di conservazione riporta nei successivi capitoli:

a) i dati dei soggetti che nel tempo hanno assunto la responsabilità del sistema di conservazione, descrivendo in caso di delega, i soggetti, le funzioni e gli ambiti oggetto della delega stessa;

b) la struttura organizzativa comprensiva delle funzioni, delle responsabilità e degli obblighi dei diversi soggetti che intervengono nel processo di conservazione;

c) la descrizione delle tipologie degli oggetti sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di documenti e delle eventuali eccezioni;

d) la descrizione delle modalità di presa in carico di uno o più pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento;

e) la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione;

f) la modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;

g) la descrizione del sistema di conservazione, comprensivo di tutte le componenti tecnologiche, fisiche e logiche, opportunamente documentate e delle procedure di gestione e di evoluzione delle medesime;

h) la descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie;

i) la descrizione delle procedure per la produzione di duplicati o copie;

j) i tempi entro i quali le diverse tipologie di documenti devono essere scartate ovvero trasferite in conservazione secondo la normativa vigente

Si precisa che il Manuale illustra il solo procedimento di conservazione di documenti nativamente informatici o resi tali da un processo di scannerizzazione e indicizzazione (anch'esso esterno al contesto qui trattato) mentre non tratta alcun aspetto in merito alla gestione dei documenti analogici e/o della loro trasformazione in digitale

1.2 PARTI DEL MANUALE DELLA CONSERVAZIONE

Il Manuale della Conservazione di Tesisquare® è composto da 2 parti, una generale, comune a tutti i clienti, e una specifica per ogni cliente in cui sono descritti tutti i dettagli relativi a ogni singola offerta gestita da Tesisquare®.

Il Manuale di Conservazione è composto quindi da:

Il documento Manuale della Conservazione, che descrive la parte generale

Il documento Allegato al Manuale della Conservazione- Scheda servizio Cliente <X>, dove <X> indica la ragione sociale del cliente.

2. TERMINOLOGIA

Di seguito vengono elencate alcune definizioni presenti in questo documento oltre che quelle previste dal DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 3 dicembre 2013 "*Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 (G.U. n. 59 del 12 marzo 2014), allegato 1.*
A integrazione del Decreto sopra citato si veda anche il DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 22 febbraio 2013 *Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, 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*. Art 1.

GLOSSARIO	
TERMINE	**DEFINIZIONE**
Accesso	Operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici
Accordo di versamento (Submission Agreement)	Accordo di versamento traduce l'inglese Submission agreement, espressione derivata dal glossario dello standard ISO 14721 (OAIS). IL produttore deposita le risorse informative di cui è titolare all'interno di un sistema articolato sul modello OAIS onde garantirne la conservazione a lungo termine. Le modalità di versamento sono descritte nel documento Scheda servizio Cliente (che corrisponde all'accordo di versamento), nel quale sono dettagliati le tipologie di documenti, i formati e i relativi metadati da conservare, nonché le procedure di trasferimento dal produttore al sistema di conservazione. Quest'ultimo mette in opera un processo di acquisizione, al termine del quale predispone le risorse digitali inviate per la conservazione all'interno dell'archivio.
Accreditamento	Riconoscimento, da parte dell'Agenzia per l'Italia digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo

Affidabilità	Caratteristica che esprime il livello di fiducia che l'utente ripone nel documento
AGID	Agenzia per l'Italia Digitale
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
AIP	Archival Information Package. In italiano PdA Pacchetto di Archiviazione (cfr. standard ISO 14721 OAIS)
Archiviazione	Processo di trattamento e gestione dei documenti di uso corrente che permette una loro classificazione (indicizzazione) ai fini della ricerca e consultazione
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
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 al documento informatico
Autenticazione del documento informatico	La validazione del documento informatico attraverso l'associazione di dati informatici relativi all'autore o alle circostanze, anche temporali, della redazione
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
CAD	Codice dell'Amministrazione Digitale (Decreto Legislativo n. 82 del 7 marzo 2005 e successive modificazioni, introdotte dal Decreto Legislativo n. 235 del 30 dicembre 2010)
Certificato Elettronico	Attestato elettronico che consente di collegare l'identità del titolare i dati utilizzati per verificare le firme elettroniche (Codice dell'Amministrazione Digitale Decreto Legislativo n. 82 del 7 marzo 2005 – Capo I – Sezione I – art. 1 – Comma 1 lettera "e")
Certificatore	Il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime. (Codice dell'Amministrazione Digitale – D. Lgs. 7 Marzo 2005, n. 82 - Capo I - Sezione I - Art.1 - Comma 1, lettera "g")
Certificato qualificato	Il certificato elettronico conforme ai requisiti di cui all'allegato. I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva. (Codice dell'Amministrazione Digitale – D. Lgs. 7 Marzo 2005, n. 82 - Capo I - Sezione I - Art.1 - Comma 1 "Definizioni", lettera "f")
Chiave privata	L'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico (Codice dell'Amministrazione Digitale – D. Lgs. 7 Marzo 2005, n. 82 - Capo I - Sezione I - Art.1 - Comma 1, lettera "h")
Chiave pubblica	L'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento

	informatico dal titolare delle chiavi asimmetriche (Codice dell'Amministrazione Digitale – D. Lgs. 7 Marzo 2005, n. 82 - Capo I - Sezione I - Art.1 - Comma 1, lettera "i")
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 dell'amministrazione digitale (CAD)	Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni
Codice eseguibile	Insieme di istruzioni o comandi software direttamente elaborabili dai Sistemi informatici
Conservatore accreditato	Soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
Conservazione	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del Sistema di Conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione
Console di amministrazione	Applicazione web che consente di amministrare il Sistema ed utilizzarne tutte le funzionalità. Consente inoltre al Responsabile del servizio di Conservazione di certificare la chiusura del processo di conservazione
Consumer	Cfr. Utente: ruolo svolto da persone o sistemi client che interagiscono con i servizi di un deposito OAIS al fine di trovare e avere accesso alle informazioni di interesse (OAIS – ISO 14721).
Copia analogica del documento informatico	Documento analogico avente contenuto identico a quello del documento informatico da cui è tratto
Copia di sicurezza	Copia di *backup* degli archivi del Sistema di Conservazione prodotta ai sensi dell'articolo 12 delle presenti regole tecniche per il Sistema di Conservazione
Copia informatica di documento analogico	Il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto
Copia informatica di documento informatico	Il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari
Copia per immagine su supporto informatico di documento analogico	Il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto
Criteri di omogeneità	Regole, configurate sul Sistema, per classificare i documenti in base alla tipologia. I pacchetti di archiviazione saranno costituiti da documenti omogenei tra loro (documenti rispondenti al medesimo criterio di omogeneità)
Destinatario	Identifica il soggetto/Sistema al quale il documento informatico è indirizzato
DIP	Dissemination Information Package In italiano PdD Pacchetto di Distribuzione (cfr. standard ISO 14721 OAIS)
Disponibilità richiesta	Tempo in cui il Sistema deve essere utilizzabile in conformità alle funzionalità previste, esclusi i tempi programmati per la manutenzione, rispetto alle ore concordate per l'esercizio.
Dispositivo sicuro per la creazione della firma	I dispositivi sicuri per la generazione della firma qualificata che devono essere dotati di certificazione di sicurezza secondo l'art. 35 del CAD
Documento analogico	La rappresentazione non informatica di atti, fatti o dati giuridicamente

	rilevanti (Modifiche ed integrazioni al CAD (D. Lgs 07-03-2005, n. 82 – Cap 1 – Sezione I – Art.1 – Comma 1, lettera "p-bis"), introdotte dal decreto legislativo 30 dicembre 2010, n. 235)
Documento informatico	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (Codice dell'Amministrazione Digitale – D. Lgs. 7 Marzo 2005, n. 82 - Capo I - Sezione I - Art.1 - Comma 1, lettera "p")
Duplicato informatico	Documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario (Modifiche ed integrazioni al CAD (D. Lgs 07-03-2005, n. 82 – Cap 1 – Sezione I – Art.1 – Comma 1, lettera "i-quinquies"), introdotte dal decreto legislativo 30 dicembre 2010, n. 235)
Duplicazione dei documenti informatici	Produzione di duplicati informatici
Esibizione	Operazione che consente di visualizzare un documento conservato e di ottenerne copia
Estratto per riassunto	Documento nel quale si attestano in maniera sintetica ma esaustiva fatti, stati o qualità desunti da dati o documenti in possesso di soggetti pubblici
Evidenza informatica	Una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica
Fascicolo informatico	Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'art. 41 del Codice dell'Amministrazione Digitale (D. Lgs. 7 marzo 2005, n. 82 e successive modifiche ed integrazioni)
Firma digitale	Un particolare tipo di firma elettronica qualificata basata su un Sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici (Modifiche ed integrazioni al CAD (D. Lgs 07-03-2005, n. 82 – Cap 1 – Sezione I – Art.1 – Comma 1, lettera "s"), introdotte dal decreto legislativo 30 dicembre 2010, n. 235)
Firma elettronica	L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica (Modifiche ed integrazioni al CAD (D. Lgs 07-03-2005, n. 82 – Cap 1 – Sezione I – Art.1 – Comma 1, lettera "q"), introdotte dal decreto legislativo 30 dicembre 2010, n. 235)
Firma elettronica avanzata	Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario stesso, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai

TESI SpA Registered office: Via Mendicità Istruita, 24 – 12042 Bra (CN) - Headquarters: Via Savigliano, 48 - 12062 Roreto di Cherasco (CN)
Phone +39 0172 476301 - Fax +39 0172 476399 - www.tesisquare.com - info@tesisquare.com
Tax Code and VAT no. 02448510046 – Cuneo Chamber of Commerce - Economic and Administrative Register no. 177331
Share Capital € 750,000 fully vested

	quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati (Modifiche ed integrazioni al CAD (D. Lgs 07-03-2005, n. 82 – Cap 1 – Sezione I – Art.1 – Comma 1, lettera q-bis"), introdotte dal decreto legislativo 30 dicembre 2010, n. 235)
Firma elettronica qualificata	La firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario (e la sua univoca autenticazione informatica), creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma (quale l'apparato strumentale usato per la creazione della firma elettronica) (Modifiche ed integrazioni al CAD (D. Lgs 07-03-2005, n. 82 – Cap 1 – Sezione I – Art.1 – Comma 1, lettera "r"), introdotte dal decreto legislativo 30 dicembre 2010, n. 235)
Formato	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
Formazione	Il processo atto ad assicurare l'autenticità dell'origine e l'integrità del contenuto dei documenti informatici, con apposizione della firma digitale su ciascun singolo documento e/o della marca temporale ai fini di associare una data certa elettronica ove richiesto
FTP server	Programma che permette di accettare connessioni in entrata e di comunicare con un Client attraverso il protocollo FTP
Funzionalità aggiuntive	Le ulteriori componenti del Sistema di protocollo informatico necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni
Funzionalità interoperative	Le componenti del Sistema di protocollo informatico finalizzate a rispondere almeno ai requisiti di interconnessione di cui all'articolo 60 del D.P.R. 28 dicembre 2000, n. 445
Funzionalità minima	La componente del Sistema di protocollo informatico che rispetta i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445
Funzione di hash	Una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
Generazione automatica di documento informatico	Formazione di documenti informatici effettuata direttamente dal Sistema informatico al verificarsi di determinate condizioni
Gestione informatica dei documenti	L'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'àmbito del sistema di classificazione d'archivio adottato, effettuate mediante sistemi informatici. (Codice dell'Amministrazione Digitale – D. Lgs. 7 Marzo 2005, n. 82 - Capo I - Sezione I - Art.1 - Comma 1, lettera "u")
jHttpTransfer	Modulo batch per automazione della trasmissione. È il software che permette di automatizzare le funzioni di upload e download dei vari flussi scambiati con il partner
IdC o Indice di	Evidenza informatica contenente un insieme di informazioni articolate come

conservazione (IPdA indice del pacchetto di archiviazione)	descritto dallo Schema XML fornito nel seguito. L'IdC deve essere corredato da: • riferimento temporale, • firma digitale dei soggetti titolati a effettuare il processo di conservazione sostitutiva, coerentemente con le disposizioni della normativa vigente. L'IdC coincide con lo Schema XML descritto nel presente documento, istanziato secondo le specifiche esigenze di contesto e provvisto di riferimento temporale e firma digitale. (Standard UNI 11386, par. 3.6 – ottobre 2010 – "Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali – SInCRO")
Identificativo univoco	Sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione
Identificazione informatica	La validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso. (Modifiche ed integrazioni al CAD (D. Lgs 07-03-2005, n. 82 – Cap 1 – Sezione I – Art.1 – Comma 1 "Definizioni", lettera "u-ter"), introdotte dal decreto legislativo 30 dicembre 2010, n. 235)
Immodificabilità	Caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso
Impronta	La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash (Standard UNI 11386, par. 3.5 – ottobre 2010 - "Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali – SInCRO")
Ingestion	Processo di acquisizione (ingestion), attraverso il quale vengono ricevuti i SIP e predisposti per l'inclusione nel sistema di conservazione (OAIS – ISO 14721)
Insieme minimo di metadati del documento informatico	Complesso dei metadati da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta, la cui struttura è descritta nell'allegato 5 del DPCM 3 dicembre 2013 (Standard UNI 11386, par. 3.6 – ottobre 2010 – "Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali – SInCRO")
Integrità	Insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato
Interoperabilità	Capacità di un Sistema informatico di interagire con altri Sistemi informatici analoghi sulla base di requisiti minimi condivisi
IPdA (o IdC)	Indice del Pacchetto di Archiviazione. Termine introdotto e descritto nell' allegato 4 dal DPCM 03-12-2014. È sinonimo di IdC.
Leggibilità	Insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti
Log di Sistema	Registrazione cronologica delle operazioni eseguite su di un Sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati
Manuale della Conservazione	Strumento che descrive il Sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 delle regole tecniche del Sistema di Conservazione
Manuale di gestione	Strumento che descrive il Sistema di gestione informatica dei documenti di cui all'articolo 5 delle regole tecniche del protocollo informatico ai sensi delle

TESI SpA Registered office: Via Mendicità Istruita, 24 – 12042 Bra (CN) - Headquarters: Via Savigliano, 48 - 12062 Roreto di Cherasco (CN)
Phone +39 0172 476301 - Fax +39 0172 476399 - www.tesisquare.com - info@tesisquare.com
Tax Code and VAT no. 02448510046 – Cuneo Chamber of Commerce - Economic and Administrative Register no. 177331
Share Capital € 750,000 fully vested

	regole tecniche per il protocollo informatico D.P.C.M. 31 ottobre 2000 e successive modificazioni e integrazioni
Marca temporale	Un'evidenza informatica che consente la validazione temporale
Memorizzazione	Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici
Metadati	Insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel Sistema di Conservazione; tale insieme è descritto nell'allegato 5 del DPCM 3 dicembre 2013
Obiettivo temporale di recupero (Recovery Point Objective)	Indica la perdita dati tollerata: rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza e, conseguentemente, fornisce la misura della massima quantità di dati che il Sistema può perdere a causa di un evento imprevisto.
Originali non unici	I documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi (Codice dell'Amministrazione Digitale – D. Lgs. 7 Marzo 2005, n. 82 - Capo I - Sezione I - Art.1 - Comma 1, lettera "v")
Pacchetto di archiviazione	Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del DPCM 3 dicembre 2013 e secondo le modalità riportate nel manuale di conservazione. In inglese AIP (Archival Information Package).
Pacchetto di distribuzione	Pacchetto informativo inviato dal Sistema di Conservazione all'utente in risposta ad una sua richiesta. In inglese DIP (Dissemination Information Package)
Pacchetto di versamento	Pacchetto informativo inviato dal produttore al Sistema di Conservazione secondo un formato predefinito e concordato descritto nel manuale della conservazione, previsto dal D.P.C.M. 03/12/2013. In inglese SIP (Submission Information Package).
Pacchetto informativo	Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare DPCM 03-12-2013 (Allegato 1) Pacchetto costituito da Contenuto informativo di un oggetto da conservare e relative informazioni sulla conservazione (PDI Preservation Description Information) necessarie per sostenere il processo di conservazione. (ISO 14721 – OAIS)
Periodo criticità servizio	Data/periodo in cui il dato o il servizio deve essere tassativamente erogato per esigenze specifiche del business, quali scadenze o presentazione dei dati.
Piano della sicurezza del Sistema di Conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il Sistema di Conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza
Piano della sicurezza del Sistema di gestione informatica dei documenti	Documento, che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il Sistema di gestione informatica dei documenti da possibili rischi nell'ambito dell'organizzazione di appartenenza
Piano della	Strumento, integrato con il Sistema di classificazione per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione

TESI SpA Registered office: Via Mendicità Istruita, 24 – 12042 Bra (CN) - Headquarters: Via Savigliano, 48 - 12062 Roreto di Cherasco (CN)
Phone +39 0172 476301 - Fax +39 0172 476399 - www.tesisquare.com - info@tesisquare.com
Tax Code and VAT no. 02448510046 – Cuneo Chamber of Commerce - Economic and Administrative Register no. 177331
Share Capital € 750,000 fully vested

Conservazione	ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445
Piano generale della sicurezza	Documento per la pianificazione delle attività volte alla realizzazione del Sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza
Posta elettronica certificata	Sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi. (Modifiche ed integrazioni al CAD (D. Lgs 07-03-2005, n. 82 – Cap 1 – Sezione I – Art.1 – Comma 1, lettera "v-bis"), introdotte dal decreto legislativo 30 dicembre 2010, n. 235)
Presa in carico	Accettazione da parte del Sistema di Conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione
Processo di conservazione	Insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 10 delle regole tecniche del Sistema di Conservazione
Produttore	Persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel Sistema di Conservazione. Producer: le persone o i sistemi *client* che forniscono le informazioni da conservare. (ISO 14721 – OAIS)
Pubbliche amministrazioni	Le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le istituzioni universitarie, gli enti pubblici non economici nazionali, l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN), le agenzie di cui al decreto legislativo 30 luglio 1999, n. 300. (Codice dell'Amministrazione Digitale – D. Lgs. 7 marzo 2005, n. 82 - Capo I - Sezione I - Art.1 - Comma 1 "Definizioni", lettera "z").
Pubblico ufficiale	Notaio o dirigente dell'ufficio responsabile della conservazione dei documenti per la pubblica amministrazione
Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del Sistema di Conservazione dei pacchetti di versamento inviati dal produttore
Registrazione informatica	Insieme delle informazioni risultanti da transazioni informatiche o dalla presentazione in via telematica di dati attraverso moduli o formulari resi disponibili in vario modo all'utente
Registro di protocollo	Registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel Sistema di gestione informatica dei documenti
Registro particolare	Registro informatico di particolari tipologie di atti o documenti; nell'ambito della pubblica amministrazione è previsto ai sensi dell'articolo 53, comma 5 del D.P.R. 28 dicembre 2000, n. 445
Repertorio informatico	Registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche con cui si formano altri atti e documenti o indici di atti e documenti secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica
Responsabile del servizio di conservazione	Soggetto persona fisica nominato responsabile del servizio di conservazione con l'assegnazione delle attività indicate nel documento dell'Agenzia per l'Italia Digitale sui profili professionali richiamati dalla Circolare n. 65/2014 (G.U. n. 89 del 16/04/2014)
Responsabile della conservazione	Soggetto responsabile dell'insieme delle attività elencate nell'articolo 7, comma 1 delle regole tecniche del sistema di conservazione

Responsabile del trattamento dei dati	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali
Responsabile della funzione archivistica di Conservazione	Soggetto persona fisica nominato responsabile della funzione archivistica di Conservazione con l'assegnazione delle attività indicate nel documento dell'Agenzia per l'Italia Digitale sui profili professionali richiamati dalla Circolare n. 65/2014 (G.U. n. 89 del 16/04/2014)
Responsabile della sicurezza	Soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza
Responsabile della sicurezza dei Sistemi per la Conservazione	Soggetto persona fisica nominato responsabile della sicurezza dei Sistemi per la Conservazione con l'assegnazione delle attività indicate nel documento dell'Agenzia per l'Italia Digitale sui profili professionali richiamati dalla Circolare n. 65/2014 (G.U. n. 89 del 16/04/2014)
Riferimento temporale	Informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento (DPCM 03-12-2013 – Allegato 1)
Scarto	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale (DPCM 03-12-2013 – Allegato 1)
Servizi esposti dal Sistema	Interfaccia software esposta dal Sistema di Conservazione verso le applicazioni del cliente, secondo lo standard dei web service
SIP	Submission Information Package. In Italiano PdV Pacchetto di Versamento (cfr. standard ISO 14721 OAIS)
Sistema	Applicazione/Servizio che deve essere disponibile agli aventi diritto in termini di esercizio e disponibilità dell'informazione
Sistema di classificazione	Strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata (DPCM 03-12-2013 – Allegato 1)
Sistema di conservazione	Sistema di Conservazione dei documenti informatici di cui all'art. 44 del Codice dell'Amministrazione Digitale (D. Lgs. 7 marzo 2005, n. 82 e successive modifiche ed integrazioni). Cfr. anche (DPCM 03-12-2013 – Allegato 1)
Sistema di gestione informatica dei documenti	Nell'ambito della Pubblica Amministrazione è il Sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445; per i privati è il Sistema che consente la tenuta di un documento informatico (DPCM 03-12-2013 – Allegato 1)
Staticità	Caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione (DPCM 03-12-2013 – Allegato 1)
Tempo ripristino richiesto (Recovery Time Objective)	Tempo entro il quale un processo informatico ovvero il Sistema Informativo primario deve essere ripristinato dopo un disastro o una condizione di emergenza (o interruzione), al fine di evitare conseguenze inaccettabili
Testo unico	Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni (DPCM 03-12-2013 – Allegato 1)
Titolare	La persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica. (Codice dell'Amministrazione Digitale – D. Lgs. 7 Marzo 2005, n. 82 - Capo I - Sezione I - Art.1 - Comma 1, lettera "aa")
Transazione informatica	Particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche della base di dati (DPCM 03-12-2013 – Allegato 1)
Ufficio utente	Riferito ad un'area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal Sistema di protocollo informatico

TESI SpA Registered office: Via Mendicità Istruita, 24 – 12042 Bra (CN) - Headquarters: Via Savigliano, 48 - 12062 Roreto di Cherasco (CN)
Phone +39 0172 476301 - Fax +39 0172 476399 - www.tesisquare.com - info@tesisquare.com
Tax Code and VAT no. 02448510046 – Cuneo Chamber of Commerce - Economic and Administrative Register no. 177331
Share Capital € 750,000 fully vested

	(DPCM 03-12-2013 – Allegato 1)
Unità di archiviazione	Insieme di uno o più file digitali, anche diversi tra la loro, che costituiscono un documento da conservare. L'unità di archiviazione costituisce l'unità minima di elaborazione per il Sistema di Conservazione, che viene conservata ed esibita come un tutt'uno
Utente	Persona, ente o Sistema che interagisce con i servizi di un Sistema di gestione informatica dei documenti e/o di un Sistema per la Conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse (DPCM 03-12-2013 – Allegato 1)
Validazione temporale	Il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi. (Codice dell'Amministrazione Digitale – D. Lgs. 7 Marzo 2005, n. 82 - Capo I - Sezione I - Art.1 - Comma 1, lettera "bb")
Versamento agli archivi di stato	Operazione con cui il Responsabile della conservazione di un organo giudiziario o amministrativo dello Stato effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservati ai sensi della normativa vigente in materia di beni culturali (DPCM 03-12-2013 – Allegato 1)

ACRONIMI	
TERMINE	**DEFINIZIONE**
AdE	Agenzia delle Entrate
AgID	Agenzia per l'Italia Digitale (già DigitPA e CNIPA)
CA	Certification Authority
CAD	Codice dell'Amministrazione Digitale
DLgs	Decreto Legislativo
DM	Decreto Ministeriale
DPCM	Decreto del Presidente del Consiglio dei Ministri
DPR	Decreto del Presidente della Repubblica
HSM	(Hardware Security Module) dispositivo sicuro per la generazione delle firme che impedisce l'intercettazione della chiave privata utilizzata
IPA	Indice delle Pubbliche Amministrazioni
IPdA	Indice del Pacchetto di Archiviazione
IPdD	Indice del Pacchetto di Distribuzione (o Rapporto di distribuzione)
IPdV	Indice del Pacchetto di Versamento
ISO	International Organization for Standardization
OAIS	ISO 14721:2012; Space Data information transfer system
PdD	Pacchetto di Distribuzione
PdS	Pacchetto di Scarto
PdV	Pacchetto di Versamento
RBAC	Role Based Access Control - Sistema di controllo accessi basato sui ruoli in cui le entità del Sistema che sono identificate e controllate rappresentano posizioni funzionali in una organizzazione o processi
RdV	Rapporto di Versamento
SdI	Sistema d'Interscambio per la fatturazione elettronica PA per lo scambio delle fatture e delle relative notifiche/ricevute ai sensi del DM 3 aprile 2013, n. 55
SLA	Service Level Agreement. È l'accordo tra produttore e Responsabile del servizio di Conservazione sui livelli di servizio da garantire ed indica i giorni entro cui devono essere conservati i documenti nel Sistema di Conservazione
TSA	Time Stamping Authority

[Torna al Sommario]

3. NORMATIVA E STANDARD DI RIFERIMENTO

3.1 NORMATIVA DI RIFERIMENTO

Di seguito si riportano le principali normative di riferimento per l'attività di conservazione a livello nazionale e quella specifica relativa alle diverse tipologie di documenti riguardanti il contratto di erogazione del servizio di conservazione.

Alla data l'elenco dei principali riferimenti normativi italiani in materia è costituito da:

- ✓ Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- ✓ Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- ✓ Decreto Legge 10 giugno 1994, n.357, convertito dalla legge 8 agosto 1994 n.489 Disposizioni tributarie urgenti per accelerare la ripresa dell'economia e dell'occupazione, nonché per ridurre gli adempimenti a carico del contribuente;
- ✓ 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; (parzialmente abrogato con l'entrata in vigore del Decreto Legislativo 7 marzo 2005 n. 82, Codice dell'amministrazione digitale in vigore dal 1° gennaio 2006);
- ✓ Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- ✓ DPCM 13 gennaio 2004 Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici (G.U. 27 aprile 2004, n. 98). (Valide per i documenti formati prima del 3 dicembre 2009);
- ✓ Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- ✓ Decreto del Ministro dell'economia e delle finanze 23 gennaio 2004 Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di supporto (G.U. 3 febbraio 2004, n. 27) - per documenti rilevanti a fini fiscali. Estensione (prevista dall'art. 43 del CAD) a tutti i documenti civilistici e fiscali, con efficacia ai fini tributari: scritture contabili, libri, registri, etc;
- ✓ Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD, come modificato dal D. Lgs. 159/2006)

  In particolare si ricordano:

  Art. 21. Valore probatorio del documento informatico sottoscritto:

  "1. Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza.

  2. Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che sia data prova contraria.

  5. Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con uno o più decreti del Ministro dell'economia e delle finanze, sentito il Ministro delegato per l'innovazione e le tecnologie."

Art. 43. Riproduzione e conservazione dei documenti:

"1. I documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento di cui è prescritta la conservazione per legge o regolamento, ove riprodotti su supporti informatici sono validi e rilevanti a tutti gli effetti di legge, se la riproduzione sia effettuata in modo da garantire la conformità dei documenti agli originali e la loro conservazione nel tempo, nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71".

Art. 44. Requisiti per la conservazione dei documenti informatici

1. Il Sistema di Conservazione dei documenti informatici garantisce:
a) l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione o dell'area organizzativa omogenea di riferimento di cui all'articolo 50, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;
b) l'integrità del documento;
c) la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi i dati di registrazione e di classificazione originari;
d) il rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del decreto legislativo 30 giugno 2003, n. 196, e dal disciplinare tecnico pubblicato in allegato B a tale decreto".

- ✓ D.P.C.M. 30 marzo 2009. Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici (Pubblicato nella Gazz. Uff. 6 giugno 2009, n. 129). (Valide per i documenti formati a partire dal 3 dicembre 2009);
- ✓ Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
- ✓ Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di Sistema di Conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- ✓ Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82;
- ✓ Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.
- ✓ Decreto Presidente Repubblica n. 68 del 11/02/2005– Regolamento per l'utilizzo della PEC
- ✓ Decreto Legislativo n.185/2008 convertito in legge dall'art. 1, Legge n. 2 del 28/01/2009– Obbligo casella PEC per Imprese e Professionisti
- ✓ Art. 5 Decreto Legge n. 179 del 18/10/2012 Agenda Digitale Italiana– Obbligo casella PEC per Imprese individuali e Artigiane – Indice nazionale indirizzi PEC (INI-PEC)
- ✓ Legge n. 35 del 4/04/2012 – Semplifica Italia – Art. 47 quinquies– Obbligo dal 2014 di Comunicazioni telematiche/PEC tra Imprese e PA
- ✓ Decreto INI-PEC del 19/03/2013 – Indice nazionale degli indirizzi di posta elettronica certificata delle imprese e dei professionisti (INI-PEC)
- ✓ CAD – Decreto Legislativo 7 marzo 2005, n. 82 (Modifica Art. 47 – Ultimo aggiornamento il 26/08/2013) – Abolito l'uso del FAX nella PA
- ✓ Regolamento UE n° 910/2014, altresì noto come Regolamento eIDAS (electronic IDentification Authentication and Signature)

- ✓ Regolamento UE n° 679/2016, altresì noto come DPGR (General Data Protection Regulation)

Torna al Sommario

3.2 RIFERIMENTI NORMATIVI IN MATERIA TRIBUTARIA

- ✓ D.M. 23 gennaio 2004 del Ministero dell'economia e delle finanze inerente le modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di supporti;
- ✓ Direttiva 2001/115/CE del 20 dicembre 2001 che modifica la direttiva 77/388/CEE al fine di semplificare, modernizzare e armonizzare le modalità di fatturazione previste in materia di imposta sul valore aggiunto (oggi "inglobata" nella direttiva 2006/112/CE);
- ✓ D. Lgs. 20 febbraio 2004, n. 52 riguardante l'attuazione della direttiva 2001/115/CE che semplifica ed armonizza le modalità di fatturazione in materia di IVA;
- ✓ Circolare 6 dicembre 2006, n. 36 dell'Agenzia delle entrate - "Decreto ministeriale 23 gennaio 2004 – Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di supporto.";
- ✓ Circolare 19 ottobre 2005, n. 45 dell'Agenzia delle entrate - "Decreto legislativo 20 febbraio 2004, n. 52 - Attuazione della direttiva 2001/115/CE che semplifica ed armonizza le modalità di fatturazione in materia di IVA.";
- ✓ Direttiva 2010/45/UE del Consiglio del 13 luglio 2010, pubblicata in Gazzetta Ufficiale l'11/12/2012 n. 288 (DL n. 216 dell'11/12/2012) e attuativa dal 1 gennaio 2013, recante modifica della direttiva 2006/112/CE relativa al Sistema comune d'imposta sul valore aggiunto per quanto riguarda le norme in materia di fatturazione;
- ✓ del Decreto del MEF del 17 giugno 2014 "Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005;
- ✓ Decreto Ministeriale n. 55 del 3/04/2013 – Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche
- ✓ Circolare n. 37 del 4 novembre 2013 – Attuazione del Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'articolo 1, commi da 209 a 213, della legge 24 dicembre 2007, n. 244 – Decreto del Ministro dell'economia e delle finanze 3 aprile 2013, n. 55
- ✓ Art. 25 del Decreto Legge IRPEF – Anticipato al 31 marzo 2015 l'avvio a regime della fattura elettronica obbligatoria nei confronti di tutte le pubbliche amministrazioni – pubblicato in Gazzetta Ufficiale del 24/04/2014
- ✓ Circolare n. 1 del 31 marzo 2014 – Circolare interpretativa del Ministero delle Finanze e della Presidenza del Consiglio di Ministri in tema di Fatturazione Elettronica verso la PA
- ✓ Risoluzione n. 81/E "Interpello - ART. 11, legge 27 luglio 2000, n. 212 – Comunicazione del luogo di conservazione in modalità elettronica dei documenti rilevanti ai fini tributari, art. 5 D.M. 17 giugno 2014". Pubblicata dall'Agenzia delle Entrate il 24 Settembre 2015;
- ✓ D.lgs. num.127 del 2015: trasmissione telematica operazioni IVA in attuazione della legge 11/03/2014 num.23;
- ✓ Legge di bilancio 2018 del 27/12/2017 n° 205 testo pubblicato in G.U. 29/12/2017; art. 1 comma 917-923 e 909.
- ✓ Circolare n. 8/E dell'Agenzia delle entrate "Legge 27 dicembre 2017 n. 205 – novità in tema fatturazione e pagamento cessione di carburanti".

Torna al Sommario

3.3 RIFERIMENTI TECNICI

- ✓ Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali - Art. 6, commi 1 e 2, del testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (GU n. 57 del 9-3-2004); Sostituita da DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 3 dicembre 2013
- ✓ Regole tecniche in materia di Sistema di Conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 (G.U. n. 59 del 12 marzo 2014);
- ✓ Determinazione DIGITPA 28 luglio 2010, n. 69 (in G.U. 17 agosto 2010, n. 191) – Modifiche alla deliberazione 21 maggio 2009, n. 45 del Centro nazionale per l'informatica nella Pubblica Amministrazione, recante «Regole per il riconoscimento e la verifica del documento informatico». (Determinazione commissariale n. 69/2010);
- ✓ Risoluzione dell'agenzia delle entrate 4/e del 19 gennaio 2014 ("Consulenza giuridica - conservazione dei documenti informatici rilevanti ai fini tributari- obbligo di invio dell'impronta dell'archivio informatico di cui all'art. 5 del D.M. 23 gennaio 2004- non sussiste").

Torna al Sommario

3.4 ASSOLVIMENTO DELL'IMPOSTA DI BOLLO SUI DOCUMENTI INFORMATICI

La comunicazione preventiva, da presentare all'ufficio delle Entrate competente territorialmente, dovrà contenere:

- ✓ il numero di atti e documenti informatici distinti per tipologia, in conformità agli articoli della tariffa, che si presume saranno emessi nel corso dell'anno;
- ✓ l'imposta dovuta su ogni singolo documento;
- ✓ l'importo globale dell'imposta relativo a ogni articolo della tariffa;
- ✓ la somma complessivamente dovuta;
- ✓ gli estremi dell'avvenuto pagamento.

L'imposta di bollo deve essere assolta preventivamente, in via presuntiva, prima che il libro giornale e il libro degli inventari siano posti in uso, ossia prima di effettuare le registrazioni, sia pure smaterializzate in quanto i registri sono tenuti in forma informatica.
Ai sensi del Decreto del MEF del 17 giugno 2014 ("Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005") art.6 l'imposta di bollo sui documenti informatici fiscalmente rilevanti è corrisposta mediante versamento nei modi di cui all'art.17 del decreto legislativo 9 luglio 1997, n. 241, con modalità esclusivamente telematica.
Il pagamento dell'imposta relativa alle fatture, agli atti, ai documenti ed ai registri emessi o utilizzati durante l'anno avviene in un'unica soluzione entro 120 giorni dalla chiusura dell'esercizio.
Le fatture elettroniche per le quali è obbligatorio l'assolvimento dell'imposta di bollo devono riportare specifica annotazione di assolvimento dell'imposta.
L'imposta sui libri e sui registri tenuti in modalità informatica, è dovuta ogni 2.500 registrazioni o frazioni di esse.

Torna al Sommario

3.5 STANDARD DI RIFERIMENTO

Si riportano di seguito gli standard di riferimento elencati nell'allegato 3 delle Regole Tecniche in materia di Sistema di Conservazione con indicazione delle versioni aggiornate al 10 ottobre 2014.

- ✓ 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.
- ✓ ISO15489:2016 Information and Documentation records management

[Torna al Sommario](#)

4. RUOLI E RESPONSABILITA'

Sono qui descritti la struttura organizzativa del Sistema di conservazione unitamente alle funzioni e alle responsabilità dei diversi soggetti che intervengono durante il processo di conservazione
Nel Sistema di Conservazione si individuano almeno i seguenti ruoli:

- ✓ produttore;
- ✓ utente;
- ✓ Responsabile del servizio di Conservazione;

I ruoli e le responsabilità descritti di seguito fanno riferimento a quanto definito nell'art. 6 "Ruoli e Responsabilità" delle Regole Tecniche (DPCM 03-12-2013).
I ruoli di produttore e utente sono svolti da persone fisiche o giuridiche interne o esterne al Sistema di Conservazione.
L'utente richiede al Sistema di Conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge.
Il Responsabile del servizio di Conservazione definisce e attua le politiche complessive del Sistema di Conservazione e ne governa la gestione con piena responsabilità ed autonomia. Egli definisce con il produttore il contenuto minimo qualitativo e quantitativo degli oggetti stessi conservati, secondo la redazione di specifici documenti, detti "Schede servizio Cliente" che riportano quanto concordato. Tali accordi vengono riportati nel documento "Allegato al Manuale della Conservazione – Scheda servizio Cliente <X>"
Il Responsabile della conservazione nelle pubbliche amministrazioni è la persona fisica presente all'interno dell'amministrazione.

RUOLI	NOMINATIVO	ATTIVITA' DI COMPETENZA	PERIODO NEL RUOLO	EVENTUALI DELEGHE
Responsabile del servizio di Conservazione	Giuseppe Crivello CRVGPP69B20B791G	• definizione ed attuazione delle politiche complessive del Sistema di Conservazione, nonché del governo della gestione del Sistema di Conservazione; • definizione delle caratteristiche e dei requisiti del Sistema di Conservazione in conformità alla normativa vigente; • corretta erogazione del servizio di conservazione all'ente produttore; • gestione delle convenzioni, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.	Dal 1 febbraio 2016	
Responsabile Sicurezza dei Sistemi per la Conservazione	Fabrizio Baldan	• rispetto e monitoraggio dei requisiti di sicurezza del Sistema di Conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; • segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e	Dal 1 febbraio 2016 al 8 settembre 2017	

		pianificazione delle necessarie azioni correttive.		
Responsabile Sicurezza dei Sistemi per la Conservazione	Claudio Rossero RSSCLD56C14L219P	• rispetto e monitoraggio dei requisiti di sicurezza del Sistema di Conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; • segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.	Dal 9 settembre 2017	
Responsabile funzione archivistica di Conservazione	Chiara Quaranta QRNCRT78A47L219B	• definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; • definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici; • monitoraggio del	Dal 1 giugno 2016	

		processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del Sistema di Conservazione; • 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.		
Responsabile trattamento dati personali	Giuseppe Crivello CRVGPP69B20B791G	• garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; • garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.	Dal 1 febbraio 2016	
Responsabile sistemi informativi per la Conservazione	Stefano Galati GLTSFN82S16L219P	• gestione dell'esercizio delle componenti hardware e software del Sistema di Conservazione; • monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore; • segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di conservazione e	Dal 1 febbraio 2016	

		individuazione e pianificazione delle necessarie azioni correttive; • pianificazione dello sviluppo delle infrastrutture tecnologiche del Sistema di Conservazione; • controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.		
Responsabile sviluppo e manutenzione del sistema di Conservazione	Giuseppe Crivello CRVGPP69B20B791G	• coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione; • pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione; • monitoraggio degli SLA relativi alla manutenzione del Sistema di Conservazione; • interfaccia con l'ente produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche; • gestione dello	Dal 1 febbraio 2016	

		sviluppo di siti web e portali connessi al servizio di conservazione.		

Torna al Sommario

5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 ORGANIGRAMMA

Il processo di conservazione viene organizzato dal Responsabile del servizio di Conservazione (RdC) che si preoccupa di definire e pianificare i compiti per ciascun attore coinvolto nel processo.
Le figure, sopra elencate come ruoli e responsabilità, sono strutturate secondo la rappresentazione di cui sotto:

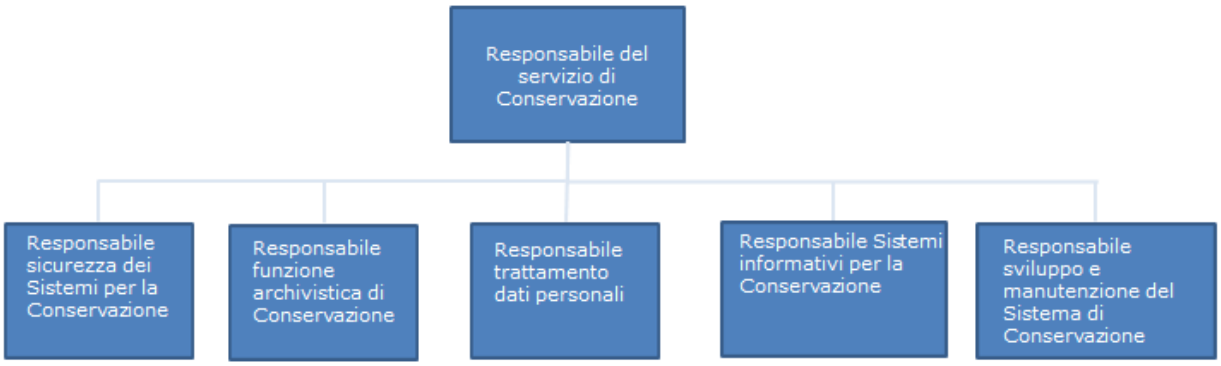

Figura 1. Organigramma

Le persone che dipendono gerarchicamente a livello di organigramma e funzionigramma dal responsabile del servizio di conservazione sono da lui autorizzate al trattamento dei dati personali nel rispetto delle vigenti disposizioni in materia di trattamento dei dati personali in tutte le fasi progettuali.

Torna al Sommario

5.2 STRUTTURE ORGANIZZATIVE

L'organizzazione di Tesisquare® è regolata, fra gli altri elementi, anche dalle seguenti certificazioni:

- ✓ Certificazione ISO/IEC 27001:2013
- ✓ Gestione della Qualità secondo la norma UNI EN ISO 9001:2015
- ✓ GS1 Italy (Indicod ECR)
- ✓ GS1 France
- ✓ GS1 Spain (AECOC)
- ✓ Membro European E-invoicing service provider association (EESPA)

- ✓ Associato ANORC
- ✓ Accreditamento presso SOGEI per la trasmissione verso il Sistema di Interscambio (SDI)
- ✓ Partner tecnologico della filiera Ediel
- ✓ Partner tecnologico della filiera Assobiomedica (ASBM)
- ✓ Partner dell'Osservatorio Fatturazione Elettronica e Dematerializzazione della School of Management del Politecnico di Milano
- ✓ SAP Member extended business program (SAP Competence Center)
- ✓ Cool vendor nel Report Gartner ("Cool vendors in supply chain execution applications, 2015)
- ✓ Registration Authority Namirial
- ✓ Access Point PEPPOL

La risposta ai requisiti di cui sopra, con particolare riferimento alla norma ISO 9001:2015 "Sistemi di Gestione per la Qualità" (SGQ), impone di rispettare processi e procedure al fine garantire una standardizzazione e un grado qualitativo costante.

Di seguito viene riportato il processo di gestione del cliente dal punto di vista commerciale-funzionale dal primo contatto alla chiusura dell'offerta secondo il Sistema di Gestione Qualità predisposto per la norma ISO9001.

Flusso	Responsabilità • Primaria ○ Supporto	Riferimenti
Richiesta di prodotto e/o servizio da parte del cliente	• Cliente	• Telefono • E-Mail se cliente consolidato • Ricerca telemarketing • Contatto diretto
Contatto con il cliente	• Account Manager (nuovi Clienti) ○ Resp.di progettazione/produzione (clienti consolidati)	• Brochure • Visite Commerciali • Richieste specifiche
Se necessario: verifica tra pdt Tesi e/o analisi/studio di fattibilità	• Account Manager ○ Resp.di progettazione/produzione	• Approfondimenti delle richieste del cliente su documentazione varia • Dimostrazione prodotto
OK? SI / NO		
Stesura Offerta	• Resp.di progettazione/produzione • Account Manager	• Doc. Tariffe/Risorse • Allegato Tecnico • Allegato Economico • Lettera di accompagnamento • Allegati contrattuali
Approvazionedell'offerta OK? NO / SI	• Direzione Commerciale • Direzione Generale (per clienti direzionali)	• Elementi per la stesura offerta

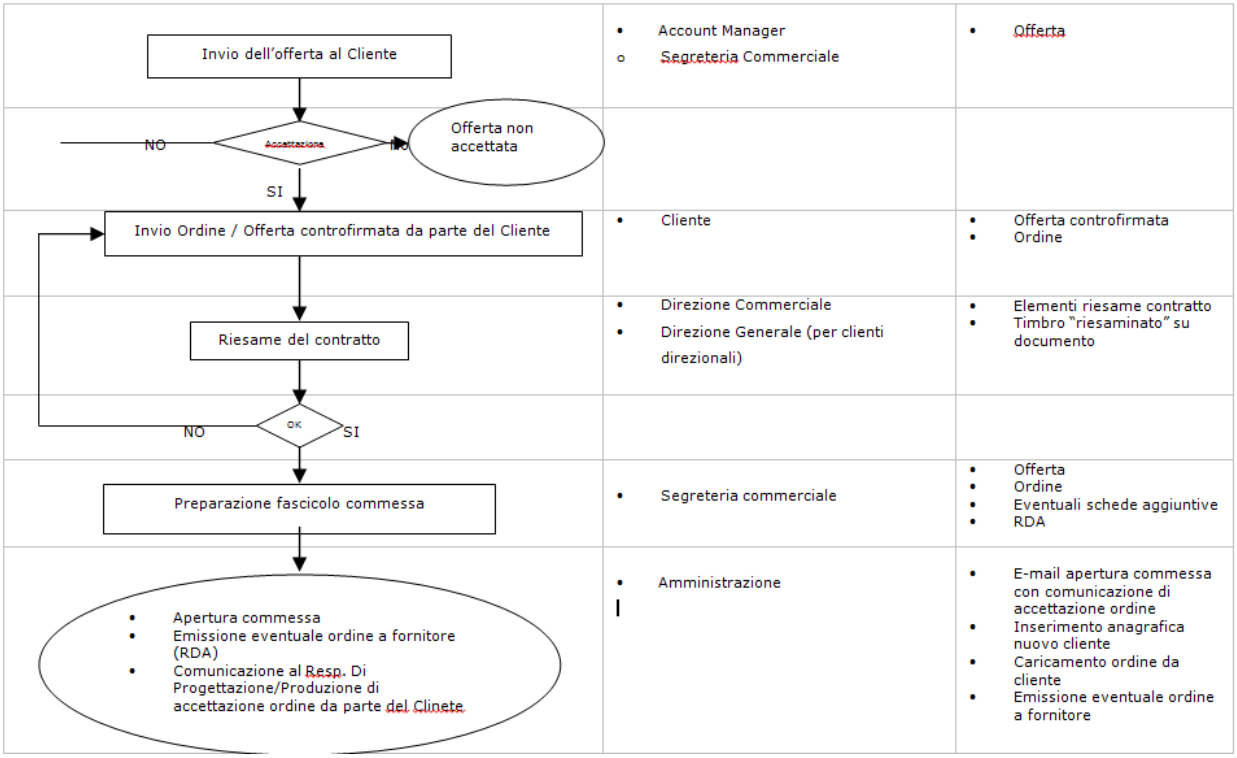

Figura 2. Processo gestione cliente

La gestione dei progetti secondo i criteri stabiliti dalle procedure definite dal SGQ prevede la produzione di documentazione relativamente ad ogni fase del ciclo di vita del progetto stesso.

Ogni progetto deve seguire un iter definito che prevede una serie di step ognuno dei quali di responsabilità di specifiche figure di progetto. Per ognuno di questi step è prevista la produzione di un output che viene raccolto nell'area di lavoro dedicata.

Schema del Flusso di Progetto:

VOCE	RESPONSABILE	DOCUMENTI RICHIESTI/PRODOTTI
Requisiti Cliente	Responsabile Funzionale	Documento Requisiti, Analisi Funzionale, Analisi Tecnica, Mail, Presentazione PPT ecc
Stesura Piano Test Funzionali	Responsabile Funzionale	Piano dei Test Funzionali
Accettazione Requisiti Cliente/Analisi Funzionale	Capo Progetto Tesisquare® Referente Cliente Responsabile Funzionale	Mail di Accettazione
Pianificazione	Capo Progetto Responsabile Delivery	Gantt Organigramma di Progetto

Analisi Tecnica	Analista	Analisi Tecnica
Stesura Piano Test Tecnici	Sviluppatore/Analista	Piano dei Test Tecnici
Piano Test	UG di Riferimento Referente Sviluppo di Area Referente Cliente	Mail di Validazione
Sviluppo	Sviluppatore	Sorgenti
System Test	Sviluppatore Analista	Documento di Esecuzione Test
Test Integrazione	Analista	Documento di Esecuzione Test
User Test	Capo Progetto Analista Referente Cliente Responsabile Funzionale	Documento di Esecuzione Test Manuale Utente
Passaggio Consegne HD/AM	Capo Progetto Analista	Documento di Passaggio Consegne, Mail di Comunicazione Rilascio
Rilascio	Capo Progetto Referente Cliente	Documento di Rilascio, Check List ecc
Follow Up	Capo Progetto Referente Cliente	Mail relative ai controlli/verifiche/attività effettuate
Validazione Progetto	Capo Progetto Referente Cliente	Mail di Fine Follow Up
Riesame	Capo Progetto Analista	Verbale di Riesame
Riesame di Fine Progetto / Lessons Learned***	Capo Progetto Analista Commerciale ecc	Azioni correttive o proposte di miglioramento

Gestione documentazione allegata al contratto.

Alla restituzione del contratto firmato da parte del cliente viene innescato un processo interno secondo cui l'allegato economico, l'allegato tecnico e le condizioni generali del servizio vengono salvati su apposita directory. Successivamente al ricevimento degli allegati relativi a deleghe per l'apposizione della firma, modulo per delega al processo di conservazione, modulo per il rilascio del certificato di firma, documento d'identità, opportunamente compilati e sottoscritti, questi documenti vengono altresì salvati su apposita directory. Successivamente tutti questi documenti vengono portati in conservazione.

Passaggio delle attività all'HD.
La BU di riferimento informa il cliente finale del rilascio in produzione delle modifiche/implementazioni commissionate. A fronte di un rilascio in produzione viene inviata una mail di informazione al supporto

tecnico all'indirizzo mail b2b@service.tesisquare.com , in questo modo avviene il passaggio di consegne all'HD. L'attività dell'HD è costantemente controllata e monitorata tramite documentazione interna atta a leggere il pannello di monitoraggio delle attività, gestire i livelli di criticità e l'escalation problematiche.

Gestione Change Request**.**
La gestione delle Change Request avverrà coerentemente con quanto definito nel SGQ (sistema di gestione della qualità) di Tesisquare®.

Gestione PACA.
La BU di competenza contribuisce alla produzione del PACA (preventive action corrective action) centralizzato Tesisquare® attraverso la figura del BU Mngr. Il PACA sarà gestito secondo il processo di gestione delle Non Conformità coerentemente con quanto definito nel SGQ (sistema di gestione della qualità) di Tesisquare®.

La procedura descrive i criteri e le modalità operative in base alle quali, dall'analisi degli incident accaduti e/o degli audit effettuati, delle situazioni non conformi verificatesi in un determinato periodo, devono essere stabilite e messe in atto opportune AC/AP finalizzate alla rimozione delle cause che effettivamente hanno generato le Non Conformità ed i reclami medesimi. L'owner del processo sarà il Quality Manager. Le azioni preventive e correttive sono tracciate: per ciascuna viene aperto un ticket che sarà messo in pianificazione e gestito dall'area di Application Maintenance.

Riassumendo: una volta identificate le attività proprie di ciascun contratto di servizio di conservazione e, dopo avere formalizzato tutti gli aspetti funzionali-commerciali, le attività vengono messe in pianificazione per poi essere oggetto di analisi, sviluppo, test (prima interno, poi con il cliente) e follow up. A seguire viene attivato ufficialmente il servizio con mail di rilascio in produzione delle procedure, consegna del link e delle credenziali di accesso al portale di consultazione.

Può essere così avviata l'acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e la generazione del rapporto di versamento; preparazione e gestione del pacchetto di archiviazione; la preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta.

Tutti questi passaggi vengono descritti nel dettaglio nell'allegato tecnico dell'offerta che viene inviata al cliente e nell'allegato Scheda Servizio Cliente -Specificità del Contratto.
Per quanto afferisce alla privacy e alla riservatezza (trattamento dati personali) si faccia riferimento a quanto indicato nelle Condizioni generali del Contratto inviate e sottoscritte dal Cliente.
Per tutta la durata contrattuale concordata, viene garantita ai documenti ed ai pacchetti informativi integrità, autenticità dell'origine, leggibilità, disponibilità e reperibilità, sicurezza e riservatezza.

Torna al Sommario

5.3 COMPITI E DOVERI DEL RESPONSABILE DEL SERVIZIO DI CONSERVAZIONE

Il Responsabile del servizio di Conservazione, anche attraverso i suoi delegati, è responsabile del processo di conservazione e di esibizione (ricerca e messa a disposizione dei documenti conservati digitalmente alla Amministrazione Finanziaria e/o Pubblica Autorità) della documentazione aziendale rilevante ai fini contabili e fiscali che si è deciso di conservare in modo digitale.
L'obiettivo principale del Responsabile del servizio di Conservazione digitale è quello di definire e realizzare, attraverso un'opportuna organizzazione delle attività e mediante procedure informatiche, il processo aziendale per il trattamento della documentazione soggetta a conservazione digitale; per il raggiungimento del suo scopo il Responsabile del servizio di Conservazione digitale, ai sensi dell'art. 6 comma 6 del DPCM 3 dicembre 2013 e s.m.i., può 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. Tale delega e' formalizzata, esplicitando chiaramente il contenuto della stessa, ed in particolare le specifiche funzioni e

competenze affidate al delegato.

I compiti del Responsabile del servizio di Conservazione e dei suoi delegati sono i seguenti:

- ✓ compiti di organizzativi
- ✓ compiti di registrazione
- ✓ compiti di manutenzione e controllo
- ✓ compiti operativi
- ✓ compiti per la protezione dei dati e delle procedure informatiche
- ✓ compiti di assistenza/ispezione
- ✓ compiti di natura fiscale

Il Responsabile per il procedimento di Conservazione, anche attraverso i suoi delegati, deve preoccuparsi della realizzazione di una base di dati relativa ai documenti digitali, gestita secondo principi di sicurezza stabiliti e documentati e deve adottare procedure di tracciabilità in modo da garantire la corretta conservazione, l'accessibilità al singolo documento e la sua esibizione in funzione della specifica tipologia di documenti.
Il Responsabile per il procedimento di Conservazione si occupa, anche attraverso i suoi delegati, di:

- ✓ partecipare a incontri e seminari formativi dedicati alle procedure di conservazione digitale;
- ✓ predisporre il manuale di conservazione di cui all'art. 8 del DPCM 3 dicembre 2013 e s.m.i. curandone l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.
- ✓ definire le caratteristiche e i requisiti del Sistema di Conservazione, in funzione della tipologia dei documenti (analogici o informatici) da conservare, e organizzare gli stessi in modo da garantire la corretta conservazione e la sicurezza dei dati, anche al fine di poterli prontamente produrre, ove necessario;
- ✓ definire le procedure di sicurezza e tracciabilità che consentano di risalire in ogni momento alle attività effettuate durante l'esecuzione operativa di conservazione;
- ✓ definire le procedure informatiche ed organizzative per la corretta tenuta dei supporti informatici su cui vengono memorizzati i documenti oggetto di conservazione;
- ✓ definire le procedure informatiche ed organizzative atte ad esibire, in caso di richieste formulate dalle Autorità Fiscali, la documentazione conservata.

Torna al Sommario

5.3.1 COMPITI ORGANIZZATIVI

Le attività necessarie per lo svolgimento dell'attività di conservazione digitale della documentazione fiscale è stata organizzata per produrre efficienza nell'ambito del Sistema di Conservazione digitale. Il processo di conservazione viene eseguito mediante l'utilizzo di procedure informatiche atte allo scopo e il personale addetto alla conservazione ne gestisce l'alimentazione e il funzionamento.
La tempistica di alimentazione del Sistema informatico di conservazione digitale viene definita dal Responsabile del servizio di Conservazione digitale e da un insieme di figure aziendali da lui coordinate.

I Responsabili nominati internamente da Tesisquare® sono a conoscenza degli aspetti inerenti alla normativa sulla sicurezza e sull'ambiente in modo tale da coordinare efficacemente tali esigenze con le esigenze produttive e, inoltre, rappresenta l'azienda di fronte alle autorità competenti.
I Responsabili nominati internamente da Tesisquare® sono a conoscenza delle modalità con cui vengono effettuati gli interventi di manutenzione/aggiornamento/sviluppo per poterli pianificare nel dettaglio e per assicurare il mantenimento delle condizioni di sicurezza ed il minore impatto sulla produzione.

La procedura di conservazione adottata si può suddividere in quattro fasi principali:

- ✓ alimentazione del Sistema di Conservazione;
- ✓ elaborazione della documentazione da conservare e registrazione del dispositivo di memorizzazione;
- ✓ conservazione dei supporti registrati;
- ✓ esibizione della documentazione fiscale.

Ogni fase è svolta da singole funzioni delegate con compiti specifici nell'assolvimento delle attività.

Torna al Sommario

5.3.2 COMPITI DI REGISTRAZIONE

Il Responsabile del servizio di Conservazione, anche attraverso i suoi delegati, si deve occupare della corretta archiviazione delle informazioni caratterizzanti ciascun supporto di memorizzazione e garantirne la disponibilità in caso di richiesta; in particolare dovrà mettere in atto delle azioni che consentano di:

- ✓ descrivere le modalità di identificazione, emissione, revisione e approvazione della documentazione;
- ✓ descrivere il contenuto dell'insieme dei documenti sottoposti a conservazione;
- ✓ descrivere gli estremi degli eventuali suoi delegati, indicando anche i compiti ad essi assegnati;
- ✓ fornire le indicazioni sul numero e sul luogo di conservazione delle copie di sicurezza;
- ✓ descrivere le modalità di pianificazione e svolgimento delle verifiche ispettive interne, compresa la registrazione e conservazione delle stesse;
- ✓ descrivere il processo di verifica delle azioni messe in atto per garantire la sicurezza delle informazioni e relativa registrazione dei risultati;
- ✓ descrivere le modalità per l'erogazione di formazione al personale;
- ✓ descrivere i requisiti per l'identificazione, l'analisi, la valutazione e la risoluzione di eventuali situazioni anomale (difformità, incidenti, etc.).

Torna al Sommario

5.3.3 COMPITI DI MANUTENZIONE E CONTROLLO

Rientrano in queste mansioni:

- ✓ mantenere un archivio dei programmi utilizzati nel corso del tempo per il processo di conservazione digitale, nelle loro diverse release;
- ✓ implementare specifici controlli di Sistema per individuare e prevenire l'azione di software che possano alterare i programmi ed i dati;
- ✓ verificare la corretta funzionalità del Sistema e dei programmi in gestione;
- ✓ analizzare e valutare periodicamente la registrazione degli eventi rilevanti ai fini della sicurezza (analisi del log di Sistema);
- ✓ mantenere il dispositivo di firma aggiornato ed allineato con le procedure gestite dal Certificatore Qualificato che ha rilasciato il certificato;
- ✓ verificare la validità della marca temporale;
- ✓ verificare periodicamente l'effettiva leggibilità dei documenti conservati, provvedendo, se si ritiene necessario, al riversamento diretto o sostitutivo del contenuto dei supporti;
- ✓ verificare l'obsolescenza dei formati adottando le misure necessarie per ripristinarne la corretta funzionalità.

Torna al Sommario

TESI SpA Registered office: Via Mendicità Istruita, 24 – 12042 Bra (CN) - Headquarters: Via Savigliano, 48 - 12062 Roreto di Cherasco (CN)
Phone +39 0172 476301 - Fax +39 0172 476399 - www.tesisquare.com - info@tesisquare.com
Tax Code and VAT no. 02448510046 – Cuneo Chamber of Commerce - Economic and Administrative Register no. 177331
Share Capital € 750,000 fully vested

5.3.4 COMPITI OPERATIVI

Il Responsabile del servizio di Conservazione, anche attraverso i suoi delegati, deve supervisionare l'intero processo di archiviazione e conservazione digitale, verificando accuratamente i processi di apposizione delle firme digitali, dei riferimenti temporali e delle marche temporali, in modo che la procedura rispetti la normativa, assicurandosi che tutto il processo si realizzi secondo le procedure descritte nel Manuale della conservazione digitale. È suo compito verificare e controllare la sincronizzazione del *clock* di Sistema per consentire registrazioni accurate e comparabili tra loro.
Deve verificare la effettiva leggibilità dei documenti prima dell'apposizione della firma digitale e della marca temporale e la leggibilità dei supporti contenenti i documenti alla fine del processo di conservazione ossia prima della loro archiviazione in luogo sicuro.
Rientra in questi compiti anche il mantenimento di tutta la documentazione descrittiva del processo di conservazione aggiornata nel corso del tempo anche attraverso le strutture di consulenza legale e tecnica da lui incaricate.
Il coordinamento e la supervisione del Responsabile del servizio di Conservazione vengono svolti anche attraverso il diretto utilizzo dell'apporto consulenziale offerto dalle strutture legali e tecniche preposte all'erogazione e sviluppo del processo.

Torna al Sommario

5.3.5 COMPITI PER LA PROTEZIONE DEI DATI E DELLE PROCEDURE INFORMATICHE

Il Responsabile del servizio di Conservazione opera d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei Sistemi informativi.
Il Responsabile per il procedimento di Conservazione è garante tutte le misure necessarie per la sicurezza fisica, logica e ambientale dei dati e del Sistema preposto alla loro conservazione, comprensivo delle copie di sicurezza dei supporti di memorizzazione, al fine di proteggere le informazioni da possibili violazioni in termini di riservatezza, integrità e disponibilità delle informazioni.
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 europea di tutela della privacy, per garantirne il corretto funzionamento contro il cosiddetto *malicious code* e contro gli accessi non autorizzati sia logici che fisici.
Il Responsabile per il procedimento di Conservazione deve stabilire, attraverso un'analisi del rischio, gli appropriati controlli di sicurezza delle informazioni da adottare.

Torna al Sommario

5.3.6 COMPITI DI ASSISTENZA ED ISPEZIONE

Il Responsabile per il procedimento di Conservazione, anche attraverso i suoi delegati, deve garantire l'adeguato supporto ai vari delegati che svolgono le attività di conservazione affinché il processo possa essere svolto senza interruzione a partire dalla fase di alimentazione per concludersi con la fase di registrazione dei dati su supporto informatico non modificabile e la relativa custodia del dispositivo di registrazione in luogo sicuro.
Deve sempre attivarsi affinché eventuali disfunzioni possano essere risolte nel più breve tempo possibile, anche attraverso il proprio sostituto.
Deve inoltre occuparsi di ispezionare i luoghi in cui vengono eseguite le attività di registrazione delle informazioni digitali e di conservazione a garanzia della validità giuridica e fiscale del processo, per non incorrere nelle sanzioni previste per mancata osservanza.
Per il Responsabile del servizio di Conservazione è utile effettuare, in base ad uno scadenzario prestabilito, appropriate verifiche ispettive interne allo scopo di verificare gli obiettivi, i controlli, i processi e le procedure messe in atto all'interno del Sistema di gestione della sicurezza.
Il Responsabile del servizio di Conservazione assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza.

TESI SpA Registered office: Via Mendicità Istruita, 24 – 12042 Bra (CN) - Headquarters: Via Savigliano, 48 - 12062 Roreto di Cherasco (CN)
Phone +39 0172 476301 - Fax +39 0172 476399 - www.tesisquare.com - info@tesisquare.com
Tax Code and VAT no. 02448510046 – Cuneo Chamber of Commerce - Economic and Administrative Register no. 177331
Share Capital € 750,000 fully vested

Il Responsabile del servizio di Conservazione provvede, per gli organi giudiziari e amministrativi dello Stato, al versamento dei documenti conservati all'archivio centrale dello Stato e agli archivi di Stato secondo quanto previsto dalle norme vigenti.

Torna al Sommario

5.3.7 COMPITI DI ASSISTENZA E AGGIORNAMENTO NORMATIVO E FISCALE

Il Responsabile per il procedimento di Conservazione, anche attraverso i suoi delegati, fornirà l'assistenza necessaria sia per la verifica, a campione, della validità dei supporti sia per eventuali aggiornamenti riguardanti la normativa fiscale e giuridica rilevante ai fini della conservazione.

Torna al Sommario

5.3.8 ASPETTI OPERATIVI E PROCEDURALI

I compiti che il Responsabile del servizio di Conservazione Digitale è tenuto ad osservare sono descritti nella normativa DPCM 3 dicembre 2013 e s.m.i. *("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 processo di conservazione impone alle aziende e/o pubbliche amministrazioni l'istituzione di una struttura e di una organizzazione coerente con le proprie politiche di efficienza gestionale, che garantisca la piena osservanza di tale normativa. A tal scopo, sulla base delle specifiche necessità aziendali/amministrative, il Responsabile per il Procedimento di Conservazione deve, sia dal punto di vista della impostazione operativa delle attività di conservazione sia dal punto di vista della scelta delle risorse coinvolte nel processo, organizzare il lavoro affinché esso venga svolto secondo i principi stabiliti dalla legislazione italiana vigente.

Il Responsabile per il procedimento di Conservazione, all'interno della propria struttura organizzativa, ha definito:

- ✓ Le procedure per la conservazione della documentazione fiscale aziendale
- ✓ Le funzioni delegate della conservazione che agiscano per suo conto a garanzia della continuità del processo
- ✓ I compiti di tali funzioni
- ✓ La documentazione cartacea di delega ed il relativo mantenimento

Le deleghe sono quindi formalizzate tramite documento apposito riportante la motivazione della delega, la data di delega e la durata dell'incarico.

Torna al Sommario

6. OGGETTI SOTTOPOSTI A CONSERVAZIONE

Gli oggetti della conservazione sono trattati dal Sistema di Conservazione in pacchetti informativi che si distinguono in:

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

Il funzionamento del Sistema di Conservazione è basato sulla compliance alle regole tecniche di cui al DPCM 3 dicembre 2013 (alla base del quale vi è il concetto di informazione da conservare e quindi di pacchetto informativo) ed allo standard ISO 27001.
Il versamento dei pacchetti (contenenti documenti e dati) sul Sistema di Conservazione da parte di un Ente Produttore e ogni distribuzione di documenti dal Sistema ad un Utente autorizzato avvengono infatti nella forma di una o più trasmissioni distinte (sessioni) ovvero tramite lo scambio (versamento o distribuzione) di pacchetti informativi.

I pacchetti informativi sono costituiti da:

- ✓ Contenuto informativo: è l'insieme delle informazioni che costituisce l'obiettivo originario della conservazione
- ✓ Informazioni sulla Conservazione (PDI): informazioni necessarie per un'adeguata conservazione del Contenuto informativo fornite dai metadati

Torna al Sommario

6.1 OGGETTI CONSERVATI

Il sistema di conservazione gestisce:

- ✓ Documenti fiscali: documenti prodotti in ambito fiscale (fatture attive e passive, bilanci, libri e registri, etc.)
- ✓ Documenti non fiscali: (es. DDT, contratti, note spese etc.)
- ✓ Posta elettronica certificata (mail e ricevute)

Nel documento "Scheda Servizio Cliente" e nel Contratto concordato tra Ente Conservatore e Ente Produttore sono elencate e descritte le tipologie di documenti sottoposte a conservazione per un determinato Produttore e le relative politiche di conservazione.
In particolare, le predette politiche di conservazione relative agli oggetti conservati riguardano per ciascuna tipologia documentale:

- ✓ la natura e l'oggetto della tipologia documentale;
- ✓ l'elenco e la descrizione dei formati dei file utilizzati;
- ✓ l'elenco dei metadati minimi previsti per legge associati ai documenti;
- ✓ il periodo di conservazione previsto dal contratto;
- ✓ i livelli di servizio (SLA) concordati con l'ente produttore;
- ✓ altre politiche (regole) che caratterizzano il processo di conservazione;

Le tipologie di documenti che caratterizzano gli oggetti digitali da versare nel Sistema di Conservazione sono definite attraverso le attività di analisi e di classificazione documentale nella fase di prevendita ed attivazione del servizio.
La descrizione delle tipologie documentali, con l'indicazione della loro natura, dei formati, dei metadati, delle tempistiche di conservazione sono riportate nel dettaglio nel documento "Scheda Servizio Cliente" e nel Contratto e sono peculiari di ciascun produttore dei documenti e di ciascuna tipologia documentale.
I formati dei files contenuti nel Pacchetti di Versamento devono essere conformi all'elenco dei formati previsti dall'Allegato 2 del DPCM 3 Dicembre 2013.

Il produttore dei documenti deve adeguarsi al seguente elenco dei formati ammessi.

- ✓ PDF-PDF/A

Sviluppato da	Adobe Systems http://www.adobe.com/
Estensione	.pdf
Tipo MIME	application/pdf
Formato aperto	Sì
Specifiche tecniche	Pubbliche
Standard	ISO 32000-1 (PDF) ISO 19005-1:2005 (vers. PDF 1.4) ISO 19005-2:2011 (vers. PDF 1.7)
Ultima versione	1.7
Collegamento utile	http://www.pdfa.org/doku.php

✓ TIFF

Sviluppato da	Aldus Corporation in seguito acquistata da Adobe
Estensioni	.tif
Tipo MIME	image/tiff
Formato aperto	No
Specifiche tecniche	Pubbliche
Ultime versioni	TIFF 6.0 del 1992 TIFF Supplement 2 del 2002
Collegamenti utili	http://partners.adobe.com/public/developer/tiff/index.html

- ✓ XML

Sviluppato da	Microsoft http://www.microsoft.com http://www.microsoft.it
Estensioni principali	.docx, .xlsx, .pptx
Tipo MIME	
Formato aperto	Sì
Derivato da	XML
Specifiche tecniche	pubblicate da Microsoft dal 2007
Standard	ISO/IEC DIS 29500:2008
Ultima versione	1.1
Possibile presenza codice maligno	Sì
Collegamenti utili	http://msdn.microsoft.com/en-us/library/aa338205.aspx http://standards.iso.org/ittf/PubliclyAvailableStandards www.iso.org

- ✓ JPG

Sviluppato da	Joint Photographic Experts Group
Estensioni	.jpg, .jpeg
Tipo MIME	image/jpeg
Formato aperto	Sì
Specifiche tecniche	Pubbliche
Standard	ISO/IEC 10918:1
Ultima versione	2009
Collegamenti utili	http://www.jpeg.org/ www.iso.org

✓ OPEN DOCUMENT FORMAT

Sviluppato da	OASIS http://www.oasis-open.org/ Oracle America (già Sun Microsystems) http://www.oracle.com/it/index.html
Estensioni	.ods, .odp, .odg, .odb
Tipo MIME	application/vnd.oasis.opendocument.text
Formato aperto	Sì
Derivato da	XML
Specifiche tecniche	pubblicate da OASIS dal 2005
Standard	ISO/IEC 26300:2006 UNI CEI ISO/IEC 26300
Ultima versione	1.0
Collegamenti utili	http://books.evc-cit.info/ http://www.oasis-open.org www.iso.org

Figura 3. Elenco formati ammessi secondo l'Allegato 2 del DPCM 3 Dicembre 2013

In tutti i casi riportati in tabella, il produttore dei documenti s'impegna a versare al Sistema di Conservazione documenti privi di codici eseguibili o macro istruzioni.
Infine, gli oggetti da conservare sono versati al Sistema di Conservazione dall'Ente Produttore all'interno di Pacchetti Informativi denominati Pacchetti di Versamento e descritti nel paragrafo successivo.

Di seguito si elencano in maniera tabellare le tipologie di documenti conservati, in conformità con quanto descritto sopra per i formati previsti all'interno dell'Allegato 2 del DPCM 3 Dicembre 2013 (come indicato nelle premesse dell'allegato stesso questo elenco potrà essere periodicamente aggiornato):

Formato del file	Tipo File	Estensione	Visualizzatore
PDF/PDF-A	Document/Pdf	.pdf	Adobe Reader, altri compatibili
TIFF	Image/tif	.tif, .tiff	Windows, altri
XML	Application/Xml	.xml	Browser/Editor testo
JPG	Image/jpeg	.jpg, .jpeg	Windows, altri
TXT	Text	.txt	Editore di testo
PEC e e-mail	Mime	.eml	Client di posta
OPEN Doc	Document	.odc	Openoffice

Relativamente ai pacchetti di archiviazione il sistema di conservazione prevede la gestione dei metadati minimi previsti dalla normativa (DPCM 13 novembre 2014, Allegato 5) per ogni classe documentale. Per

l'elenco completo delle configurazioni minime applicate, si faccia riferimento al documento seguente: "ds_tigital_tdoc_classi_documentali_metadati_standard".

[Torna al Sommario]

6.2 PACCHETTO DI VERSAMENTO

È il pacchetto informativo inviato dal Produttore al Sistema di Conservazione e oggetto dell'accordo stipulato con il contratto di affidamento del servizio di conservazione; può essere definito secondo le modalità di seguito dettagliate:

- **Modalità 1**

È il caso in cui il Produttore invia direttamente il Pacchetto di Versamento, che corrisponde a un contenitore (archivio) nel formato zip compresso, costituito da:

- ✓ i documenti da conservare;
- ✓ un file Indice IPdV (Indice del Pacchetto di Versamento) finalizzato alla descrizione delle informazioni relative all'oggetto della conservazione, all'identificazione del produttore, ai dati descrittivi ed informativi sull'impacchettamento e su ciascun documento contenuto nel pacchetto, così come indicato dall'allegato 5 delle Regole tecniche in materia di Sistemi di Conservazione (e ISO 14721:2012 OAIS).

Il file Indice del Pacchetto di Versamento (IPdV) è un file che assicura:

- ✓ l'identificazione del soggetto che ha prodotto il Pacchetto di Versamento (produttore dei documenti);
- ✓ la definizione della tipologia documentale (a cui appartengono i documenti inclusi nel pacchetto)
- ✓ la presenza dei metadati minimi richiesti dalla normativa:
  - Identificativo univoco del documento;
  - Produttore PdV;
  - Ragione sociale cliente/titolare della documentazione;
  - Classe Documentale.

I dati contenuti nel Pacchetto di Versamento, le modalità di caricamento e i formati sono concordati di volta in volta con ciascun Produttore nei singoli contratti.

- **Modalità 2**

È il caso in cui il Produttore, utilizzando la piattaforma proprietaria Tesi E-integration leader di mercato nell'ambito delle soluzioni di trasmissione dati EDI (Electronic Data Interchange), invia una serie di documenti e metadati che costituiscono un "singolo versamento": superati i controlli formali e di valorizzazione dei contenuti, questi vengono acquisiti sul Sistema di Conservazione in attesa di elaborazione.

Sulla base delle tempistiche definite per la singola classe documentale, il Sistema di Conservazione provvede ad elaborare tutti i documenti ed i relativi metadati che risultano in attesa e pronti per la conservazione, avviando una sessione di versamento che si concluderà con la generazione del relativo Rapporto di Versamento.
Il Pacchetto di Versamento corrisponde quindi all'insieme dei file acquisiti sul Sistema di Conservazione e dei rispettivi metadati, per i quali è stato restituito un Rapporto di Versamento con esito positivo al momento del versamento.

Una volta generato il RdV, è comunque possibile scaricare un contenitore (archivio) logico corrispondente al PdV nel formato zip compresso, costituito dai documenti da conservare e dal relativo file indice.

Torna al Sommario

6.3 PACCHETTO DI ARCHIVIAZIONE

Il pacchetto di Archiviazione (PdA) generato nel processo di conservazione del Sistema è composto dalla trasformazione dei Pacchetti di Versamento secondo le modalità riportate nel presente manuale di conservazione.
Un Pacchetto di Archiviazione (PdA) è un contenitore informativo che contiene:

- ✓ gli oggetti informativi individuati per la conservazione (documenti da conservare);
- ✓ un Indice del Pacchetto di Archiviazione (IPdA) che rappresenta le Informazioni sulla Conservazione.

I dati contenuti nel Pacchetto di Archiviazione (PdA), le modalità di caricamento e i formati sono concordati di volta in volta con ciascun Produttore nei singoli contratti. I metadati (indici) presenti del PdA vengono gestiti secondo quanto previsto dai singoli contratti, viene in ogni caso verificata la presenza degli indici minimi previsti dalla normativa per ciascun tipo documento.

Indice del pacchetto di archiviazione.
L'indice del pacchetto di archiviazione (IPdA) è un file XML creato da Sistema di Conservazione di Tesisquare® a chiusura del processo di conservazione secondo le specifiche dello standard UNI SInCRO, come richiesto dall'Allegato 4 del DPCM 3/12/2013.
Al suo interno si trovano:

- ✓ informazioni riguardanti l'azienda che ha generato l'indice;
- ✓ informazioni riguardanti l'azienda proprietaria dei documenti, per la quale viene prodotto l'indice;
- ✓ informazioni riguardanti la classe documentale e il periodo di riferimento dei documenti conservati;
- ✓ informazioni specifiche di ogni documento. In questa sezione trovano posto l'ID univoco del documento, il nome del file, la sua impronta e tutti i metadati ad esso correlati;
- ✓ informazioni riguardanti tutti i soggetti (fisici e giuridici) interessati dal processo di conservazione. In tale sezione trovano posto almeno il soggetto che appone la firma all'IPdA e l'azienda che offre il servizio di conservazione.

Di seguito la struttura dell'Indice del Pacchetto di Archiviazione:

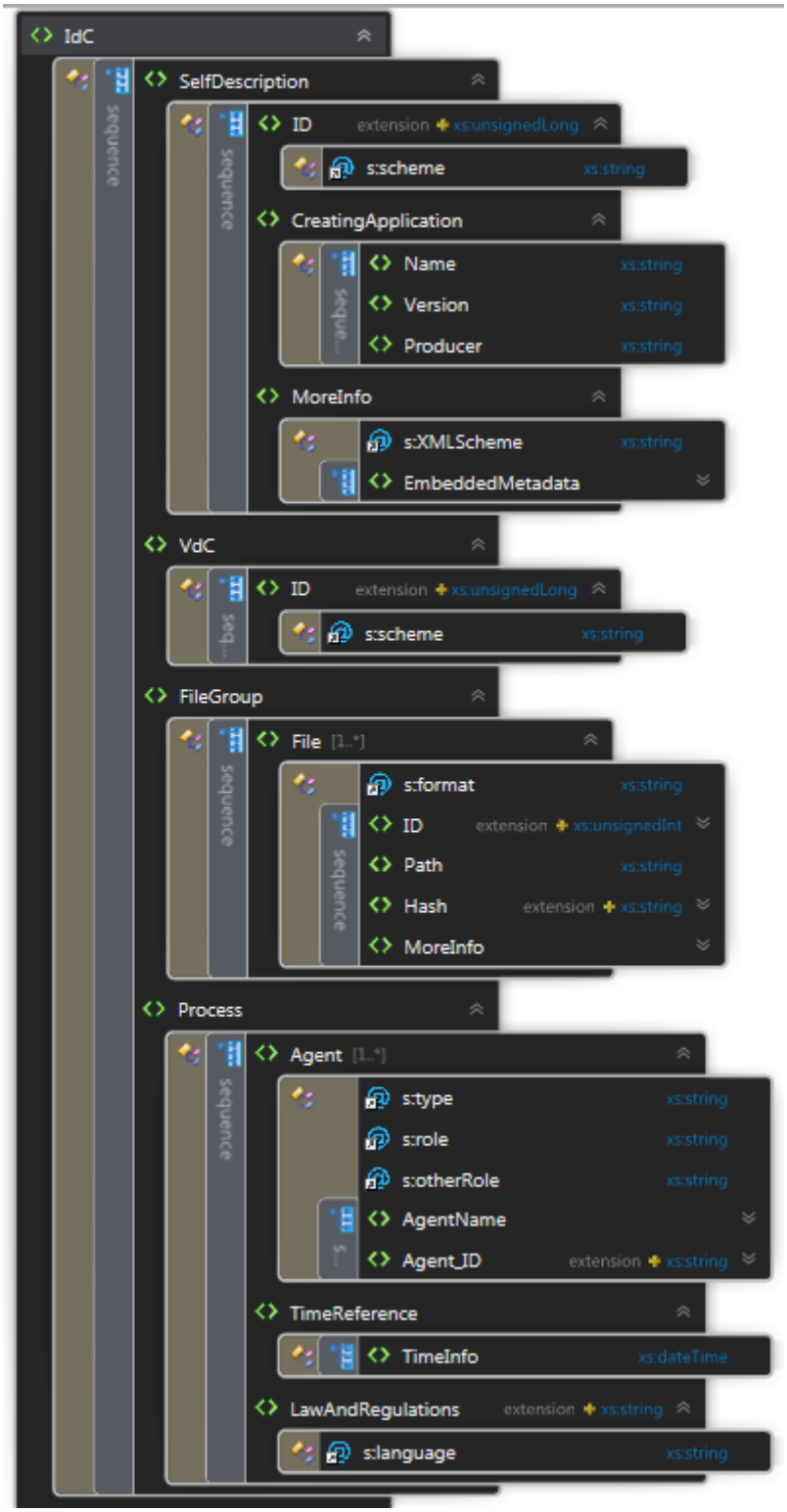

Figura 4. Indice del PDA con campi obbligatori evidenziati

L'indice del pacchetto di archiviazione viene firmato in modalità CAdES e marcato, pertanto all'interno del pacchetto di archiviazione sarà un file con estensione .p7m.

Struttura del Pacchetto di Archiviazione.
Il pacchetto di archiviazione (PDA), prodotto al termine del processo di conservazione, è composto da un insieme di file e directory, organizzati come evidenziato dalla figura seguente:

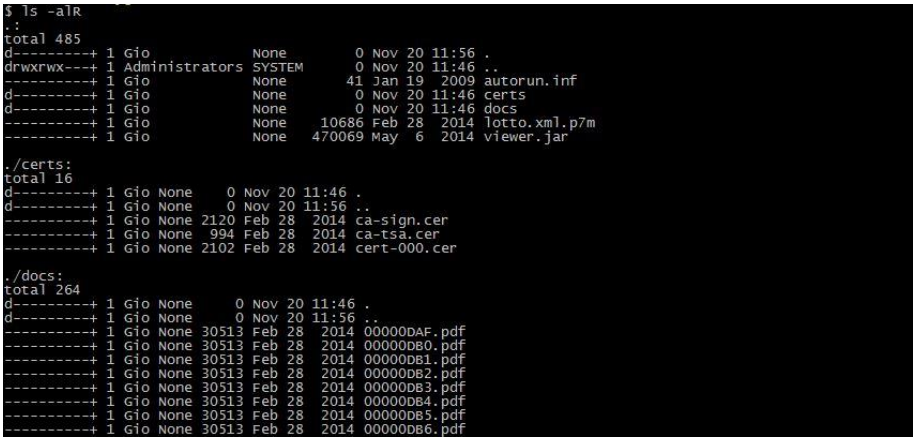

Figura 5. Lista dei file e delle directory di un PDA

Gli elementi che compongono un PDA sono:

- ✓ file.xml.p7m: indice del pacchetto di archiviazione firmato in modalità CAdES e marcato;
- ✓ docs: directory contenente tutti i documenti facenti parte del PDA;
- ✓ viewer.jar: applicazione java che consente la verifica della firma apposta sull'IPdA e la visualizzazione del PDA stesso. L'applicazione consente di visualizzare i documenti contenuti nel PDA con i relativi metadati e consente di fare ricerche interne al PDA;
- ✓ certs: directory contenente i certificati necessari per la verifica della firma apposta sull'indice del pacchetto di archiviazione;
- ✓ autorun.inf: file contenente le istruzioni per avviare automaticamente l'applicazione viewer.jar.

Tutti gli elementi appena descritti vengono inseriti in un unico file .ISO che costituisce il pacchetto di archiviazione.
Il formato .ISO fa sì che il PDA possa comodamente essere masterizzato su DVD.

Figura 6. Visualizzatore di PDA

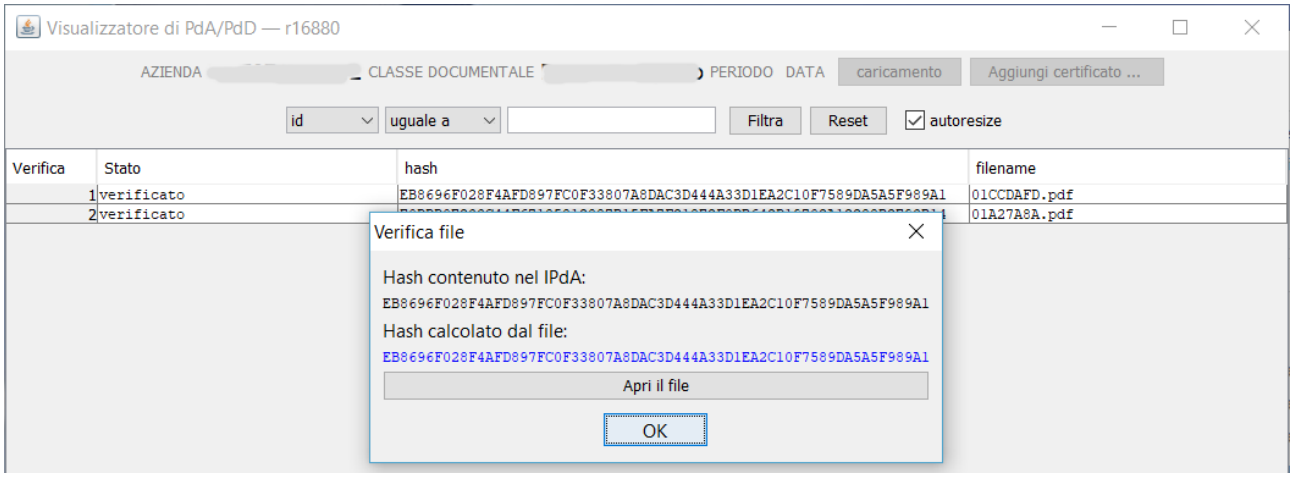

Figura 7. Verifica hash documento

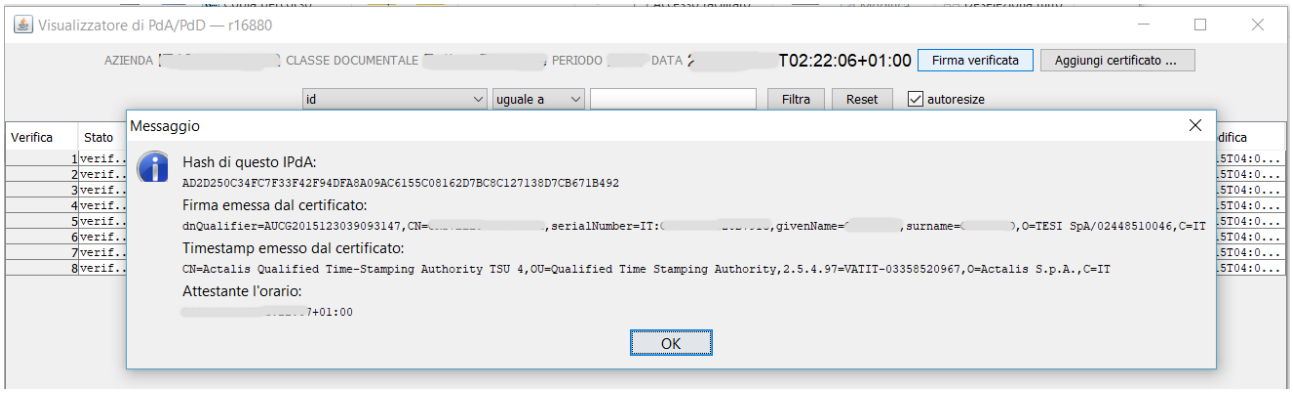

Figura 8. Controllo della firma

Verifica integrità PdA**.**
Relativamente a questo punto si rimanda al cap. 9.2 del presente documento.

[Torna al Sommario]

6.4 PACCHETTO DI DISTRIBUZIONE

Un Pacchetto di Distribuzione (PdD) è un archivio distribuito a seguito di ricerca di uno o più documenti, in risposta alla richiesta dell'Utente. Viene generato dal Sistema a partire dai PdA ed è finalizzato a rispondere agli obblighi di esibizione. Il PdD può essere anche generato al momento della richiesta da parte di un utente e non conservato nel Sistema di Conservazione.

Il Sistema di Conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, ai documenti informatici conservati. Per esibizione si intende dunque l'operazione che consente a tali soggetti la visualizzazione di uno o più documenti conservati e la loro esportazione dal Sistema di Conservazione attraverso la produzione di un pacchetto di distribuzione selettiva.

Struttura del Pacchetto di Distribuzione – PDD.
Il pacchetto di distribuzione (PDD), è un file in formato ZIP che comprende i seguenti elementi:

- ✓ L'insieme dei documenti ricercati attraverso l'interfaccia di esibizione suddivisi per Azienda, classe documentale e per PDA di appartenenza;
- ✓ viewer.jar: applicazione java che consente la visualizzazione di tutti i documenti contenuti nel pacchetto di distribuzione e dei relativi metadati.
- ✓ certs: directory contenente i certificati necessari per la verifica delle firme apposte sugli indici del pacchetto di archiviazione;
- ✓ schemas: directory contenente gli schemi XSD che descrivono la struttura degli indici dei pacchetti di archiviazione;
- ✓ autorun.inf: file contenente le istruzioni per avviare automaticamente l'applicazione viewer.jar;
- ✓ index.txt.p7m: file indice del PDD firmato dal Responsabile del servizio di Conservazione secondo il formato CAdES.

Il file contiene l'elenco dei documenti e dei relativi hash.
Questo, unitamente alla firma consente di garantire l'autenticità e l'integrità dei documenti.

Torna al Sommario

7. IL PROCESSO DI CONSERVAZIONE

7.1 IL PROCESSO DI CONSERVAZIONE DIGITALE

Il processo di conservazione è l'insieme delle attività finalizzate alla conservazione dei documenti informatici, secondo i seguenti step:

- ✓ l'acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa incarico;
- ✓ la verifica che il pacchetto di versamento e gli oggetti contenuti siano coerenti con le modalità previste dal manuale di conservazione;
- ✓ l'eventuale rifiuto del pacchetto di versamento, nel caso in cui i controlli di cui sopra abbiano evidenziato delle anomalie;
- ✓ la generazione in modo automatico del rapporto di versamento relativo ad un pacchetto di versamento, univocamente identificato dal sistema di conservazione, secondo le modalità descritte nel presente manuale di conservazione;
- ✓ la preparazione, la sottoscrizione con firma digitale del responsabile della conservazione o di un suo delegato e la gestione del pacchetto di archiviazione sulla base delle specifiche della struttura dati contenute nell'allegato 4 del DPCM del 3 dicembre 2013 e secondo le modalità riportate nel presente manuale della conservazione;
- ✓ la preparazione e la sottoscrizione con firma digitale e con l'apposizione della marca temporale sull'Indice del pacchetto di distribuzione ai fini di ottemperare alla richiesta di esibizione dell'utente.

Il Sistema di Conservazione di Tesisquare® si basa su un processo di acquisizione dei Pacchetti di Versamento, preventivamente acquisiti dal motore di gestione Tesi e-Integration.

Di seguito il dettaglio del processo:

TESI SpA Registered office: Via Mendicità Istruita, 24 – 12042 Bra (CN) - Headquarters: Via Savigliano, 48 - 12062 Roreto di Cherasco (CN)
Phone +39 0172 476301 - Fax +39 0172 476399 - www.tesisquare.com - info@tesisquare.com
Tax Code and VAT no. 02448510046 – Cuneo Chamber of Commerce - Economic and Administrative Register no. 177331
Share Capital € 750,000 fully vested

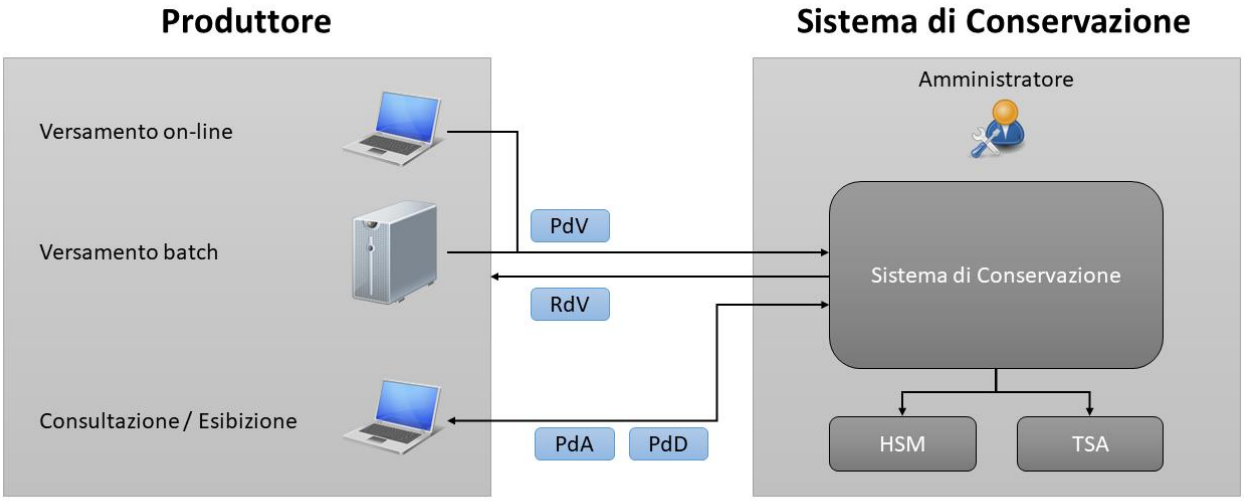

Figura 9. Schema generale

Il processo di conservazione è articolato in tre sotto fasi:

- ✓ Versamento
- ✓ Conservazione
- ✓ Distribuzione

Tutti i processi afferenti al versamento, all'accettazione, alla validazione degli oggetti digitali contenuti nel pacchetto informativo sono tracciati nei log.

Durante la fase progettuale, Tesisquare® nominerà una figura di riferimento che si interfaccerà con il referente nominato dal cliente. Una volta avviato il progetto gli utenti potranno fare riferimento al servizio di help desk. Sarà in ogni caso disponibile un contatto Tesisquare® per gestire problematiche di particolare rilevanza ed eventuali criticità.

Torna al Sommario

7.2 DESCRIZIONE DELLA SOLUZIONE DI CONSERVAZIONE DIGITALE

Dal punto di vista architetturale, la Soluzione di Conservazione Digitale è un'applicazione enterprise distribuita.

Possiamo distinguere i seguenti elementi:

- ✓ Application Server: ospita la business logic del Sistema;
- ✓ DBMS: database server per la gestione dei dati applicativi;
- ✓ File server o Network Attached Storage: ospita i file che costituiscono i documenti da archiviare;
- ✓ Supporti ottici probatori: supporti ottici su cui vengono salvati i pacchetti di archiviazione secondo le regole definite;
- ✓ Applicazione 1 … Applicazione n: le applicazioni del cliente che utilizzano la Soluzione di Conservazione Ottica Digitale, interfacciandosi alla stessa tramite i Web Service (protocollo SOAP) esposti.

L'applicativo è provvisto di una console web che consente agli utenti abilitati, a seconda del profilo, di eseguire operazioni di:

- ✓ amministrazione e configurazione del Sistema;
- ✓ gestione delle operazioni di Conservazione Digitale;
- ✓ ricerca, consultazione e estrazione di documenti, pacchetti di archiviazione ecc.

La soluzione proposta si basa sulla piattaforma Tesi e-Integration composta da un'infrastruttura di mappatura, smistamento, veicolazione e consultazione tracking dei documenti, ospitata presso la Server Farm Tim di Rozzano, e sull'applicativo di gestione della conservazione a norma con relativa consultazione.

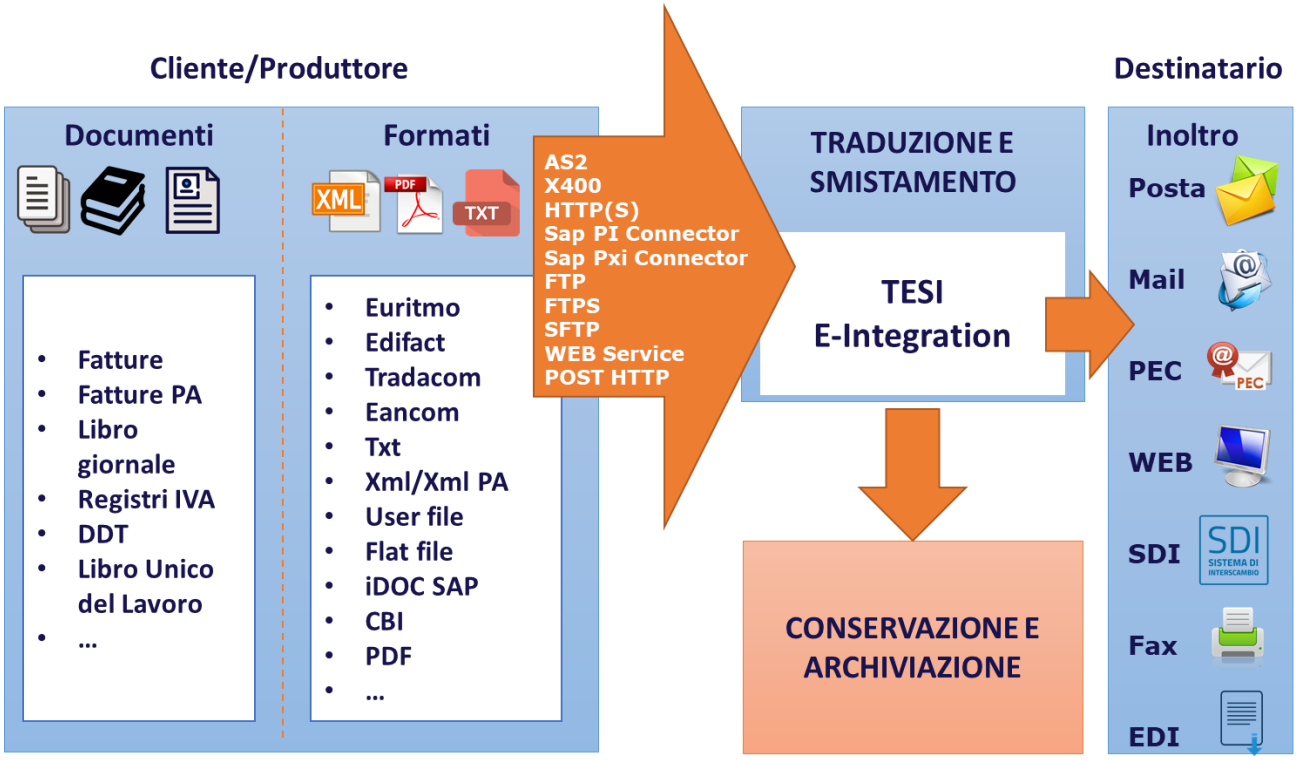

Figura 10. Multicanalità

Relativamente alla gestione e veicolazione dei documenti, lo schema seguente rappresenta le varie possibilità messe a disposizione da Tesisquare®. Ovviamente è possibile definire altri processi e personalizzazioni.

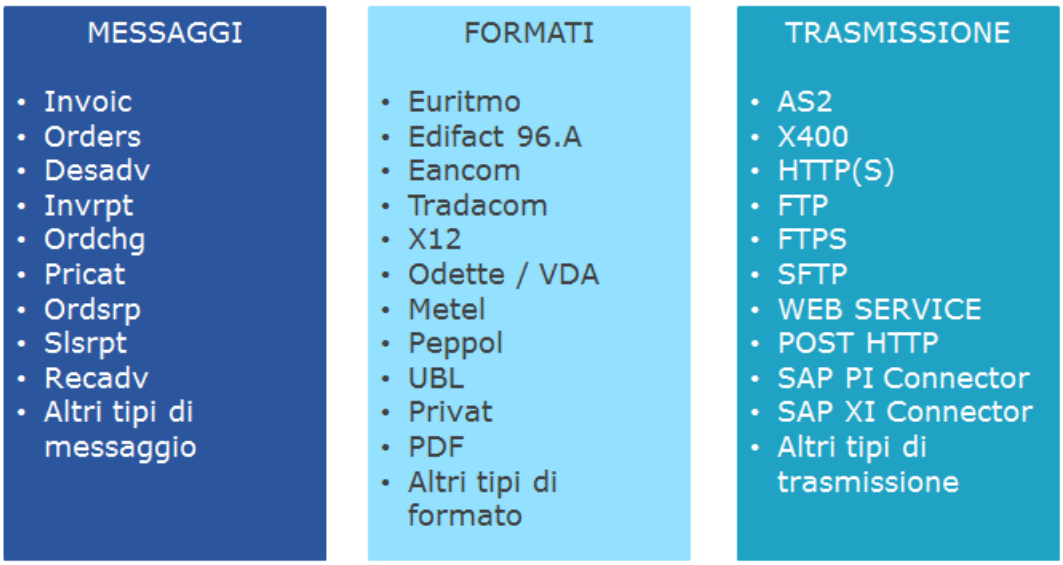

Figura 11. Multicanalità

Gli step progettuali per quanto riguarda la parte di Conservazione Digitale sono i seguenti:

- ✓ Acquisizione dei documenti in formato elettronico;
- ✓ Caricamento sul portale di conservazione;
- ✓ Creazione dei pacchetti di archiviazione da portare in Conservazione;
- ✓ Apposizione della firma sui pacchetti di archiviazione;
- ✓ Apposizione della Marca Temporale;
- ✓ Conservazione Digitale su supporto di memorizzazione;
- ✓ Indicizzazione personalizzabile dei documenti ed estrazione dei campi di ricerca aggiuntivi;
- ✓ Automatismi per le operazioni periodiche.

La soluzione proposta è indipendente dal programma gestionale con cui sono prodotti i documenti che vengono acquisiti automaticamente.

Durante la fase di start-up si prevedono le seguenti attività:

- ✓ Attivazione del Cliente su piattaforma Tesisquare® centralizzata (piattaforma di acquisizione Tesi e-Integration);
- ✓ Attivazione del Cliente su piattaforma di Conservazione Digitale;
- ✓ Impostazione dei tipi documenti previsti con relativi indici;
- ✓ Profilatura di utenti web e relative autorizzazioni per tipo documento;
- ✓ Test e certificazione ambiente di smistamento flussi per tipo documento;
- ✓ Test e certificazione ambiente di Conservazione Digitale per tipo documento;
- ✓ Test e certificazione servizio di Fatturazione Elettronica se previsto nell'ambito del progetto;
- ✓ Avviamento in produzione.

L'invio dei flussi verso la piattaforma messa a disposizione potrà essere effettuato in diverse modalità come dettagliato nel capitolo successivo.

Ogni processo sarà completamente tracciato e sarà data la possibilità al Cliente di consultare i log generati via web. Il Servizio di Conservazione a Norma è fornito sulla piattaforma centralizzata nell'area riservata al Cliente, ed assicura:

- ✓ La completa separazione logica dei documenti ad esso riferiti;
- ✓ L'accesso esclusivo in consultazione ai dati di propria pertinenza.

Il corretto funzionamento del Servizio è garantito solo con dispositivi di firma forniti da Tesisquare®.

Torna al Sommario

7.3 MODALITÀ DI ACQUISIZIONE DEI PACCHETTI DI VERSAMENTO PER LA LORO PRESA IN CARICO

Il Sistema prevede che i PdV o i "singoli versamenti" (secondo la definizione data degli stessi al cap. 6.2) vengano trasmessi da parte dell'Ente Produttore verso l'Ente Conservatore secondo modalità definibili in base ai singoli contratti. Le più comuni sono:

- ✓ Web Services: rendono più facile lo sfruttamento di uno dei beni principali di ogni azienda, l'informazione, permettendo di rendere possibile l'interoperabilità via Internet dei Sistemi Informativi;
- ✓ AS2: permette lo scambio di documenti in sicurezza su Internet, usando: Crittografia, Conferma di ricezione, Certificato digitale per identificare il mittente (non ripudio);
- ✓ HTTPS: con l'HTTPS si interpone un livello di crittografia/autenticazione, creando un canale di comunicazione criptato tra il client e il server attraverso lo scambio di certificati;
- ✓ X400: protocollo che permette lo scambio di documenti basato su TCP/IP (spesso over VPN), attestando la connessione su reti internazionali;
- ✓ Integrazione ERP SAP ECC (attraverso SAP PI e SAP XI) e con altri ERP come JDE, Navision, etc;
- ✓ Connettori verso i middleware TIBCO ESB, JBOSS, BIZ TALK.

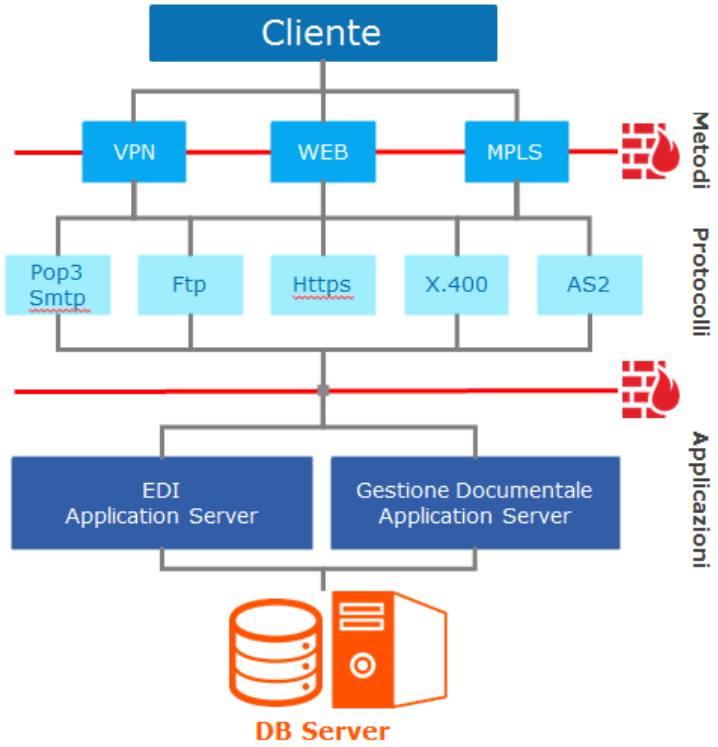

Figura 12. Connessioni

Il caricamento dei dati da parte del produttore può avvenire con diverse modalità:

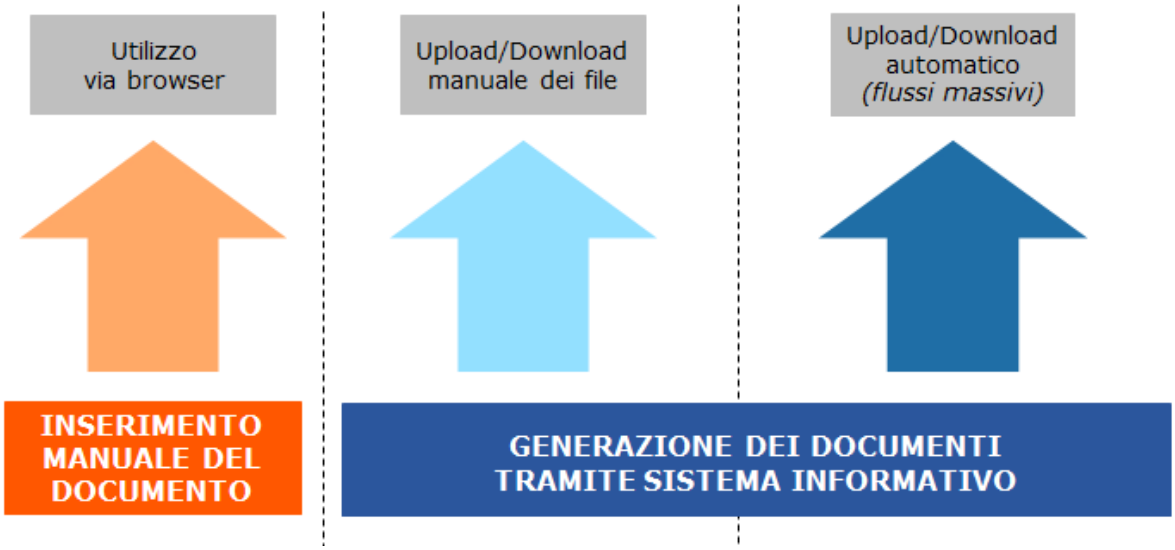

Figura 13. Multicanalità

Tutte le modalità di versamento garantiscono la sicurezza e riservatezza dei dati trasmessi grazie alla crittografia del canale adottato (HTTPS e sFTP).

I Sistemi di Tesisquare® per la presa in carico dei pacchetti di versamento sono tutti in alta disponibilità garantendo la ridondanza dei dati.

Inoltre, nel servizio sono attive procedure per la generazione di backup dei PdV versati dal Produttore. Lo storage che mantiene le copie di backup ha una retention di due mesi.
Le specifiche sulla sessione di versamento e presa in carico del PdV, il modello-dati del PdV sono dettagliate nella "Scheda Servizio Cliente - Specificità del Contratto."

Tutti i PdV ricevuti alimentano un Log specifico per ciascun canale di ricezione, mantenuto su ciascun server dedicato, con una retention pari ad 1 mese.

Torna al Sommario

7.4 VERIFICHE EFFETTUATE SUI PACCHETTI DI VERSAMENTO E SUGLI OGGETTI IN ESSI CONTENUTI

Il Sistema di Conservazione riceve i PdV o i "singoli versamenti" (secondo la definizione data degli stessi al cap. 6.2) dal Sistema Tesi e-Integration, che, se opportuno, verifica preventivamente la presenza dei dati necessari e il formato definito in sede di configurazione a seguito di quanto concordato in sede contrattuale.
Eventuali anomalie sono segnalate al Cliente tramite l'invio automatico di una mail che riporta la motivazione dell'eventuale scarto.

Di seguito l'elenco dei controlli effettuati sul flusso in ingresso al Sistema di Conservazione:

- ✓ Identificazione certa del Produttore, tramite la preventiva creazione di un canale sicuro, sopra descritto; ogni Produttore ha una relazione sul Sistema di veicolazione dei flussi configurato ad hoc, in modo da identificare univocamente il proprietario dei flussi;
- ✓ Tutti i files ricevuti vengono backuppati su di una cartella di Sistema, in modo da assicurare la verifica dei pacchetti stessi preventivamente al momento di versamento, al fine di dimostrare l'integrità degli stessi anche dopo che essi siano stati portati nel Sistema;
- ✓ In caso di "singolo versamento", effettuato sul sistema E-integration, viene effettuata la verifica preventiva alla creazione del Pacchetto di Versamento secondo lo schema del file che il Sistema si aspetta per il determinato flusso, esemplificando:
    - Se il file è un XML: verifica che il file risulti conforme allo schema XSD previsto (es se XML deve andare verso la PA, il file XML dovrà essere rispondente allo schema XSD realizzato da SOGEI);
    - Se il file è in un formato predefinito con il Produttore, deve rispondere alle caratteristiche di base inserite nel documento di Analisi Tecnica e condivise in sede di progetto;
    - Se il file deve essere un qualsiasi formato, comprensivo dell'indice contenente i metadati necessari per il versamento e/o postalizzazione, viene verificato che i dati siano presenti:
        - Nel caso di dati minimi necessari alla conservazione (come da normativa);
        - Nel caso di dati minimi concordati con il cliente per il determinato processo;
    - Per tipologie di documenti che richiedano la verifica della continuità della numerazione, viene attivato un controllo di sequenza che allerta automaticamente il Produttore del pacchetto di versamento in caso di mancanza di documenti;
- ✓ Ogni flusso in ingresso al Sistema viene tracciato tramite la creazione di Log che vengono salvati sul web-server e backuppati con frequenza notturna;

- ✓ La fase di caricamento dei PdV o dei "singoli versamenti" prevede una validazione del metadato. Questa validazione verifica che il numero dei metadati ed i loro valori siano coerenti con la definizione della classe documentale sulla quale dovranno essere caricati.
- ✓ Se la validazione non va a buon fine:
    - Nella gestione del PdV standard il sistema di conservazione rifiuta l'intero pacchetto, l'errore sarà segnalato con una mail automatica al supporto e successivamente al Produttore per informarlo del rifiuto e per consentirgli di gestire la risoluzione dell'anomalia che lo ha generato;
    - In caso di "singolo versamento" la porzione non corretta dello stesso viene esclusa dal caricamento e salvata su un file con estensione .err. Gli errori vengono registrati sui file di log applicativi, all'interno dei quali è presente il motivo dell'errore, e trasmessi via mail all'ente Produttore.
- ✓ Se la validazione va a buon fine viene generato un file con estensione .ok

[Torna al Sommario](#)

7.5 ACCETTAZIONE DEI PACCHETTI DI VERSAMENTO E GENERAZIONE DEL RAPPORTO DI VERSAMENTO DI PRESA IN CARICO

La generazione del Rapporto di Versamento può avvenire in due modi distinti a seconda che ci si trovi nella casistica in cui il Produttore invia direttamente il PdV (Modalità 1 definita nel cap. 6.2) o quando si tratti di "singolo versamento" (Modalità 2 definita nel cap. 6.2).

Modalità 1 – PdV inviato dal Produttore

A seguito della ricezione di un pacchetto di versamento inviato dal Produttore e validato dalle verifiche di cui sopra, il Sistema di Conservazione produce un Rapporto di Versamento che viene restituito al Produttore stesso e che viene salvato in una classe documentale predefinita.

Modalità 2 – "singolo versamento"

Il sistema di conservazione, a seguito del caricamento del "singolo versamento" e secondo la configurazione delle specifiche classi documentali impostata sul sistema, elabora tutti i documenti in stato "pronto per la Conservazione" generando il corrispettivo rapporto di Versamento che viene restituito al Produttore stesso e che viene salvato in una classe documentale predefinita.

Il Pacchetto di Versamento viene inviato dal Produttore verso la piattaforma Tesi e-Integration tramite uno dei canali di comunicazione previsti (rif. cap. 7.3), la cui abilitazione si basa sulla configurazione di una "relazione" di tipo tecnico che determina in modo certo l'identificazione del path di acquisizione del pacchetto ed il relativo path di destinazione del Sistema di Conservazione. Lo spostamento del pacchetto dal primo al secondo path viene effettuato da procedure automatiche che si basano sulla definizione delle "relazioni" stesse, rendendo in questo modo certa la correttezza della trasmissione.
In caso di errori sono previste procedure di monitoraggio automatiche (rif. cap. 9) che intercettano l'anomalia segnalandola immediatamente al team di Supporto.
In aggiunta a quanto sopra, a garanzia di ulteriore sicurezza nel controllo dei flussi acquisiti, è previsto un controllo di coerenza tra il path di destinazione atteso del Pacchetto di Versamento e la cartella in cui tale file viene effettivamente posizionato: qualora il controllo rilevi un'incongruenza tra queste due informazioni, il sistema restituirà una segnalazione automatica che sarà gestita dal team di Supporto.

Per entrambe le modalità sopra descritte la Classe documentale *RdV – Rapporti di Versamento* presenta i seguenti metadati:

- ✓ N. documenti: numero di documenti presenti nel pacchetto di versamento;
- ✓ Data creazione: data di creazione del rapporto di versamento;
- ✓ ID: identificativo univoco del pacchetto di versamento;
- ✓ Nome file: nome del file XML rappresentante il pacchetto di versamento;
- ✓ Azienda: azienda proprietaria del PDA;
- ✓ Classe documentale: classe documentale dei documenti contenuti nel PDA;
- ✓ Utente: utente che ha effettuato il versamento;
- ✓ Esito versamento: esito del versamento;
- ✓ Note: il metadato è opzionale e contiene eventuali note relative al processo di versamento.

L'azione di versamento di un Pacchetto di Versamento all'interno del Sistema di Conservazione produce:

- ✓ La generazione automatica del rapporto di versamento relativo al PdV, univocamente identificato dal Sistema di Conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo universale coordinato (UTC), e una o più impronte, calcolate sull'intero contenuto del PdV;
- ✓ La sottoscrizione del rapporto di versamento con la firma digitale o firma elettronica qualificata apposta dal Responsabile del servizio di Conservazione.
- ✓ La fase di caricamento dei PdV prevede una validazione del metadato. Questa validazione verifica che il numero dei metadati ed i loro valori siano coerenti con la definizione della classe documentale sulla quale dovranno essere caricati.
- ✓ Il corretto caricamento del PdV viene segnato sul file di log applicativo legato alla classe documentale di appartenenza.

Torna al Sommario

7.5.1 STRUTTURA DEL RAPPORTO DI VERSAMENTO - RDV

Il rapporto di versamento è un file XML firmato secondo lo standard CAdES dal Responsabile del servizio di Conservazione.
Il suo contenuto è definito dal seguente schema XSD:

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns="http://andxor.it/tDoc/report.xsd"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    targetNamespace="http://andxor.it/tDoc/report.xsd"
    elementFormDefault="qualified">
  <xs:import namespace="http://www.w3.org/2000/09/xmldsig#"
schemaLocation="http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/xmldsig-core-
schema.xsd"/>
  <xs:attribute name="function" type="xs:NMTOKEN" default="SHA-1" />
  <xs:simpleType name="TimeInfo">
    <xs:restriction base="xs:dateTime" />
  </xs:simpleType>
  <xs:complexType name="TimeReference">
    <xs:sequence>
      <xs:element name="TimeInfo" type="TimeInfo" />
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="Identifier">
    <xs:simpleContent>
```


TESI SpA Registered office: Via Mendicità Istruita, 24 – 12042 Bra (CN) - Headquarters: Via Savigliano, 48 - 12062 Roreto di Cherasco (CN)
Phone +39 0172 476301 - Fax +39 0172 476399 - www.tesisquare.com - info@tesisquare.com
Tax Code and VAT no. 02448510046 – Cuneo Chamber of Commerce - Economic and Administrative Register no. 177331
Share Capital € 750,000 fully vested

```
    <xs:extension base="xs:NMTOKEN">
      <xs:attribute name="scheme" type="xs:string" default="local" />
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
<xs:complexType name="CreatingApplication">
  <xs:sequence>
    <xs:element name="Name" type="xs:string" />
    <xs:element name="Version" type="xs:string" />
    <xs:element name="Producer" type="xs:string" />
  </xs:sequence>
</xs:complexType>
<xs:complexType name="File">
  <xs:sequence>
    <xs:element name="ID" type="xs:string" />
    <xs:element name="Path" type="xs:string" minOccurs="0" />
    <xs:element name="Hash" type="Hash" />
    <xs:element name="metadata" type="metadata" />
  </xs:sequence>
  <xs:attribute name="format" type="xs:string" use="required"/>
</xs:complexType>
<xs:complexType name="Hash">
  <xs:simpleContent>
    <xs:extension base="xs:string">
      <xs:attribute name="function" type="xs:NMTOKEN" default="SHA-1" />
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
<xs:complexType name="metadata">
  <xs:sequence>
    <xs:element name="meta" maxOccurs="unbounded">
      <xs:complexType>
        <xs:attribute name="class" type="xs:string" use="optional" />
        <xs:attribute name="name"  type="xs:string" use="required" />
        <xs:attribute name="value" type="xs:string" use="required" />
      </xs:complexType>
    </xs:element>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="SelfDescription">
  <xs:sequence>
    <xs:element name="CreatingApplication" type="CreatingApplication" />
    <xs:element name="ID" type="Identifier" />
    <xs:element name="IPdV" type="xs:string" />
    <xs:element name="company" type="xs:string" />
    <xs:element name="doctype" type="xs:string" />
    <xs:element name="TimeReference" type="TimeReference" />
    <xs:element name="Result" type="xs:string" />
  </xs:sequence>
</xs:complexType>
<xs:complexType name="FileGroup">
  <xs:sequence>
    <xs:element name="File" type="File" maxOccurs="unbounded" />
    <xs:element name="Extra" type="xs:string" minOccurs="0" />
```

```
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="RdV">
    <xs:sequence>
      <xs:element name="SelfDescription" type="SelfDescription" />
      <xs:element name="FileGroup" type="FileGroup" maxOccurs="unbounded" />
      <xs:element ref="ds:Signature"/>
    </xs:sequence>
  </xs:complexType>
  <xs:element name="RdV" type="RdV" />
</xs:schema>
```

Torna al Sommario

7.6 RIFIUTO DEI PACCHETTI DI VERSAMENTO E MODALITA' DI COMUNICAZIONE DELLE ANOMALIE

Il presente punto si collega a quanto già evidenziato al cap. 7.4 *"VERIFICHE EFFETTUATE SUI PACCHETTI DI VERSAMENTO E SUGLI OGGETTI IN ESSI CONTENUTI"*, ovvero le modalità di segnalazione del rifiuto dei Pacchetti di Versamento o dei "singoli versamenti"; ricordiamo brevemente le motivazioni dovute al rifiuto degli stessi:

- ✓ Problemi relativi al formato (rispetto a procedura di conversione del file o alla classe documentale di riferimento);
- ✓ File corrotto;
- ✓ Mancanza di informazioni (metadati) nell'indice del documento;
- ✓ Pacchetto non rispondente agli accordi commerciali condivisi.

Il Servizio di Tesisquare® mantiene il monitoraggio dei flussi ricevuti dal Produttore tramite i vari canali; il monitoraggio è possibile grazie ad una dashboard che centralizza i flussi del cliente, permettendo un rapido riconoscimento delle problematiche per ogni flusso ricevuto.
Di seguito una schermata del monitor:

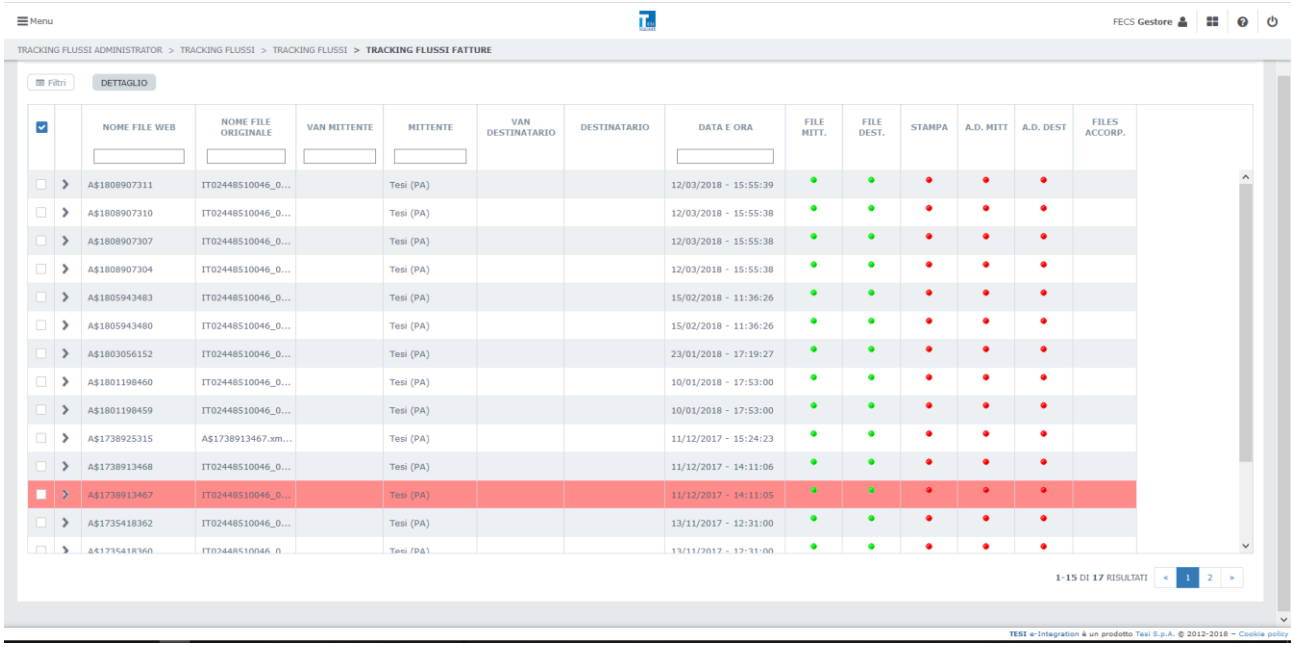

Figura 14. Monitoraggio flussi

La struttura dei campi è la seguente:

- ✓ Nome flusso rinominato dai Sistemi Tesisquare®;
- ✓ Nome del file originale in ingresso;
- ✓ Mittente;
- ✓ Eventuali dati del Van EDI (se utilizzato);
- ✓ Data e ora di ricezione del flusso;
- ✓ Situazione del file da Mittente verso Destinatario;
    - Verifica File Mittente (verde – OK, rosso – KO) se il flusso in ingresso è conforme;
    - Verifica File Destinatario è stato correttamente elaborato;

La struttura a semafori permette la facile comprensione dello stato dei flussi. Il dettaglio della trasmissione si apre cliccando sul semaforo. Di seguito un esempio:

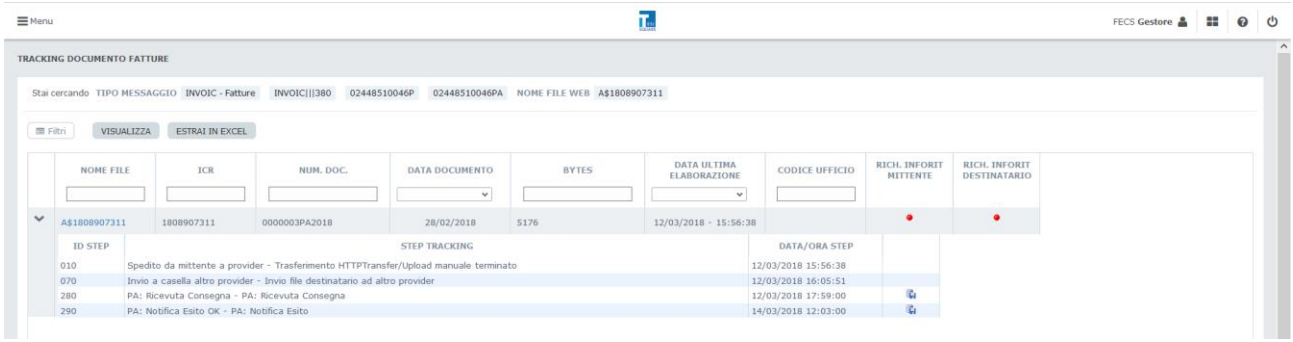

Figura 15. Dettaglio della trasmissione

TESI SpA Registered office: Via Mendicità Istruita, 24 – 12042 Bra (CN) - Headquarters: Via Savigliano, 48 - 12062 Roreto di Cherasco (CN)
Phone +39 0172 476301 - Fax +39 0172 476399 - www.tesisquare.com - info@tesisquare.com
Tax Code and VAT no. 02448510046 – Cuneo Chamber of Commerce - Economic and Administrative Register no. 177331
Share Capital € 750,000 fully vested

In caso di rifiuto del "singolo versamento", oltre ad apparire il semaforo di colore rosso, viene anche inviata una mail direttamente al Produttore del pacchetto contenente le motivazioni della mancata presa in carico, di seguito il dettaglio dei dati contenuti nella comunicazione:

- ✓ La data di comunicazione;
- ✓ Il nome del mittente;
- ✓ Il Destinatario atteso per il messaggio allegato;
- ✓ Il nome del file;
- ✓ La data in cui si è verificato l'incasellamento e la conseguente verifica che ha prodotto la segnalazione di errore;
- ✓ L'allegato che contiene il dettaglio dell'errore rilevato.

Pertanto se la validazione non va a buon fine, la porzione di PdV non corretta viene esclusa dal caricamento e salvata su un file con estensione .err. Gli errori vengono anche segnati sul file di log applicativi, all'interno dei quali è presente il motivo dell'errore.

In caso di rifiuto del Pacchetto di Versamento da parte del sistema di Conservazione sarà tracciato un errore consultabile tramite interfaccia grafica e ne sarà data comunicazione al supporto e al Produttore.

Di seguito un esempio di esito di versamento in errore registrato sul sistema di Conservazione a fronte di un PdV con anomalie:

Figura 16. Dettaglio RdV in errore

[Torna al Sommario]

7.7 PREPARAZIONE E GESTIONE DEL PACCHETTO DI ARCHIVIAZIONE

L'indice del pacchetto di archiviazione (IPdA) è un file XML creato dalla soluzione a chiusura del processo di Conservazione secondo le specifiche dello standard SInCRO, come richiesto dall'Allegato 4 del DPCM 3/12/2013.
Al suo interno si trovano:

- ✓ Informazioni riguardanti l'azienda e il prodotto che generano l'indice;
- ✓ Informazioni riguardanti l'azienda proprietaria dei documenti, per la quale viene prodotto l'indice;
- ✓ Informazioni riguardanti la classe documentale e il periodo di riferimento dei documenti conservati;
- ✓ Informazioni specifiche di ogni documento. In questa sezione trovano posto l'ID univoco del documento, il nome del file, la sua impronta e tutti i metadati ad esso correlati;
- ✓ Informazioni riguardanti tutti i soggetti (fisici e giuridici) interessati dal processo di Conservazione. In tale sezione trovano posto almeno il soggetto che appone la firma all'IPdA e l'azienda che offre il servizio di Conservazione.

L'indice del pacchetto di archiviazione (IPdA) viene firmato in modalità CAdES e marcato, pertanto all'interno del pacchetto di archiviazione sarà un file con estensione .p7m.

[Torna al Sommario]

TESI SpA Registered office: Via Mendicità Istruita, 24 – 12042 Bra (CN) - Headquarters: Via Savigliano, 48 - 12062 Roreto di Cherasco (CN)
Phone +39 0172 476301 - Fax +39 0172 476399 - www.tesisquare.com - info@tesisquare.com
Tax Code and VAT no. 02448510046 – Cuneo Chamber of Commerce - Economic and Administrative Register no. 177331
Share Capital € 750,000 fully vested

7.7.1 STRUTTURA DEL PACCHETTO DI ARCHIVIAZIONE - PDA

Il pacchetto di archiviazione (PDA), prodotto al termine del processo di Conservazione, è composto da un insieme di file e directory, organizzati come evidenziato dalla figura seguente:

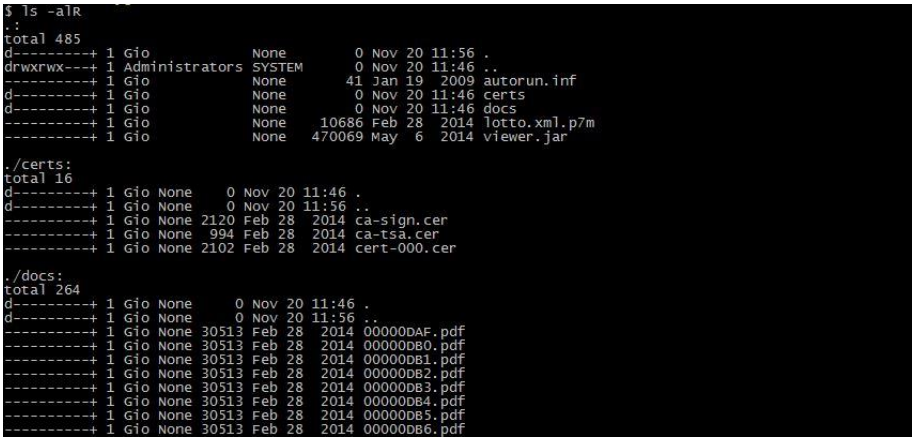

Figura 17. Lista dei file e delle directory di un PDA

Gli elementi che compongono un PDA sono:

- ✓ file.xml.p7m: indice del pacchetto di archiviazione firmato in modalità CAdES e marcato;
- ✓ Docs: directory contenente tutti i documenti facenti parte del PDA;
- ✓ Viewer.jar: applicazione java che consente la verifica della firma apposta sull'IPdA e la visualizzazione del PDA stesso. L'applicazione consente di visualizzare l'elenco dei documenti contenuti nel PDA con i relativi metadati e consente di fare ricerche interne al PDA. La visualizzazione del PDA avviene tramite il software installato sul terminale dell'utente, in caso di impossibilità di lettura sarà fornito via mail al Produttore il viewer necessario;
- ✓ Certs: directory contenente i certificati necessari per la verifica della firma apposta sull'indice del pacchetto di archiviazione;
- ✓ Autorun.inf: file contenente le istruzioni per avviare automaticamente l'applicazione viewer.jar.

Tutti gli elementi appena descritti vengono inseriti in un unico file .ISO che costituisce il pacchetto di archiviazione. Il formato .ISO fa sì che il PDA possa comodamente essere masterizzato su DVD.

Sul portale è possibile ricercare i PdA tramite apposita funzione:

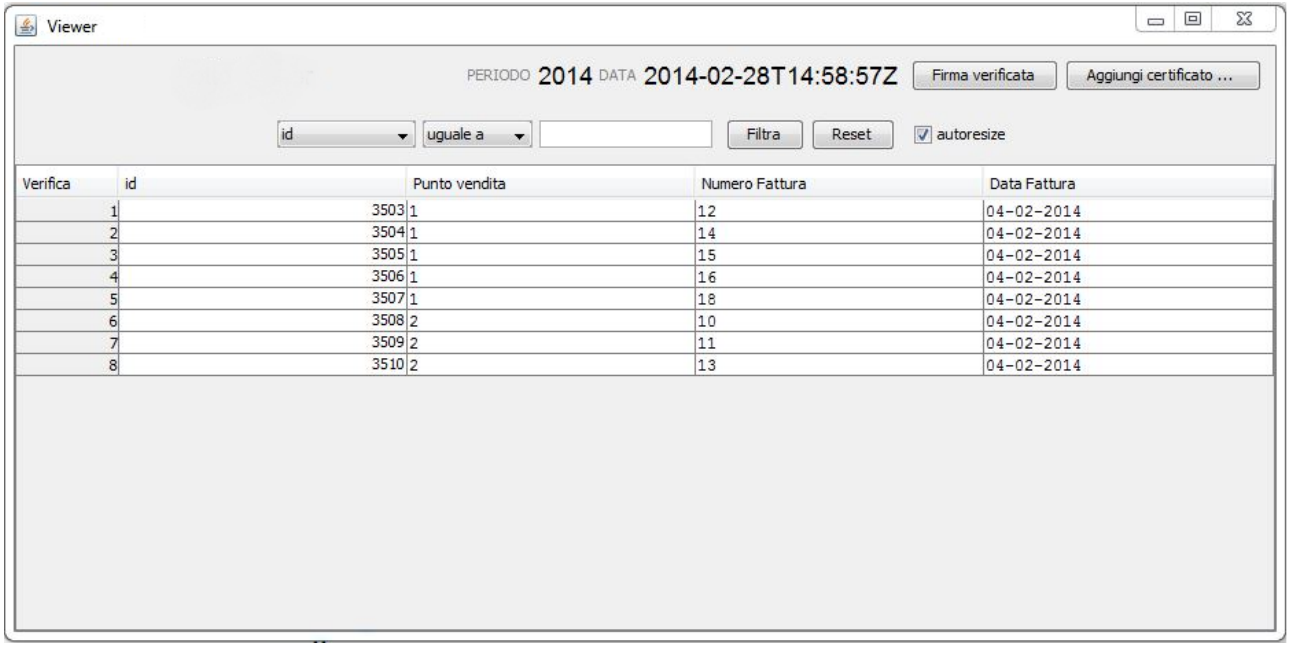

Figura 18. Visualizzatore di PDA

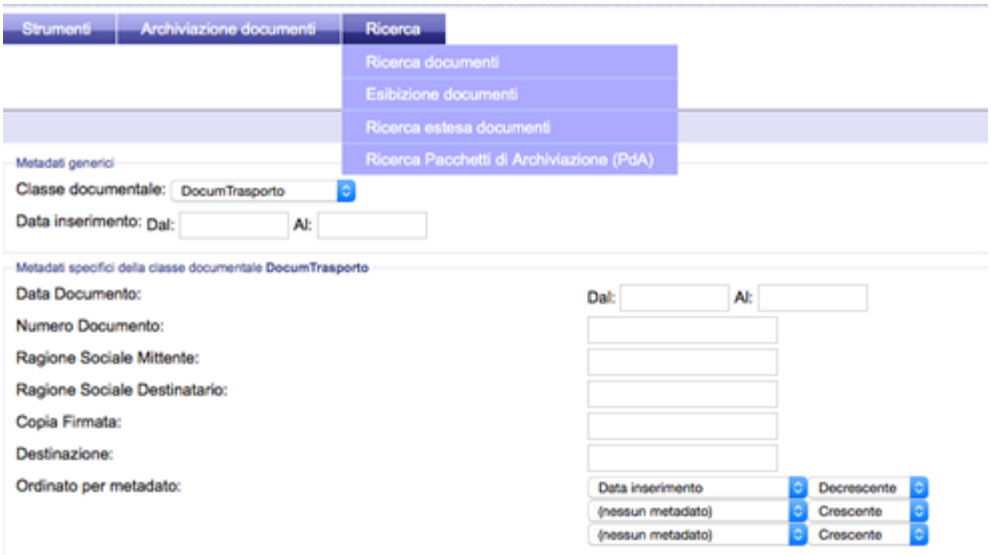

Figura 19. Ricerca dei PDA

La procedura di ripristino in caso di corruzione o perdita dei dati dei PdA prevede la gestione dell'incident con livello di priorità massima ed il ripristino attraverso l'utilizzo del PdA copia di backup da parte del team preposto, secondo quanto definito all'interno della procedura di gestione dei backup all'interno del SGSI ISO/IEC 27001:2013.

[Torna al Sommario]

TESI SpA Registered office: Via Mendicità Istruita, 24 – 12042 Bra (CN) - Headquarters: Via Savigliano, 48 - 12062 Roreto di Cherasco (CN)
Phone +39 0172 476301 - Fax +39 0172 476399 - www.tesisquare.com - info@tesisquare.com
Tax Code and VAT no. 02448510046 – Cuneo Chamber of Commerce - Economic and Administrative Register no. 177331
Share Capital € 750,000 fully vested

7.8 PREPARAZIONE E GESTIONE DEL PACCHETTO DI DISTRIBUZIONE AI FINI DELL'ESIBIZIONE

Il Sistema di Conservazione deve permettere ai soggetti autorizzati l'accesso diretto, anche da remoto, ai documenti informatici conservati.
Per esibizione si intende dunque l'operazione che consente a tali soggetti la visualizzazione di uno o più documenti conservati e la loro esportazione dal Sistema di Conservazione attraverso la produzione di un pacchetto di distribuzione selettiva.
Gli utenti del Sistema di Conservazione di Tesisquare®, opportunamente abilitati, possono accedere al menù della soluzione che permette lo scaricamento del Pacchetto di Distribuzione creato:

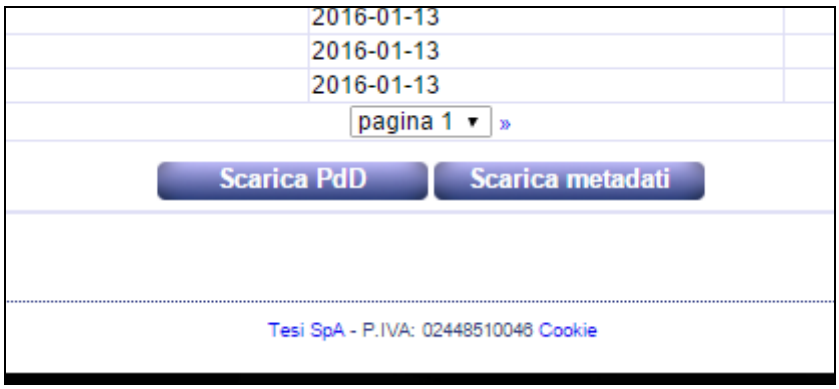

Figura 20. Scaricare i PDD

7.8.1 COMUNITA' DI RIFERIMENTO

La **comunità di riferimento del sistema di conservazione** è il gruppo identificato di potenziali consumer (utenti) in grado di comprendere un determinato insieme di informazioni. Tale comunità di riferimento è ben definita ma è anche facilmente modificabile per meglio adattarsi a possibili variazioni future.
Il sistema di conservazione mette a disposizione strumenti tali da garantire l'**intelligibilità dei PDD** da parte della comunità di riferimento. I PDD vengono costruiti in modo sufficientemente completo da permettere la loro interpretazione e comprensione da parte della comunità di riferimento senza bisogno di ulteriori risorse informative.
La comunità di riferimento del sistema di conservazione è composta dai suoi utenti, distinti in due tipologie:

- ✓ **utenti diretti**, sono le persone fisiche che operano direttamente sul sistema di conservazione in accordo ai vari profili di permessi e visibilità;
- ✓ **utenti indiretti**, sono gli utenti che accedono a informazioni e oggetti conservati, operando su altre applicazioni informatiche interconnesse, in modo certificato (trusted) con il sistema di conservazione.

UTENTI DIRETTI

Gli utenti diretti sono le persone che accedono e operano direttamente nel sistema di conservazione. Ogni utente è necessariamente appartenente ad una struttura organizzativa, censita all'interno del sistema di conservazione.
Ad ogni utente viene associato un ruolo, un profilo di permessi operativi, un profilo di permessi di visibilità.

UTENTI INDIRETTI

Gli utenti indiretti accedono a informazioni e oggetti presenti sul sistema di conservazione, operando su altre applicazioni informatiche interconnesse.
Gli utenti indiretti, operano su altre applicazioni informatiche che sono integrate con funzionalità di query/retrieve degli oggetti conservati (metadati e/o documenti) o delle informazioni relative al processo di conservazione ad essi associate.

Torna al Sommario

7.8.2 STRUTTURA DEL PACCHETTO DI DISTRIBUZIONE – PDD

Il pacchetto di distribuzione (PDD), prodotto al termine del processo di esibizione, è un file in formato ZIP che comprende i seguenti elementi:

- ✓ L'insieme dei documenti ricercati attraverso l'interfaccia di esibizione suddivisi per Azienda, classe documentale e per PDA di appartenenza;
- ✓ Viewer.jar: applicazione java che consente la verifica della firma apposta sugli IPdA contenuti nel pacchetto e la visualizzazione del PDD stesso. L'applicazione consente di visualizzare l'elenco dei documenti contenuti nel PDD con i relativi metadati e consente di fare ricerche interne al PDD. La visualizzazione del PDD avviene tramite il software installato sul terminale dell'utente, in caso di impossibilità di lettura sarà fornito via mail al Produttore il viewer necessario;
- ✓ Certs: directory contenente i certificati necessari per la verifica delle firme apposte sugli indici del pacchetto di archiviazione;
- ✓ Schemas: directory contenente gli schemi XSD che descrivono la struttura degli indici dei pacchetti di archiviazione;
- ✓ Autorun.inf: file contenente le istruzioni per avviare automaticamente l'applicazione viewer.jar;
- ✓ Index.txt.p7m: file indice del PDD firmato dal Responsabile del servizio di Conservazione secondo il formato CAdES.

Il file contiene l'elenco dei documenti e dei relativi hash.
Questo, unitamente alla firma, consente di garantire l'autenticità e l'integrità dei documenti.
La presenza di un file così strutturato all'interno del PDD fornisce le stesse garanzie che fornirebbe una firma CAdES esterna al pacchetto, con il vantaggio di evitare proprio la firma esterna al PDD, che potrebbe essere tecnicamente improponibile vista la potenziale dimensione di un PDD, che potrebbe raggiungere decine o centinaia di GB.

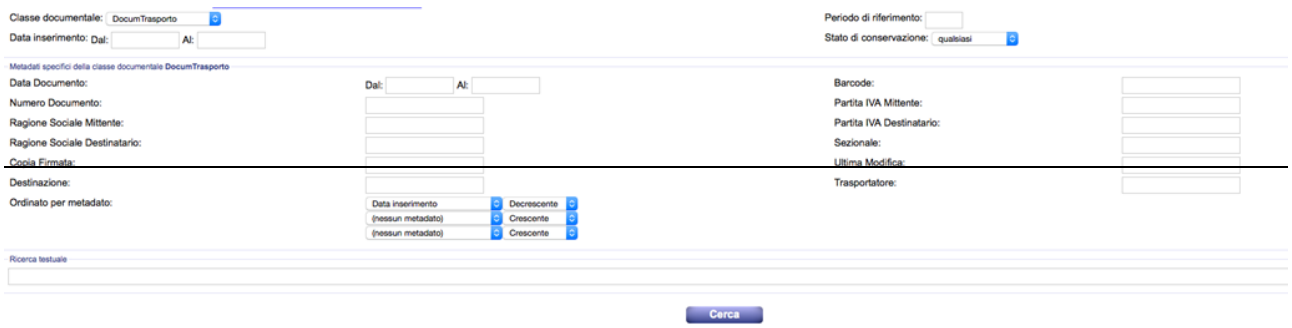

Figura 21. Ricerca dei PDD

I documenti così reperiti possono essere scaricati sotto forma di pacchetto di distribuzione.
Il PDD viene pertanto scaricato direttamente dal Portale Web dalla persona di riferimento abilitata alla classe documentale.
Non sono previsti invii tramite email.

Torna al Sommario

7.8.3 TRACCIA DEGLI ACCESSI

Tutte le esibizioni vengono tracciate nel sistema di conservazione. Il log di queste operazioni è consultabile dagli utenti dotati di specifici permessi.

Torna al Sommario

7.9 PRODUZIONE DI DUPLICATI E COPIE INFORMATICHE E DESCRIZIONE DELL'EVENTUALE INTERVENTO DEL PUBBLICO UFFICIALE NEI CASI PREVISTI

Il Sistema permette agli utenti autorizzati di ottenere una copia (o duplicato, nel caso in cui non siano necessarie conversioni di formato) dei documenti conservati tramite la richiesta di generazione del Pacchetto di Distribuzione, come da paragrafo 7.8.
Nel caso in cui venga richiesto l'utilizzo di supporti fisici rimovibili per la trasmissione dei pacchetti di distribuzione, il personale incaricato del trasporto dei supporti fisici viene scelto sulla base dei requisiti definiti dal Responsabile del servizio di conservazione.
Si precisa che tali supporti fisici non presentano riferimenti esterni tali da permettere l'identificazione dell'ente produttore, dei dati contenuti e della loro tipologia. Inoltre, al tipo di contenitore individuato per i Pacchetti di Distribuzione potrebbero essere impostate delle credenziali crittografiche tali da proteggere i dati in essi contenuti limitatamente alla distribuzione tramite supporti fisici.

Torna al Sommario

7.9.1 NOTE RELATIVE ALLA RICHIESTA DI INTERVENTO DI UN PUBBLICO UFFICIALE

La richiesta di intervento del pubblico ufficiale avviene nelle seguenti casistiche:

Processo di Conservazione.
Per i soli documenti digitali originati da "documenti analogici originali unici" è prevista, oltre all'apposizione del riferimento temporale e della firma digitale da parte del Responsabile del servizio di Conservazione, anche l'apposizione del riferimento temporale e della firma digitale sull'insieme di documenti destinati alla Conservazione da parte di un pubblico ufficiale.
Quest'ultimo adempimento è finalizzato ad attestare la conformità di quanto conservato al documento d'origine.

Processo di riversamento.
In caso di riversamento sostitutivo, i documenti informatici sono stati assimilati a quelli digitali generati da documenti analogici originali unici. Per entrambe le tipologie, considerate le loro peculiari caratteristiche, a differenza di quanto previsto per la generalità dei documenti, è richiesto oltre l'intervento del Responsabile del servizio di Conservazione, anche quello ulteriore del pubblico ufficiale per l'apposizione del riferimento temporale e della firma digitale allo scopo di attestare la conformità all'originale.

Distruzione del documento analogico.
Il documento analogico d'origine, del quale sia obbligatoria la Conservazione, può essere distrutto soltanto al termine del processo di Conservazione. Per questo sarà necessario che sia avvenuta la sua digitalizzazione sul supporto di memorizzazione e che siano stati apposti dal Responsabile del servizio di Conservazione il riferimento temporale e la firma digitale. Per i documenti analogici originali unici dovrà anche essere attestata la conformità da parte del pubblico ufficiale, con l'apposizione del riferimento temporale e della firma digitale.

Obblighi di esibizione.
Le scritture e i documenti conservati sotto forma di registrazioni su supporti di immagini devono essere, in ogni momento, resi leggibili con mezzi messi a disposizione dal soggetto che utilizza tali supporti per la conservazione.
Nel caso di documento conservato originato da un documento analogico originale unico è richiesto l'intervento del pubblico ufficiale al fine di dichiarare la conformità di quanto riprodotto su carta a quanto conservato sul supporto di memorizzazione. La procedura prevista trova origine nell'intrinseca natura del documento d'origine.

Torna al Sommario

7.9.2 RIVERSAMENTO DEI DOCUMENTI

Nei casi in cui il Responsabile del servizio di Conservazione lo ritenga necessario è possibile effettuare il riversamento diretto o il riversamento sostitutivo.

- ✓ Riversamento diretto

  Il riversamento diretto consiste nel trasferimento di uno o più documenti conservati da un supporto di memorizzazione a un altro, senza modificare la loro rappresentazione informatica.
  Si procederà col tale riversamento quando si dovrà procedere con la creazione delle copie di backup di un supporto o nel caso in cui la marca temporale sia in scadenza per cui sui file contenuti nel supporto deve essere apposta una nuova marca temporale.
  La rappresentazione del contenuto dei supporti non subisce alcuna variazione.

- ✓ Riversamento sostitutivo

  A differenza del riversamento diretto, il riversamento sostitutivo consiste nel trasferimento di uno o più documenti conservati da un supporto di memorizzazione a un altro, modificando la rappresentazione informatica del suo contenuto.
  Il Responsabile del servizio di Conservazione deve eseguire il riversamento sostitutivo nel caso in cui sia necessario un aggiornamento tecnologico dell'archivio informatico, in quanto non è più conveniente mantenere nel tempo il formato di rappresentazione digitale dei documenti originariamente conservati. Il processo si conclude con l'apposizione, sull'insieme dei documenti o su una evidenza informatica contenente una o più impronte dei documenti, del riferimento temporale e della firma digitale da parte del Responsabile del servizio di Conservazione, salvi i casi previsti dalla legge secondo i quali risulti indispensabile la presenza di un pubblico ufficiale a chiusura del processo di Conservazione.

Torna al Sommario

7.10 SCARTO DEI PACCHETTI DI ARCHIVIAZIONE

Il Responsabile della Conservazione, in collaborazione con tutte le risorse impegnate nella gestione e manutenzione del sistema di conservazione, valuterà e definirà i tempi entro cui le varie tipologie di documenti devono essere inviate in conservazione e il tempo di tenuta in conservazione prima di essere scartati secondo le indicazioni della normativa vigente, previa comunicazione al Cliente. Per i tempi di scarto si fa sempre riferimento alla data di inserimento a sistema dei documenti stessi.

In fase di avvio progetto viene concordato con il Cliente l'insieme dei documenti (suddivisi per tipologia e flussi di ingresso) e i relativi tempi di tenuta, la cui conservazione ricade nella responsabilità del Conservatore durante il periodo contrattuale.

La procedura di scarto (cfr. svecchiamento), accessibile solo da utenti con i permessi *Firma IPdA* e *Cancellazione documenti*, permette di eliminare dal Sistema di conservazione documenti e/o pacchetti di archiviazione per i quali sono trascorsi i termini legali di Conservazione.
Per ogni classe documentale è possibile definire cosa si vuole eliminare. Gli elementi cancellabili sono:

- ✓ Documenti: i documenti della classe documentale contenuti nel SdC;
- ✓ Metadati: i metadati relativi ai documenti;
- ✓ ISO: le ISO create all'atto della conservazione (contenenti il PdA e i documenti).

Il solo vincolo è che eliminando i metadati vengano automaticamente eliminati anche i documenti relativi poiché non avrebbe senso l'eliminazione dei soli metadati in quanto renderebbe i documenti inaccessibili.

Una regola di svecchiamento prevede di definire i seguenti parametri

- ✓ Classe documentale: la classe documentale per la quale effettuare lo svecchiamento;
- ✓ Età svecchiamento: età in giorni dei documenti da svecchiare. Supponendo di avere Età *svecchiamento=3650*, verranno svecchiati i documenti più vecchi di 10 anni;
- ✓ Metadata: Indica se svecchiare i metadati relativi ad un documento (abilitando questa caratteristica viene automaticamente abilitato lo svecchiamento dei documenti);
- ✓ Documenti: Indica se svecchiare i documenti;
- ✓ ISO: Indica se svecchiare le ISO.

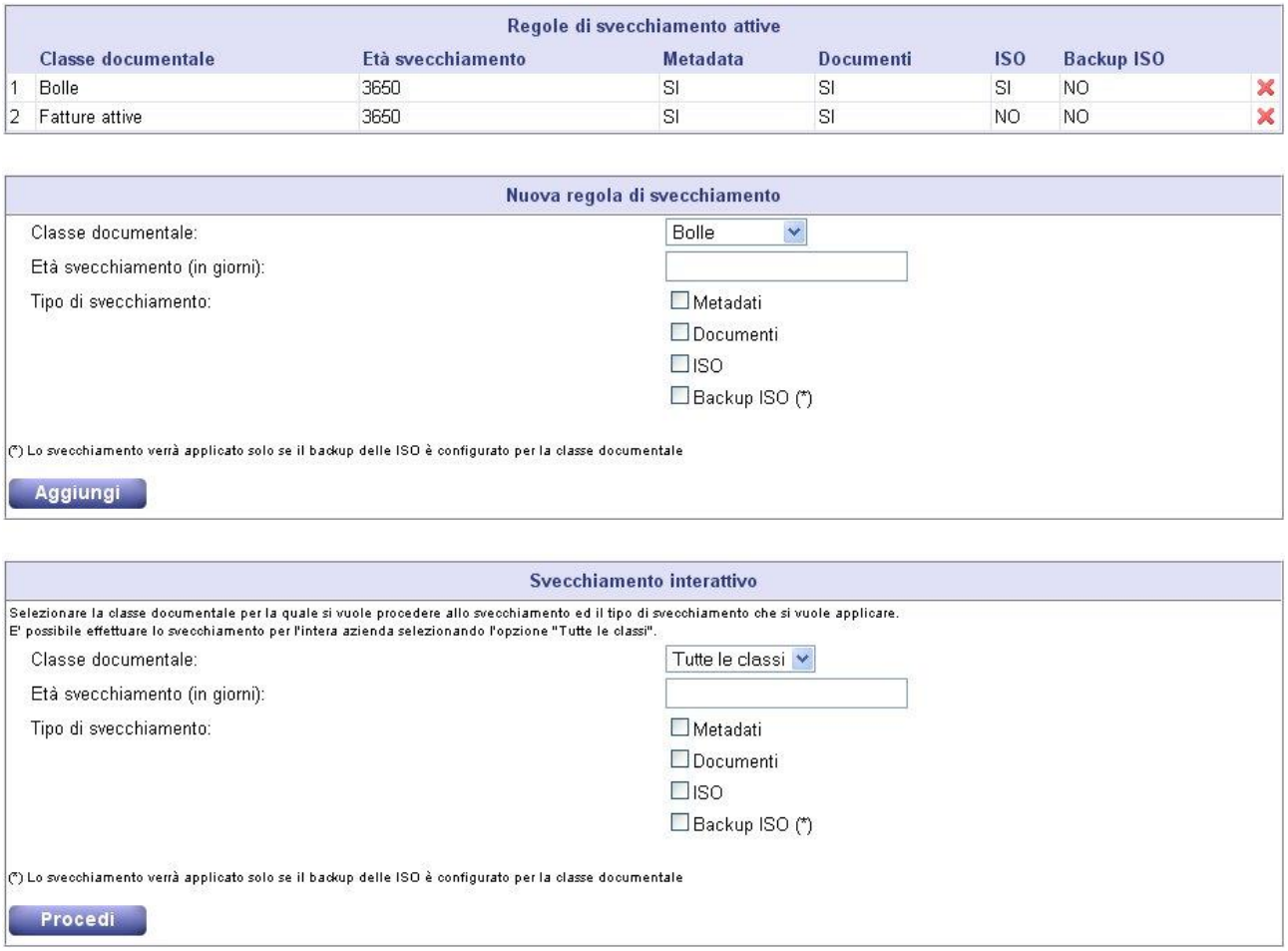

Figura 22. Modalità di svecchiamento

Lo svecchiamento può avvenire in modalità batch, in base a regole impostate dal Responsabile del servizio di Conservazione, oppure può essere interattivo.

La figura mostra l'interfaccia per lo svecchiamento.
La sezione *Regole di svecchiamento attive* elenca le regole correnti. Da questa sezione è possibile eliminare le regole attive utilizzando l'icona ✖.
La sezione *Nuova regola di svecchiamento* consente di definire nuove regole, valorizzando i campi richiesti e premendo sul bottone *Aggiungi*.
La sezione *Svecchiamento interattivo* permette di selezionare una regola di svecchiamento ed applicarla istantaneamente.
In questo caso è possibile scegliere il valore *Tutte le classi* per il campo *Classe documentale*. Questo avvierà lo svecchiamento per tutte le classi documentali della società alle quali ha accesso il Responsabile del servizio di Conservazione.
Nel caso di archivi pubblici o privati di particolare interesse culturale, le procedure di scarto avvengono previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo per il tramite della Soprintendenza competente per territorio.

[Torna al Sommario]

7.11 PREDISPOSIZIONE DI MISURE A GARANZIA DELL'INTEROPERABILITA' E TRASFERIBILITA' AD ALTRI CONSERVATORI

Sono disponibili le interfacce applicative per poter operare l'estrazione dei documenti tramite applicazione esterna. Il sistema di conservazione è in grado di accettare il versamento di pacchetti strutturati secondo lo standard UNI 11386:2010, in accordo con quanto definito dalla normativa vigente. Allo stesso modo, il sistema è in grado di versare ad altri sistemi di conservazione pacchetti e indici secondo la medesima struttura, trasformando i pacchetti di archiviazione in opportuni pacchetti di distribuzione.
Nel caso di trasferimento ad altro conservatore il Produttore potrà richiedere a Tesisquare® di interfacciarsi direttamente con il nuovo conservatore per la migrazione dei dati in modo da concordare tempistiche e formati.
Le attività saranno personalizzate sulle esigenze del cliente e saranno descritte nella "Scheda Servizio Cliente – Specificità del Contratto".

Torna al Sommario

7.12 CESSAZIONE DEL SERVIZIO

In caso di cessazione del servizio verso un Produttore, per naturale scadenza della durata del contratto o nei casi di risoluzione o recesso per qualsivoglia motivo occorso:

- ✓ il ruolo di Conservatore rivestito da Tesisquare® cessa di avere efficacia a partire dalla data di recesso del contratto e con essa tutte le responsabilità civili;
- ✓ Tesisquare® provvede a riconsegnare al Produttore i documenti conservati presso i propri archivi, completi dei PdA, con le modalità concordate per il servizio stesso che possono prevedere:
  - ➢ invio immagine ISO dei pacchetti archivio;
  - ➢ recupero via API/web service da parte del Produttore attraverso le interfacce di interoperabilità messe a disposizione dalla piattaforma;
  - ➢ altre modalità preventivamente concordate.
- ✓ Tesisquare® provvede a redigere un apposito verbale di consegna che verrà inviato tramite PEC;
- ✓ Tesisquare® si impegna a non comunicare e/o diffondere e/o comunque utilizzare ulteriormente i documenti oggetto del verbale di consegna;
- ✓ il Produttore si impegna a verificare il contenuto dei pacchetti consegnati entro 30 gg dalla ricezione; trascorso questo periodo i supporti forniti si intendono verificati e accettati senza riserve e Tesisquare® provvederà alla cancellazione definitiva dei dati dal server;
- ✓ Tesisquare® provvederà a richiedere la revoca del certificato di firma del Produttore alla registration authority;
- ✓ Tesisquare® provvederà ad aggiornare la "Scheda Servizio Cliente – Specificità del Contratto" per registrare la chiusura del servizio;

È predisposta la specifica procedura *Piano per la cessazione* che descrive le strategie e le attività operative che Tesisquare® si propone di avviare qualora si verifichi la cessazione del servizio di conservazione.

Torna al Sommario

TESI SpA Registered office: Via Mendicità Istruita, 24 – 12042 Bra (CN) - Headquarters: Via Savigliano, 48 - 12062 Roreto di Cherasco (CN)
Phone +39 0172 476301 - Fax +39 0172 476399 - www.tesisquare.com - info@tesisquare.com
Tax Code and VAT no. 02448510046 – Cuneo Chamber of Commerce - Economic and Administrative Register no. 177331
Share Capital € 750,000 fully vested
Tesi SpA is ISO 9001 certified Tesi SpA in ISO 27001 certified (certification no. 350/15)

8. IL SISTEMA DI CONSERVAZIONE

L'architettura del servizio di Conservazione dei documenti informatici offerto da Tesisquare® è concepito in modalità modulare e scalabile.
Il servizio offerto ai clienti è pensato come una piattaforma basata su accesso Web come Software as a Service; il Sistema di Conservazione, e la relativa soluzione software, è installato presso il Data Center Tim di Rozzano, provider di Sistemi IT di primaria importanza sul mercato italiano e certificato secondo lo standard ISO/IEC 27001:2013.

Torna al Sommario

8.1 COMPONENTI LOGICHE

Il Sistema di Conservazione offerto da Tesisquare® è la soluzione che consente la Conservazione a norma di qualsiasi tipologia di documentazione digitale garantendone, dal momento della presa in carico, le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità.
Di seguito una rappresentazione grafica del Sistema di Conservazione, con le principali parti e funzionalità:

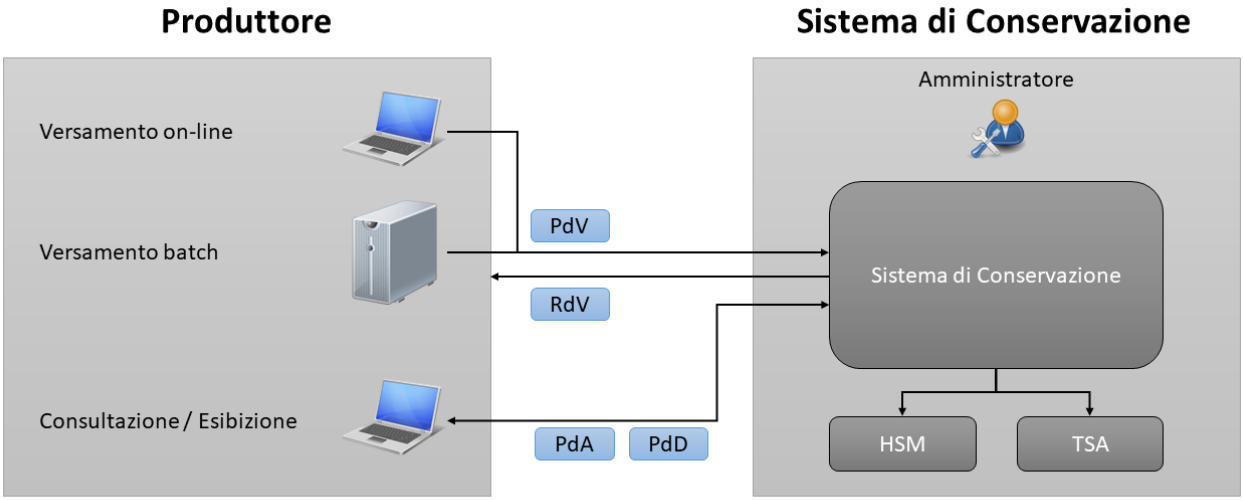

Figura 23. Schema generale

Lo schema in figura mostra i componenti con i quali il Sistema di Conservazione si integra al fine di effettuare la Conservazione a norma di legge:

- ✓ HSM: Hardware Security Module utilizzato per l'apposizione delle firme in fase di creazione dei pacchetti di archiviazione. Può essere utilizzato anche per firmare i documenti durante la fase di versamento;
- ✓ TSA: Time Stamping Authority certificata, alla quale vengono richieste le marche temporali incluse nei pacchetti di archiviazione. Può essere utilizzata anche per marcare le firme apposte durante la fase di versamento;

La figura qui sotto riportata mostra uno schema più dettagliato del Sistema di Conservazione nel quale si vedono le diverse componenti interne:

TESI SpA Registered office: Via Mendicità Istruita, 24 – 12042 Bra (CN) - Headquarters: Via Savigliano, 48 - 12062 Roreto di Cherasco (CN)
Phone +39 0172 476301 - Fax +39 0172 476399 - www.tesisquare.com - info@tesisquare.com
Tax Code and VAT no. 02448510046 – Cuneo Chamber of Commerce - Economic and Administrative Register no. 177331
Share Capital € 750,000 fully vested
Tesi SpA is ISO 9001 certified Tesi SpA in ISO 27001 certified (certification no. 350/15)

- ✓ DB: il data base è il repository della configurazione del Sistema di Conservazione (aziende, utenti, classi documentali, ecc.) e di tutti i metadati relativi ai documenti.
  Il database può essere MySQL oppure Oracle e può essere configurato in alta disponibilità;

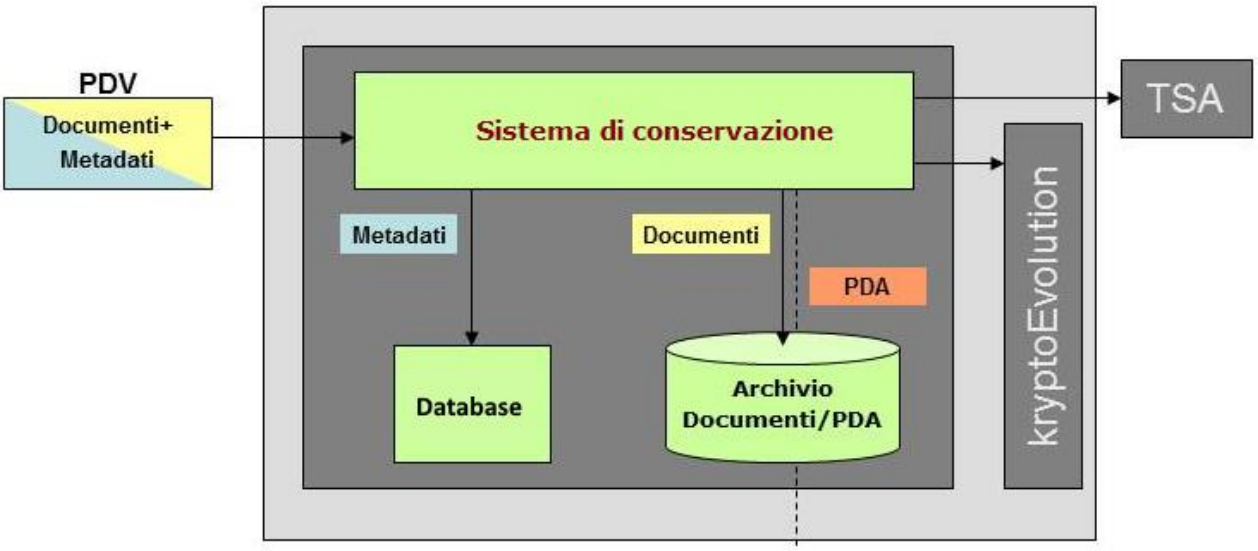

Figura 24. Schema del Sistema di Conservazione

- ✓ Archivio: nell'archivio vengono salvati i documenti e i PDA. L'archivio può essere ad esempio il file system locale, un disco condiviso, una partizione montata in NFS;
- ✓ Sistema di Conservazione: è l'applicazione che svolge il lavoro di archiviazione e conservazione interfacciandosi con le altre componenti appena descritte.

Il tab Generale consente di definire i seguenti dettagli di una classe documentale:

- ✓ Classe documentale: nome della classe documentale. Normalmente il campo è libero e consente di inserire un nome a scelta, ma selezionando il check-box *Agenzia Entrate* il campo si trasforma in un menù a tendina che propone una serie di nomi predefiniti dall'Agenzia delle Entrate;
- ✓ Descrizione: descrizione della classe documentale;
- ✓ Frequenza Max di Conservazione: limite in giorni oltre al quale il documento va conservato. Questo campo non può essere inserito durante la creazione della classe in quanto verrà impostato dal Responsabile del servizio di Conservazione;
- ✓ Giorni conservati: numero massimo di giorni conservati unitamente. Questo campo non può essere inserito durante la creazione della classe in quanto verrà impostato dal Responsabile del servizio di Conservazione;
- ✓ Consultazione On-Line: limite in giorni oltre al quale i documenti non sono più visibili agli utenti. I documenti più vecchi di tale valore verranno quindi esclusi dalle ricerche;
- ✓ Durata di Conservazione: limite in giorni oltre al quale i documenti possono essere eliminati;
- ✓ Alias di firma: alias utilizzato per firmare tutti i documenti della classe documentale nel momento dell'archiviazione. Questo campo non può essere inserito durante la creazione della classe in quanto verrà impostato da un utente manager della società;
- ✓ Timestamp: se specificata verrà aggiunta una marca temporale a tutti i documenti firmati (CAdES) della classe documentale;
- ✓ Listino: listino da applicare alla classe documentale;
- ✓ Crea le ISO: check-box che permette di specificare se le ISO relative alla classe documentale vanno create contestualmente alla creazione dei PDA;

- ✓ Classe documentale di test: se selezionato viene creata una seconda classe documentale identica a quella che si sta definendo. Il nome di tale classe viene creato aggiungendo la stringa "_test" al nome della classe documentale;
- ✓ Mail di conferma archiviazione: se selezionato viene generata una mail di conferma a seguito di ciascuna archiviazione;
- ✓ Firme presenti nel documento: se il numero di firme è maggiore di 0 viene controllato che ciascun documento della classe documentale contenga il numero di firme indicato. In tal caso ogni firma viene verificata;
- ✓ Marca temporale: Selezionando questo check-box viene verificata la marca temporale, che deve essere presente in ogni documento archiviato.

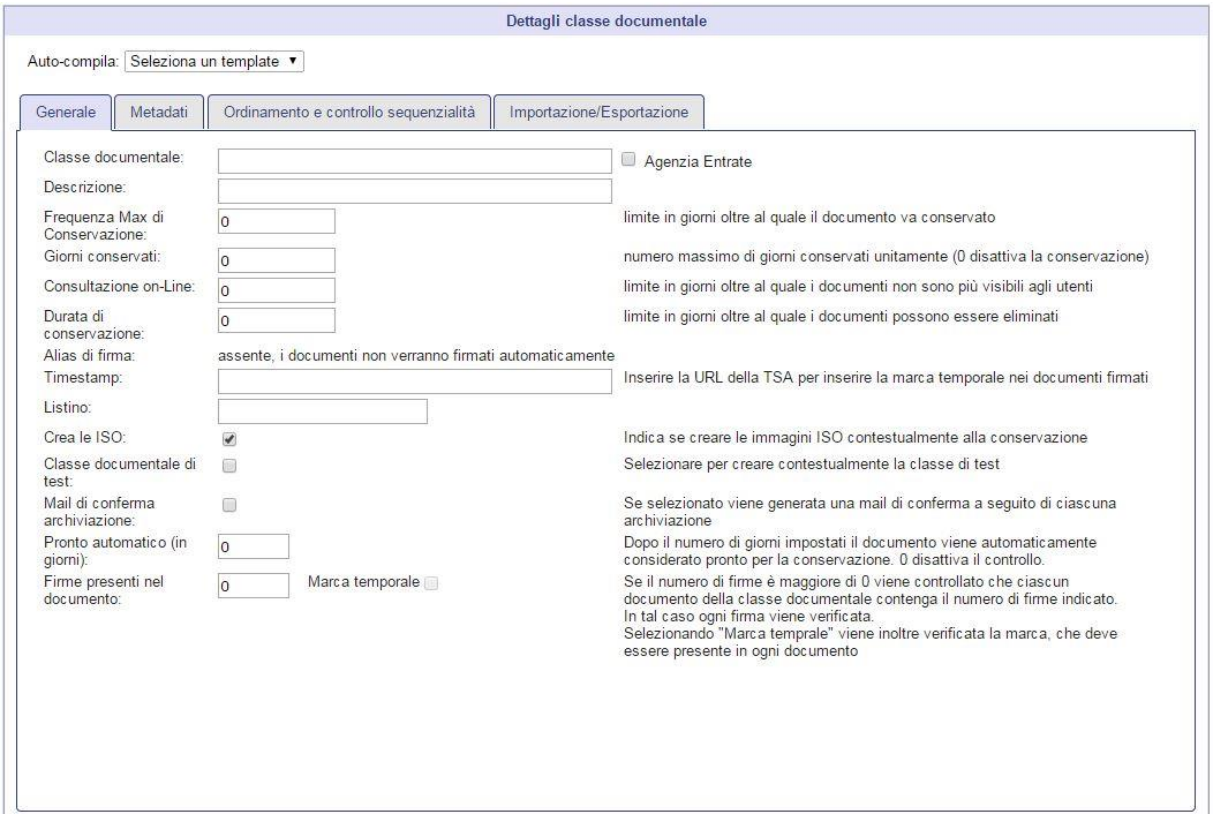

Figura 25. Dettagli classe documentale - tab generale

[Torna al Sommario]

8.2 COMPONENTI TECNOLOGICHE

Il Sistema di Conservazione è installato su server virtuali, a loro volta ospitati su server fisici di proprietà di Tim, presso il Data Center di Rozzano.
I server virtuali sono progettati in modo da assicurare la ridondanza degli stessi in caso di malfunzionamenti della macchina hardware, con riavvio immediato degli stessi.

Il Data Center di Tim inoltre dispone dei seguenti servizi di network:

Connettività Internet:

- ✓ Nr. 1 Banda Virtuale profilo Sigma Flat – 10 Mbps;

Connettività MPLS:

- ✓ Nr. 1 Banda profilo 10 Mbps;

Firewalling e VPN

I servizi di firewalling ed i servizi di VPN vengono implementati su un'istanza virtuale dedicata di firewall denominata VDOM. Tale istanza è implementata su infrastruttura condivisa e ridondata di data center.
Le configurazioni dei VDOM dei Clienti vengono sottoposte a backup, con una retention degli ultimi 3 backup.
Nell'implementazione delle VPN, i server possono presentarsi sia con IP pubblici, sia con IP privati.

Di seguito le caratteristiche tecniche e software delle macchine:

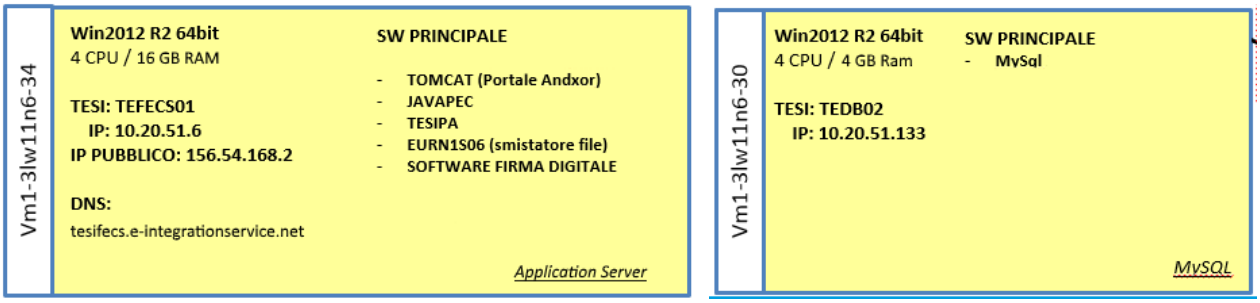

Figura 26. Caratteristiche tecniche

Il disegno dell'infrastruttura di Hosting Evoluto, integra le seguenti caratteristiche di alta affidabilità:

- ✓ I server fisici della Server Farm su cui sono attivate le macchine virtuali, sono raggruppati in cluster vmware da almeno 3 ESX per cluster;
- ✓ Il fault di un ESX garantisce la rilocazione automatica di tutte le VM su altro ESX in cluster;
- ✓ I Server ESX sono di classe Enterprise (server da 24 core di big player vendor di mercato);
- ✓ Le schede di rete di ogni singolo ESX sono ridondate e configurate in teaming/trunking;
- ✓ Le HBA FC di ogni singolo ESX sono ridondate e configurate in bilanciamento vs gli switch della SAN;
- ✓ Gli storage box sono di livello enterprise ad alimentatori ridondati, controller ridondati, dischi in configurazione RAID, porte fc ridondate ed in bilanciamento vs gli switch della SAN;
- ✓ Switch e pattern FC della SAN ridondati sia a livello edge che core, con realizzazione dual fabric;
- ✓ Switch di rete ridondati a livello access, core e distribution.

Congiuntamente alle scelte architetturali la tecnologia VMWare consente di massimizzare l'uptime dell'infrastruttura rispetto ai disservizi planned e unplunned attraverso:

- ✓ Vmotion: consente di migrare real time le VM tra un host fisico ed un altro del cluster;
- ✓ Storage Vmotion: per la rilocazione di una VM da un datastore all'altro senza interruzione del servizio;
- ✓ HA (High Availability): per la ripartenza automatica delle VM in caso di failure dell'ESX o failure della VM (assenza di heartbeat).

Inoltre il Sistema dispone di una NAS dedicata per il mantenimento sicuro dei dati e dei Backup (descritti all'interno del Sistema di Gestione per la Sicurezza delle Informazioni ISO/IEC 27001:2013)

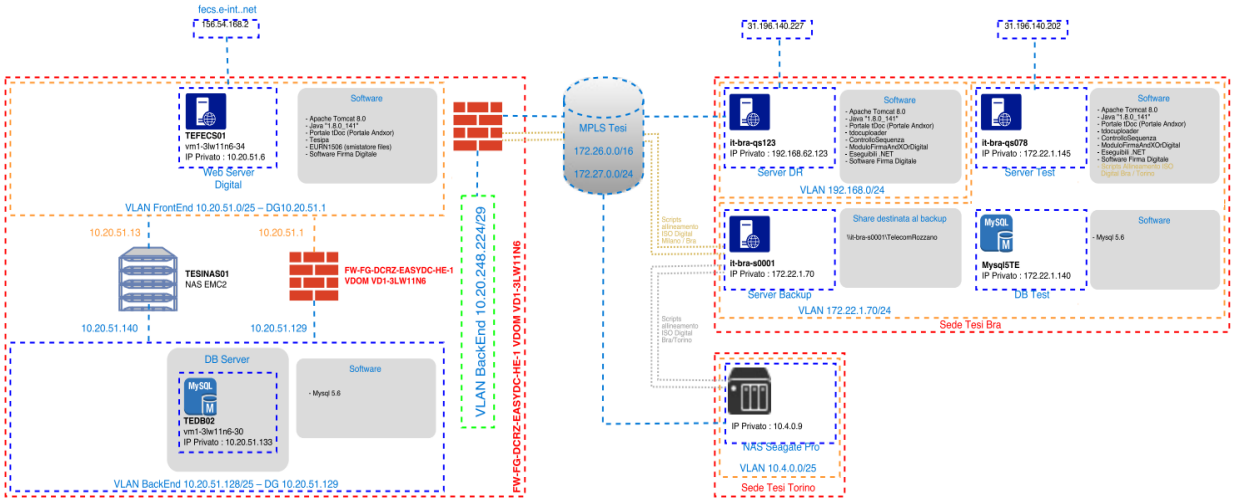

Figura 27. Infrastruttura

[Torna al Sommario](#)

8.3 COMPONENTI FISICHE

Il Sistema di Conservazione è attestato sul servizio di IAAS (Infrastructure as a service) di Tim, afferenti all'offerta Hosting Evoluto, forniti presso il Data Center di Rozzano (MI).

Il Sistema di Conservazione è installato su macchine virtuali che in caso di necessità, possono essere spostate su altre macchine fisiche all'interno dello stesso Data Center ed a necessità eventuali sul Data Center Tim di Pomezia (RM) e Cesano (MI), per garantire la continuità del servizio.

La distanza massima tra i DC è circa 600 km.

Inoltre il Sistema è strutturato con una tipologia di accesso MPLS.

Questa tipologia di servizio di accesso nasce per consentire ai Clienti che hanno già sottoscritto un contratto di servizio di una rete MPLS ed intendano avere visibilità attraverso la stessa rete dei propri server attestati nei Data Center (Server Intranet). Ciò ovviamente senza dover costruire architetture di accesso dedicate, ma usufruendo di un'infrastruttura condivisa ad alta affidabilità (doppio path, doppio CE, Doppio PE dedicato) su cui la rete MPLS del Cliente potrà essere integrata. Il Cliente verrà attestato su SUBNET di campus in DC con opportuni indirizzi IP privati. Questi saranno "routabili"sulla Rete Mpls geografica per consentire quindi la visibilità dei Sistemi presenti in DC. Gli indirizzi IP privati fanno parte di una classe di indirizzi molto ampia per minimizzare i rischi di overlapping con quelli della rete geografica.

Di seguito la struttura logica:

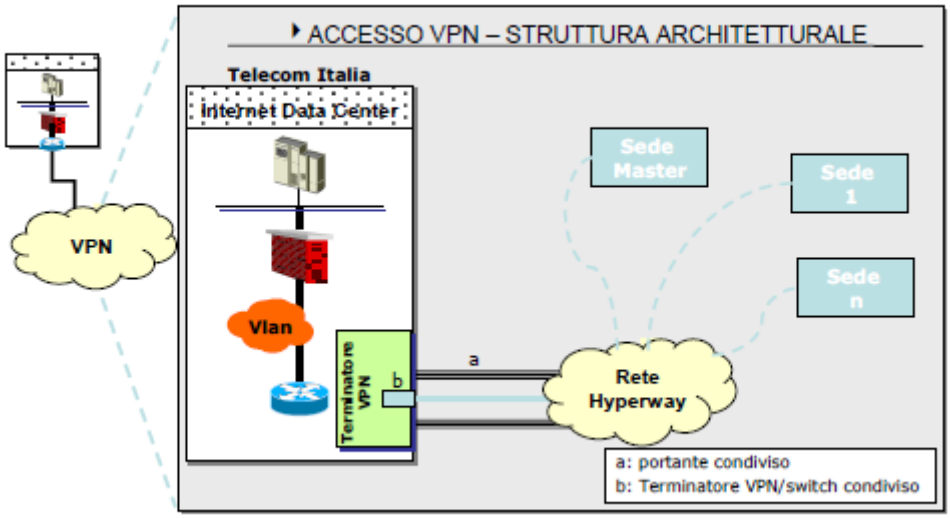

Figura 28. Struttura logica

È predisposto inoltre un ambiente di Disaster Recovery situato nell'infrastruttura della sede Tesisquare® di Roreto di Cherasco (CN) che assicura il servizio al cliente permettendogli la consultazione dei documenti inviati fino all'attivazione del DR stesso. Al ripristino dell'infrastruttura primaria sarà garantita l'acquisizione dei documenti inviati durante tutto il periodo di attivazione del DR.

[Torna al Sommario]

8.4 PROCEDURE DI GESTIONE E DI EVOLUZIONE

Il servizio offerto da Tesisquare®, è atto a garantire attraverso il rispetto delle norme in materia di qualità e di sicurezza informatica, la gestione riservata delle informazioni nonché la loro leggibilità, integrità e reperibilità. Inoltre il servizio ha lo scopo di:

- ✓ Formalizzare e garantire i requisiti del Sistema in conformità alla normativa vigente attraverso continuo aggiornamento e manutenzione;
- ✓ Gestire i log e le altre informazioni per garantire tracciabilità;
- ✓ Monitorare il Sistema, anche attraverso gestione degli incidenti e delle anomalie;
- ✓ Monitorare i livelli di sicurezza e il rischio;

Il Sistema di Conservazione è parte del Sistema di Gestione per la Sicurezza delle Informazioni certificato secondo lo standard ISO/IEC 27001:2013, risponde ai requisiti di sicurezza, descritti nel Piano della Sicurezza in termini di sicurezza fisica, logica e organizzativa.

Il rilascio di ogni nuova versione del sistema di conservazione prevede:

- ✓ la definizione dei requisiti;
- ✓ la realizzazione di un progetto funzionale e tecnico;
- ✓ lo sviluppo
- ✓ il collaudo interno

- ✓ la formazione del personale interno
- ✓ il rilascio delle modifiche;
- ✓ la comunicazione dell'avvenuto rilascio (unicamente per le major release);

Tesisquare® mantiene un registro in cui vengono tracciate le diverse release del Sistema di Conservazione e la Change list collegata con l'elenco delle caratteristiche eventualmente aggiunte.
Nel caso la modifica sia scaturita da modifiche portate dal legislatore o la soluzione sia sottoposta ad una major release, la responsabilità del rilascio della release è sottoposta all'approvazione del Responsabile del servizio di Conservazione; inoltre ogni rilascio viene preventivamente testato in ambiente di quality prima di venire rilasciato in produzione.

Al fine di tracciare eventuali criticità che possano concretizzarsi durante l'erogazione del servizio, Tesisquare® mette a disposizione dei soggetti esterni (clienti, fornitori e partner), un servizio di Supporto dedicato, Help Desk, con vari turni di copertura, suddiviso in 1 e 2 livello, che ricevono segnalazioni tramite strumenti di ticketing, via telefono e via mail:

- ✓ Supporto HD 1: prende in carico le segnalazioni e si preoccupa di suddividerle tra le segnalazioni direttamente risolvibili e le segnalazioni invece da scalare all'HD 2; tipicamente vengono affrontate problematiche legate ad utenze, segnalazioni di scarti, elaborazioni dei flussi ricevuti ecc;
- ✓ Supporto HD 2: prendono in carico le segnalazioni dirette se correttamente di competenza ed eventualmente scalano all'HD 1 le segnalazioni non corrette. Si occupano di risolvere le problematiche di complessità maggiore ed eventualmente ingaggiano il team di analisi e/o sviluppo se necessario.

Inoltre, come definito all'interno del SGSI ISO/IEC 27001:2013, è stata definita una procedura ed uno strumento di ticketing per la segnalazione e gestione degli incident, direttamente collegata alla Valutazione dei Rischi in termini di Sicurezza dell'informazione.
A livello di risorse hardware, software e network, come verrà descritto nel capitolo successivo, è attiva una soluzione di monitoraggio H24 con politiche di escalation ai diversi livelli di competenza in funzione dell'urgenza (es. verifica capacità delle macchine in termini di CPU, RAM ecc,) e soglie di segnalazione configurate.

Torna al Sommario

9. MONITORAGGIO E CONTROLLI

Tesisquare® ha previsto una serie di controlli, anticipati nel paragrafo 8.4, per assicurare la rilevazione di eventuali criticità in maniera proattiva, al fine di evitare il concretizzarsi di eventuali incident che possano mettere a repentaglio la Riservatezza, l'Integrità e la Disponibilità del dato trattato e portato in conservazione.
Di seguito si descrivono i controlli principali in atto nell'erogazione del servizio.

Torna al Sommario

9.1 PROCEDURE DI MONITORAGGIO

Il Sistema di Conservazione viene costantemente monitorato da un Sistema proattivo che rileva potenziali malfunzionamenti a livello di hardware, software o network.
Il Sistema di monitoring è gestito direttamente dal Responsabile dei sistemi informativi per la conservazione, che si preoccupa di manutenere il Sistema e avvertire il Responsabile del servizio di Conservazione in caso di malfunzionamenti; i controlli sono ovviamente stati configurati per inviare alert

TESI SpA Registered office: Via Mendicità Istruita, 24 – 12042 Bra (CN) - Headquarters: Via Savigliano, 48 - 12062 Roreto di Cherasco (CN)
Phone +39 0172 476301 - Fax +39 0172 476399 - www.tesisquare.com - info@tesisquare.com
Tax Code and VAT no. 02448510046 – Cuneo Chamber of Commerce - Economic and Administrative Register no. 177331
Share Capital € 750,000 fully vested

in modalità automatica sia in caso di malfunzionamenti sia in caso di superamento di soglie di controllo pre impostate.
Il Sistema attualmente in uso da parte di Tesisquare® è Nagios, strumento leader di mercato nella gestione e verifiche delle componenti IT.

Di seguito si elencano i principali servizi posti sotto monitoraggio da parte del Sistema Nagios, con le colonne rappresentanti:

- ✓ Nome dell'Host posto sotto monitoring;
- ✓ Servizio posto sotto monitoring;
- ✓ Stato del servizio;
- ✓ Durata del controllo (giorni di attività del controllo, che può partire dal momento che viene riavviato il servizio);
- ✓ Tentativi di verifica;
- ✓ Ultimo controllo effettuato;
- ✓ Stato del controllo di dettaglio (informazioni tipiche per tipo di controllo).

Host	Service	Status	Duration	Attempt	Last Check	Status Information
EINT_TEFECS01	HW - CPU Usage	Ok	40d 16h 20m 2s	1/5	2016-01-12 16:45:20	CPU Load 33% (5 min average)
	HW - HD C: Disk Usage	Ok	4d 20h 44m 24s	1/5	2016-01-12 16:45:50	C:\ - total: 39.90 Gb - used: 32.46 Gb (81%) - free 7.44 Gb (19%)
	HW - HD E: Disk Usage	Ok	13d 3h 48m 34s	1/5	2016-01-12 16:43:12	E:\ - total: 990.00 Gb - used: 864.33 Gb (87%) - free 125.67 Gb (13%)
	HW - HD F: Disk Usage	Ok	12d 9h 46m 17s	1/5	2016-01-12 16:49:19	F:\ - total: 30.00 Gb - used: 6.05 Gb (20%) - free 23.95 Gb (80%)
	HW - HD G: Disk Usage	Ok	40d 16h 13m 2s	1/5	2016-01-12 16:50:28	G:\ - total: 30.00 Gb - used: 0.76 Gb (3%) - free 29.23 Gb (97%)
	HW - RAM Memory Usage	Ok	20d 2h 7m 5s	1/5	2016-01-12 16:42:52	Memory usage: total:12285.73 MB - used: 7321.93 MB (60%) - free: 4963.80 MB (40%)
	HW - Uptime	Ok	19d 7h 8m 11s	1/5	2016-01-12 16:45:36	System Uptime - 19 day(s) 1 hour(s) 44 minute(s)
	NAS: check free space fecs_stor	Ok	26d 1h 44m 36s	1/5	2016-01-12 16:46:52	path: \\TESINAS01\fecs_stor\
	NW - Ping da Nagios	Ok	10d 11h 31m 29s	1/3	2016-01-12 16:52:21	OK - 10.20.47.16: rta 6.909ms, lost 0%
	NW - Ping DC a TEBTCH01	Ok	19d 2h 14m 50s	1/3	2016-01-12 16:49:43	OK: - PKT-LS=0%, RT-AV=1ms
	NW - Ping DC a TEBTCH02	Ok	13d 3h 48m 26s	1/3	2016-01-12 16:50:10	OK: - PKT-LS=0%, RT-AV=0ms
	NW - Ping DC a TEBTCH03	Ok	1d 20h 44m 51s	1/3	2016-01-12 16:49:40	OK: - PKT-LS=0%, RT-AV=0ms
	NW - Ping DC a TEBTCH04	Ok	19d 2h 12m 59s	1/3	2016-01-12 16:50:04	OK: - PKT-LS=0%, RT-AV=0ms
	NW - Ping DC a TEDB01	Ok	13d 3h 48m 32s	1/3	2016-01-12 16:49:42	OK: - PKT-LS=0%, RT-AV=1ms
	NW - Ping DC a TEDB02	Ok	19d 7h 50m 3s	1/3	2016-01-12 16:51:23	OK: - PKT-LS=0%, RT-AV=0ms
	NW - Ping DC a TEDROMOS01	Ok	19d 1h 52m 29s	1/3	2016-01-12 16:50:31	OK: - PKT-LS=0%, RT-AV=0ms

Figura 29. Schermata Nagios

Al fine di avere un controllo visivo più rapido e facilmente comprensibile, Nagios dispone anche di una dashboard dotata di una GUI composta da semafori per ogni tipologia di controllo, di seguito un estratto della schermata di controllo:

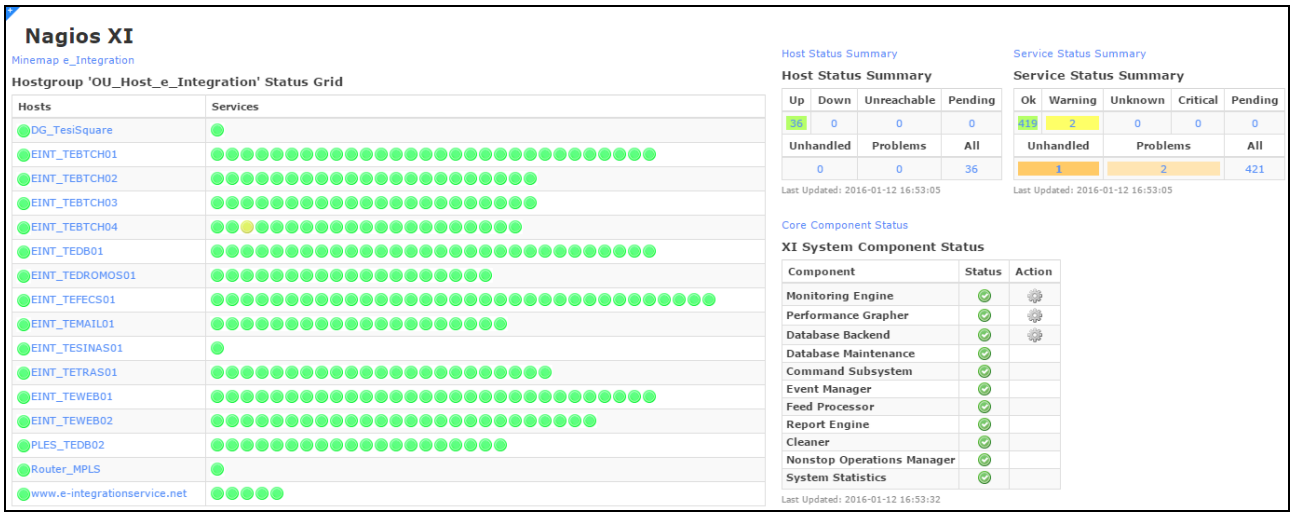

Figura 30. Schermata di controllo Nagios

I log di controllo del Sistema vengono mantenuti all'interno del Sistema di monitoraggio, anch'esso posto sotto backup per evitare potenziali perdite a seguito di incident e poter ricostruire l'accaduto.
In caso di malfunzionamento, il Sistema reagisce inviando alert via mail e sms al responsabile dei sistemi informativi per la conservazione e al responsabile HD i quali si preoccupano di informare tempestivamente in via informale il Responsabile della Conservazione e/o il gruppo tecnico di riferimento; appena possibile la comunicazione sarà effettuata formalmente.

Per il dettaglio sul funzionamento del sistema Nagios si faccia riferimento al documento DH_Tesi_e-Integration_documentazione_Nagios.doc.

[Torna al Sommario]

9.2 VERIFICA DELL'INTEGRITA' DEGLI ARCHIVI

Il Sistema contiene dei tool che permettono di verificare l'integrità dei pacchetti di archiviazione posti in Conservazione.
L'operazione di verifica di integrità dei pacchetti, disponibile solo per gli utenti con i permessi Firma IPdA e Configurazione, permette di controllare l'integrità dei pacchetti appartenenti ad una classe documentale.
La verifica di integrità si occupa di controllare i seguenti aspetti tecnici:

- ✓ coerenza dell'hash letto dal file presente su disco con quello che è stato memorizzato nel DB al momento della creazione
- ✓ parsing dell'XML
- ✓ validità della firma dell'XML
- ✓ parsing dei metadati di quel lotto

L'interfaccia prevede di specificare la classe documentale sulla quale si vuole effettuare la verifica e quindi di premere sul bottone *Procedi* per avviare il controllo.

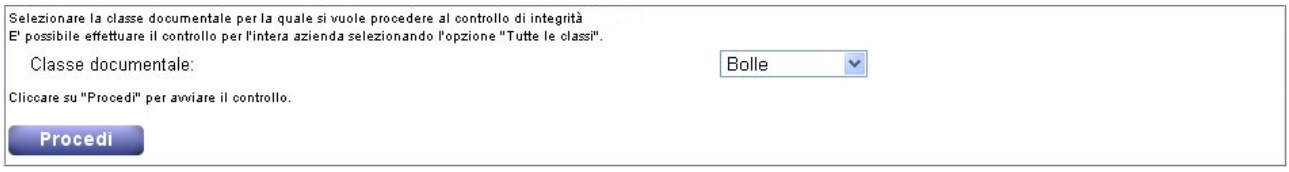

Figura 31. Controllo di integrità

Nel caso in cui vengano rilevate delle anomalie oppure il PDA non venga trovato, viene prodotta una segnalazione a video e l'anomalia viene tracciata all'interno dei log applicativi

Sono stati controllati 6 PdA

	PdA	Azienda	Classe documentale	Hash XML	Hash ISO	Verifica XML	Verifica ISO	Verifica DB
1	1518777520907	IT99999999999	FattureRicevute	E5C83AB3FDDB085A4DBE2E99211B81D38B2D97AE89DB3EEE2EDD5529118CC05C	929CA03E507E457FE460EB48CFD2DC293EB9D522520B17E5193749C0BD021331	VERIFICATO	VERIFICATO	VERIFICATO
2	1518777522545	IT99999999999	FattureRicevute	F0EDC049F6F02318EC1FA85C8E3F5748BCCF9248921BFB83ABAAE169DBD99302	16ED41F466BA2A563F848D17BC1B801123145EF7F823C7870FD5D6D6778FD948	VERIFICATO	VERIFICATO	VERIFICATO
3	1518777523154	IT99999999999	FattureRicevute	5A0F2599CDF6EB38AC8E84B0BE8E177DB123F80EB211072BC2B0204BFCA80E4F	45018B0CB80F0DDBCB36CA1E8958C75429B31206C1DB2C60270E054FD24FD390	VERIFICATO	VERIFICATO	VERIFICATO
4	1518777523637	IT99999999999	FattureRicevute	37D8C4C62159A9E8351988A1BA82107AD9E7E90727D63FC48C2D161CB57135F8	7E601363762B34F6D73381502D9B4EF4B690F9ADAFC73C75EA4B2720322E18D7	VERIFICATO	VERIFICATO	VERIFICATO
5	1518777524058	IT99999999999	FattureRicevute	459BCB61230ED42C0EF816BA8F7C0CAB85A4EEBA93B870A4B8CEA1951B9546CF	B5581F27FF83D10827A35F8491D92EC1584BC7F90A3A02CDFFE2F2E152F139FB	VERIFICATO	NON VERIFICATO	NON VERIFICATO
6	1520557232495	IT99999999999	FattureRicevute	EE5B191743E023007AAEFCE5B9CFD575FCCAA4C96AC398B9A86ADD7E42669B5B	7919F953A16D870F184D675B79C4DC5EFA91AE44DEC54449364229A0A1EB74A8	VERIFICATO	VERIFICATO	VERIFICATO

Figura 32. Risultato controllo integrità

Il risultato del controllo di integrità è una tabella che mostra l'identificativo dei pacchetti di archiviazione controllati e, per ognuno di essi, l'esito della verifica dell'IPdA e del PdA.
Le icone presenti nella tabella permettono di:

- ✓ : accedere all'interfaccia relativa al PdA;
- ✓ : effettuare il download dell'IPdA;
- ✓ : effettuare il download del PdA.

I controlli vengono effettuati anche in modalità automatica e a rotazione su tutti i PDA dei pacchetti di conservazione, in modo da verificare con costanza lo storage degli stessi. In caso di rilevazioni anomale viene prodotta una mail automatica di segnalazione della problematica inviata all'indirizzo di posta elettronica del supporto.

Nel caso in cui venga riscontrata un'anomalia di integrità del PDA, è possibile recuperare una copia dello stesso che per sicurezza viene automaticamente archiviata in doppio su due server logicamente e fisicamente distinti.

[Torna al Sommario](#)

9.3 SOLUZIONI ADOTTATE IN CASO DI ANOMALIE

Vengono qui descritte, nelle loro linee generali, le modalità adottate per fronteggiare eventi eccezionali nell'ambito della funzione del Sistema di Conservazione. Quello che qui si vuole evidenziare sono le metodologie e procedure adottate affinché il Sistema di Conservazione digitale possa sviluppare un servizio il più possibile continuativo e meno esposto a eventuali rischi catastrofici.

- ✓ Guasti agli elaboratori. L'ambiente operativo utilizzato, in accordo con le politiche aziendali in essere, è stato progettato e realizzato in modo da garantire la sicurezza della integrità e reperibilità dei dati e delle informazioni conservate, anche a fronte di guasti improvvisi agli elaboratori utilizzati. I backup si avvalgono sostanzialmente di 2 modalità operative fondamentali:

- ✓ Backup completo effettuato con cadenza settimanale
- ✓ Backup incrementale effettuato con cadenza giornaliera

Il backup incrementale copia soltanto i files che hanno subito una modifica rispetto all'ultimo backup completo o incrementale. Il ripristino pertanto avverrà tramite l'ultima copia del backup completo e tutte le copie dei backup incrementali fino al momento dell'interruzione;

- ✓ Compromissione del software. Il software utilizzato per la Conservazione Digitale è governato e gestito da Giuseppe CRIVELLO, nella sua qualità di Responsabile interno della Conservazione di Tesisquare®, e, per le sole funzioni a loro attribuite, dai delegati. In caso di guasto dell'elaboratore, la versione in produzione può essere ripristinata nei tempi e nei modi previsti dalle politiche di ripristino dei backup aziendali. Qualora ciò non fosse possibile (ipotesi veramente remota) si dovrà ricorrere alla copia originale e provvedere alla relativa installazione del software di Conservazione Digitale sulla macchina che ha presentato il guasto;

- ✓ Guasti al dispositivo sicuro di firma . In caso di guasto al dispositivo di firma occorre procedere alla individuazione della tipologia di guasto e provvedere immediatamente alla sua riparazione. Nel caso si renda necessario, viene utilizzato il dispositivo sicuro del sostituto o altro delegato alla firma;

- ✓ Compromissione del sito della Certification Authority. La compromissione del sito della Certification Authority per il rilascio della marca temporale da apporre sull'evidenza informatica a chiusura del processo di Conservazione Digitale, è un evento particolarmente remoto, in quanto l'Authority implementa politiche di continuità di erogazione del servizio con SLA di altissimo livello in linea con la normative di settore;

- ✓ Compromissione del server Network Time Protocol (NTP). La compromissione del server di collegamento al Network Time Protocol (NTP) utilizzato per la sincronizzazione dell'orologio interno del Sistema di Conservazione Digitale e utile al fine di apporre il riferimento temporale, è un evento particolarmente remoto, in quanto esso implementa politiche di continuità di erogazione del servizio con SLA di altissimo livello.

La gestione degli incidenti viene governata, come da norma ISO/IEC 27001:2013 e dalla norma ISO 27035:2011, attraverso:

- ✓ Strumenti di rilevazione
- ✓ Strumenti di tracciatura e analisi
- ✓ Processi informativi
- ✓ Misure atte a correggere eventuali criticità materializzate

La gestione degli incidenti risponde ad un workflow molto strutturato su uno strumento di ticketing, che parte dalla Segnalazione dell'Incidente al momento del concretizzarsi dello stesso, e tramite una gestione suddivisa su 3 livelli, permette di tracciare i diversi momenti di gestione del ticket stesso, con la registrazione dei dati legati all'ora di accadimento e alle successive azioni di presa in carico e correzione delle eventuali problematiche create (es: irraggiungibilità di un servizio, superamento capacità macchina, attacchi sterni, denial of service ecc).

Di seguito per completezza di rappresentazione, il workflow di gestione degli incident:

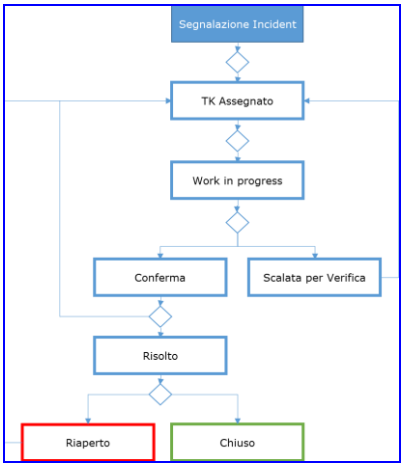

Figura 33. Gestione incident

[Torna al Sommario]

IL Responsabile del servizio di Conservazione
TESI S.p.A.

*Giuseppe **CRIVELLO***