MANUALE DEL SERVIZIO DI CONSERVAZIONE

VERSIONE 2.2

Firmato digitalmente da
Marco Polsi
CN = Polsi Marco
O = LAND Srl

Firmato digitalmente da
Ettore Alloggia
CN = Alloggia Ettore
O = Land Srl/04554571002

MANUALE DEL SERVIZIO DI CONSERVAZIONE

AZIONE	DATA	NOMINATIVO	FUNZIONE
Redazione		Marco Polsi	Responsabile del Servizio di Conservazione
Verifica		Claudio Dosio	Responsabile della Sicurezza del Sistema di Conservazione
Verifica		Giovanni Manca	Consulente
Approvazione		Ettore Alloggia	Amministratore Unico e Titolare del Trattamento dei Dati Personali di LAND

REGISTRO DELLE VERSIONI

VER/REV/BOZZA	DATA EMISSIONE	MODIFICHE	OSSERVAZIONI
1.0	01/10/2014	Documento iniziale	---
1.1	01/04/2015	Aggiunta paragrafo "Aderenza alla normativa del Manuale della Conservazione"	---
2.0	01/07/2015	Rivisitazione completa per Accreditamento	---
2.1	06/10/2015	Integrazioni varie	---
2.2	01/12/2015	Sostituzione Archivista	---

MANUALE DEL SERVIZIO DI CONSERVAZIONE

Sommario

1. SCOPO ED AMBITO DEL DOCUMENTO

Il presente manuale descrive il servizio di conservazione messo a disposizione da LAND S.r.l. (di seguito definita con l'acronimo LAND) ai sensi del Decreto del Presidente del Consiglio dei Ministri del 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" pubblicato nel Supplemento ordinario alla "Gazzetta Ufficiale„ n. 59 del 12 marzo 2014 - Serie generale.

In esso vengono definiti:

1. i soggetti coinvolti nei processi;
2. l'oggetto della conservazione;
3. gli obblighi e le responsabilità,
4. il processo di conservazione;
5. le modalità e le procedure attivate per garantire la conservazione permanente dei documenti;
6. le modalità per ottenere l'esibizione dei documenti/fascicoli conservati.

1.1. DATI IDENTIFICATIVI DEL MANUALE OPERATIVO

Il presente Manuale del Servizio di Conservazione è identificato con l'acronimo MSC ed è consultabile, nell'ultima versione rilasciata, firmata e marcata temporalmente, al seguente indirizzo internet:

http://www.land.it/it/sicurezza.html

1.2. RESPONSABILE DEL MANUALE

Il presente Manuale del Servizio di Conservazione è stato elaborato e verificato dal "Responsabile del Servizio di Conservazione".

Il Responsabile della redazione e del mantenimento del Manuale è:

Nome: Marco

Cognome: Polsi

Telefono: +39 06 657481.1

Email: polsi@land.it

PEC: marco.polsi@sicurezzapostale.it

2. TERMINOLOGIA (GLOSSARIO ED ACRONIMI)

2.1. GLOSSARIO

Di seguito si riporta il glossario dei termini contenuti nelle regole tecniche di cui all'articolo 71 del decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni in materia di documento informatico e sistema di conservazione dei documenti informatici che si aggiungono alle definizione del citato decreto ed a quelle del decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445 e successive modificazioni e integrazioni.

Accesso

Operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici.

Accreditamento

Riconoscimento, da parte dell'Agenzia per l'Italia digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione.

Affidabilità

Caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico.

Aggregazione documentale informatica

Aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'Ente.

Archivio

Complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualsiasi natura e formato, prodotti o comunque acquisiti da un Produttore durante lo svolgimento dell'attività.

Archivio informatico

Archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico.

Area organizzativa omogenea

Un insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445.

Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico

Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.

Autenticità

Caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico.

Base di dati

Collezione di dati registrati e correlati tra loro.

Certificatore accreditato

Soggetto, pubblico o privato, che svolge attività di emissione di certificati qualificati (per la firma digitale) e certificati di autenticazione (per le carte nazionali dei servizi) al quale sia stato riconosciuto, dall' Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza.

Ciclo di gestione

Arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo.

Classificazione

Attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati.

Codice

Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni.

Codice eseguibile

Insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici.

Conservatore accreditato

Soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, dall'Agenzia per l'Italia digitale.

Conservazione

Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione.

Coordinatore della Gestione Documentale

Responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 nei casi di amministrazioni che abbiano istituito più Aree Organizzative Omogenee.

Copia analogica del documento informatico

Documento analogico avente contenuto identico a quello del documento informatico da cui è tratto.

Copia di sicurezza

Copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 delle presenti regole tecniche per il sistema di conservazione.

Destinatario

Identifica il soggetto/sistema al quale il documento informatico è indirizzato.

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.

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.

Formato

Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.

Funzionalità aggiuntive

Le ulteriori componenti del sistema di protocollo informatico necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni.

Funzionalità interoperative

Le componenti del sistema di protocollo informatico finalizzate a rispondere almeno ai requisiti di interconnessione di cui all'articolo 60 del D.P.R. 28 dicembre 2000, n. 445.

Funzionalità minima

La componente del sistema di protocollo informatico che rispetta i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445.

Funzione di 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.

Glifo, Contrassegno elettronico, Timbro Digitale o Codice Bidimensionale

Come indicato nella Circolare AgID n. 62 del 30 aprile 2013 dal titolo "Linee guida per il contrassegno generato elettronicamente ai sensi dell'articolo 23-ter, comma 5 del CAD" nei vari contesti il contrassegno generato elettronicamente può essere indicato, anche in relazione alle specificità dello scenario implementato, con termini differenti, quali "Contrassegno elettronico", "Timbro digitale", "Codice bidimensionale", "Glifo", tutti i termini che sono da intendersi come sinonimi.

Identificativo univoco

Sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione.

Immodificabilità

Caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso.

Impronta

La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash.

Insieme minimo di metadati del documento informatico

Complesso dei metadati, la cui struttura è descritta nell'allegato 5 delle "Regole tecniche in materia di sistema di conservazione", da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta.

Integrità

Insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato.

Interoperabilità

Capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi.

Leggibilità

Insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti.

Log di sistema

Registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati.

Manuale di Conservazione

Strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 delle "Regole tecniche in materia di sistema di conservazione".

Manuale di Gestione

Strumento che descrive il sistema di gestione informatica dei documenti di cui all'articolo 5 delle regole tecniche del protocollo informatico ai sensi delle regole tecniche per il protocollo informatico D.P.C.M. 31 ottobre 2000 e successive modificazioni e integrazioni.

Memorizzazione

Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici.

Metadati

Insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 delle "Regole tecniche in materia di sistema di conservazione".

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.

Pacchetto di archiviazione

Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 delle "Regole tecniche in materia di sistema di conservazione" e secondo le modalità riportate nel manuale di conservazione.

Pacchetto di distribuzione

Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta.

Pacchetto di versamento

Pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione.

Pacchetto informativo

Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare.

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 di conservazione

Strumento, integrato con il sistema di classificazione per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445.

Piano generale della sicurezza

Documento per la pianificazione delle attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza.

Presa in carico

Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione.

Processo di conservazione

Insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 10 delle regole tecniche del sistema di conservazione.

Produttore

Persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale.

Rapporto di versamento

Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.

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.

Registrazione informatica

Insieme delle informazioni risultanti da transazioni informatiche o dalla presentazione in via telematica di dati attraverso moduli o formulari resi disponibili in vario modo all'utente.

Registro particolare

Registro informatico di particolari tipologie di atti o documenti; nell'ambito della pubblica amministrazione è previsto ai sensi dell'articolo 53, comma 5 del D.P.R. 28 dicembre 2000, n. **445.**

Registro di protocollo

Registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti.

Repertorio informatico

Registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche con cui si formano altri atti e documenti o indici di atti e documenti secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica.

Responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi

Dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre

2000, n. 445, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione.

Rapporto di versamento

Documento informatico che attesta l'avvenuta presa in carico, da parte del sistema di conservazione, dei pacchetti di versamento inviati dal Produttore

Responsabile della conservazione

Responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 delle "Regole tecniche in materia di sistema di conservazione".

Responsabile del trattamento dei dati

La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

Responsabile della sicurezza

Soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza.

Riferimento temporale

Informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento.

Scarto

Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale.

Sistema

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.

Sistema di conservazione

Sistema di conservazione dei documenti informatici di cui all'articolo 44 del Codice.

Sistema di gestione informatica dei documenti

Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445; per i privati è il sistema che consente la tenuta di un documento informatico.

Staticità

Caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione

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.

Transazione informatica

Particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche della base di dati Testo unico decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni.

Ufficio utente

Riferito ad un area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico

Utente

Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.

Versamento agli archivi di stato

Operazione con cui il responsabile della conservazione di un organo giudiziario o amministrativo dello Stato effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali.

2.2. ACRONIMI

AgID - Agenzia per l'Italia Digitale (subentrato a DigitPA dal 2012)

AIPA - Agenzia per l'Informatica nella Pubblica Amministrazione

ASP - Application Service Provider

CA - Certification Authority

CAD - Codice dell'Amministrazione Digitale (decreto legislativo 7 marzo 2005 n. 82 e successive modifiche)

CAS - Content-Addressed Storage

CDes - Soluzione di Conservazione Digitale di LAND

CNIPA - Centro Nazionale per l'Informatica nella Pubblica Amministrazione (subentrato all'AIPA)

D.LGS. - Decreto legislativo

DigitPA - Organismo governativo che dal 2009 al 2012 ha preso il posto del CNIPA

DM - Decreto Ministeriale

DPCM - Decreto del Presidente del Consiglio dei Ministri

DPR - Decreto del Presidente della Repubblica

Formati Messaggi di posta elettronica - Ai fini della conservazione, per preservare l'autenticità dei messaggi di posta elettronica, lo standard a cui fare riferimento è RFC 2822/MIME per la gestione degli allegati ci si riferisce ai precedenti formati meglio descritti e approfonditi nell'allegato 2 del DPCM 3 dicembre 2013.

FE - Firma Elettronica

FEA - Firma Elettronica Avanzata

FEQ - Firma Elettronica Qualificata

FD - Firma Digitale

GSC - Gestore del Servizio di Conservazione

GU - Gazzetta Ufficiale della Repubblica Italiana

HSM -Hardware Security Module

MEF - Ministero dell'Economia e delle Finanze

NTP - Network Time Protocol

ODF - Open Document Format, abbreviazione di OASIS Open Document Format for Office Applications (Formato OASIS Open Document per Applicazioni da Ufficio)

PA - Pubblica Amministrazione

PDF – Portable Document Format

PDF/A 1b – formato detto comunemente anche (PDF/A) per l'archiviazione nel lungo periodo di documenti elettronici, è basato sulla versione 1.4 del formato PDF di Adobe Systems Inc

PEC - Posta Elettronica Certificata

PU - Pubblico Ufficiale

REST - Representational State Transfer

RdC - Responsabile della Conservazione

RSC - Responsabile del Servizio di Conservazione

SaaS - Service as a Service

SOAP - Simple Object Access Protocol

SPID - Sistema Pubblico per la gestione dell'Identità Digitale

TSA - Time Stamping Authority

TSS - Time Stamping Service

TU - Testo Unico

UDDI - Universal Description Discovery and Integration

URL - Universal Resource Locator

UTC - Universal Coordinated Time – Tempo Universale Coordinato

WORM - Write Once Read Many

W3C - World Wide Web Consortium

WSDL - Web Services Description Language

XML - eXtensible Markup Language

XLST - EXtensible Stylesheet Language

3. NORMATIVA E STANDARD DI RIFERIMENTO

3.1. CONTESTO NORMATIVO

Il sistema di Conservazione Digitale di LAND, è stato realizzato in piena conformità alla normativa vigente in materia di conservazione dei documenti informatici.

Nel caso non siano indicate una versione e una data specifica si intende, come riferimento, la più recente versione disponibile del documento citato.

- **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;
- **DPR 28 dicembre 2000, n. 445**, e successive modificazioni - "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa" o "TUDA";
- **DPR 11 febbraio 2005, n. 68** - Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3;
- **Decreto legislativo 30 giugno 2003, n. 196**, e successive modificazioni, recante "Codice in materia di protezione dei dati personali";
- **Decreto legislativo 22 gennaio 2004, n. 42**, e successive modificazioni, recante "Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137";
- **Decreto legislativo 7 marzo 2005, n. 82**, e successive modificazioni - "Codice dell'amministrazione digitale" o "CAD";
- **Circolare n. 5/d Agenzia delle dogane del 25 gennaio 2005** - D.M. 23/1/2004 recante "modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di supporto".
- **Circolare dell'Agenzia delle Entrate n. 45/E del 19 ottobre 2005** - 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;
- **Circolare dell'Agenzia delle Entrate n. 36/E del 6 dicembre 2006** - Decreto ministeriale 23 gennaio 2004; Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici e alla loro riproduzione in diversi tipi di supporto;
- **Risoluzione Agenzia delle entrate n. 298 del 18 ottobre 2007** - Istanza di interpello, articolo 11 legge 27 luglio 2002, n. 212, - Conservazione su supporti informatici delle copie delle dichiarazioni da parte dei CAF - Adempimenti correlati e termine per l'invio dell'impronta dell'archivio informatico;
- **Risoluzione n. 349 Agenzia delle entrate del 28 novembre 2007** - IVA - biglietto di trasporto elettronico - articolo 1 del decreto ministeriale 30 giugno 1992 Istanza di interpello -ART.11, legge 27 luglio 2000, n. 212;

- **Risoluzione n. 67/E Agenzia delle entrate del 28 febbraio 2008** - Articoli 21 e 39 del D.P.R. 26 ottobre 1972, n.633, D.M. 23 gennaio 2004, conservazione sostitutiva dei documenti rilevanti ai fini delle disposizioni tributarie- obblighi del vettore o dello spedizioniere. Messa a disposizione delle fatture tramite strumenti elettronici;

- **Risoluzione n.85/E Agenzia delle entrate del 11 marzo 2008** - Conservazione sostitutiva delle distinte meccanografiche di fatturazione;

- **DM 09 luglio 2008** - Modalità di tenuta e conservazione del libro unico del lavoro e disciplina del relativo regime transitorio;

- **Risoluzione n. 354/E Agenzia delle entrate del 8 agosto 2008** - Interpello – ALFA Ass.ne prof.le dott. comm. e avv. – Articolo 3, comma 9-bis, del D.P.R. n. 322 del 1998 – Incaricati della trasmissione delle dichiarazioni – Conservazione delle copie delle dichiarazioni – Obbligo di sottoscrizione da parte del contribuente delle copie conservate dall'incaricato su supporti informatici;

- **Circolare 20/2008 - Ministero del lavoro, della salute e delle politiche sociali del 21/08/2008** - Libro Unico del Lavoro e attività ispettiva – articoli 39 e 40 del decreto legge n. 112 del 2008: prime istruzioni operative al personale ispettivo;

- **Regolamento ISVAP n. 27 del 14 ottobre 2008** -Tenuta dei registri assicurativi;
- **Provvedimento Agenzia delle entrate del 25 ottobre 2010** - Provvedimento attuativo ella comunicazione dell'impronta relativa ai documenti informatici rilevanti ai fini tributari, ai sensi dell'articolo 5 del decreto 23 gennaio 2004;
- **Decreto legge del 06 dicembre 11, n. 201** - Estratto Art.40, comma 4 - Libro Unico del Lavoro;
- **Decreto legge 24 gennaio 2012, n. 1** - Estratto – Dematerializzazione Contrassegni Assicurativi;
- **Circolare n. 5/E Agenzia delle entrate del 29 febbraio 2012** - Quesiti riguardanti la comunicazione dell'impronta relativa ai documenti informatici rilevanti ai fini tributari, ai sensi dell'articolo 5 del decreto 23 gennaio 2004 e del provvedimento del Direttore dell'Agenzia delle Entrate del 25 ottobre 2010;
- **Circolare MEF del 31 marzo 2014 n. 1/DF** – circolare interpretativa del DECRETO 3 aprile 2013, n. 55 - 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 Ministero dell'Economia e delle Finanze 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. (Ministero dell'economia e delle finanze) – in vigore dal 27.06.2014;
- **Circolare Agenzia delle Entrate del 24 giugno 2014 n. 18/E** - OGGETTO: IVA. Ulteriori istruzioni in tema di fatturazione.
- **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. (15A00107) (GU Serie Generale n.8 del 12-1-2015)
- **Regolamento UE n. 910/2014** - eIDAS Regulation - Identification and trusted services for electronic transactions in the internal market.

- **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.

3.2. RIFERIMENTI TECNICI

Il sistema di conservazione digitale di LAND, è stato realizzato in conformità dei seguenti riferimenti tecnici.

- **Decreto 02 novembre 2005** – Ministero per l'innovazione e le tecnologie - Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata;
- **D.P.C.M. 22 Febbraio 2013** - Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali;
- **Decreto 3 aprile 2013, n. 55** - 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.
- **D.P.C.M. 03 Dicembre 2013** - Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.
- **D.P.C.M. 03 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.

3.3. STANDARD DI RIFERIMENTO

Il sistema di conservazione digitale di LAND, è stato realizzato in conformità dei seguenti standard di riferimento.

- **ISO 14721:2012 OAIS** (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- **ISO/IEC 27001:2013**, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- **ETSI TS 101 533-1 V1.3.1** (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- **ETSI TR 101 533-2 V1.3.1** (2012-04)Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- **UNI 11386:2010 Standard SInCRO** - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- **ISO 15836:2009** Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

4. RUOLI E RESPONSABILITÀ

4.1. TABELLA DI RIFERIMENTO

RUOLI	RESPONSABILE DI APPARTENENZA
Gestore del Servizio di Conservazione (GSC)	LAND
Produttore	Cliente
Responsabile della Conservazione (RdC)	Cliente
Referenti del Cliente	Cliente
Responsabile del Servizio di Conservazione	Nominato dal GSC
Utenti	Cliente e/o Terzi con espressa autorizzazione

Il **Gestore del Servizio di Conservazione (GSC)** è l'Azienda titolare del Servizio di Conservazione dei documenti da conservare che definisce insieme a Responsabile del Servizio di Conservazione le modalità di affidamento, di controllo e di supervisione del procedimento di conservazione.

Il **Cliente** è il soggetto titolare e responsabile a tutti gli effetti dei documenti che devono essere sottoposti al processo di conservazione digitale; è il soggetto che sottoscrive il Contratto con il **GSC** ed è **l'unico responsabile del contenuto del pacchetto di versamento**, trasmette tale pacchetto al sistema di conservazione secondo i modi, nei termini ed in conformità a quanto stabilito nel presente Manuale, nel Contratto di Servizio e nei rispettivi allegati.

Ai fini dello svolgimento del Servizio di Conservazione il **Cliente**, con specifica delega, nomina **LAND** come **Gestore del Servizio di Conservazione** dei propri documenti informatici.

Il **Responsabile del Servizio di Conservazione (RSC)** è nominato dal **GSC**.

Il **Produttore** è il Cliente e le eventuali persone fisiche dallo stesso incaricate della produzione, formazione, emissione e sottoscrizione dei documenti informatici da inviare al Servizio di Conservazione.

Il **Responsabile della Conservazione (RdC)** è il Cliente, nella persona fisica dallo stesso indicata nell'apposito allegato al Contratto di Servizio.

Il **RSC** è colui che ha definito le politiche complessive del sistema di conservazione esplicitate nel presente Manuale e che si occupa di darne attuazione attraverso i Servizi oggetto del Contratto.

Il **RdC** governa la gestione dei processi di formazione dei documenti informatici con piena responsabilità, in relazione al modello organizzativo adottato anche in conseguenza ed in funzione del Contratto di Servizio.

I **Referenti** del Cliente sono le persone fisiche che il Cliente indica a LAND quali riferimenti tecnico ed organizzativo per gli aspetti che riguardano le comunicazioni relative all'erogazione ed all'organizzazione del Servizio di Conservazione.

Marco Polsi, quale **Responsabile del Servizio di Conservazione dei Documenti Informatici** del Cliente per conto di **LAND**, agisce nei limiti della delega ad esso conferita e nell'osservanza degli obblighi ivi previsti nonché nel rispetto della normativa vigente in tema di Conservazione Digitale di Documenti Informatici e delle presenti prescrizioni agendo attraverso le persone fisiche da LAND stessa formalmente incaricate.

L'attività del **GSC** riguarda la sola Conservazione Digitale dei Documenti Informatici del Cliente, senza alcuna responsabilità, intervento ed accesso al contenuto degli stessi.

A carico del **GSC**, non è posto alcun obbligo e/o dovere di elaborazione dei documenti informatici inviati in Conservazione al fine di estrarre i relativi metadati che, pertanto, devono essere forniti e associati ai rispettivi documenti a cura e carico del Cliente (a meno di ulteriori specifici accordi non previsti nel presente Manuale del Servizio di Conservazione).

Il **RSC** opera nell'osservanza di quanto stabilito nel presente Manuale ed è responsabile nell'apportare tutte le modifiche, le integrazioni e gli aggiornamenti necessari e/o conseguenti al mutato contesto tecnico-giuridico della normativa regolante la Conservazione Digitale di Documenti Informatici.

L'**utente** è il soggetto che richiede al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge. Tali informazioni vengono fornite dal sistema di conservazione secondo le modalità previste nel presente Manuale.

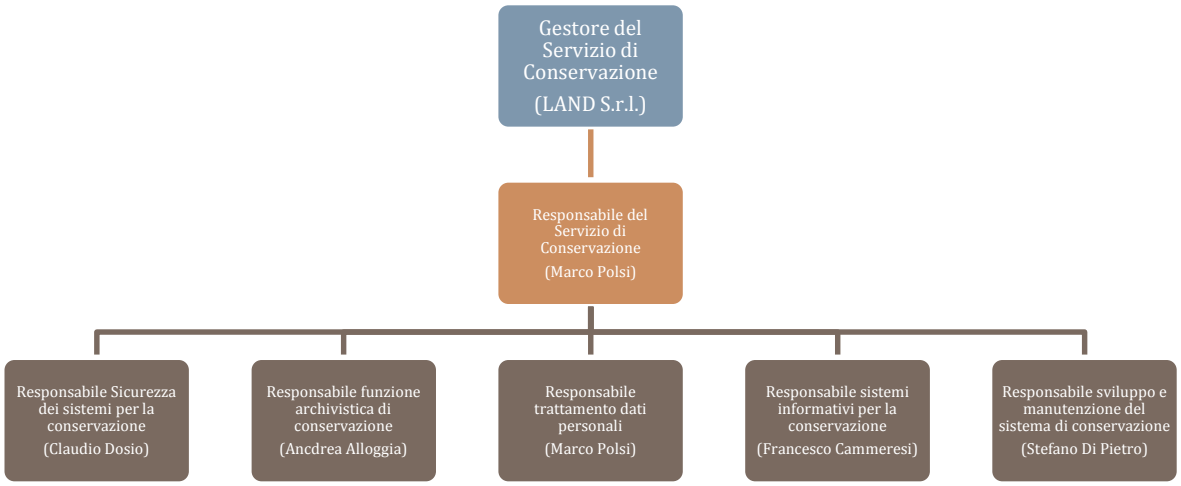
Come già anticipato, il processo di Conservazione impone al Cliente l'istituzione di una struttura ed una organizzazione interna, coerente con le proprie politiche di efficienza gestionale, che garantisca la piena osservanza alle disposizioni normative di riferimento e di quanto previsto dal presente Manuale, dal Contratto di Servizio e dai rispettivi allegati.

A tale scopo, in base alle specifiche necessità, il Cliente deve, sia dal punto di vista dell'impostazione operativa delle attività propedeutiche alla Conservazione Digitale dei propri documenti informatici sia dal punto di vista della scelta delle risorse coinvolte nel processo, organizzare il lavoro all'interno della propria organizzazione affinché esso venga svolto secondo i principi stabiliti dalla normativa in materia nonché dalle specifiche Regole Tecniche.

Tutto il personale del **GSC** è stato assunto nel rispetto di politiche rigorose volte ad accertarne, tra l'altro, l'alto grado di professionalità nonché i requisiti morali e di onorabilità.

5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1. ORGANIGRAMMA



5.2. STRUTTURE ORGANIZZATIVE

RUOLI	NOMINATIVO	PERIODO NEL RUOLO
Responsabile del Servizio di Conservazione (RSC)	Marco Polsi	dal 2 gennaio 2015
Responsabile Sicurezza dei sistemi per la conservazione (RSSC)	Claudio Dosio	dal 2 gennaio 2015
Responsabile funzione archivistica di conservazione (RFAC)	Andrea Alloggia	dal 1 dicembre 2015
Responsabile trattamento dati personali (RTDP)	Marco Polsi	dal 20 luglio 2015
Responsabile sistemi informativi per la conservazione (RSIC)	Francesco Cammeresi	dal 2 gennaio 2015
Responsabile sviluppo e manutenzione del sistema di conservazione (RSMSC)	Stefano Di Pietro	dal 2 gennaio 2015

5.2.1. GESTORE DEL SERVIZIO DI CONSERVAZIONE

Il Gestore del Servizio di Conservazione Digitale è:

LAND S.r.l.

Indirizzo della Sede Legale: Via di Affogalasino, 40 - 00148 ROMA

Indirizzo primario erogazione servizi di conservazione (CED02): c/o LAND Via di Affogalasino, 40 - 00148 ROMA

Indirizzo secondario erogazione servizi conservazione: c/o Aruba S.p.A. Via Piero Gobetti, 96 - 52100 Arezzo.

CCIAA, Partita IVA e Codice Fiscale: IT04554571002

Amministratore Unico e Legale Rappresentante: Ettore Alloggia

Telefono: +39 06 657481.1

Fax: +39 06 657481.264

Numero Verde: 800.910598

Posta elettronica: land_conservazione@land.it

Posta Elettronica Certificata: land_conservazione@pec.it

Indirizzo internet: www.land.it

Numero Verde: 800.910598

Le sottoscrizioni digitali, necessarie per corretta esecuzione del processo di conservazione, saranno apposte dal Rappresentante Legale della LAND, ovvero dal soggetto espressamente individuato dalla stessa Società, in questo caso la persona individuata è il Responsabile della Conservazione.

5.2.2. RESPONSABILE DEL SERVIZIO DI CONSERVAZIONE

Il Responsabile del Servizio di Conservazione è:

Nome: **Marco**

Cognome: **Polsi**

Telefono: +39 06 657481.1

Email: polsi@land.it

PEC: marco.polsi@sicurezzapostale.it

Compiti specifici:

- definizione e attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione;
- definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente;

- 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.

DELEGATO PER LE ATTIVITÀ DI CONSERVAZIONE

Il Responsabile della Conservazione può delegare lo svolgimento, di alcune delle proprie attività, ad una o più persone che per, competenza ed esperienza, garantiscano la corretta esecuzione delle operazioni di conservazione.

Eventuali delegati sono descritti nell'allegato "A" del presente manuale.

5.2.3. RESPONSABILE SICUREZZA DEI SISTEMI PER LA CONSERVAZIONE

Il Responsabile Sicurezza dei Sistemi per la Conservazione è:

Nome: **Claudio**

Cognome: **Dosio**

Telefono: +39 06 657481.1

Email: dosio@land.it

Compiti specifici:

- 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.

DELEGATO PER LE ATTIVITÀ SICUREZZA DEI SISTEMI PER LA CONSERVAZIONE

Il Responsabile per le attività di Sicurezza dei Sistemi di Conservazione può delegare lo svolgimento, di alcune delle proprie attività, ad una o più persone che per, competenza ed esperienza, garantiscano la corretta esecuzione delle operazioni di conservazione.

Eventuali delegati sono descritti nell'allegato "A" del presente manuale.

5.2.4. RESPONSABILE FUNZIONE ARCHIVISTICA DI CONSERVAZIONE

Il Responsabile della funzione archivistica di conservazione è:

Nome: **Andrea**

Cognome: **Alloggia**

Telefono: +39 06 657481.1

Email: a.alloggia@land.it

Compiti specifici:

- definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; - definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici;
- monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione;
- 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.

DELEGATO PER LE ATTIVITÀ DI RESPONSABILE DELLA FUNZIONE ARCHIVISTICA DI CONSERVAZIONE

Il Responsabile della funzione archivistica di conservazione può delegare lo svolgimento, di alcune delle proprie attività, ad una o più persone che per, competenza ed esperienza, garantiscano la corretta esecuzione delle operazioni di conservazione.

Eventuali delegati sono descritti nell'allegato "A" del presente manuale.

5.2.5. RESPONSABILE DEL TRATTAMENTO DATI PERSONALI

Il Responsabile trattamento dati personali, appositamente delegato dal Titolare del trattamento dei Dati Personali di LAND, è:

Nome: **Marco**

Cognome: **Polsi**

Telefono: +39 06 657481.1

Email: polsi@land.it

Compiti specifici:

- 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.

DELEGATO PER LE ATTIVITÀ DI RESPONSABILE DEL TRATTAMENTO DATI PERSONALI

Il Responsabile per le attività del trattamento dei dati personali può delegare lo svolgimento, di alcune delle proprie attività, ad una o più persone che per, competenza ed esperienza, garantiscano la corretta esecuzione delle operazioni di conservazione.

Eventuali delegati sono descritti nell'allegato "A" del presente manuale.

5.2.6. RESPONSABILE SISTEMI INFORMATIVI PER LA CONSERVAZIONE

Il Responsabile dei Sistemi Informativi per la Conservazione è:

Nome: **Francesco**

Cognome: **Cammeresi**

Telefono: +39 06 657481.1

Email: cammeresi@land.it

Compiti specifici:

- 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 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.

DELEGATO PER LE ATTIVITÀ DI RESPONSABILE SISTEMI INFORMATIVI PER LA CONSERVAZIONE

Il Responsabile per le Responsabile dei Sistemi Informativi per la Conservazione delegare lo svolgimento, di alcune delle proprie attività, ad una o più persone che per, competenza ed esperienza, garantiscano la corretta esecuzione delle operazioni di conservazione.

Eventuali delegati sono descritti nell'allegato "A" del presente manuale.

5.2.7. RESPONSABILE SVILUPPO E MANUTENZIONE DEL SISTEMA DI CONSERVAZIONE

Il Responsabile Sviluppo e Manutenzione del Sistema Conservazione è:

Nome: **Stefano**

Cognome: **Di Pietro**

Telefono: +39 06 657481.1

Email: dipietro@land.it

Compiti specifici:

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

DELEGATO PER LE ATTIVITÀ DI RESPONSABILE SVILUPPO DEL SISTEMA DI CONSERVAZIONE

Il Responsabile per lo Sviluppo e Manutenzione del Sistema può delegare per lo svolgimento di alcune delle proprie attività, ad una o più persone che, per competenza ed esperienza, garantiscano la corretta esecuzione delle operazioni di conservazione.

Eventuali delegati sono descritti nell'allegato "A" del contratto di servizio.

6. OGGETTI SOTTOPOSTI A CONSERVAZIONE

6.1. OGGETTI CONSERVATI

Sono principalmente accettati, per il Servizio di Conservazione, i documenti nei seguenti formati:

- PDF versione 1.4 o successive;
- PDF/A 1b;
- TXT;
- EML;
- XML.

I documenti sottoscritti sono accettati nei formati:

- P7M (CAdES);
- PDF (PAdES);
- XML (XAdES).

I documenti marcati temporalmente sono accettati nei seguenti formati:

- TSR;
- TST;
- M7M (nel caso si parta da un file P7M);
- PDF (nel caso dei PDF CAdES l'estensione rimane invariata).

La Conservazione Digitale, come previsto dalla normativa vigente, è possibile per un documento, per un fascicolo, o per un'aggregazione documentale informatica.

Non è consentita la conservazione di documenti cifrati anche se solo parzialmente.

In caso di necessità e previo accordo tra le parti, possono essere conservati tutti i formati documentali previsti dall'attuale normativa.

I Documenti Informatici inviati al Servizio di Conservazione devono essere statici (non devono contenere macro atte a modificarne nel tempo i contenuti) e possono essere muniti di sottoscrizione elettronica e/o marca temporale.

6.1.1. METADATI

Come previsto dall'art. 3, c. 1 del Decreto della Presidenza del Consiglio dei Ministri 3 dicembre 2013 Regole tecniche in materia di sistema di conservazione, il sistema di conservazione assicura, dalla presa in carico dal Produttore fino all'eventuale scarto o alla restituzione, la conservazione di documenti digitali.

Questo avviene tramite l'adozione di regole, procedure e tecnologie degli oggetti in esso conservati e grazie a questo ne garantisce, oltre all'autenticità, all'integrità, all'affidabilità e alla leggibilità nel tempo, anche la reperibilità.

Al fine di rendere agevole ed efficiente la ricerca di un documento, di un fascicolo, o di un'aggregazione documentale informatica conservati sarà necessario individuare dei metadati, ovvero un insieme di dati da associare all'oggetto informatico o al fascicolo informatico che ne descrivano il contenuto e lo identifichino all'interno del sistema.

LAND, in piena conformità con le Regole tecniche, individua un insieme minimo di metadati che, insieme ai metadati aggiuntivi, saranno indicati dal Produttore nel Contratto di Servizio.

Non saranno accettati in conservazione oggetti con metadati incompleti e comunque che non corrispondano almeno ai seguenti set di metadati minimi previsti dalla normativa:

- del documento informatico,
- del documento informatico avente rilevanza tributaria,
- del fascicolo informatico o dell'aggregazione documentale informatica,
- del documento informatico sanitario,
- del fascicolo informatico sanitario.

6.2. PACCHETTO DI VERSAMENTO

I Pacchetti di Versamento possono essere gestiti in 3 modalità in base alle esigenze ed alla tipologia di documento da archiviare.

Il Pacchetto di Versamento per Documenti Singoli (è composto da una Cartella (directory) principale contenente una serie di Cartelle Secondarie ed un file XML di indice chiamato input_XXXX.xml (XXXX è un codice numerico generato dal sistema).

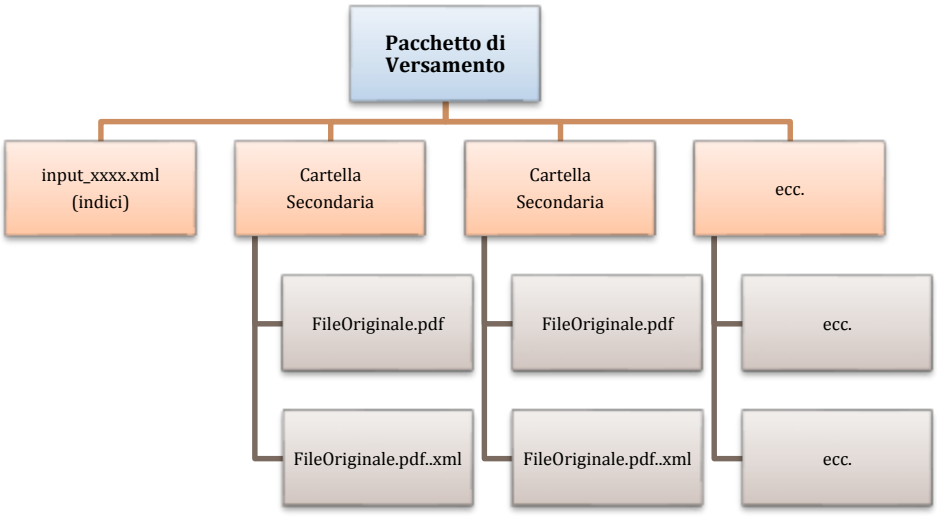


Figura 1 - Esempio di struttura del Pacchetto di Versamento per documento

Il File input_XXXX.xml contiene gli indici dei file del pacchetto di versamento.

Ogni singola directory è dedicata ad un documento del pacchetto (ne replica anche il nome comprensivo di estensione).

E' possibile gestire anche gruppi di documenti (ad esempio una fattura e relativo allegato) che non devono essere confusi con il Fascicolo che è gestito in modalità diversa.

La posizione su disco del pacchetto è mappata all'interno della struttura del file input_XXXX.xml.

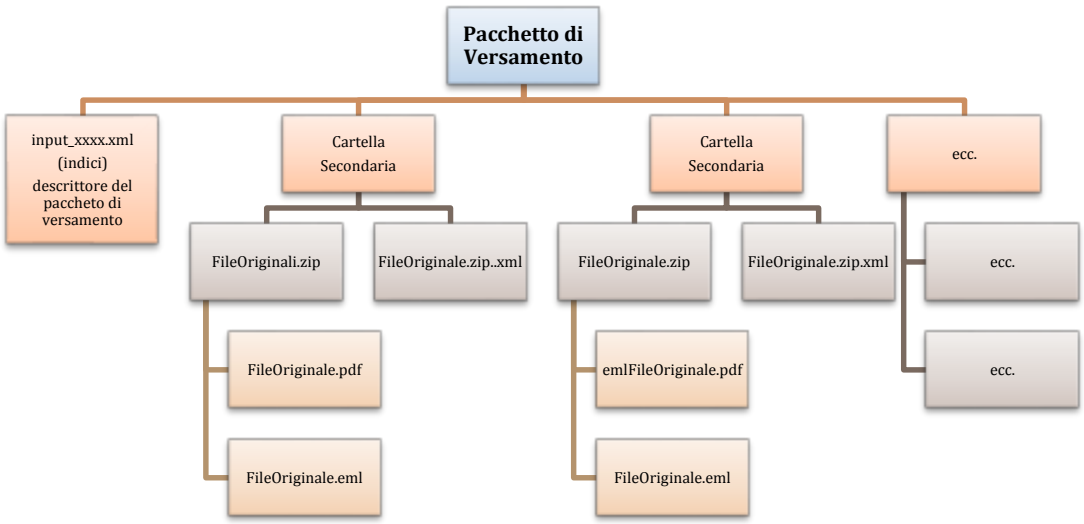


Figura 2 - Esempio di struttura del Pacchetto di Versamento per gruppi di documenti

Il Pacchetto di Versamento può gestire anche Fascicoli Informatici, in questo caso la struttura è composta da una Cartella principale (Figura 2), che include una serie di cartelle secondarie ed il file XML di indice chiamato input_XXXX.xml (codice numerico generato dal sistema).

Ogni Cartella Secondaria contiene, a sua volta, il file zip con tutti i documenti relativi al Fascicolo Informatico ed il relativo file XML di indice, detto file è denominato con lo stesso nome del file originale ma con l'aggiunta dell'estensione .xml.

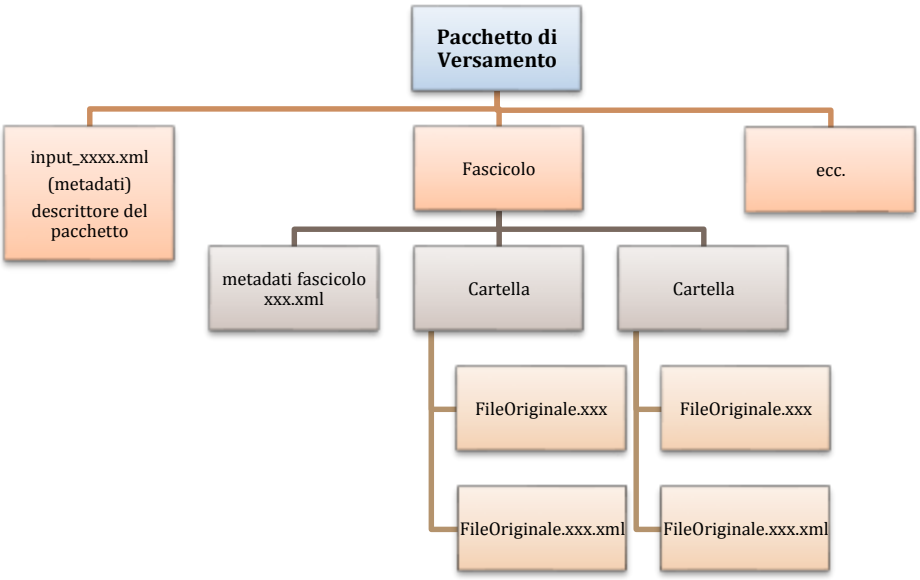


Figura 3 - Esempio di struttura del Pacchetto di Versamento per fascicoli

Il Servizio di Conservazione può analizzare il pacchetto di versamento (in modalità manuale o automatica) e registrarla nella coda di versamento, in questa fase nessun file viene firmato, marcato, spostato, archiviato o indicizzato.

E' possibile a breve una generalizzazione del pacchetto di versamento che ci permetterà di utilizzare la presente struttura anche per documenti non organizzati in fascicoli, la data di attivazione della nuova modalità verrà tracciata nel presente manuale.

La coda di versamento è un passaggio preparatorio per il successivo Pacchetto di Archiviazione.

6.3. PACCHETTO DI ARCHIVIAZIONE

Il Pacchetto di Archiviazione è salvato per intero in una directory situata all'interno della struttura del Software di Archiviazione la cui cartella specifica può variare a seconda del sistema di storage utilizzato.

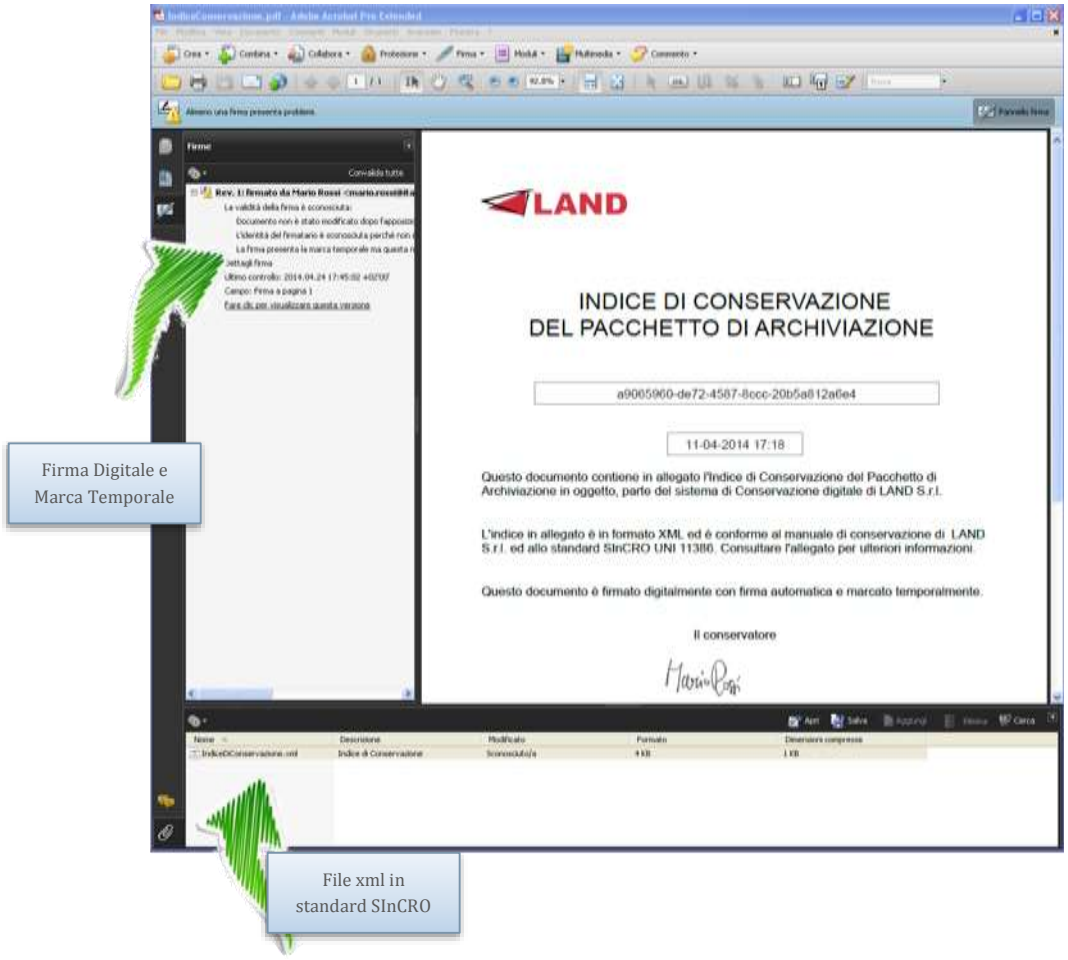
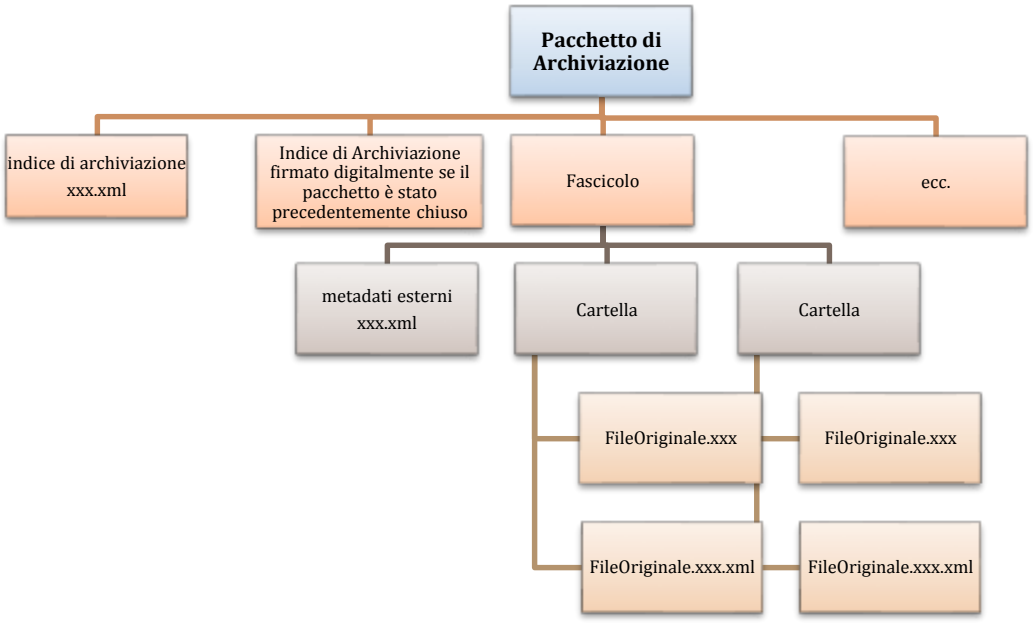


Figura 4 - Esempio di indice di conservazione

Il Pacchetto di Archiviazione è composto da un PDF/A 1b a cui è allegato (attachment PDF) un Indice di Conservazione (xml) generato in formato **UNI 11386:2010** (Standard SInCRO).

Nel file xml sono presenti la lista completa dei documenti del pacchetto ed i riferimenti ai file xml esterni contenenti i metadati di ogni singolo documento.

iCDeS, all'atto della chiusura del pacchetto di archiviazione (automatica o manuale), oltre alla Firma Elettronica Qualificata del RSC appone il riferimento temporale nell'Indice di Conservazione (xml UNI 11386:2010) e, se richiesto, applica la Marca Temporale al PDF.



Di seguito descriviamo la struttura del file xml dell'Indice di Conservazione contenuto come attachment generato in formato UNI 11386:2010 (Standard SInCRO).

Nella seguente figura sono descritti il nome, la versione ed il produttore del software di Conservazione.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns1:IdC xmlns:ns1="http://www.uni.com/U3011/sincro/">
    <ns1:SelfDescription>
        <ns1:ID>84401e6a-db54-4aa2-b255-b6996be96080</ns1:ID>
        <ns1:CreatingApplication>
            <ns1:Name>CDeS</ns1:Name>
            <ns1:Version>1.0.0</ns1:Version>
            <ns1:Producer>LAND</ns1:Producer>
        </ns1:CreatingApplication>
    </ns1:SelfDescription>
```

In questa invece troviamo la descrizione del cosiddetto Volume di Conservazione dove troviamo la label (tipologia/categoria/archivio) e l'ID identificativo del volume.

```
<ns1:VdC>
    <ns1:ID>84401e6a-db54-4aa2-b255-b6996be96080</ns1:ID>
    <ns1:VdCGroup>
        <ns1:Label>fatture</ns1:Label>
        <ns1:ID>fatture</ns1:ID>
        <ns1:Description ns1:language="IT">fatture</ns1:Description>
    </ns1:VdCGroup>
</ns1:VdC>
```

Di seguito troviamo la parte riguardate il riferimento al file esterno xml contenente i metadati del fascicolo completo del relativo ID, Path e Hash del file.

```
        <ns1:MoreInfo ns1:XMLScheme="file://null">
            <ns1:ExternalMetadata ns1:format="xml">
                <ns1:ID>000281740707586260801 4_meta</ns1:ID>
                <ns1:Path>file:1-000281740707586260801 4/file:000281740707586260801 4.xml</ns1:Path>
                <ns1:Hash ns1:function="SHA256">6f3be08259e93bb1ac891247054544c92b69b81bb1023711c3c59c8abf5738a2
</ns1:Hash>
            </ns1:ExternalMetadata>
        </ns1:MoreInfo>
```

Di seguito troviamo la parte riguardate i veri e propri file archiviati, ovviamente questa parte sarà ripetuta per quanti file o fascicoli sono presenti nel pacchetto.

Sono presenti sia il file del documento sia il file xml dei metadati (tutti e due vengono salvati con lo stesso nome ma con estensioni diverse) i relativi ID, Path e Hash dei file.

```
    <ns1:FileGroup>
        <ns1:Label>000281740707586260801 4</ns1:Label>
        <ns1:File ns1:format="application/octet-stream" ns1:extension="p7m" ns1:encoding="binary">
            <ns1:ID>IT00000000000_14001.xml.p7m</ns1:ID>
            <ns1:Path>file:1-000281740707586260801 4/IT00000000000_14001.xml.p7m</ns1:Path>
            <ns1:Hash ns1:function="SHA256">f243c224ef80a68288905c44cb161fdcd2d32fcfc5156ec7de2fd348d954c78a</ns1:Hash>
            <ns1:MoreInfo ns1:XMLScheme="file://null">
                <ns1:ExternalMetadata ns1:format="Application/xml" ns1:encoding="binary">
                    <ns1:ID>IT00000000000_14001.xml.p7m_meta</ns1:ID>
                    <ns1:Path>file:1-000281740707586260801 4/IT00000000000_14001.xml.p7m.xml</ns1:Path>
                    <ns1:Hash ns1:function="SHA256">7768cca18b3d0294f6568545179f27df4ea2c1da2690f6387ae6784ed5bd3aa9
  </ns1:Hash>
                </ns1:ExternalMetadata>
            </ns1:MoreInfo>
        </ns1:File>
```

Questa è la parte di chiusura dell'Indice di Conservazione e sono presenti i dati del Conservatore.

```
<ns1:Process>
        <ns1:Agent ns1:role="PreservationManager" ns1:type="person">
            <ns1:AgentName>
                <ns1:NameAndSurname>
                    <ns1:FirstName>Marco</ns1:FirstName>
                    <ns1:LastName>Polsi</ns1:LastName>
                </ns1:NameAndSurname>
            </ns1:AgentName>
            <ns1:Agent_ID ns1:scheme="TaxCode">PLSMRC65H03H501I</ns1:Agent_ID>
        </ns1:Agent>
        <ns1:TimeReference>
            <ns1:TimeInfo>2015-04-22T12:29:56.465+02:00</ns1:TimeInfo>
        </ns1:TimeReference>
        <ns1:LawAndRegulations ns1:language="IT">DPCM 13 novembre 2014</ns1:LawAndRegulations>
    </ns1:Process>
```

Di seguito un esempio di un xml di metadati salvato insieme al file originale.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<fatture>
    <cognome>VERDE</cognome>
    <nome>MARIAGRAZIA</nome>
    <denominazione>INPS - ISTITUTO NAZIONALE DELLA PREVIDENZA
SOCIALE</denominazione>
    <codice_fiscale>80078750587</codice_fiscale>
    <partita_iva>IT02121151001</partita_iva>
    <cig>37372024A6</cig>
    <importo_inclusa_iva>294020,77</importo_inclusa_iva>
    <numero_fattura>7200000006</numero_fattura>
    <data_fattura>2014-07-31</data_fattura>
    <numero_di_invio_a_sdi>14006</numero_di_invio_a_sdi>
</fatture>
```

La chiusura dei Pacchetti di Archiviazione è solitamente mensile, fatte salve necessità particolari del Cliente o costrizioni normative ed è comunque prevista nel Contratto di Servizio.

6.4. PACCHETTO DI DISTRIBUZIONE

Il Pacchetto di Distribuzione consiste in una cartella contenente al suo interno il file o i file ricercati il relativo Indice del Pacchetto di Archiviazione.

Il Pacchetto di Distribuzione può comprendere una ulteriore Cartella di Servizio contente gli installer dei programmi necessari per la visualizzazione e la verifica dei file in esso contenuto.

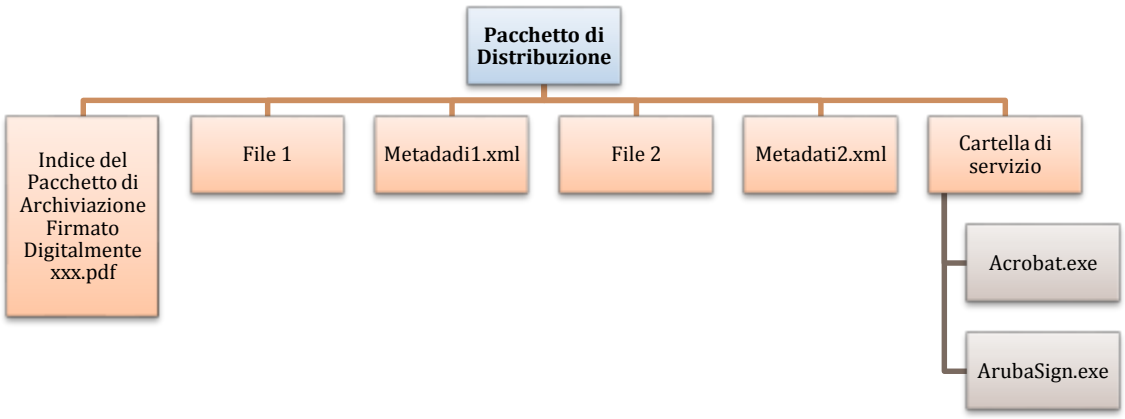


Figura 5 - Esempio di struttura del pacchetto di Distribuzione

7. IL PROCESSO DI CONSERVAZIONE

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

In questa fase il Produttore invia a GSC la richiesta di attivazione del servizio tramite la compilazione e la Firma Digitale del Contratto di Servizio che regola, tra l'altro, l'invio dei Pacchetti di Versamento.

Il RSC, verifica se il Contratto di Servizio è stato compilato correttamente ed inoltra la richiesta di attivazione.

Il RSC, una volta ricevuta la richiesta, si impegna a valutarne l'impatto stimando la data di evasione e fornendo al Produttore la pianificazione delle fasi successive.

Se la richiesta di configurazione implica un aggravio di costi, verrà fornita parallelamente al produttore la quotazione economica dell'attività redatta dal Referente Commerciale di riferimento.

L'acquisizione dei Pacchetti di versamento avviene mediante i tre canali messi a disposizione tramite Interfaccia web su HTTPS, FTPS e/o Web service, sempre tramite HTTPS.

Ad ogni attivazione verranno consegnate le credenziali per accedere all'applicativo web reso disponibile da LAND, in base ai dati presenti nella Scheda cliente vincolando il chiamante all'utilizzo di un certificato HTTPS (questo è valido anche se la chiamata avviene da WebService).

Tale accesso garantirà anche la possibilità di esibizione dei Pacchetti di Distribuzione.

Il registro delle attività dei Pacchetti di Versamento è descritto al punto 7.10.

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

I parametri gestionali del Pacchetto di versamento vengono verificati e messi a punto dal Responsabile del servizio di Conservazione e dal Responsabile della Funzione Archivistica in accordo con il **Produttore**.

Le verifiche effettuate sui Pacchetti di versamento sono le seguenti:

- **identificazione** certa del **Produttore** (tramite autenticazione utente o server);
- **verifica** della firma digitale, se presente, mediante un controllo crittografico dell'integrità del documento e della validità formale della firma stessa e l'identità del sottoscrittore.
- **verifica** che i formati degli oggetti da conservare siano conformi con quanto dichiarato nel "Contratto di Servizio" e nell'allegato 2 al Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 Regole tecniche in materia di sistema di conservazione e dichiarati nel presente Manuale;

- **verifica** che i metadati siano conformi a quanto dichiarato nel Contratto di Servizio e, comunque, che siano il set minimale previsto dalla Legislazione corrente.

Il registro contenente le attività di verifica sui Pacchetti di Versamento è descritto al punto 7.10.

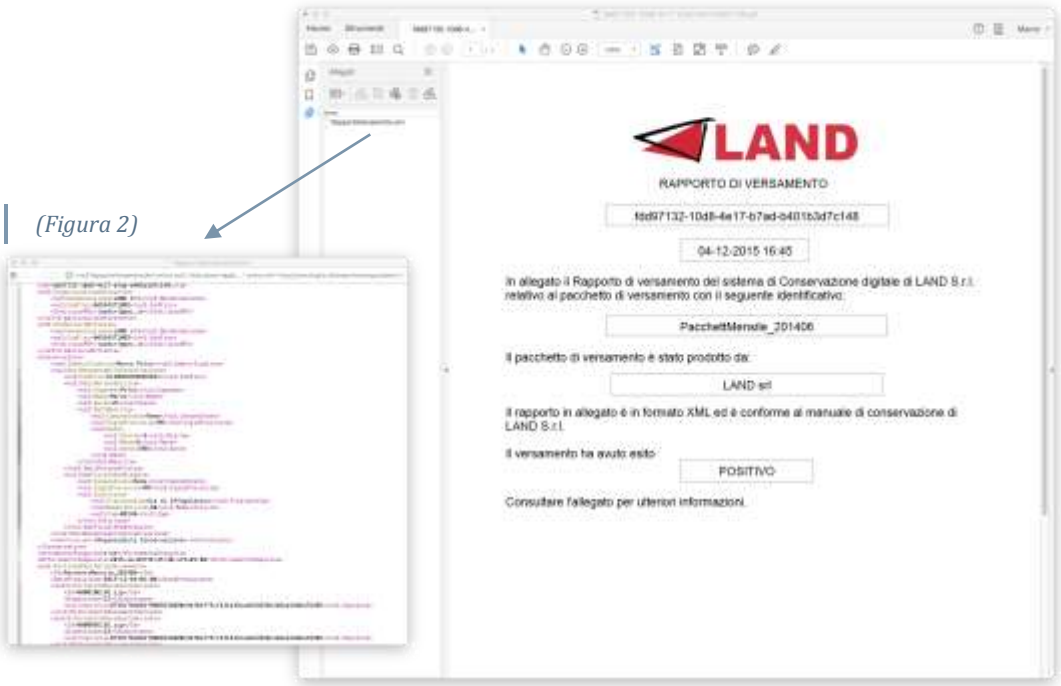
7.3. ACCETTAZIONE DEI PACCHETTI DI VERSAMENTO E GENERAZIONE DEL RAPPORTO DI VERSAMENTO DI PRESA IN CARICO

L'esito positivo delle verifiche effettuate sui Pacchetti di versamento viene registrato in un Rapporto di versamento.

Il Rapporto contiene l'impronta del file originale comprensivo con l'indicazione dell'algoritmo con la quale tale impronta viene calcolata.

In questa fase vengono associate all'indice tutte le evidenze di autenticità delle firme digitali che verranno verificate all'istante del riferimento temporale.

Di seguito un esempio di Rapporto di Versamento in PDF (Figura 1) che viene restituito dal sistema a cui viene allegato l'XML (Figura 2) in standard SInCRO UNI 11386:2010.



(Figura 2)

(Figura 1)

Il Rapporto di versamento è sempre disponibile e scaricabile dagli Utenti, in questa forma, tramite interfaccia web.

Eventuali procedure automatizzate come risposta al pacchetto di versamento avranno il solo XML.

Il registro contenente tutte le attività di accettazione dei Pacchetti di Versamento è descritto al punto 7.10.

7.4. RIFIUTO DEI PACCHETTI DI VERSAMENTO E MODALITÀ DI COMUNICAZIONE DELLE ANOMALIE

Le verifiche effettuate sui Pacchetti di versamento possono risultare negative.

Nei casi in cui anche solo su uno dei controlli indicati nel punto 2 si dovesse riscontrare una mancanza o non corrispondenza di informazioni viene generato un Rapporto di versamento negativo al Produttore. Tale Comunicazione comprenderà i dettagli delle verifiche eseguite sui Pacchetti di versamento comprensive degli errori che hanno causato il fallimento del processo.

Le anomalie, in relazione a quanto descritto nel punto 2, possono essere identificate nella mancata corrispondenza di ciò che viene versato a quanto dichiarato dal Produttore nel contratto di Servizio in termini di firma digitale, formati e metadati.

Il Rapporto di Versamento conterrà la comunicazione dell'anomalia ed archiviato anche da GSC.

Il registro contenente tutte le attività di accettazione dei Pacchetti di Versamento comprese le anomalie è descritto al punto 7.10.

7.5. PREPARAZIONE E GESTIONE DEL PACCHETTO DI ARCHIVIAZIONE

I Pacchetti versati in iCDeS, con la supervisione del Responsabile del Servizio di Conservazione e del Responsabile della Funzione Archivistica saranno raggruppati in Pacchetti di Archiviazione.

Questi pacchetti vengono assemblati dal sistema nei tempi e con i criteri di raggruppamento scelti e concordati con il Produttore, indicati nella Scheda Cliente (ad es. Pacchetti di archiviazione per tipologie documentali o in base alla cadenza temporale di consegna).

Il processo di costruzione dei Pacchetti di archiviazione, così come previsto dallo standard SInCRO UNI 11386:2010 – Supporto all'interoperabilità nella conservazione e nel recupero degli oggetti digitali, avviene individuando i documenti destinati a far parte del Pacchetto di archiviazione sulla base dei criteri scelti.

Tali criteri vengono concordati con il cliente e sono definiti nel Contratto di Servizio e si possono basare sia su caratteristiche legate allo stato del documento, sia su sui metadati minimi indicati nell'allegato 5 al Decreto del presidente del consiglio dei ministri Regole tecniche in materia di sistemi di conservazione.

Pacchetti di archiviazione vengono chiusi in seguito a due tipi di regole:

- **automatiche**: impediscono ad un documento di scadere una volta inserito in un Pacchetto di archiviazione,
- **manuale;** quindi gestite, tramite interfaccia web, dal RSC in accordo con il Produttore.

Comunque le regole sopraindicate sono definite ed autorizzate tramite il Contratto di Servizio.

Tutte le attività (Automatiche e/o manuali sono tracciate in tempo reale tramite il Registro delle attività di Verifica (RegVER) e il Registro attività dei Pacchetti (RegPAK).

I due registri che contengo tutte le attività sono descritti al punto 7.10.

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

La gestione dei Pacchetti di distribuzione fa capo al Responsabile del Servizio di Conservazione, al Responsabile della Funzione archivistica e al Responsabile del trattamento dei dati personali.

La produzione di Pacchetti di distribuzione avviene in seguito alla richiesta da parte dell'Utente.

Tali Pacchetti, però, possono differire nei casi in cui l'utente richiede l'esibizione tramite supporto ottico in quanto questo dovrà necessariamente contenere elementi utili all'avvio del supporto e alla visualizzazione dei contenuti informativi.

Il software iCDeS permette l'accesso ai Pacchetti di distribuzione esclusivamente agli utenti autorizzati.

I livelli di accesso vengono definiti in base alle esigenze delle richieste effettuate, rendendo disponibile soltanto il materiale richiesto grazie all'utilizzo di filtri predefiniti che selezionano i canali previsti per la visualizzazione di un determinato pacchetto.

È possibile visualizzare i documenti tramite duplice canale:

- **via web**: il Produttore titolare dei documenti potrà ricercare e visualizzare tutti i documenti conservati direttamente sul portale, messo a disposizione dal GSC, con l'utilizzo dell'apposita funzionalità. L'accesso avviene tramite iCDeS al quale è demandata la sicurezza e la gestione della sessione. I documenti saranno disponibili per l'esibizione on line per tutto il periodo di conservazione. La descrizione di dettaglio dell'interfaccia web per le richieste di esibizione dei documenti è contenuta nel "Manuale d'uso del servizio web di Conservazione",
- **tramite Web Service**: la chiamata può avvenire tramite qualsiasi altro applicativo.

La struttura architetturale di iCDeS consente di definire diversi livelli operativi e garantisce che ciascuna Azienda/Ente, Area Organizzativa, Agenzia, Ufficio, Dipartimento, ecc. possa accedere solo ed esclusivamente ai suoi documenti, in base alle credenziali e alle politiche di accesso attivate.

IL GSC mette a disposizione, in caso di necessità, al Cliente e agli eventuali organismi preposti una postazione dalla quale scaricare i Pacchetti di Distribuzione.

Con la richiesta da parte dell'Utente di esibizione dei Pacchetti di distribuzione mediante supporto fisico (CD, DVD, USB Key, UDD esterni, ecc.) il personale incaricato al trasporto è scelto dal RdC, inoltre:

- i supporti fisici non presenteranno riferimenti esterni che possano ricondurre all'identificazione del Produttore, dei dati contenuti, della loro tipologia, ecc.
- i dati trasmessi saranno crittografati.

In caso di esibizione dei Pacchetti di distribuzione mediante supporto ottico, viene generata una copia autentica del documento, conforme all'originale in seguito alla richiesta del Cliente a cui vengono attribuiti i costi di gestione.

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

iCDeS fornisce credenziali con ruoli amministratore, utente e visualizzatore dei pacchetti. Qualsiasi attività di produzione di Duplicati e Copie Informatiche dei documenti conservati può essere effettuata direttamente dall'indirizzo web comunicato al Cliente sotto forma di "Pacchetti di Distribuzione".

Nei casi in cui, come previsto dall'art. 23-bis, c. 2 del Codice dell'Amministrazione Digitale il Produttore richieda la presenza di un Pubblico Ufficiale, LAND ne garantirà tale presenza mettendo a disposizione tutte le necessarie risorse che serviranno all'espletamento delle attività, rimandando in ogni caso la scelta al Produttore al quale saranno addebitate le spese.

Inoltre, per garantire la leggibilità dei documenti nel tempo in caso di adeguamento del formato, dovuto all'evoluzione tecnologica, si tengono sotto controllo i formati inviati (previsti dalla normativa) e, nel caso uno di questi non sia più supportato i file saranno trasferiti su file più recente ed il pacchetto di Archiviazione sarà firmato e marcato temporalmente dal responsabile della conservazione.

Anche in questo caso, l'eventuale presenza del pubblico ufficiale per l'attestazione di conformità, sarà garantita in seguito alla richiesta del Cliente a cui vengono attribuiti i costi di gestione.

7.8. SCARTO DEI PACCHETTI DI ARCHIVIAZIONE

Nel caso venga prevista la tempistica di scarto (in caso contrario il sistema di conservazione non prevede attività specifica sull'argomento), sei mesi prima della scadenza del periodo di conservazione dei documenti, LAND comunicherà al Produttore, in modalità certa (tramite messaggio PEC) che, in assenza di ulteriori comunicazioni e trascorsi i termini previsti, provvederà alla cancellazione dei documenti.

Lo scarto dei Pacchetti di archiviazione, in caso di pacchetti versati da Pubbliche Amministrazioni, avverrà previa autorizzazione della Soprintendenza archivistica così come prevede la normativa vigente in materia, in caso contrario LAND attiverà le procedure di restituzione al Cliente dei documenti conservati.

L'intervento della Soprintendenza archivistica è previsto anche nel caso di archivi privati per i quali è stato dichiarato l'interesse culturale, secondo quanto disposto dall'art. 21, comma 1, lettera d del Codice dei beni culturali (D. Lgs. 22 gennaio 2004, n. 42).

I tempi di scarto vengono dettati dal Produttore mediante il proprio Massimario di Scarto, nel caso non venga indicato LAND, al termine del Contratto ed in caso di mancato rinnovo, metterà a disposizione del Cliente un'area di download dei Pacchetti di Archiviazione.

LAND mette a disposizione dei Referenti del Cliente l'accesso diretto ai Pacchetti di Archiviazione, mediante un'apposita interfaccia web, attraverso la quale potranno selezionare direttamente i Pacchetti che si intende scartare.

Al termine del processo, LAND rilascerà un rapporto di scarto che verrà Firmato dal Referente del Cliente e controfirmato dal Responsabile della Conservazione di LAND.

Il Rapporto di Scarto sarà marcato temporalmente così da provare quali Pacchetti di Archiviazione siano stati scartati.

Il rapporto di scarto viene conservato all'interno del sistema di Conservazione.

Una volta rilasciato il rapporto di scarto, verranno fisicamente eliminati i Pacchetti e le relative prove di conservazione.

7.9. PREDISPOSIZIONE DI MISURE A GARANZIA DELL'INTEROPERABILITÀ E TRASFERIBILITÀ AD ALTRI CONSERVATORI

Sono previste apposite procedure software che facilitano l'interoperabilità dei pacchetti di archiviazione ad eventuali altri Conservatori.

In particolare, vengono fornite le strutture dei Pacchetti di Archiviazione di ogni singolo Cliente che sono principalmente composti da una cartella (con il nome parlante) contenente un file PDF Firmato con Firma Elettronica Qualificata del Responsabile della Conservazione con i dati del "Pacchetto di Archiviazione" che avrà in allegato, un file xml con struttura SInCRO (UNI ISO 11386:2010) contenenti le impronte di tutti i file contenuti nel pacchetto e, naturalmente, tutti i file conservati (nella forma di documenti, di fascicoli, o di un'aggregazioni documentali informatiche).

7.10. DESCRIZIONE DEI REGISTRI PREVISTI PER LA TRACCIATURA DELLE AZIONI MANUALI ED AUTOMATICHE EFFETTUATE NEL PROCESSO DI CONSERVAZIONE

Sono previsti due registri, tenuti in un DB (PostgreSQL) che mantengono in memoria tutte le attività Manuali ed Automatiche nel processo di conservazione, uno dedicato alle attività di cambio di stato dei pacchetti e l'altro per le attività di verifica dei pacchetti di archiviazione.

Registro attività dei Pacchetti (RegPAK)

- id univoco
- id_pacchetto_versamento
- id_pacchetto_archiviazione
- username
- operazione
- timestamp
- risposta Ricevuto, Accettato, Rifiutato
- errore (popolato solo nel caso il pacchetto sia stato rifiutato, nel caso sia vuoto il pacchetto risulta controllato
- tipo pacchetto_versamento (versamento, archiviazione)
- tipo pacchetto_archiviazione (archiviazione, chiusura)

Registro delle attività di Verifica (RegVER) Manuali e/o Automatiche

- id univoco
- id_pacchetto_archiviazione
- username
- operazione
- timestamp
- errore (popolato solo nel caso il pacchetto abbia problemi)
- id_pacchetto_archiviazione (archiviazione, chiusura)

La visualizzazione in tempo reale delle attività ed il monitoraggio avvengono tramite software di Business Intelligence Infovision di Zucchetti che gestisce, oltre alle normali visualizzazioni di controlla standard, anche eventuali allarmi (invio mail) in caso di problematiche riscontrate nelle attività ricorrenti.

8. IL SISTEMA DI CONSERVAZIONE

8.1. DESCRIZIONE DELLA COMPONENTE SOFTWARE

LAND adotta un proprio software per la Conservazione denominato CDeS.

La versione per i servizi remoti è denominata iCDeS, il software assicura che tutto il flusso documentale, dalla presa in carico del documento fino all'eventuale scarto (distruzione del documento/fascicolo informatico), non possa essere manomesso.

La soluzione, tramite l'adozione di regole, procedure e tecnologie garantisce le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità nel tempo dei:

a. **documenti informatici** e dei documenti amministrativi informatici con i metadati ad essi associati;
b. **fascicoli informatici** ovvero le aggregazioni documentali informatiche con i metadati ad essi associati, contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che appartengono al fascicolo o all'aggregazione documentale.

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.**

Ai fini dell'interoperabilità tra i sistemi di conservazione è stato adottato, come previsto dalle Regole Tecniche (di seguito denominate "Regole Tecniche") in materia di sistema di conservazione (pubblicate nella Gazzetta Ufficiale n. 59 del 12 marzo 2014), una struttura che fa riferimento allo standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI ISO 11386:2010), che è lo standard riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione.

Tutte le componenti funzionali della soluzione di conservazione, assicurano il trattamento dell'intero ciclo di gestione dell'oggetto conservato nell'ambito del processo di conservazione.

Il sistema di conservazione garantisce l'accesso all'oggetto conservato, per il periodo prescritto dalla norma, indipendentemente dall'evolversi del contesto tecnologico.

Gli elenchi degli standard, delle specifiche tecniche e dei formati utilizzabili quali riferimento per il sistema di conservazione sono quelli indicati negli allegati 2 e 3 delle "Regole Tecniche".

8.2. SISTEMA DI BACK UP E DISASTER RECOVERY

8.2.1. BACK UP

La politica di backup prevede di salvaguardare mediante backup periodico tutti i file indispensabili al ripristino di un sistema. In questa definizione rientrano i file di configurazione individuali dei singoli sistemi e ovviamente i file dati.

E' stata predisposto un apposito sistema dedicato alla gestione di backup, così come un insieme di procedure che ne definiscono l'utilizzo che sono riportate nel presente documento.

I backup vengono eseguiti in automatico mediante un sistema centralizzato in ogni sito (locale e remoto).

Per ogni sistema verranno messi sotto backup i dati ritenuti essenziali, come le configurazioni, i dati legati ai servizi o i dati relativi alla sicurezza.

Al termine di ogni backup vengono inviate delle mail di riepilogo al gruppo dei sistemisti mediante la mailing list.

Eventuali anomalie che emergono durante le fasi di monitoraggio e verifica devono avviare la procedura di "Incident Management".

Il sistema di backup adottato è basato sul software open source "Bacula".

Questo software è già in uso in LAND da anni e ha dato risultati soddisfacenti, candidandolo a software da utilizzare per la gestione dei backup nell'ambito dell'erogazione dei servizi.

Il sistema è composto da 3 componenti principali:

Il director, ossia la componente che orchestra tutte le attività di backup dei vari sistemi interessati;

Il file daemon, ossia la componente da installare sui sistemi da tenere sotto backup, che riceve dal Director i comandi da eseguire per effettuare il backup, come l'elenco delle directory sottoposte a backup. Il File Daemon esegue quindi i vari comandi in locale, e comunica a sua volta con lo Storage Daemon per inviare i file di backup;

Lo storage daemon, ossia la componente che gestisce le partizioni in cui vengono inviati i backup. Nell'architettura interna lo Storage Daemon e il Director risiedono sulla stessa macchina virtuale).

Oltre alle 3 componenti installate lato server e ai dispositivi da mettere sotto backup, sono presenti due console, la prima a riga di comando (Bacula Console) e la seconda grafica (BAT – Bacula Administration Tool). Questi tool vengono installati appositamente sulle postazione del personale sistemistico, per poter lavorare sul sistema.

I backup vengono salvati su di un'apposita partizione dei NAS (dedicata ai backup. La partizione è stata suddivisa in partizioni di 4TB che vengono poi montate mediante protocollo iSCSI come dischi aggiuntivi delle macchine di backup.

La pianificazione dei backup segue lo schema classico dove sono previsti:

- Backup incrementali giornalieri;
- Backup differenziali settimanali;

- Backup completi mensili.

Attualmente viene attuata una politica di "retention" dei dati del Cliente annuale.

8.2.2. DISASTER RECOVERY

Il Disaster Recovery è inserito nella "Procedura Operativa di "Business Continuity" prevista nella certificazione ISO 27001:2013.

Lo scopo della procedura è quello di definire la procedura operativa da attuare in caso sia necessario attivare il sito di Disaster Recovery e garantire quindi la Business Continuity aziendale e dei Clienti.

Infatti, nel documento vengono identificati possibili eventi di tipo bloccante per la normale erogazione dei servizi, che possono richiedere di attivare il processo di Business Continuity che possono essere:

- Eventi naturali (terremoto, alluvione, eruzione vulcanica, ecc.);
- Incendio nella struttura o nei locali deputati all'erogazione;
- Effrazione nei locali deputati all'erogazione dei servizi con danneggiamento delle apparecchiature;
- Intrusione informatica;
- Guasto hardware;
- Guasto alla rete;
- Interruzione delle linee di comunicazione a causa di lavori stradali o di problemi in centrale;
- Interruzione delle linee elettriche a causa di lavori stradati o di problemi legati alla rete.

L'elenco non è esaustivo, e sarà facoltà del management aziendale valutare se situazioni non contemplate nel presente elenco possano richiedere comunque l'attivazione della procedura.

A seguito di uno degli eventi elencati precedentemente dovrà essere attivata la procedura di Business Continuity.

La procedura sarà attivata dopo l'attivazione di una procedura di Incident Management, tutte le annotazioni relative alla Business Continuity verranno annotare nell'apposito modulo.

Tutti i Clienti hanno facoltà di aderire alla procedura di Disaster Recovery o decidere di attendere il ripristino delle funzionalità del sito principale.

L'attivazione dei vari sistemi sul sito di Disaster Recovery prevede:

- Spegnimento (se necessario) delle macchine sul sito primario, per evitare repliche di dati inopportune;

- Verifica dell'ultima replica dei dati, in modo da avvisare il Cliente se vi possano essere dati incompleti (la replica dovrebbe avvenire con una frequenza sufficientemente alta per garantire che tutti i dati siano sempre replicati);
- Attivazione dei servizi sul sito di DR;
- Testing dei servizi, sia dall'interno che dall'esterno;
- Comunicazione dell'avvenuta attivazione al Cliente.

A prescindere dall'erogazione dei servizi sul sito di Disaster Recovery, dovranno essere intraprese tutte le azioni necessarie al ripristino nel più breve tempo possibile del sito primario.

Nel caso vi siano condizioni tali che il sito primario non possa essere ripristinato (a seguito di catastrofi naturali o incendi), sarà cura della direzione individuare un nuovo sito per l'erogazione dei servizi, anche presso terze parti. La nuova struttura dovrà essere approntata seguendo le policy e le procedure di sicurezza ed operatività di cui si è dotata la LAND. Dovrà essere valutato se il nuovo sito diventerà il nuovo sito primario oppure se diventerà un sito di DR, e in tal caso dovranno essere messe in campo tutte le attività necessarie al consolidamento dell'attuale sito di DR, per renderlo idoneo a diventare sito primario.

Analogamente, se dovessero nascere problemi con la struttura deputata a sito di DR, sarà cura della direzione individuare un nuovo sito dove spostare le attività di DR.

Una volta ripristinato il sito primario dovranno essere spostati i servizi in regime di Disaster Recovery per operare nuovamente dal sito primario.

Questa operazione richiede di:

- Spegnere il servizio sul sito di DR;
- Replicare i dati verso il sito primario;
- Verificare che i dati siano correttamente copiati;
- Attivare il servizio sul sito primario;
- Effettuare le verifiche di funzionamento;
- Avvisare il Cliente

Il ripristino del servizio sul sito primario ha dei tempi di disservizio necessari ad effettuare le attività sopra elencate, che dovranno essere concordati con il Cliente per minimizzare l'impatto sul servizio fruito.

Il ripristino dei servizi andrà gestito mediante attivazione di una procedura di Change Management specifica per ogni sistema, ed essere poi riportata all'interno della modulistica di Incident Report aperta all'inizio dell'intero disservizio.

8.3. COMPONENTI LOGICHE

Di seguito la descrizione e lo schema delle componenti logiche relative al sistema di conservazione e al loro funzionamento.

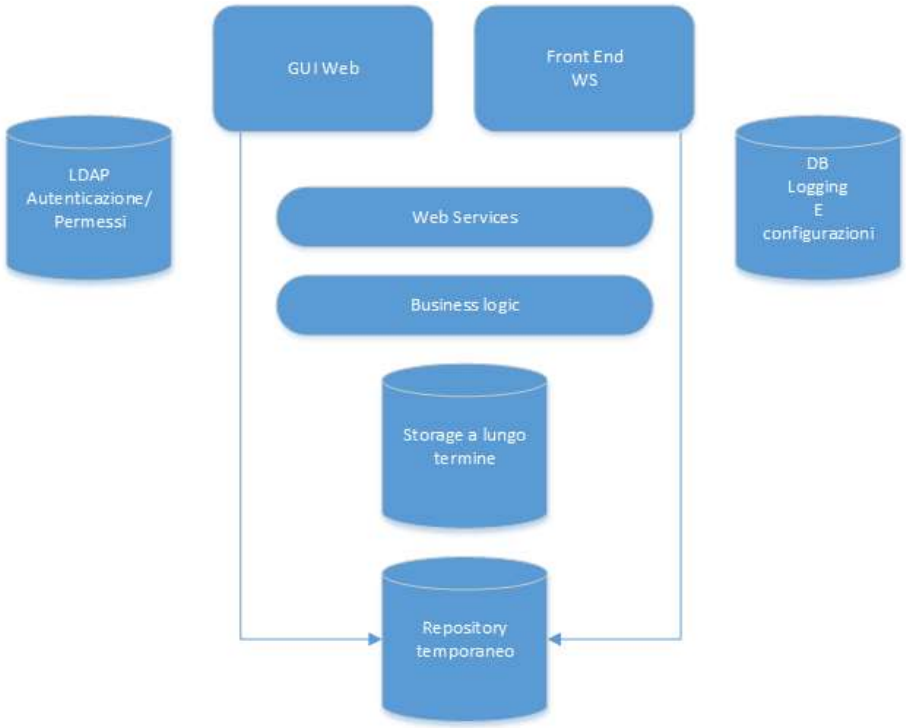
Descrizione componenti Logiche:

- **GUI Web**: consente ad un utente del sistema di conservazione di:
  - caricare i documenti su di un'area temporanea, e quindi effettuarne il versamento
  - archiviare i pacchetti di versamento
  - chiudere i pacchetti di archiviazione
  - effettuare ricerche
  - esportare i pacchetti di distribuzione

L'accesso alla GUI Web avviene mediante protocollo HTTPS, eventualmente con client authentication basata su certificato X.509 personale.

- **Front End WS**: si occupa dell'autenticazione delle chiamate web service al sistema, mediante client authentication (non opzionale) basata su certificato X.509 emesso per il singolo sistema chiamante.
- **sFTP**: consente di depositare su di un'area temporanea dei documenti che verranno poi elaborati mediante GUI Web, Web service oppure processi batch. L'accesso avviene mediante certificato SSL emesso per il sistema chiamante.
- **Processi batch**: processi automatizzati che consentono di pre-elaborare i dati presenti nell'area temporanea, chiamare i metodi dei web service per inserire i file all'interno del ciclo di conservazione
- **Web Services**: interfaccia applicativa che consente di effettuare le operazioni di:
  - versamento
  - archiviazione
  - chiusura
  - riapertura
  - creazione del pacchetto di versamento a partire da un'area temporanea
  - ricerca
  - estrazione
- **Business logic**: è lo strato che implementa tutte le funzionalità richieste dallo standard SiNCRo, si interfaccia con il layer di storage a lungo termine, espone i metodi utili per lavorare sui dati.
- **Storage a lungo termine**: è il repository dove vengono messi i dati una volta che entrano nel ciclo di conservazione (versamento, archiviazione e conservazione).
- **Repository temporaneo**: è un'area dove vengono depositati i documenti provenienti dalla modalità di input sFTP e/o GUI Web, in attesa della creazione dei relativi pacchetti di versamento.
- **LDAP Autenticazione/Permessi**: Database LDAP deputato alla gestione dei dati di autenticazione e profilazione degli utenti che possono accedere al sistema.
- **DB Logging e configurazioni**: Database relazionale deputato a tenere le informazioni di logging delle attività e delle configurazioni di sistema.

Schema delle componenti logiche:



8.4. COMPONENTI FISICHE

Il sito primario di conservazione è ubicato presso il CED_02 di LAND in Via di Affogalasino, 40 a Roma mentre il Sito secondario di DR (Disaster Recovery) è ubicato presso il datacenter Aruba PEC S.p.A. Via Ramelli, 8 52100 Arezzo.

Tutti gli oggetti di conservazione sono salvati su apparati storage dedicati fisicamente distinti.

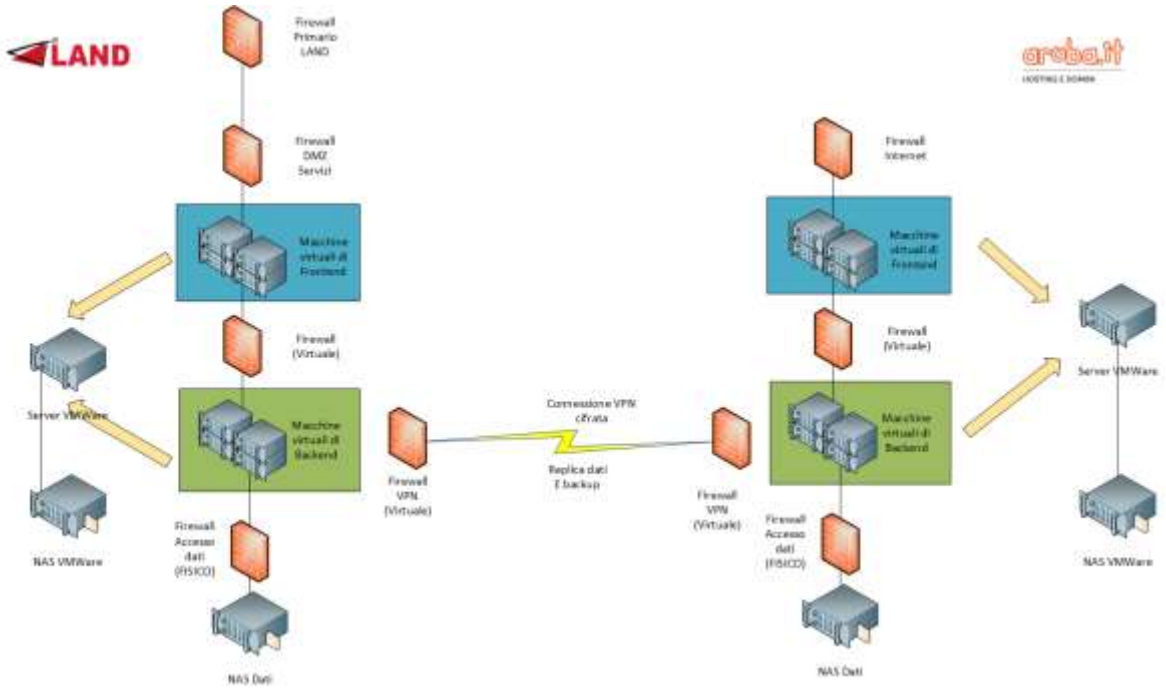
Le componenti applicative sono eseguite su server virtuali ospitati su cluster VMWare in configurazione attiva-attiva.

L'apposizione delle firme elettroniche qualificate da parte del RdC e suoi eventuali delegati è effettuata per mezzo di dispositivo di firma remota.

Applicazioni e dati (PdA) sono replicati tra le due infrastrutture (principale e secondaria).

Le procedure di replica, sono basate su RSYNC ed utilizzano un tunnel crittografico VPN IPSEC.

Di seguito il disegno dell'architettura in esercizio:



8.5. PROCEDURE DI GESTIONE E DI EVOLUZIONE

Esistono adeguate procedure di gestione e di evoluzione dei sistemi e dei software descritte nella procedura di “Change Management”.

La procedura di “Change Management” gestisce il cambiamento che è definito come: l'aggiunta, la modifica, o la rimozione approvata di hardware, firmware, software, applicazioni, servizi, sistemi, procedure o documentazione associata inerenti all’ambito dell’erogazione dei servizi.

Il “Change Management” è definito come: il processo di controllo, per gestire i cambiamenti di sistema in modo da assicurare il minimo disturbo nella fornitura dei servizi erogati e nelle procedure di supporto.

Il processo di “Change Management”, in generale, è responsabile del controllo delle modifiche ai componenti che compongono un sistema informatico e per estensione includono le procedure e policy di supporto.

Si possono evincere le seguenti voci:

- strutture fisiche
- hardware
- apparecchiature di comunicazione
- sistemi operativi
- applicazioni
- assistenza clienti
- procedure

- policy

Il processo delinea il meccanismo di approvazione (o negazione) delle modifiche proposte.

9. MONITORAGGIO E CONTROLLI

La particolare natura del processo di conservazione LAND ha definito, descritto ed applicato, in ambito ISO/IEC 27001:2013, un insieme di attività di analisi e di verifica del funzionamento del sistema nella sua interezza.

Tutti i processi sono finalizzati ad anticipare qualsiasi problematica o ad intervenire velocemente nel caso la problematica si verifichi e crei un disservizio (interno od esterno).

9.1. PROCEDURE DI MONITORAGGIO

LAND adotta una infrastruttura di monitoraggio continua effettuata da apparecchiature elettroniche, sonde e opportuno software.

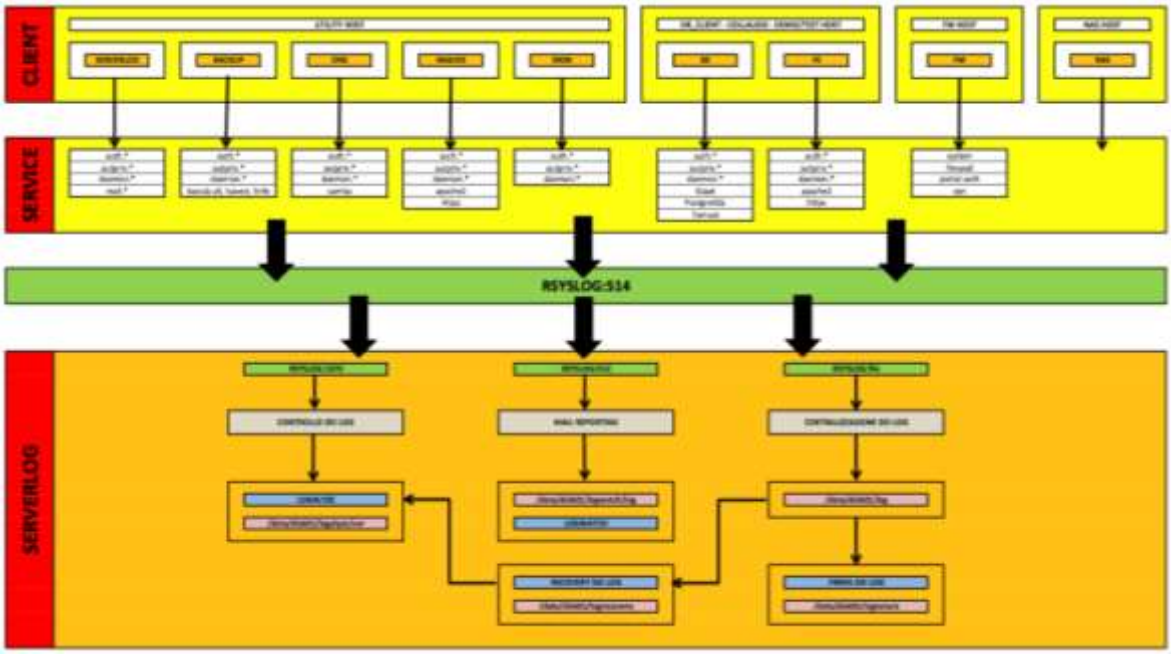
Nel laboratorio di sviluppo software esiste una centrale di monitoraggio con presidio continuo di personale nei giorni lavorativi dalle 8,30 alle 19,00.

Al di fuori dell'orario sopraindicato esiste un sistema automatico di avvisi che ci permette di intervenire da remoto o, nel caso non sia possibile, tramite intervento fisico in tempi brevissimi.

Tutti servizi e gli applicativi, come anche le autenticazioni, mantengono traccia dei propri errori in modalità locale su ogni host.

Nel CED_02 dedicato alla Conservazione di LAND e nei CED delocalizzato di Disaster Recovery su Aruba, esistono 2 Server dedicati alla centralizzazione dei log denominati serverlog.

Nella centralizzazione vengono convogliati tutti i log di autenticazione e daemon di ogni client ed i log di autenticazione e di errore di ogni servizio attivo negli stessi client in formato SYSLOG.



9.2. VERIFICA DELL'INTEGRITA' DEGLI ARCHIVI

La verifica di integrità degli archivi, permette la verifica dell'integrità del documento al momento della sua conservazione ed avviene confrontando l'impronta calcolata al momento sul file di quella contenuta nell'indice di conservazione.

Tale verifica viene applicata durante il processo di conservazione è utilizzabile per l'assolvimento dei requisiti di verifica periodica della leggibilità dei documenti.

Questa funzionalità è presente nel sistema di conservazione ed è possibile automatizzarla se ritenuto necessario da RSC.

Ogni verifica effettuata (manuale o automatica) è registrata nell'apposito Registro (RegVer) che può essere consultato dal RSC per attestare la corretta esecuzione della verifica o per diagnosticare eventuali anomalie.

9.3. SOLUZIONI ADOTTATE IN CASO DI ANOMALIE

Esiste un'apposita procedura in ambito ISO/IEC 27001:2013 c che definisce le procedure operativa da adottare nel caso di eventi legati alla sicurezza dei sistemi, a malfunzionamenti dei sistemi, dei software, e di altre anomalie ritenute importanti da tracciare, gestire e risolvere.

Le problematiche sono state categorizzate nel seguente modo:

- Anomalia sistemi;
- Anomalia linee di comunicazione;
- Sicurezza informatica;
- Sicurezza fisica/ambientale;
- Anomalia software;
- Problema hardware

In tutti questi casi dovrà essere avviata la procedure di Incident Management.

La procedura sarà avviata dalla persona che riceve la segnalazione o che verifica in prima persona la situazione anomala, a prescindere dal suo ruolo nell'ambito dell'erogazione dei servizi di conservazione.

10. ADERENZA ALLA NORMATIVA DEL MANUALE DELLA CONSERVAZIONE

10.1.1. NORMATIVA DI RIFERIMENTO

Il manuale è redatto seguendo la vigente normativa, in particolare le "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" pubblicato nel Supplemento ordinario alla "Gazzetta Ufficiale„ n. 59 del 12 marzo 2014 - Serie generale.

10.1.2. CERTIFICAZIONE ISO/IEC 27001:2013

LAND è certificata per i servizi di data center di Conservazione Digitale.

LAND applica un sistema di Gestione della Sicurezza delle Informazioni in conformità ai requisiti della ISO/IEC 27001:2013 con riferimento al seguente scopo: "Il sistema di gestione della sicurezza delle informazioni per la progettazione ed erogazione di servizi di data center identificati nelle attività di Conservazione Digitale in accordo con la dichiarazione dell'applicabilità versione 1.0 del 13 aprile 2015".

Tutte le informazioni riguardanti la sicurezza ed i seguenti documenti:

- certificato ISO/IEC 27001:2013 in italiano
- certificato ISO/IEC 27001:2013 in inglese
- indicazione degli SLA
- adozione di un modello di organizzazione, gestione e controllo ex D.lgs. n. 231 del 2001
- politica della sicurezza

Sono disponibili per la consultazione al link: http://www.land.it/it/sicurezza.html

10.1.3. CERTIFICAZIONE ISO 9001:2008

Per LAND la qualità dei prodotti e dei servizi è sempre stata fondamentale e per questo è certificata ISO 9001:2008 (Categorie IAF/EA 29, 33 e 35) per le seguenti attività:

- sviluppo software, integrazione di sistemi informatici ed erogazione di servizi professionali a supporto della realizzazione di sistemi informativi;
- attività di commercio, noleggio, assistenza tecnica e outsourcing di macchine e prodotti per ufficio;
- commercio di soluzioni ed arredi per ufficio.

Il certificato è disponibile per la consultazione al link: http://www.land.it/it/qualita.html