



CORVALLIS DM

EN/ISO 14001:2015 IE-0915-05
ISO/IEC 27001:2013 IIS-1014-01
EN/ISO 9001:2015 IQ-1015-02



Dasa-Rägister

00-CDM-Manuale Conservazione-Rev-1-13-del-15-gennaio-2019.docx

Manuale di Conservazione di Corvallis DM

EMMISSIONE DEL DOCUMENTO VERSIONE 1.13

Azione	Data	Nominativo	Funzione
<i>Redazione</i>	15 gennaio 2019	Nicola Savino	Responsabile della funzione archivistica
<i>Verifica</i>	15 gennaio 2019	Giuseppe Cannone	Responsabile del Servizio di Conservazione
<i>Approvazione</i>	15 gennaio 2019	Giuseppe Cannone	Responsabile del Servizio di Conservazione

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
Versione 1.0	23/06/2015	Prima Emissione	Bozza
Versione 1.1	30/06/2015	Tolta parte generazione documenti informatico	Bozza
Versione 1.2	27/07/2015	Aggiornata con descrizioni tecniche	Bozza
Versione 1.3	17/08/2015	Aggiornamenti paragrafi 5.8-5.9, 7.2-7.3, 8.1-8.6, 8.8, 9.4	Versione Finale
Versione 1.4	22/01/2016	Aggiornamento formattazione testo e tabelle per l'accessibilità del documento	Versione Finale
Versione 1.5	24/06/2016	Aggiornamento nominativo responsabile dello sviluppo e della manutenzione del sistema di conservazione	Versione Finale
Versione 1.6	23/01/2017	Aggiornamento nominativo responsabile dello sviluppo e della manutenzione del sistema di conservazione, indirizzo sede legale	Versione Finale
Versione 1.7	02/10/2017	Aggiornamento nominativo responsabile della funzione archivistica	Versione Bozza
Versione 1.8	07/11/2017	Aggiornamento Nominativo Responsabile della funzione Archivistica, nominativo responsabile dello sviluppo e della manutenzione del sistema di conservazione, nominativo responsabile dei sistemi informativi per la conservazione e aggiornamento sistema di conservazione con l'introduzione del software EasyLegal	Versione Finale
Versione 1.9	06/02/2018	Recepimento segnalazione di modifiche pervenute da AgID ricevute con e-mail del 21 dicembre 2017	Versione Finale





CORVALLIS DM

EN/ISO 14001:2004 IE-0915-05
ISO/IEC 27001:2013 IIS-1014-01
ISO 9001 IQ-1015-02



Dasa-Rägister

00-CDM-Manuale Conservazione-Rev-1-13-del-15-gennaio-2019.docx

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
Versione 1.10	11/04/2018	Recepimento segnalazione di modifiche Par. 7.14 pervenute da AgID ricevute con e-mail del 9 aprile 2018	Versione Finale
Versione 1.11	19/07/2018	Reimpaginazione documento (Versione 1.10) con ripristino reference interni ed aggiornamento dei certificati riportati nell'intestazione di pagina	Versione Finale
Versione 1.12	18/09/2018	Aggiornamento della normativa di riferimento in materia di trattamento di informazioni personali: GDPR 679 / 2016 e DLgs 101 del 10 agosto 2018	Versione Finale
Versione 1.13	15/01/2019	Sostituzione del Responsabile dello Sviluppo e della Manutenzione del Sistema di Conservazione , Aggiornamento versione delle norme di riferimento delle certificazioni del Conservatore Corvallis DM.	Versione Finale



CORVALLIS DM

EN/ISO 14001:2015 IE-0915-05
ISO/IEC 27001:2013 IIS-1014-01
EN/ISO 9001:2015 IQ-1015-02



Dasa-Rägister

00-CDM-Manuale Conservazione-Rev-1-13-del-15-gennaio-2019.docx

SOMMARIO

1. SCOPO E AMBITO DEL DOCUMENTO	6
1.1 SOFTWARE IMPIEGATO PER IL PROCESSO DI CONSERVAZIONE.....	6
1.2 LOCALIZZAZIONE E CONSERVAZIONE DEL MANUALE.....	7
2. TERMINOLOGIA (GLOSSARIO, ACRONIMI).....	7
2.1. GLOSSARIO	7
2.2. ACRONIMI	13
3. NORMATIVA E STANDARD DI RIFERIMENTO.....	13
3.1. NORMATIVA.....	13
3.2. STANDARD DI RIFERIMENTO	15
4. RUOLI E RESPONSABILITÀ.....	15
4.1. DATI IDENTIFICATIVI DEL SOGGETTO CONSERVATORE.....	15
4.2. CERTIFICAZIONE DEL SOGGETTO CONSERVATORE	16
4.3. RESPONSABILE DEL SERVIZIO DI CONSERVAZIONE.....	17
4.4. RESPONSABILE DELLA FUNZIONE ARCHIVISTICA DELLA CONSERVAZIONE	17
4.5. RESPONSABILE DEL TRATTAMENTO DEI DATI.....	17
4.6. RESPONSABILE DELLA SICUREZZA DEI SISTEMI PER LA CONSERVAZIONE.....	18
4.7. RESPONSABILE DEI SISTEMI INFORMATIVI PER LA CONSERVAZIONE	18
4.8. RESPONSABILE DELLO SVILUPPO E DELLA MANUTENZIONE DEL SISTEMA DI CONSERVAZIONE	18
4.9. SOGGETTI CHE NEL TEMPO HANNO ASSUNTO RUOLI DI RESPONSABILITÀ NEL SERVIZIO DI CONSERVAZIONE	19
5. STRUTTURA ORGANIZZATIVA DEL SERVIZIO DI CONSERVAZIONE.....	20
5.1. PRODUTTORE	21
5.2. UTENTE.....	21
5.3. RESPONSABILE DELLA CONSERVAZIONE	21
5.4. ORGANISMO DI TUTELA E VIGILANZA	21
5.5. ORGANIGRAMMA DEL SERVIZIO DI CONSERVAZIONE.....	23
5.6. STRUTTURE ORGANIZZATIVE.....	23
5.6.1. <i>Attività proprie del contratto di servizio di conservazione</i>	<i>23</i>
5.6.2. <i>Attività Proprie di Gestione dei Sistemi Informativi.....</i>	<i>24</i>
6. OGGETTI SOTTOPOSTI A CONSERVAZIONE.....	25





6.1.	OGGETTI CONSERVATI	25
6.1.1.	<i>I metadati</i>	25
6.1.2.	<i>I Formati</i>	28
6.2.	PACCHETTO DI VERSAMENTO	30
6.3.	PACCHETTI DI ARCHIVIAZIONE	36
6.4.	PACCHETTI DI DISTRIBUZIONE.....	46
7.	IL PROCESSO DI CONSERVAZIONE	47
7.1.	MODALITÀ DI ACQUISIZIONE DEI PACCHETTI DI VERSAMENTO PER LA LORO PRESA IN CARICO.....	52
7.2.	VERIFICHE EFFETTUATE SUI PACCHETTI DI VERSAMENTO E SUGLI OGGETTI IN ESSI CONTENUTI	52
7.3.	ACCETTAZIONE DEI PACCHETTI DI VERSAMENTO E GENERAZIONE DEL RAPPORTO DI VERSAMENTO	53
7.4.	RIFIUTO DEI PACCHETTI DI VERSAMENTO E MODALITÀ DI COMUNICAZIONE DELLE ANOMALIE	54
7.5.	PREPARAZIONE E GESTIONE DEL PACCHETTO DI ARCHIVIAZIONE.....	59
7.6.	PREPARAZIONE E GESTIONE DEL PACCHETTO DI DISTRIBUZIONE AI FINI DELL'ESIBIZIONE.....	59
7.7.	MODALITÀ DI ACQUISIZIONE DEI PACCHETTI DI VERSAMENTO PER LA LORO PRESA IN CARICO.....	60
7.8.	VERIFICHE EFFETTUATE SUI PACCHETTI DI VERSAMENTO E SUGLI OGGETTI IN ESSI CONTENUTI	63
7.9.	ACCETTAZIONE DEI PACCHETTI DI VERSAMENTO E GENERAZIONE DEL RAPPORTO DI VERSAMENTO	63
7.10.	RIFIUTO DEI PACCHETTI DI VERSAMENTO E MODALITÀ DI COMUNICAZIONE DELLE ANOMALIE	64
7.11.	PREPARAZIONE E GESTIONE DEL PACCHETTO DI ARCHIVIAZIONE.....	68
7.12.	PREPARAZIONE E GESTIONE DEL PACCHETTO DI DISTRIBUZIONE AI FINI DELL'ESIBIZIONE.....	69
7.12.1.	<i>Procedure di supporto in caso di anomalie dei due sistemi</i>	70
7.13.	PRODUZIONE DI DUPLICATI E COPIE INFORMATICHE E DESCRIZIONE DELL'EVENTUALE INTERVENTO DEL PUBBLICO UFFICIALE NEI CASI PREVISTI	72
7.14.	SCARTO DEI PACCHETTI DI ARCHIVIAZIONE	73
7.15.	PREDISPOSIZIONE DI MISURE A GARANZIA DELL'INTEROPERABILITÀ E TRASFERIBILITÀ AD ALTRI CONSERVATORI.....	76
8.	IL SISTEMA DI CONSERVAZIONE.....	76
8.1.	CARATTERISTICHE OAIS DEL SISTEMA DI CONSERVAZIONE	77
8.2.	COMPONENTI LOGICHE.....	79
8.2.1.	<i>Sistema di versamento</i>	79
8.2.2.	<i>Sistema di gestione dati</i>	80
8.2.3.	<i>Sistema di memorizzazione</i>	80
8.2.4.	<i>Sistema di autenticazione e Accesso ai Dati</i>	81
8.2.5.	<i>Sistema per la firma digitale</i>	82
8.2.6.	<i>Componente per la marca temporale</i>	82
8.2.7.	<i>Certificatore utilizzato</i>	83
8.2.8.	<i>Procedure per la continuità operativa</i>	83
8.3.	COMPONENTI TECNOLOGICHE	83
8.3.1.	<i>ARCHITETTURE</i>	83
8.3.2.	<i>Scalabilità volumi</i>	84
8.3.3.	<i>Scalabilità utenti</i>	85
8.3.4.	<i>Data Base</i>	86
8.3.5.	<i>Storage</i>	86
8.4.	LOG DI SISTEMA	86



CORVALLIS DM

EN/ISO 14001:2004 IE-0915-05
ISO/IEC 27001:2013 IIS-1014-01
ISO 9001 IQ-1015-02



Dasa-Rägister

00-CDM-Manuale Conservazione-Rev-1-13-del-15-gennaio-2019.docx

8.5.	COMPONENTI FISICHE	87
9.	MONITORAGGIO E CONTROLLI	89
9.1.	PROCEDURE DI MONITORAGGIO	89
9.2.	VERIFICA DELL'INTEGRITÀ DEGLI ARCHIVI	89
9.3.	SOLUZIONI ADOTTATE IN CASO DI ANOMALIE.....	90



1. SCOPO E AMBITO DEL DOCUMENTO

Il presente documento, ai sensi del DPCM 13 dicembre 2013, descrive il sistema ed il processo di erogazione del servizio di conservazione ed in particolare:

- Individua e attribuisce ruoli e responsabilità alle figure professionali coinvolte nel Servizio di Conservazione;
- Descrive le tipologie degli oggetti sottoposti a conservazione, con indicazione dei formati gestiti e relativi metadati;
- Descrive le modalità di generazione dei documenti ed oggetti digitali;
- Descrive il processo di versamento, conservazione, esibizione e scarto;
- Descrive il sistema di conservazione e relative caratteristiche tecnologiche, fisiche e logiche;
- Descrive le procedure di monitoraggio delle funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie;
- Descrive le normative in vigore nei luoghi in cui sono conservati i documenti.

[TORNA AL SOMMARIO](#)

1.1 SOFTWARE IMPIEGATO PER IL PROCESSO DI CONSERVAZIONE

Corvallis DM utilizza il software EasyLegal® implementato dalla stessa Corvallis DM ed il software LegalArchive® di proprietà della società IFIN Sistemi.

EasyLegal® e LegalArchive® rispettano i seguenti standard, così come richiesto dall'allegato 3 delle nuove regole tecniche:

- OAIS: ISO 14721 Open Archival Information System.
- Dublin Core: ISO 15386 The metadata element set.
- UniSInCRO: UNI 11386 Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.

EasyLegal® e LegalArchive® sono software in linea con quanto disposto dalla normativa attualmente in vigore ed è stato sviluppato rispettando le nuove regole tecniche emanate dall'Agenzia per l'Italia Digitale (AgID).

[TORNA AL SOMMARIO](#)



1.2 [LOCALIZZAZIONE E CONSERVAZIONE DEL MANUALE](#)

Una copia del manuale della conservazione è presso la sede del Soggetto conservatore: in quanto documento informativo è sottoposto a conservazione elettronica.

Una copia del manuale della conservazione è presso la sede dei Soggetti Produttori (Clienti di Corvallis DM)

[TORNA AL SOMMARIO](#)

2. [TERMINOLOGIA \(GLOSSARIO, ACRONIMI\)](#)

[TORNA AL SOMMARIO](#)

2.1. [GLOSSARIO](#)

TERMINE	DEFINIZIONE
Accesso	Operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici
Accreditamento	Riconoscimento, da parte dell'Agencia per l'Italia digitale, del possesso dei requisiti per svolgere l'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 in relazione alle funzioni dell'ente
Archivio	Complesso di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività
Archivio informatico	Archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestite 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 un 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, senza aver subito alterazioni o modifiche. L'autenticità può



TERMINE	DEFINIZIONE
	essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico
Base di dati	Collezione di dati registrati e correlati tra loro
Certificatore Accreditato	Soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, dall' Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
Ciclo di gestione	Arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo.
Classificazione	Attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati,
Codice	Decreto legislativo 7 marzo 2005 n. 82 e successive modificazioni ed integrazioni
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 della 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 21 regole tecniche per il sistema di conservazione
Destinatario	Identifica il soggetto/sistema al quale il documento informatico è indirizzato
Duplicazione dei documenti informatici	Produzione di duplicati informatici
Esibizione	Operazione che consente di visualizzare un documento conservato e di ottenerne copia
Estratto per riassunto	Documento nel quale si attestano in maniera sintetica ma esaustiva fatti, stati o qualità desunti da dati o documenti in possesso di soggetti pubblici
Evidenza informatica	Una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica
Fascicolo informatico	Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del Codice.



TERMINE	DEFINIZIONE
Formato	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
FTP server	Programma che permette di accettare connessioni in entrata e di comunicare con un Client attraverso il protocollo FTP
Funzionalità Aggiuntive	Le ulteriori componenti del sistema di protocollo informatico necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni
Funzionalità interoperative	Le componenti del sistema di protocollo informatico finalizzate a rispondere almeno ai requisiti di interconnessione di cui all'articolo 60 del D.P.R. 28 dicembre 2000, n. 445
Funzionalità Minima	La componente del sistema di protocollo informatico che rispetta i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445
Funzione di hash	Una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
Generazione automatica di documento informatico	Formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni
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
IdP:	Strumento per rilasciare le informazioni di identificazione di tutti i soggetti che cercano di interagire con un Sistema; ciò si ottiene tramite un modulo di autenticazione che verifica un token di sicurezza come alternativa all'autenticazione esplicita di un utente all'interno di un ambito di sicurezza.
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 DPCM 03/2013 o, 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



TERMINE	DEFINIZIONE
Leggibilità	Insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti
Log di sistema	Registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati
Manuale di conservazione	Strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 delle regole tecniche del sistema di conservazione
Manuale della gestione	Strumento che descrive il sistema di gestione informatica dei documenti di cui all'articolo 5 delle regole tecniche del protocollo informatico ai sensi delle regole tecniche per il protocollo informatico D.P.C.M. 31 ottobre 2000 e successive modificazioni e integrazioni
Memorizzazione	Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici
Metadati	Insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 del DPCM 03/12/2013
Pacchetto di archiviazione	Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del DPCM 03/12/2013 e secondo le modalità riportate nel manuale di conservazione
Pacchetto di distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta
Pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione
Pacchetto informativo	Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare
Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza
Piano della sicurezza del sistema di gestione informatica dei documenti	Documento, che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi nell'ambito dell'organizzazione di appartenenza
Piano di conservazione	Strumento, integrato con il sistema di classificazione per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445



TERMINE	DEFINIZIONE
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
Presenza in carico	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione
Processo di conservazione	Insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 10 delle regole tecniche del sistema di conservazione
Produttore	Persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale.
Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore
Registrazione informatica	Insieme delle informazioni risultanti da transazioni informatiche o dalla presentazione in via telematica di dati attraverso moduli o formulari resi disponibili in vario modo all'utente
Registro particolare	Registro informatico di particolari tipologie di atti o documenti; nell'ambito della pubblica amministrazione è previsto ai sensi dell'articolo 53, comma 5 del D.P.R. 28 dicembre 2000, n. 445
Registro di protocollo	Registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti
Regole tecniche del sistema di conservazione	Regole tecniche in materia di conservazione ai sensi degli articoli 20, commi 3 e 5 bis, 23-ter, comma 4, 43, 43, commi 1 e 3 aa, 44-bis e 71, comma 1, del Codice dell'Amministrazione digitale di cui al DLgs. n. 82 del 2005, approvate con DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI, 3 DICEMBRE 2013
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.



TERMINE	DEFINIZIONE
Responsabile della conservazione	Soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 delle regole tecniche del sistema di conservazione
Responsabile del trattamento dei dati	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali
Responsabile della sicurezza	Soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza
Riferimento temporale	Informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento
Scarto	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale
Sistema di classificazione	Strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata
Sistema di conservazione	Sistema di conservazione dei documenti informatici di cui all'articolo 44 del Codice
Sistema di gestione informatica dei documenti	Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445; per i privati è il sistema che consente la tenuta di un documento informatico
Staticità	Caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione
Transazione informatica	Particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche della base di dati
Testo unico	Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni
Ufficio utente	Riferito ad un'area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico
Utente	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse
Versamento agli Archivi di Stato	Operazione con cui il responsabile della conservazione di un organo giudiziario o amministrativo dello Stato effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali
Volume di Conservazione (VdC)	Unità logica elementare, risultato finale di un processo di conservazione. Il VdC è composto logicamente da: <ul style="list-style-type: none">— Uno o più file ai quali si applica unitariamente il processo di conservazione;— L'indice di conservazione (IdC);



TERMINE	DEFINIZIONE
	<p>— Gli indice di conservazione antecedenti, se l'indice di conservazione attuale è stato originato da questi.</p> <p>In aggiunta ai precedenti elementi il VdC, può contenere ulteriori componenti, per lo più con finalità di carattere gestionale.</p>

[TORNA AL SOMMARIO](#)

2.2. [ACRONIMI](#)

ACRONIMO	SIGNIFICATO
AGID	Agenzia Italia Digitale (Agenda digitale italiana per l'Europa 2020)
CA	Certification authority – Autorità di certificazione
CAD	Codice dell'Amministrazione Digitale
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione (ora AGID)
DLGS	Decreto Legislativo
DPCM	Decreto del Presidente del Consiglio dei Ministri
FTP	File Transfer Protocol
GMT	Greenwich Mean Time
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol con SSL
ISO	International Standard Organization
PIN	Personal identification number
SSL	Secure Sockets Layer
TSA	Time Stamping Authority (sistema di marcatura temporale)
URL	Uniform Resource Locator
WWW	World Wide Webs

[TORNA AL SOMMARIO](#)

3. [NORMATIVA E STANDARD DI RIFERIMENTO](#)

[TORNA AL SOMMARIO](#)

3.1. [NORMATIVA](#)

- 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. e i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;



- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m. e i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m. e i. – Codice in materia di protezione dei dati personali;
- DECRETO LEGISLATIVO 10 agosto 2018, n. 101: Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129)
- GDPR: REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m. e i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m. e i. – Codice dell'amministrazione digitale (CAD);
- Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Decreto del Presidente del Consiglio 21 marzo 2013 “Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni”
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e



3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;

- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.
- Aggiornamento del Codice dell'Amministrazione Digitale DLgs. 179 / 2016 - Pubblicato in gazzetta ufficiale il 13 / 9 / 2016.

[TORNA AL SOMMARIO](#)

3.2. 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.
- ISO 15489: 2001 Information and Documentation - Records Management.

[TORNA AL SOMMARIO](#)

4. RUOLI E RESPONSABILITÀ

[TORNA AL SOMMARIO](#)

4.1. DATI IDENTIFICATIVI DEL SOGGETTO CONSERVATORE



Denominazione	Corvallis Document Management Srl
Indirizzo sede legale	Piazzale Luigi Sturzo 15, 00144 Roma
Indirizzo sede amministrativa	Piazzale Luigi Sturzo 15, 00144 Roma
Consigliere Delegato	Artusi Andrea
Procuratore Speciale	Luca Ialongo
Telefono	06-50796223
Fax	06-50797919
E- mail istituzionale	corvallisdm@pec.corvallis.it
Sito istituzionale	www.corvallisdm.it

[TORNA AL SOMMARIO](#)

4.2. CERTIFICAZIONE DEL SOGGETTO CONSERVATORE

- ISO/IEC 27001: **2017** Gestione della riservatezza integrità, disponibilità relativamente ai servizi di Conservazione di documenti informatici e cartacei
- ISO 9001: **2015**: Progettazione ed erogazione di servizi di archiviazione documentale: cartacea, ottica e gestione elettronica degli archivi attraverso applicativi software customizzabili, gestione in back office di processi documentali di terzi. Servizio di hosting di siti web
- ISO 14001: **2015**: Progettazione di soluzioni personalizzate ed erogazione di servizi informatizzati per la gestione della documentazione cartacea, elettronica, ottica e campioni fisici attraverso applicativi software customizzabili. Progettazione ed erogazione di servizi di archiviazione documentale: presa in carico, risanamento, custodia, reperimento ed accesso informatizzato anche via internet, acquisizione dati ed immagini, codifica, controllo gestione flussi dati. Gestione in back office di processi documentali di terzi. Servizio di hosting di siti web. Gestione controllata dei processi di distruzione della documentazione alla fine del suo ciclo di vita.

[TORNA AL SOMMARIO](#)



4.3. RESPONSABILE DEL SERVIZIO DI CONSERVAZIONE

Nominativo	Funzioni
Giuseppe Cannone	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.

La nomina è stata formalizzata con documento sottoscritto per accettazione dal responsabile. La nomina decorre dal 02/01/2015

[TORNA AL SOMMARIO](#)

4.4. RESPONSABILE DELLA FUNZIONE ARCHIVISTICA DELLA CONSERVAZIONE

Nominativo	Funzioni
Nicola Savino	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. disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.

La nomina è stata formalizzata con documento sottoscritto per accettazione dal responsabile. La nomina decorre dal 02/10/2017.

[TORNA AL SOMMARIO](#)

4.5. RESPONSABILE DEL TRATTAMENTO DEI DATI

Nominativo	Funzioni
Severino Cirimelli	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 - monitoraggio



	del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione.
--	--

La nomina è stata formalizzata con documento sottoscritto per accettazione dal responsabile. La nomina decorre dal 02/01/2015

[TORNA AL SOMMARIO](#)

4.6. RESPONSABILE DELLA SICUREZZA DEI SISTEMI PER LA CONSERVAZIONE

Nominativo	Funzioni
Giulio Del Tavano	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.

La nomina è stata formalizzata con documento sottoscritto per accettazione dal responsabile. La nomina decorre dal 02/01/2015

[TORNA AL SOMMARIO](#)

4.7. RESPONSABILE DEI SISTEMI INFORMATIVI PER LA CONSERVAZIONE

Nominativo	Funzioni
Cristian Micarelli	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

La nomina è stata formalizzata con documento sottoscritto per accettazione dal responsabile. La nomina decorre dal 07/11/2017.

[TORNA AL SOMMARIO](#)

4.8. RESPONSABILE DELLO SVILUPPO E DELLA MANUTENZIONE DEL SISTEMA DI CONSERVAZIONE



Nominativo	Funzioni
Giandomenico Bosco	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. Gestione delle relazioni con la società produttrice del sistema di conservazione LegalArchive e coordinamento per quanto attiene le attività di sviluppo del sistema EasyLegal di sviluppo interno.

La nomina è stata formalizzata con documento sottoscritto per accettazione dal responsabile il **08/01/2019**

[TORNA AL SOMMARIO](#)

4.9. SOGGETTI CHE NEL TEMPO HANNO ASSUNTO RUOLI DI RESPONSABILITÀ NEL SERVIZIO DI CONSERVAZIONE

RESPONSABILE DEL SERVIZIO DI CONSERVAZIONE

Nominativo	Ruolo	Data inizio mandato	Data fine mandato
Sig. Simone Muzzarelli	Direttore ICT	02/10/2013	01/01/2015
Ing. Giuseppe Cannone	Direzione Tecnica	02/01/2015	In essere

RESPONSABILE DELLA FUNZIONE ARCHIVISTICA DELLA CONSERVAZIONE

Nominativo	Ruolo	Data inizio mandato	Data fine mandato
Moiza Pitocco	Archivista Documentale	Dal 02/01/2015	30/09/2017
Nicola Savino	Consulente	Dal 02/10/2017.	In essere



RESPONSABILE DEL TRATTAMENTO DEI DATI

Nominativo	Ruolo	Data inizio mandato	Data fine mandato
Severino Cirimelli	Consulente	Dal 02/01/2015	In essere

RESPONSABILE DELLA SICUREZZA DEI SISTEMI PER LA CONSERVAZIONE

Nominativo	Ruolo	Data inizio mandato	Data fine mandato
Giulio Del Tavano	Sistemi Informativi	Dal 02/01/2015	In essere

RESPONSABILE DEI SISTEMI INFORMATIVI PER LA CONSERVAZIONE

Nominativo	Ruolo	Data inizio mandato	Data fine mandato
Giulio Del Tavano	Sistemi Informativi	Dal 02/01/2015	Al 6/11/2017
Cristian Micarelli	Networking	Dal 7/11/2017	In essere

RESPONSABILE DELLO SVILUPPO E DELLA MANUTENZIONE DEL SISTEMA DI CONSERVAZIONE

Nominativo	Ruolo	Data inizio mandato	Data fine mandato
Andrea Pellegrini	Sviluppo Software	Dal 2/01/2015	Al 6/11/2017
Valentino Angeloni	Sviluppo Software	Dal 7/11/2017	Al 7/01/2019
Giandomenico Bosco	Sviluppo Software	Dal 8/01/2019	In essere

[TORNA AL SOMMARIO](#)

5. STRUTTURA ORGANIZZATIVA DEL SERVIZIO DI CONSERVAZIONE

L'articolo 6 del citato DPCM 3 Dicembre 2013 individua i seguenti ruoli nel sistema di conservazione:

- a) Produttore
- b) Utente
- c) Responsabile della Conservazione
- d) Organismo di tutela e Vigilanza;



5.1.PRODUTTORE

E' il soggetto (persona fisica ovvero giuridica, interna od esterna al sistema di conservazione), 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

I rapporti fra Produttore e Corvallis DM sono disciplinati dal **Contratto di Affidamento** e **dalle relative specifiche tecniche** che definiscono i dettagli di erogazione del servizio (set di metadati, modalità e tempistiche dei versamenti etc). Il Produttore è responsabile dell'integrità ed autenticità del pacchetto di versamento.

In qualità di Società di gestione documentale, la Corvallis DM, può fungere, in relazione a specificità del contratto di affidamento del servizio di conservazione, da produttore dei documenti informatici tramite acquisizione della copia per immagine su supporto informatico di documenti analogici (art. 3 comma 1 lettera b) del DPCM 13 novembre 2014), e dei relativi pacchetti di versamento al sistema di conservazione.

[TORNA AL SOMMARIO](#)

5.2.UTENTE

E' il soggetto (persona fisica ovvero giuridica, interna od esterna al sistema di conservazione) che accede al sistema medesimo per acquisire le informazioni di interesse nei limiti previsti dalla legge. Il contratto di affidamento e le relative specifiche tecniche individuano i soggetti all'interno della struttura del produttore che assumono il ruolo di utente: il sistema di autenticazione ed accesso è definito in coerenza con il piano della sicurezza previsto dagli articoli 31-36 del DLgs. 196/2003 così come modificato dal DLgs. 101/2018, dal Regolamento Europeo (UE) 2016 / 679 ed agli articoli 50 e 51-bis del Codice dell'Amministrazione Digitale.

[TORNA AL SOMMARIO](#)

5.3.RESPONSABILE DELLA CONSERVAZIONE

Ai sensi del DPCM 3 dicembre 2013 è la figura responsabile dell'insieme delle attività elencate all'art 8 del citato DPCM (si veda paragrafo 5.6). ed sempre interno al soggetto produttore¹.

[TORNA AL SOMMARIO](#)

5.4.ORGANISMO DI TUTELA E VIGILANZA

Il decreto Legislativo 22 gennaio 2004 n. 42 definisce le competenze del Ministero dei Beni e le Attività Culturali per la tutela e la valorizzazione dei beni culturali

¹ Il responsabile del servizio di conservazione è invece una figura interna al soggetto conservatore



“Al fine di garantire l’esercizio unitario delle funzioni di tutela, ai sensi dell’Articolo 118 della Costituzione, le funzioni stesse sono attribuite al Ministero per i beni e le attività culturali, di seguito denominato «Ministero», che le esercita direttamente o ne può conferire l’esercizio alle regioni, tramite forme di intesa e coordinamento ai sensi dell’Articolo 5, commi 3 e 4. Sono fatte salve le funzioni già conferite alle regioni ai sensi dei commi 2 e 6 del medesimo Articolo 5”

Il Ministero esercita le sue funzioni sugli archivi e documenti prodotti e /o ricevuti dalla pubblica amministrazione centrale e locale e, sugli archivi e documenti di soggetti privati che rivestono interesse storico particolarmente importante.

Sono soggetti a preventiva autorizzazione del Ministero:

-
- a) la demolizione delle cose costituenti beni culturali, anche con successiva ricostituzione;*
 - b) lo spostamento, anche temporaneo, dei beni culturali, salvo quanto previsto ai commi 2 e 3;*
 - c) lo smembramento di collezioni, serie e raccolte;*
 - d) lo scarto dei documenti degli archivi pubblici e degli archivi privati per i quali sia intervenuta la dichiarazione ai sensi dell’Articolo 13;*
 - e) il trasferimento ad altre persone giuridiche di complessi organici di documentazione di archivi pubblici, nonché di archivi di soggetti giuridici privati.*
-

2. Lo spostamento di beni culturali, dipendente dal mutamento di dimora o di sede del detentore, è preventivamente denunciato al soprintendente, che, entro trenta giorni dal ricevimento della denuncia, può prescrivere le misure necessarie perché i beni non subiscano danno dal trasporto

3. Lo spostamento degli archivi correnti dello Stato e degli enti ed istituti pubblici non è soggetto ad autorizzazione.

4. Fuori dei casi di cui ai commi precedenti, l’esecuzione di opere e lavori di qualunque genere su beni culturali è subordinata ad autorizzazione del soprintendente. 5. L’autorizzazione è resa su progetto o, qualora sufficiente, su



descrizione tecnica dell'intervento, presentati dal richiedente, e può contenere prescrizioni

Nell'ambito del servizio di conservazione elettronica i soggetti conservatori accreditati sono sottoposti alla vigilanza dell'AGID.

[TORNA AL SOMMARIO](#)

5.5. [ORGANIGRAMMA DEL SERVIZIO DI CONSERVAZIONE](#)

Si riporta l'organigramma del servizio di conservazione

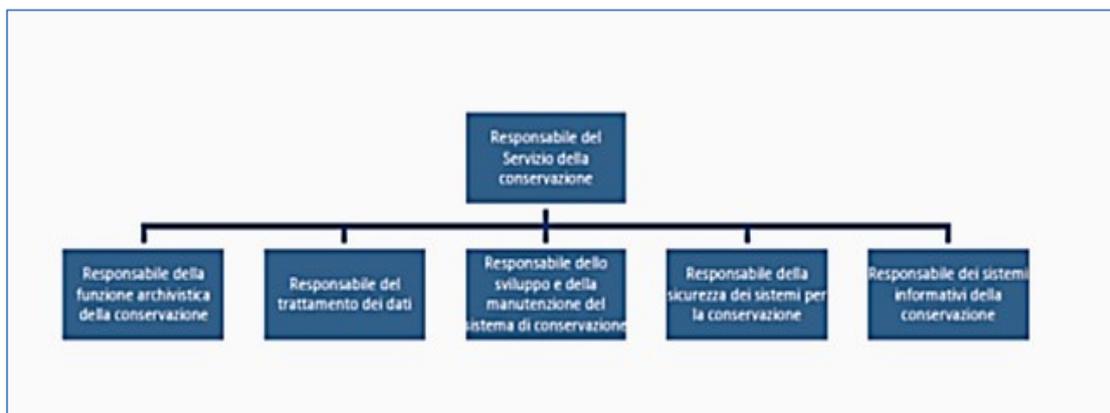


Figura 1: Organigramma del servizio di conservazione di Corvallis DM

[TORNA AL SOMMARIO](#)

5.6. [STRUTTURE ORGANIZZATIVE](#)

5.6.1. ATTIVITÀ PROPRIE DEL CONTRATTO DI SERVIZIO DI CONSERVAZIONE

Attività	Figura Responsabile
Attivazione contratto	Responsabile del Servizio di Conservazione
Acquisizione, verifica e gestione dei pacchetti di versamento persi in carico e generazione del rapporto di versamento	Responsabile del Servizio di Conservazione, Responsabile delle sviluppo e della manutenzione; Responsabile funzione archivistica



Preparazione e gestione del pacchetto di archiviazione	Responsabile del Servizio di Conservazione, Responsabile funzione archivistica
Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione	Responsabile del Servizio di Conservazione, Responsabile della sicurezza dei sistemi per la conservazione Responsabile trattamento dati Responsabile funzione archivistica
Scarto dei pacchetti di archiviazione	Responsabile del Servizio di Conservazione, Responsabile funzione archivistica
Chiusura del servizio di conservazione (al termine di un contratto)	Responsabile del Servizio di Conservazione

[TORNA AL SOMMARIO](#)

5.6.2. *[ATTIVITÀ PROPRIE DI GESTIONE DEI SISTEMI INFORMATIVI](#)*

Attività	Figura Responsabile
Conduzione e manutenzione del sistema di conservazione	Responsabile della sicurezza dei sistemi per la conservazione Responsabile dei sistemi informativi per la conservazione
Monitoraggio del sistema del sistema di conservazione	Responsabile dello sviluppo e della manutenzione Responsabile dei sistemi informativi per la conservazione
Change management	Responsabile della sicurezza dei sistemi per la conservazione Responsabile dello sviluppo e della manutenzione Responsabile dei sistemi informativi per la conservazione
Verifica periodica di	Responsabile della sicurezza dei sistemi per la conservazione Responsabile dei sistemi informativi per la conservazione Responsabile funzione archivistica

[TORNA AL SOMMARIO](#)



6. OGGETTI SOTTOPOSTI A CONSERVAZIONE

6.1. OGGETTI CONSERVATI

In EasyLegal® ed in LegalArchive® la descrizione archivistica è l'insieme di configurazioni che mette in relazione:

- Soggetto Produttore;
- Tipologia documentaria;
- Informazioni sulla rappresentazione (metadati ed informazioni di conservazione).

La descrizione archivistica delinea le modalità con cui è eseguito il processo di conservazione e può essere di due tipi differenti:

- **Unità documentaria:** aggregazione di uno o più file, dove uno solamente di essi è il documento principale al quale sono associati dei metadati; gli altri file sono allegati/annessi al documento principale ai quali NON è associato alcun metadato.
- **Fascicolo:** aggregazione di una o più unità documentarie o di uno o più fascicoli.

Il sistema prevede, inoltre, le cosiddette **descrizioni archivistiche speciali**, il cui scopo è fornire le configurazioni per conservare viewer ed informazioni sulla rappresentazione dei documenti, che saranno versati e conservati nel sistema.

Si distinguono tre descrizioni archivistiche speciali:

- **Viewer** di tipologia “unità documentaria” con file indice di tipo multi-indice.

Si tratta di una descrizione che obbligatoriamente e necessariamente deve essere conservata prima di una qualsiasi conservazione di file ad essa associato. Oltre ai metadati previsti dal Dublin Core, questo tipo di descrizione ne prevede alcuni che, permettono di associare

- l'oggetto conservato, cioè l'eseguibile del visualizzatore,
- la versione del visualizzatore;
- la lingua del visualizzatore;
- il sistema operativo di riferimento.

- **Informazioni sulla rappresentazione di tipologia “Documento”** con file indice di tipo indice singolo.

Le descrizioni di questo tipo definiscono i documenti contenenti informazioni sulla rappresentazione, sia di tipo sintattico che di tipo semantico, distinte queste per mezzo del metadato “Tipo” di Dublin Core.

- **Informazioni sulla rappresentazione di tipo Fascicolo**

Le descrizioni in specie, raccolgono, in un unico fascicolo, per ciascun formato file le informazioni di cui sopra

[TORNA AL SOMMARIO](#)

6.1.1. [I METADATI](#)

Il sistema di conservazione deve assicurare:



Dalla presa in carico dal produttore [...] fino all'eventuale scarto, la conservazione tramite l'adozione di regole, procedure e tecnologie, dei seguenti oggetti in esso conservati, garantendone le caratteristiche di autenticità, integrità, affidabilità, reperibilità [...]

L'autenticità del documento è assicurata dall'integrità, intesa come completezza e non modificabilità del contenuto informativo e dall'identificazione univoca del soggetto produttore nel contesto di riferimento: un documento autentico, certo ed integro, è un documento affidabile, cioè un documento che assolve alla sua funzione di "rappresentazione di atti, fatti, e/o dati giuridicamente rilevanti".

Gli elementi archivistici che concorrono a determinare l'identità di un documento informatico e analogico sono (cfr. ISAD):

- Nome del Soggetto produttore (cfr ISAAR (CPF));
- Oggetto del documento;
- Date di produzione e trasmissione;
- Espressione del vincolo archivistico (classificazione/fascicolazione)
- Indicazione di eventuali allegati.

Gli elementi archivistici che concorrono a determinare l'integrità del documento sono:

- Nome dell'ufficio competente a trattare l'argomento,
- Nome dell'ufficio cui inerisce la responsabilità principale per la tenuta del documento;
- Indicazioni dei tipi di eventuali annotazioni presenti sul documento;
- Indicazioni di eventuali modifiche tecniche;
- Privilegi di accesso.

Il documento, nella sua funzione di testimonianza culturale, deve essere fruibile ed interpretabile anche dai futuri utenti: l'interpretabilità sottende ed implica, necessariamente, la possibilità di ricostruire "ad post" il procedimento amministrativo/operativo da cui è stato generato (contesto di produzione: autore, destinatario, data di produzione, responsabile del procedimento, oggetto del procedimenti, documenti collegati etc. etc.).

Da quanto sopra è evidente il ruolo fondamentale dei metadati; in particolare dei metadati archivistici, nel processo di conservazione a lungo termine degli oggetti digitali, deputati fra l'altro a:

- Garantire l'identificazione permanente dei singoli oggetti informati (numero di protocollo, data, autore etc);
- Garantire l'identificazione permanente delle relazione fra gli oggetti informativi (indice di classificazione, fascicolazione);



- Conservare le informazioni che ì rendono possibile la comprensione degli oggetti informativi (procedimento amministrativo);

In relazione alla loro funzione i metadati sono classificati in:

- Metadati descrittivi: necessari per il recupero degli oggetti digitali e si riferiscono al contenuto dell'oggetto (EAD "Encoded Archival Description", EAC "Encoded Archival of Context – Corporate bodies, Persons, and Families," Dublin Core Metadata Initiative);
- Metadati amministrativi: relativi alle operazione per la gestione degli oggetti digitali (owner, localizzazione, provenienza, diritti e copyright);
- Metadati strutturali : relativi alle relazioni tra gli oggetti;
- Metadati tecnici: relativi alla gestione, archiviazione e preservazione degli oggetti, nonché informazione sul formato dei file impiegati per la loro rappresentazione (tipo, versione, etc) ed alla creazione dell'oggetto digitale (METS – "Metadata Encoding and Trasmission Standard").

Nel modello informativo e funzionale OAIS, l'oggetto informativo è costituito dall'oggetto e dalle informazioni sulla rappresentazione che ne consentono l'intelligibilità: il pacchetto informativo, quale somma dell'oggetto digitale e dei relativi metadati per la conservazione, è pertanto composto da due componenti:

- informazioni sul contenuto;
- informazioni sulla conservazione:
 - informazioni di identificazione dell'oggetto nel patrimonio conservato (es codice ISBN)
 - informazioni di contesto, relative alle relazioni tra il contenuto di un dato pacchetto informativo e altri pacchetti;
 - informazioni di provenienza relativi alla storia del contenuto, quale creazione, passaggio di proprietà etc;
 - informazioni sull'integrità relativi ai controlli affinché un contenuto informativo non sia alterato ed alterabile.

Nei sistemi di conservazione EasyLegal® e LegalArchive® i metadati possono essere di vari tipi, in particolare vengono gestiti i seguenti tipi:

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

Inoltre, per ogni metadato è possibile definire:



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

Inoltre, il sistema, in quanto sistema di conservazione, è in grado di classificare i metadati versati in base alla gestione Privacy a cui sono soggetti.

La classificazione permette di gestire i seguenti casi.

- Dato generico;
- Dato personale;
- Dato sensibile;
- Dato giudiziario.

[TORNA AL SOMMARIO](#)

6.1.2. [I FORMATI](#)

I sistemi di conservazione EasyLegal® e LegalArchive® supportano ed utilizzano come formati tutti quelli previsti nell'allegato 2 al DCPM 03/12/2013, ed è in grado di gestire, su richiesta del Soggetto Produttore, anche formati non presenti nel su citato allegato, ma che tuttavia il Soggetto Produttore utilizza nei propri sistemi e che ritiene opportuno conservare.

Tutti i formati gestiti sono, opportunamente, elencati e descritti in un registro interno al sistema di conservazione "Registro dei Formati", nel quale ogni formato è corredato da informazioni descrittive relative alla versione ed al Mimetype.

L'elenco dei formati ammessi è riportato e gestito nelle funzionalità "Amministrazione strutture versanti" del sistema, ed è aggiornato in base alle esigenze del Soggetto Produttore, con cui sono concordate le modalità di aggiornamento: tale elenco è parte integrante delle specifiche tecniche di servizio contrattualizzato.

I sistemi EasyLegal e LegalArchive® identificano i formati alla ricezione del SIP attraverso l'analisi del magic number o del contenuto del file, in modo tale da individuare lo specifico Mimetype. L'informazione sul formato parte integrante dei Metadati dei componenti dell'unità documentaria e costituisce un elemento delle Informazioni sulla rappresentazione.

Di seguito si riportano i formati attualmente previste dalle Regole Tecniche

Formato	Caratteristiche
PDF-PDF/A	Proprietario: Adobe Systems
	Estensione: .PDF
	Tipo mime: application/pdf



	Aperto: SI
	Ultima versione: 1.7
	Standard: ISO 32000-1 (PDF) ISO 19005-1:2005 (vers. PDF 1.4) ISO 19005-2:2011 (vers. PDF 1.7)

Formato	Caratteristiche
Tiff	Proprietario: Aldus Corporation in seguito acquistata da Adobe
	Estensione: .tiff
	Tipo mime: image/tiff
	Aperto: NO
	Ultima versione: 2009
	Standard: TIFF 6.0 del 1992 TIFF Supplement 2 del 2002

Formato	Caratteristiche
JPG	Proprietario: Joint Photographic Experts Group
	Estensione: .jpg, .jpeg
	Tipo mime: image/jpeg
	Aperto: SI
	Ultima versione: 2009
	Standard: ISO/IEC 10918:1

Formato	Caratteristiche
Office Open XML (OOXML)	Proprietario: Microsoft
	Estensione: .docx, .xlsx, .pptx
	Tipo mime:
	Aperto: SI
	Ultima versione: 1.1
	Standard: ISO/IEC DIS 29500:2008

Formato	Caratteristiche
Open Document Format	Proprietario: OASIS
	Estensione: .ods, .odp, .odg, .odb
	Tipo mime: application/vnd.oasis.opendocument.text
	Aperto: SI
	Ultima versione: 1.0
	Standard: ISO/IEC 26300:2006 UNI CEI ISO/IEC 26300



Formato	Caratteristiche
XML	Proprietario: W3C
	Estensione: .xml
	Tipo mime: application/xml text/xml
	Aperto: SI
	Ultima versione:
	Standard:

Nella scelta dei formati è necessario tener conto di caratteristiche ²peculiari quali:

- **Apertura:** il formato è conforme a specifiche pubbliche, cioè disponibili a chiunque abbia interesse ad utilizzare quel formato. La disponibilità delle specifiche del formato rende sempre possibile la decodifica dei documenti rappresentati in conformità con dette specifiche, anche in assenza di prodotti che effettuino tale operazione automaticamente. Questa condizione si verifica sia quando il formato è documentato e pubblicato da un produttore o da un consorzio al fine di promuoverne l'adozione, sia quando il documento è conforme a formati definiti da organismi di standardizzazione riconosciuti. In quest'ultimo caso tuttavia si confida che quest'ultimi garantiscono l'adeguatezza e la completezza delle specifiche stesse.
- **Sicurezza:** dipende dal grado di modificabilità del contenuto del file e dalla capacità di essere immune dall'inserimento di codice maligno
- **Portabilità:** facilità con cui i formati possano essere usati su piattaforme diverse, sia dal punto di vista dell'hardware che del software, inteso come sistema operativo. Di fatto è indotta dall'impiego fedele di standard documentati e accessibili
- **Funzionalità:** la possibilità da parte di un formato di essere gestito da prodotti informatici, che prevedono una varietà di funzioni messe a disposizione dell'utente per la formazione e gestione del documento informatico.
- **Supporto allo sviluppo:** modalità con cui si mettono a disposizione le risorse necessarie alla manutenzione e sviluppo del formato e i prodotti informatici che lo gestiscono (organismi preposti alla definizione di specifiche tecniche e standard, società, comunità di sviluppatori, ecc.).
- **Diffusione:** l'estensione dell'impiego di uno specifico formato per la formazione e la gestione dei documenti informatici. Questo elemento influisce sulla probabilità che esso venga supportato nel tempo, attraverso la disponibilità di più prodotti informatici idonei alla sua gestione e visualizzazione.

[TORNA AL SOMMARIO](#)

6.2. [PACCHETTO DI VERSAMENTO](#)

Si tratta del pacchetto informativo inviato dal Soggetto Produttore al sistema di conservazione e oggetto dell'accordo stipulato in occasione del contratto di affidamento del servizio di conservazione.

² Allegato 2 DPCM 03/12/2013



Nel sistema di conservazione sono accettati pacchetti di versamento, che rispondono alle caratteristiche tecnologiche e informative previste nelle rispettive specifiche tecniche, documento allegato al contratto di affidamento.

Un Soggetto Produttore può decidere, nella fase di negoziazione iniziale alla stipula del contratto di affidamento del servizio, di versare i pacchetti di versamento in maniera automatizzata, semiautomatizzata oppure manuale da interfaccia web.

Il sistema di conservazione supporta i pacchetti di versamento nel formato CSV in tre varianti:

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

i sistemi EasyLegal® e LegalArchive® supportano quattro tipi di file metadati:

- **File di metadati semplice:** trattasi di un (1) file referenziato in 1 riga che identifica 1 documento,

```
parere01.pdf | 14146 | 2010-01-08 | N.D.  
parere02.pdf.p7m | 14158 | 2010-01-08 | Tizio  
parere03.pdf.p7m | 14158 | 2010-01-08 | Caio
```

Figura 2: File di metadati semplice

- **File di metadati con documenti ed allegati:** trattasi di n file referenziati in n righe che identifica 1 documento,

```
determina77157755820329.pdf | 2010-01-08 | 1 | 2010-01-  
08 | 2010 | LIQUIDAZIONE | 2010/02.12/000001  
+fattura001.pdf.p7m  
+graffetta.xls  
+ordine.doc  
+parere.doc
```

Figura 3: File di metadati con documenti ed allegati

- **File di metadati multi-indice :** trattasi di un (1) file referenziato in n righe che identificano n documenti, dove ogni riga rappresenta un documento in un unico file



CORVALLIS DM

EN/ISO 14001:2004 IE-0915-05
ISO/IEC 27001:2013 IIS-1014-01
ISO 9001 IQ-1015-02



Dasa-Rägister

00-CDM-Manuale Conservazione-Rev-1-13-del-15-gennaio-2019.docx

```
ciclofatturazione.pdf | 14146 | 2014-11-08 | 1  
ciclofatturazione.pdf | 14157 | 2014-11-08 | 2  
ciclofatturazione.pdf | 14158 | 2014-11-08 | 4
```

Figura 4: File di metadati multi-indice



- **File di metadati fascicolo:** righe con metadati variabili. L' esempio sotto riportato, si riferisce ad un fascicolo che contiene:
- Un fascicolo determina;
 - Documenti generici;
 - Unità documentaria.

```
fasc_7715304577755820329.xml|fascicolo|2010/02.12/000001
determ77.pdf|determina||2010-01-08|2010-01-08 1|2010|LIQUIDAZIONE
||2010/02.12/000001
13917.merge.doc.p7m|documento generico|13917|2010-01-08 1|Tizio
13918.graffetta.xls| documento generico|13918|2010-01-08 1|N.D.
13990.parere.doc| documento generico|13990|2010-01-08 1|N.D.
14158.parere.doc.p7m|ud|14158|2010/02.12/000001|Caio
+ordine.doc
+parere.doc
```

Figura 5:file di metadati fascicolo

Analizzando la struttura dei file di metadati riportati, si evidenzia come le regole per comporre il file di metadati siano:

- La prima colonna è sempre il percorso al file:
- Nel caso in cui non sia riportato il percorso, il sistema assume che il file referenziato si trovi sempre nelle stessa cartella del file di metadati.
 - Il separatore può essere il carattere “|” o il carattere “;”;
 - Il carattere + ad inizio riga indica al sistema che il file referenziato è un allegato/annesso al documento referenziato dalla riga che riporta i metadati;
 - Nel caso di versamento di un fascicolo è indispensabile conoscere i metadati che legano i documenti tra loro.

Generalmente la sintassi del file di metadati è la seguente



```
directory1]
[path] file1;valoremetadato1;valoremetadato2;valoremetadato3;...;
valoremetadaton
+) [path] file2;valoremetadato1;valoremetadato2;valoremetadato3;...;
valoremetadaton
..
directory2]
[path] file3;valoremetadato1;valoremetadato2;valoremetadato3;...;
valoremetadaton
..
directoryk]
[path] filen;valoremetadato1;valoremetadato2;valoremetadato3;...;
valoremetadaton
..
```

Figura 6: Sintassi file di metadati

La fase relativa alla preparazione del pacchetto di versamento (SIP) e il conseguente invio al sistema di conservazione può avvenire in modi diversi, essendo dipendente fortemente dalla situazione specifica del soggetto produttore.

Il sistema di conservazione dispone di tre modi per sottoporre un pacchetto di versamento:

- via web service (rest);
- via file system;
- via (s)FTP;

Il sistema di versamento mette a disposizione del Soggetto Produttore una serie di funzionalità di validazione che gli consentono, se necessario, di correggere la composizione dei pacchetti di versamento prima della sua acquisizione da parte del conservatore. Il Soggetto Produttore potrà correggere i metadati descrittivi e le relazioni con il contesto archivistico laddove queste non fossero state correttamente impostate in fase di prima produzione dei singoli SIP.



Il sistema, superate le validazioni dei documenti del pacchetto di versamento restituisce al Produttore, il rapporto di versamento che, può essere acceduto del Soggetto Produttore direttamente dal sistema di conservazione.

Di seguito viene riportato un esempio di rapporto di versamento. Nell'intestazione vengono riportate le informazioni relative al Responsabile della conservazione, al produttore ed alla data e ora di creazione del report. Successivamente vengono riportati i totali dei documenti corretti ed errati e l'esito del versamento, dopodiché per ogni documento versato viene mostrata una tabella contenente le informazioni sul documento e sui metadati e l'esito del controllo di validità.

Il file contenente il report dovrà essere in formato PDF e firmato digitalmente.

RAPPORTO DI VERSAMENTO

Responsabile della conservazione: Mario Rossi

Produttore: Test

Date e ora creazione: 2016-06-09 15:01:32

Esito del versamento:

Documenti corretti	1
Documenti errati:	1
Esito	KO

Documento 1 di 2

Nome file:	2013_V-300-99957.pdf
Tipo documento	Fattura elettronica
Hash - SHA256:	79fd5fe12d11264e5bef72cc11dd5317b35627a47c4602f91d60b6f0abd9ca49
[Tag]	n/a
[Numero_Fattura]	FT/2013/00479/178
[Anno_Compentenza]	2013
[Data_Registrazione]	2013-12-10
[Partita_IVA]	11111111111
[Denominazione]	Prova
[Codice_Fiscale]	ABCDEF83T43H703N
[Data_Fattura]	2013-12-03
Esito del versamento:	OK

Documento 2 di 2

Nome file:	2013_V-300-99958..pdf
Tipo documento	Fattura elettronica
Hash - SHA256:	79fd5fe12d11264e5bef72cc11dd5317b35627a47c4602f91d60b6f0abd9ca49
[Tag]	n/a
[Numero_Fattura]	
[Anno_Compentenza]	
[Data_Registrazione]	2013-12-10



[Partita_IVA]	22222222222
[Denominazione]	Prova2
[Codice_Fiscale]	ABCDEF83T43H703N
[Data_Fattura]	2013-12-03
Esito del versamento	KO. Metadati obbligatori mancanti

Le validazioni sono concordate con il Soggetto Produttore nel contratto di servizio di conservazione. Una volta che i pacchetti di versamento sono stati acquisiti, questi vengono trasformati in pacchetti di archiviazione (AIP).

[TORNA AL SOMMARIO](#)

6.3. [PACCHETTI DI ARCHIVIAZIONE](#)

L’AIP è l’elemento fondamentale dei due sistemi di conservazione: è il pacchetto informativo che racchiude in sé tutti gli elementi sufficienti e necessari per una conservazione a lungo termine.

Lo standard UNI11386 “Supporto all’interoperabilità nella conservazione e nel recupero degli oggetti digitali (SInCRO) definisce la struttura del pacchetto di archiviazione come sotto riportata

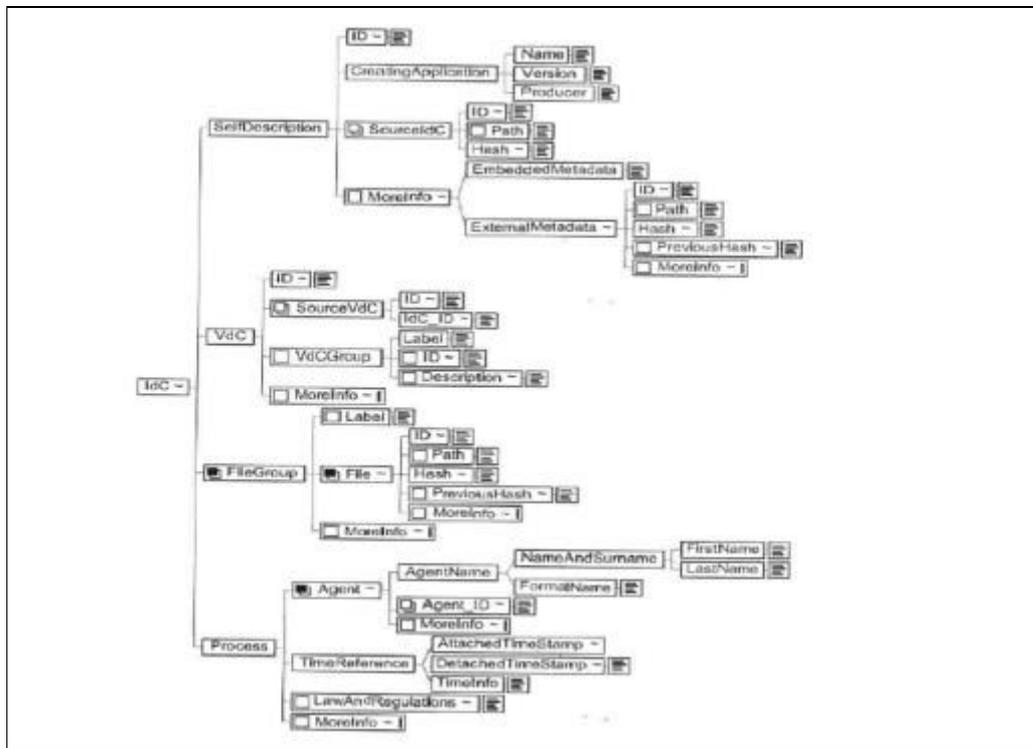


Figura 7:Struttura pacchetto di archiviazione secondo lo standard UNI 11386



Vediamo nel dettaglio valore e funzione dei singoli elementi

Elemento	Definizione
Self Description	Descrizione: Informazioni relative all'indice di conservazione stesso, associato al volume di conservazione
	Elemento Padre: Idc
	Elemento Figlio : CreatingApplication ID, MoreInfo SourceIF

Elemento	Definizione
ID	Descrizione : Identificatore univoco dell'entità descritta
	Elemento Padre: External Metadata, File, SelfDescription, SourceID, SourceVdC, VdC, VdcGroup
	Elemento Figlio : Nessuno

Elemento	Definizione
CreatingApplication	Descrizione : Informazioni sull'applicazione che ha generato l'IdC
	Elemento Padre: SelfDescription,
	Elemento Figlio : Name, Producer, Version

Elemento	Definizione
Name	Descrizione: Nome dell'applicazione che ha generato l'IdC
	Elemento Padre: CreatingApplication
	Elemento Figlio : nessuno

Elemento	Definizione
Producer	Descrizione: Nome del produttore dell'applicazione che ha generato l'IdC
	Elemento Padre: CreatingApplication
	Elemento Figlio : nessuno

Elemento	Definizione
Version	Descrizione: Versione dell'applicazione che ha generato l'idC
	Elemento Padre: CreatingApplication
	Elemento Figlio : nessuno

Elemento	Definizione
SourceID	Descrizione: Informazioni relative a uno o più IdC da cui è originato quello oggetto della specifica conservazione: queste informazioni sono



	rilevanti per ricostruire la storia degli oggetti digitali sottoposti a conservazione
	Elemento Padre: SelfDescription,
	Elemento Figlio : Hash, Id, Path

Elemento	Definizione
Path	Descrizione: Informazioni relative alla localizzazione del file cui l'elemento si riferisce, espressa come indirizzo URI
	Elemento Padre: ExternalMetadata , File, SourceId
	Elemento Figlio : nessuno

Elemento	Definizione
Hash	Descrizione: Informazioni sull'impronta del file sui li elemento si riferisce
	Elemento Padre: ExternalMetadata , File, SourceId
	Elemento Figlio : nessuno

Elemento	Definizione
MoreInfo	Descrizione: Informazioni ulteriori: all'interno dell'elemento <File>, può essere utilizzato per descrivere i file oggetto di conservazione coerentemente con un schema che utilizzi un insieme di metadati specializzati nel dominio/contesto d'uso
	Elemento Padre: Agent, ExternalMetadata, File, FileGroup, Process, SelfDescription, VdC
	Elemento Figlio : EmbeddedMetadata, ExternalMetadata

Elemento	Definizione
Embedded Metadata	Descrizione: Informazioni dell'elemento <MoreInfo> integrate all'interno dell'IdC e strutturate in format XML
	Elemento Padre: MoreInfo
	Elemento Figlio : Nessuno

Elemento	Definizione
External Metadata	Descrizione: Informazioni dell'elemento <MoreInfo> contenute all'esterno dell'IdC in un file XML le cui caratteristiche sono descritte nei sub elementi di <ExternalMetadata>
	Elemento Padre: MoreInfo



	Elemento Figlio : Hash, ID, MoreInfo, Path, Previous-Hash
--	---

Elemento	Definizione
Previous-Hash	Descrizione: Informazioni su precedenti impronte del file oggetto di conservazione o del file di metadati (esterno all'IdC) che contiene le informazioni dell'elemento <MoreInfo>
	Elemento Padre: ExternalMetadata, File
	Elemento Figlio : Nessuno
Elemento	Definizione
VdC (Volume di conservazione)	Descrizione: Informazioni relative al volume di conservazione
	Elemento Padre: IdC
	Elemento Figlio : ID, MoreInfo, SourceVdC, VdCGroup

Elemento	Definizione
Source VdC	Descrizione: Informazioni relative a uno o più volumi di conservazione da cui è originato quello oggetto di specifica conservazione (per esempio migrazione di un volume o aggregazione di più volumi)
	Elemento Padre: VdC
	Elemento Figlio : ID, IdC_ID

Elemento	Definizione
IdC_ID	Descrizione: Identificatore univoco dell'indice di conservazione associato al precedente volume di conservazione oggetto della descrizione. Il valore dell'identificatore deve coincidere con il valore dell'elemento <ID> contenuto all'interno dell'elemento <SourceIdC>
	Elemento Padre: SourceIdC
	Elemento Figlio Nessuno

Elemento	Definizione
VdCGroup	Descrizione: Informazioni relative ad una eventuale tipologia/aggregazione, di natura fisica o logica, cui il VdC appartiene
	Elemento Padre: VdC
	Elemento Figlio Description, Id, Label

Elemento	Definizione
Label	Descrizione: Nome dell'eventuale tipologia/aggregazione cui appartiene il File o il VdC
	Elemento Padre: FileGroup, VdCGroup
	Elemento Figlio Nessuno



Elemento	Definizione
Description	Descrizione: Informazioni descrittive relative ad un eventuale tipologia/aggregazione , di natura logica o fisica, cui il VdC appartiene
	Elemento Padre: VdCGroup
	Elemento Figlio Nessuno

Elemento	Definizione
FileGroup	Descrizione: Elemento di aggregazione di più file oggetto di conservazione. Tale elemento è funzionale alla creazione di insiemi di file sulla base di criteri di ordine logico o tipologico.
	Elemento Padre: IdC
	Elemento Figlio File, Label, MoreInfo

Elemento	Definizione
File	Descrizione: Informazioni relative al file oggetto di conservazione.
	Elemento Padre: FileGroup
	Elemento Figlio Hah, ID, MoreInfo, Path, PreviousHash

Elemento	Definizione
Process	Descrizione: Informazioni relative alle modalità di svolgimento del processo di conservazione.
	Elemento Padre: IdC
	Elemento Figlio Agent, LawAndRegulations, MoreInfo, Timereference

Elemento	Definizione
Agent	Descrizione: Informazioni relative ai soggetti che intervengono nel processo di conservazione.
	Elemento Process
	Elemento Figlio Agent_ID, AgentName, MoreInfo

Elemento	Definizione
AgentName	Descrizione: Nome o denominazione dell'agente che interviene nel processo di conservazione.
	Elemento Agent
	Elemento Figlio FormalName, NameAndSurname

Elemento	Definizione
----------	-------------



AgentName	Descrizione: Nome o denominazione dell'agente che interviene nel processo di conservazione.
	Elemento Agent
	Elemento Figlio FormalName, NameAndSurname

Elemento	Definizione
NameAndSurname	Descrizione: Nome e Cognome dell'agente che interviene nel processo di conservazione. Questo elemento deve essere valorizzato nel caso in cui l'agente sia una persona, on caso contrario, sarà valorizzato l'elemento <FormalName>
	Elemento Agent
	Elemento Figlio FirstName, LastName

Elemento	Definizione
FirstName	Descrizione: Nome di battesimo dell'agente che interviene nel processo di conservazione
	Elemento NameAndSurname
	Elemento Figlio Nessuno

Elemento	Definizione
LastName	Descrizione: Cognome dell'agente che interviene nel processo di conservazione
	Elemento NameAndSurname
	Elemento Figlio Nessuno

Elemento	Definizione
FormalName	Descrizione: Denominazione dell'agente che interviene nel processo di conservazione. Questo elemento deve essere valorizzato nel caso in cui l'agente sia un ente.
	Elemento AgentName
	Elemento Figlio Nessuno

Elemento	Definizione
Agent_ID	Descrizione: Identificatore univoco dell'agente che interviene nel processo di conservazione. Se l'identificatore è un codice valido in un ambito nazionale (es codice fiscale) a tale codice deve essere premesso il codice di paese individuato da ISO 3166, seguito dal carattere ",". Se l'agente è colui che appone la firma digitale sull'IdV, è da privilegiare l'uso di un codice identificativo presente in un campo del suo certificato digitale.
	Elemento AgentName



	Elemento Figlio Nessuno
--	-------------------------

Elemento	Definizione
TimeReference	Descrizione: nformazioni relative a data ed ora di realizzazione dell'indice di conservazione. Tale elemento funge solo da mero contenitore di elementi subordinati, per distinguere i seguenti casi <ul style="list-style-type: none"> • Generico riferimento temporale (usato per valorizzare l'elemento <TimeInfo>); • Marca temporale <i>detached</i> (il cui indirizzo URI valorizza l'elemento <DetachedTimeStamp>); Marca temporale <i>attached</i> (all'elemento vuoto<AttachedTimeStamp> è associata la data in forma normale).
	Elemento Process
	Elemento Figlio AttachedTimeStamp, DetachedTimeStamp, TiemInfo

Elemento	Definizione
AttachedTimeStam	Descrizione: Data ed ora di realizzazione dell'indice di conservazione, in forma normalizzata, nel caso in cui questa sia testimoniata con marca temporale collegata all'IdC stesso. Al contrario dell'analogo elemento <DetachedTimeStamp>, in questo caso non ha senso indicare l'URI (identificativo univoco di risorse) della marca temporale : pertanto l'elemento è di tipo EMPTY. È obbligatorio associare un valore all'attributo normal al fine di esprimere in forma normalizzata data ed ora di realizzazione dell'IdC. In pratica questo elemento è utilizzato qualora l'IdC venga inserito in una busta crittografica.
	Elemento TimeReference
	Elemento Figlio Nessuno

Elemento	Definizione
DetachedTimeStamp	Descrizione: Informazioni sulla localizzazione della marca temporale <i>detached</i> relativa a data ed ora di realizzazione dell'indice di conservazione. Il valore dell'elemento deve essere espresso nel formato URI:
	Elemento TimeReference
	Elemento Figlio Nessuno

Elemento	Definizione
TimeInfo	Descrizione: Informazioni relative a data ed ora di realizzazione dell'indice di conservazione, nel caso in cui queste non assumano la



	forma di una marca temporale. Il valore dell'elemento deve essere nel formato UNI ISO 8601:2010.
	Elemento TimeReference
	Elemento Figlio Nessuno
Elemento	Definizione
LawAndRegulations	Descrizione: Informazioni su norme, regolamenti e standard che guidano il processo di conservazione I:
	Elemento Process
	Elemento Figlio Nessuno

La coerenza di un pacchetto informativo è data da due componenti logiche fondamentali:

- l'insieme delle informazioni statiche, che prevedono un set complesso di metadati che descrivono in maniera "piatta" tutti gli elementi identificativi, descrittivi, gestionali, tecnologici, etc., relativi ad uno e un solo pacchetto informativo;
- l'insieme delle relazioni di contesto, che permettono la correlazione logica del pacchetto informativo agli altri pacchetti informativi e, in generale ad un qualsiasi contesto di natura archivistico-gerarchica.

Concretamente, si può prevedere che nei due sistemi si conserveranno all'interno di un medesimo pacchetto informativo (e quindi incapsulate in una medesima busta) le seguenti componenti, codificate in un XML:

- l'oggetto digitale possibilmente in un formato standard non proprietario;
- l'impronta del documento generata con funzione di hash;
- il riferimento temporale (rappresentato dalla marca temporale o altro riferimento temporale opponibile a terzi, come la segnatura di protocollo);
- il set di metadati per la conservazione;
- metadati identificativi (per esempio possono essere utilizzati i metadati dello standard ISAD);
 - metadati descrittivi (per esempio possono essere utilizzati i metadati dello standard ISAD);
 - metadati gestionali (UNI SinCRO);
 - metadati tecnologici (per esempio possono essere utilizzati i metadati dello standard METS);
- la documentazione tecnica necessaria alla comprensione del viewer stesso (anch'esso può essere un puntatore/riferimento che rimanda alla componente digitale descritta per più pacchetti informativi) oppure la documentazione per la comprensione del documento digitale e/o della classe documentale di riferimento.

L'AIP ha un insieme completo di informazioni sulla conservazione, necessari per ostacolare l'obsolescenza tecnologica, che si aggiungono al file dei metadati versato dal Soggetto Produttore.



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

Ad ogni oggetto versato nel sistema di conservazione sarà associato:

- l'UID del software per la visualizzazione;
- l'UID del fascicolo delle informazioni sulla rappresentazione sintattica;
- l'UID del fascicolo delle informazioni sulla rappresentazione semantica.

Sinteticamente si mostra come sarà costruito l'AIP.

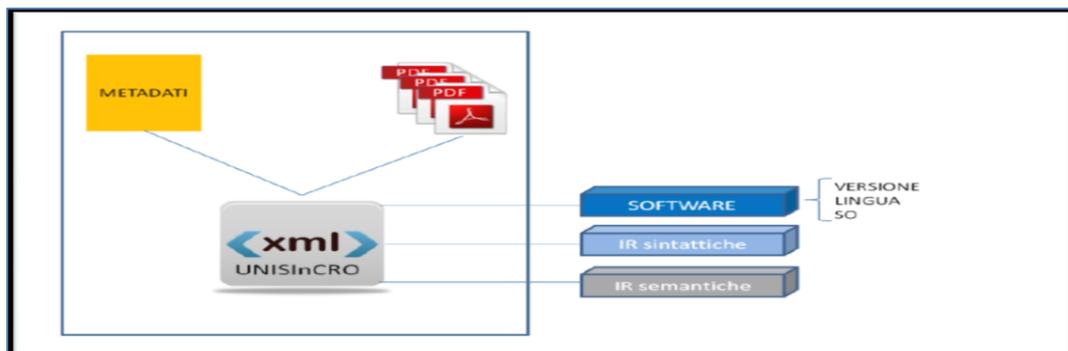


Figura 8: Struttura AIP



Nel riquadro rosso sono evidenziati gli elementi che delineano e parametrizzano le componenti relative alle informazioni sulla rappresentazione mentre nel riquadro blu sono evidenziati gli elementi che descrivono le componenti relative ai metadati.



Figura 10: Contenuto file metadata

Nel riquadro rosso sono messi in evidenza i metadati associati ai file oggetto di conservazione definiti nella descrizione Archivistica cui appartengono i documenti (DocumentoGenerico). troviamo:

- UID con il relativo valore: codice univoco assoluto del file oggetto di conservazione. NB: l'associazione NomeFile – UID viene creata nel file Indice_xxxx.xml;
- DataDocumento con il relativo valore;
- Progressivo con il relativo valore;
- Matricola con il relativo valore;
- Stabilimento con il relativo valore;
- Codice con il relativo valore.

[TORNA AL SOMMARIO](#)

6.4.PACCHETTI DI DISTRIBUZIONE

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

In questo caso, un DIP può anche non coincidere con l'AIP originale conservato nel data center: anzi, molto spesso, ragioni di opportunità inducono a distribuire pacchetti informativi che sono un'estrazione del contenuto informativo di un AIP (negando ad esempio l'accesso ad una parte di esso). Può anche verificarsi il caso di DIP che sono il frutto di più AIP che vengono "spacchettati" e rimpacchettati per un più fruibile utilizzo da parte dell'utente.



Un utente autorizzato di un soggetto produttore, quindi, è in grado di interrogare il sistema per ricevere in uscita uno specifico DIP. L'utente utilizzerà le funzionalità di richiesta di esibizione di un documento o di un insieme di documenti, per ottenerne una replica esatta secondo i fini previsti dalla norma.

I sistemi di conservazione gestiscono un archivio dei software eseguibili ciascuno dei quali utile a visualizzare un determinato formato file cui appartengono i documenti conservati.

I software dell'archivio possono essere associati ad una descrizione archivistica in modo tale che, al momento della generazione dei pacchetti di distribuzione dei documenti informatici da esibire, vengano automaticamente inclusi anche e solo i software necessari alla loro visualizzazione.

In risposta alla richiesta iniziale di esibizione, da parte dell'utente, il sistema risponderà restituendo un DIP che nel caso più completo conterrà:

- i documenti richiesti nel formato previsto per la loro visualizzazione;
- un'estrazione dei metadati associati ai documenti;
- l'indice di conservazione firmato e marcato;
- i viewer necessari alla visualizzazione dei documenti del pacchetto.

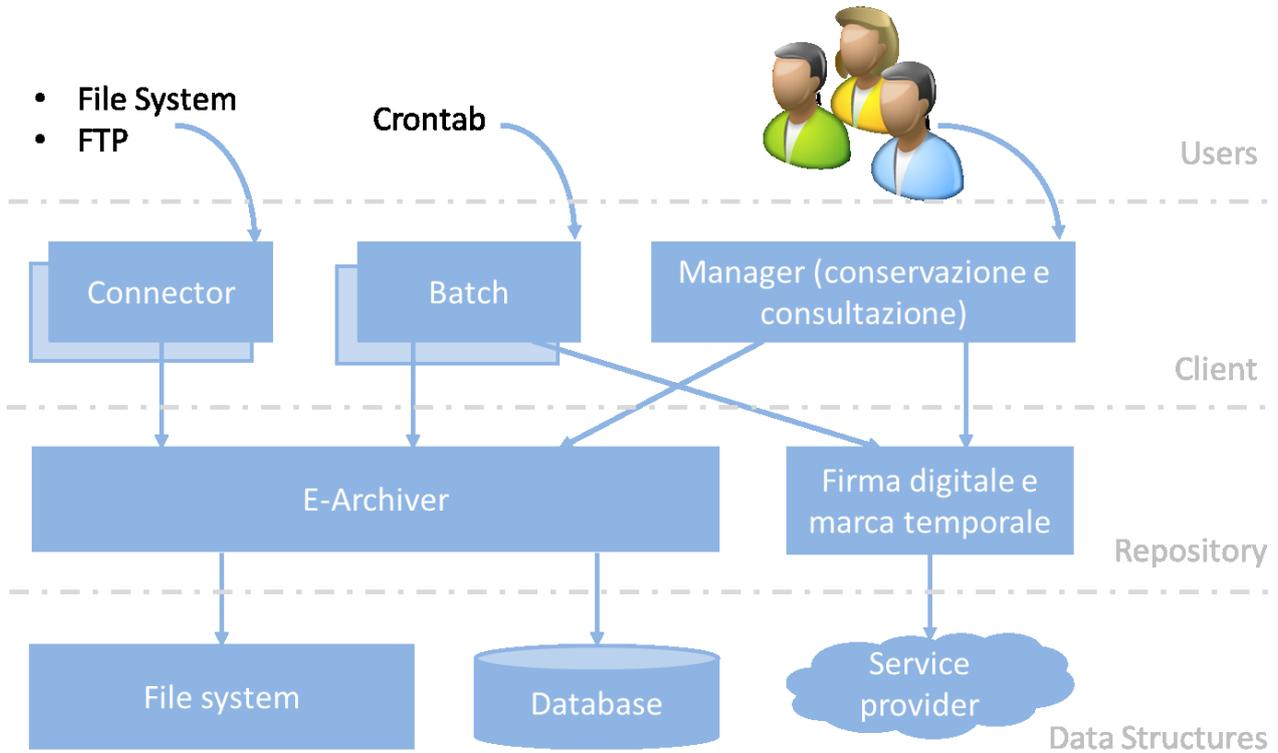
[TORNA AL SOMMARIO](#)

7. IL PROCESSO DI CONSERVAZIONE

EasyLegal® e LegalArchive® definiscono al loro interno un insieme di processi che possono essere schedati in autonomia, al fine di supportare il responsabile della conservazione nelle sue mansioni previste dalla normativa. I processi possono essere classificati ragionevolmente in tre tipologie:

- 1) Presa in carico pacchetti di versamento
- 2) Creazione pacchetto di archiviazione
- 3) Creazione pacchetto di distribuzione per la consultazione

I processi sono implementati mediante moduli e servizi software come nell'architettura che segue:



SISTEMA DI CONSERVAZIONE LegalArchive®

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

Nella tabella seguente si riportano tutti i processi attualmente implementati:

Nome processo	Processo
ProcessoAnonimizza	ANONIMIZZA
ProcessoCancellaProcesso	CANCELLAPROCESSI
ProcessoConservazioneDaIndice	CONSERVAZIONEFS
ProcessoConservazioneDaDB	CONSERVAZIONEDB
ProcessoConservazioneLog	VERSAMENTOLOG
ProcessoConteggi	ACCOUNTING
ProcessoCopialSO	GENERAISO
ProcessoEsibizione	ESIBIZIONE
ProcessoMetadataDictionary	IMPORTADIZIONARIO
ProcessoVerificaMassiva	VERIFICAMASSIVA
Nome processo	Processo
ProcessoCreazioneReport	CREAREPORT



Nome processo	Processo
ProcessoImportazione	IMPORTAZIONE
ProcessoNotificheLimiti	NOTIFICHELIMITI
ProcessoVerificaLicenza	
ProcessoErmes	
Nome processo	Processo
ProcessoErmesCleaner	
ProcessoErmesImport	

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

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

Di seguito il workflow degli stati

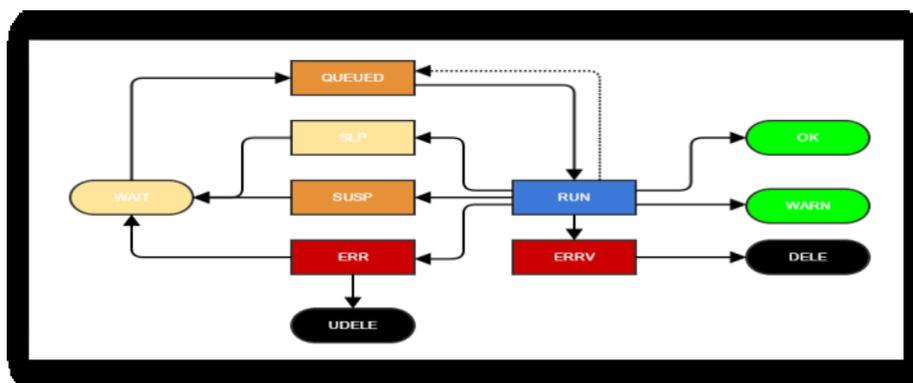


Figura 11: work flow degli stati processo di LegalArchive®



Esistono due processi di conservazione:

- Il primo per i pacchetti di versamento provenienti da file system;
- Il secondo per i pacchetti di versamento provenienti da web services.

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

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

CODICE ATTIVITÀ	SISTEMA DI RIFERIMENTO	DESCRIZIONE
REQUISITI	Sistema di versamento	È verificato: <ul style="list-style-type: none">• Il Soggetto Produttore non sia bloccato• Non siano stati raggiunti i limiti di contratto• Sia definito almeno un certificato di firma• Sia definito un responsabile della conservazione per il Soggetto Produttore• Sia definito un account di marca temporale per la descrizione archivistica• Siano definite delle informazioni di rappresentazioni valide
CREASOTTOPROCESSI	Sistema di versamento	Per ogni SIP vengono creati dei sottoprocessi per migliorare le performance di conservazione
TRADUZIONEPdV	Sistema di versamento	Normalizzazione del file di metadati del pacchetto di versamento
CREATEMPDATA	Sistema di versamento	Caricamento nel database dei metadati del pacchetto di versamento
VALIDATEMPDATA	Sistema di versamento	Validazione dei metadati secondo le specifiche concordate con il Soggetto Produttore
CANCELLATEMPDATA	Sistema di versamento	Cancellazione delle tabelle temporanee create per la fase di validazione
CREAPdA	Sistema di versamento	Creazione del pacchetto di archiviazione
CREAFILEMETADATI	Sistema di versamento	Crea il file di metadati per il pacchetto di archiviazione
CREAIdC	Sistema di versamento	Crea l'indice di conservazione secondo lo standard UNI SINCRO
FIRMAIdC	Sistema di versamento	Firma l'indice di conservazione
MARCAIdC	Sistema di versamento	Marca l'indice di conservazione
MEMORIZZAPdA	Sistema di gestione dati	Memorizza nel database tutte le informazioni inerenti al pacchetto di archiviazione



CODICE ATTIVITÀ	SISTEMA DI RIFERIMENTO	DESCRIZIONE
COIAPdA	Sistema di memorizzazione	Copia i pacchetti di archiviazione nel repository di destinazione
VALIDAPdA	Sistema di gestione dati	Verifica che la copia sia andata a buon fine (controllo di hash)
COLLEGAIR	Sistema di gestione dati	Collega il pacchetto di archiviazione alle informazioni sulla rappresentazione
ENCRYPTMETADATA	Sistema di memorizzazione	Cripta i metadati con tipo di privacy impostato a giudiziario o sanitario
CREARdV	Sistema di versamento	Genera il rapporto di versamento
MARCARdV	Sistema di versamento	Marca il rapporto di versamento

[TORNA AL SOMMARIO](#)



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

Il sistema consente modalità multiple di presa in carico dei pacchetti di versamento:

— **Versamento automatico via file system:**

Solitamente I file vengono inviati tramite un canale sftp sul nostro server. Una volta arrivati, tramite processi automatizzati i file vengono immessi nel sistema il software LegalArchive® per il processo di conservazione.

— **Versamento via web services:**

Viene stabilito un collegamento VPN con il cliente e utilizzati i webservices nativi di LegalArchive®

LegalArchive®, come già evidenziato, supporta i Pacchetti di versamento nel formato definito nell'allegato 5 delle nuove regole tecniche e nel formato CSV in tre varianti:

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

Il sistema prevede la presenza di log/registri dei pacchetti di versamento ricevuti (si rimanda al paragrafo 8.4 Log di sistema)

TORNA AL SOMMARIO

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

Il Sistema di versamento prevede:

- La verifica dell'identificazione certa del Soggetto Produttore;
- La verifica che il Soggetto Produttore non sia bloccato;
- La verifica del raggiungimento dei limiti di contratto;
- La verifica che sia stato definito almeno un certificato di Firma;
- La verifica che sia stato definito un responsabile della conservazione per il Soggetto Produttore;
- La verifica che sia stato definito un account di marca temporale per la descrizione archivistica;
- La verifica che siano state definite informazioni di rappresentazioni valide;
- La normalizzazione del file di metadati del pacchetto di versamento;
- Il caricamento nel database dei metadati del pacchetto di versamento;
- La validazione dei metadati secondo le specifiche concordate con il Soggetto Produttore.

LegalArchive® prevede la generazione di log per la funzione engine, deputata all'esecuzione dei processi (cfr paragrafo 8.4 a cui si rimanda), nei quali sono riportate le seguenti informazioni:

- <data e ora di esecuzione del processo>,



- <utente che ha richiesto il processo>,
- <tipo di processo richiesto>,
- <esito del processo>

[TORNA AL SOMMARIO](#)

7.3. [ACCETTAZIONE DEI PACCHETTI DI VERSAMENTO E GENERAZIONE DEL RAPPORTO DI VERSAMENTO](#)

Per attestare l'avvenuta acquisizione e presa in carico del pacchetto di versamento (SIP), per ogni pacchetto accettato, il Sistema genera un Rapporto di versamento che è memorizzato nel database e associato logicamente al pacchetto di archiviazione cui si riferisce.

Il Rapporto di versamento contiene:

- l'Identificativo univoco del Rapporto, ovvero l'identificativo univoco del processo che l'ha generato;
- il Riferimento temporale relativo alla sua creazione (specificato con riferimento al tempo UTC);
- gli identificativi univoci dei documenti versati;
- gli identificativi univoci dei file versati;
- le Impronte degli Oggetti-dati che ne fanno parte;
- la lista dei metadati versati suddivisi per documento.

L'esito restituito, contiene, in un file in formato XML, la lista dei file, il relativo hash e l'identificativo univoco che è stato assegnato al file dal sistema di conservazione e che potrà essere utilizzato per accedere al file.

Nell'impostazione della singola descrizione archivistica, il sistema LegalArchive® consente di definire l'apposizione della firma digitale e la marca temporale al rapporto di versamento generato dal sistema, che avverrà in modalità automatica.

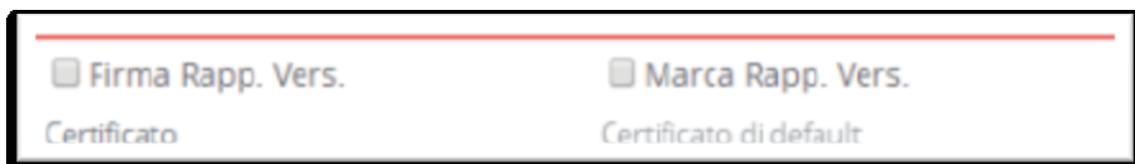


Figura 12: LegalArchive®: definizione apposizione firma e marca temporale sul rapporto di versamento

Il Riferimento temporale può essere apposto anche mediante marca temporale secondo le specifiche tecniche concordate con il soggetto produttore.

Il Rapporto di versamento è reso disponibile al soggetto Produttore in varie modalità:



- è trasmesso in risposta al Versamento del SIP;
- può essere richiesto utilizzando un apposito web service;
- può essere visualizzato e scaricato dall'interfaccia web del Sistema di conservazione dagli utenti abilitati utilizzando le apposite funzionalità del Sistema.

Il sistema prevede la presenza di log dei pacchetti di versamento ricevuti e verifica (si rimanda al paragrafo 8.4 Log di sistema) nei quali sono riportate le seguenti informazioni:

- <data e ora di esecuzione del processo>,
- <utente che ha richiesto il processo>,
- <tipo di processo richiesto>,
- <esito del processo>

[TORNA AL SOMMARIO](#)

[7.4. RIFIUTO DEI PACCHETTI DI VERSAMENTO E MODALITÀ DI COMUNICAZIONE DELLE ANOMALIE](#)

Sui documenti versati nel sistema di conservazione è possibile avviare un'attività di validazione sia dei file che dei metadati rispetto alle regole ed agli standard previsti dalle descrizioni archivistiche di appartenenza. I risultati della convalida possono essere allegati al documento oggetto della convalida per essere eventualmente portati in conservazione insieme al documento. (cfr anche paragrafo 8.2.1 Sistema di versamento)

Il processo di convalida include:

- la verifica dell'integrità del documento memorizzato sul supporto rispetto all'impronta associata allo stesso;
- la verifica che il formato del contenuto binario sia coerente con quanto dichiarato nei suoi metadati, oppure, si potrebbe consentire l'invio di formati di file non adatti alla conservazione;
- la verifica delle eventuali firme digitali apposte su di esso, comprensiva di convalida del certificato rispetto ad uno "store" locale ed alle liste di revoca on-line;
- l'eventuale verifica della presenza in archivio di un documento identico (i.e.: stessa impronta e/o metadati);
- la compilazione metadati: alcuni metadati potrebbero essere compilati in questa fase in maniera automatica (ad esempio potrebbero essere aggiunte le informazioni relative all'utente che ha effettuato il versamento e la data di versamento).

Il sistema LegalArchive® consente di definire l'invio di notifiche relativi ad eventi associati alle conservazioni specificando campi quali:

- Descrizione Archivistica.
- Gruppo Notificato.



- Tipo Notifica: Notifica via Email e/o Notifica via Web (nella pagina di accesso).
- Evento Notifica:
 - In fase di esecuzione.
 - Eseguito senza errori.
 - Sospeso/Da non terminare.
 - Eseguito con segnalazioni.
 - Eseguito con errori
 - In attesa/Da terminare.
 - In attesa di conclusione conservazione.
 - Errore di validazione.
 - Annullato dall'utente.
 - Cancellato

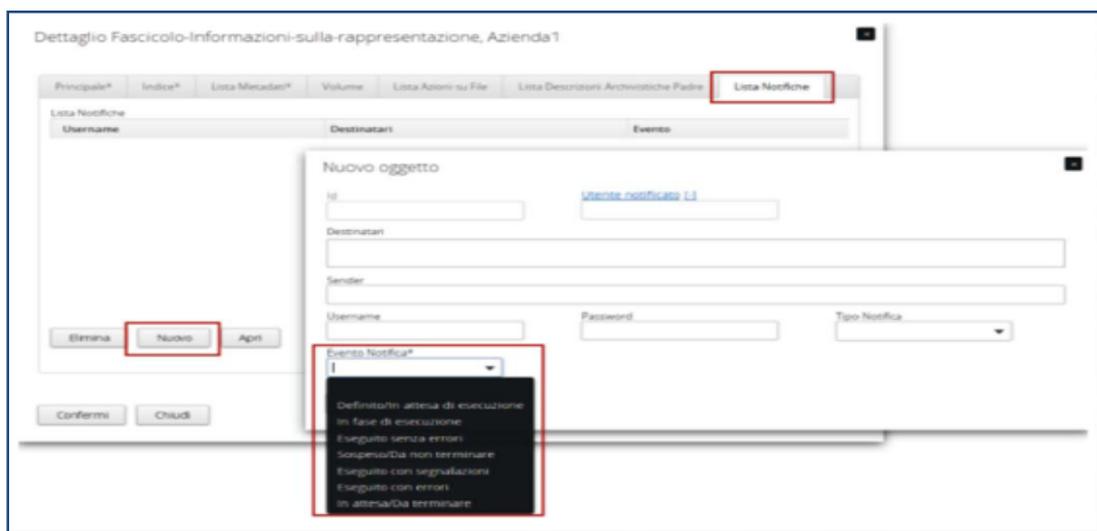


Figura 13: LegalArchive® - pannello definizione invio notifiche



E' possibile aggiungere alla notifica mail:

- L'oggetto della mail.
- Testo della mail

L'oggetto ed il testo della mail sono personalizzabili in termini di:

- Testo libero
- [ID_Volumes] : identificativi dei volumi di conservazione
- [SP_ALIAS]: alias del Soggetto produttore
- **[DATA], [MESSAGE] data e messaggio della notifica**
- [PRO_ID], [PRO-DATE],[PRO_STATUS]: identificativi del processo

Figura 14:LegalArchive®- Personalizzazione notifiche- notifica rifiuto pacchetto di versamento

Le notifiche via e-mail saranno inviate da un server predefinito da cui il sistema LegalArchive® invierà le comunicazioni di sistema.

Le notifiche di cui sopra non sono firmate digitalmente



Nella tabella sottostante si riportano le anomalie che determinano il rifiuto del pacchetto di versamento e relativa modalità di gestione

Tipo Anomalia	Descrizione	Gestione
Mancata risposta al versamento	L'unità documentaria è correttamente versata, ma per svariati motivi, la risposta di avvenuta ricezione non è pervenuta al produttore, che di conseguenza, erroneamente, la considera non versata.	Il soggetto produttore deve versare nuovamente: il sistema di conservazione restituirà una risposta di esito negativo con l'indicazione che l'unità documentaria risulta già versata. Tale risposta deve essere usata dal produttore come attestazione di avvenuto versamento e l'unità documentaria deve risultare come versata.
Errori temporanei	È il caso di errori dovuti a problemi temporanei che pregiudicano il versamento, ma si presume non si ripresentino a un successivo tentativo di Versamento. Il caso più frequente è l'impossibilità temporanea di accedere alle CRL degli enti certificatori. In questi casi il sistema di conservazione dopo aver riprovato 10 volte, genera un messaggio di errore perché non riesce a completare le verifiche previste sulla validità della firma e il versamento viene quindi rifiutato impostando il processo in stato ERRV.	Il soggetto produttore deve provvedere a rinviare l'unità documentaria in un momento successivo. L'operazione potrebbe dover essere ripetuta più volte qualora il problema, seppur temporaneo, dovesse protrarsi nel tempo.
Versamenti non conformi alle regole concordate	È il caso in cui il versamento non viene accettato perché non conforme alle regole concordate (firma non valida, Formato file non previsto, file corrotto, mancanza di Metadati obbligatori, ecc.).	Il soggetto conservatore invia via e-mail una segnalazione dell'anomalia ai referenti del soggetto produttore, con i quali viene concordata la soluzione del problema.
Errori interni o dovuti a casistiche non previste o non gestite	In alcuni casi è possibile che il sistema di Conservazione risponda con un messaggio di errore generico che non indica le cause dell'anomalia riscontrata in quanto dovuta a un errore interno o perché legata a una casistica non prevista, non gestita o non gestibile dal sistema di conservazione.	I referenti del soggetto produttore segnalano il problema via e-mail al soggetto conservatore, che si attiverà per la sua risoluzione



Il Sistema LegalArchive® consente di verificare quali processi siano in esecuzione ed il loro esito

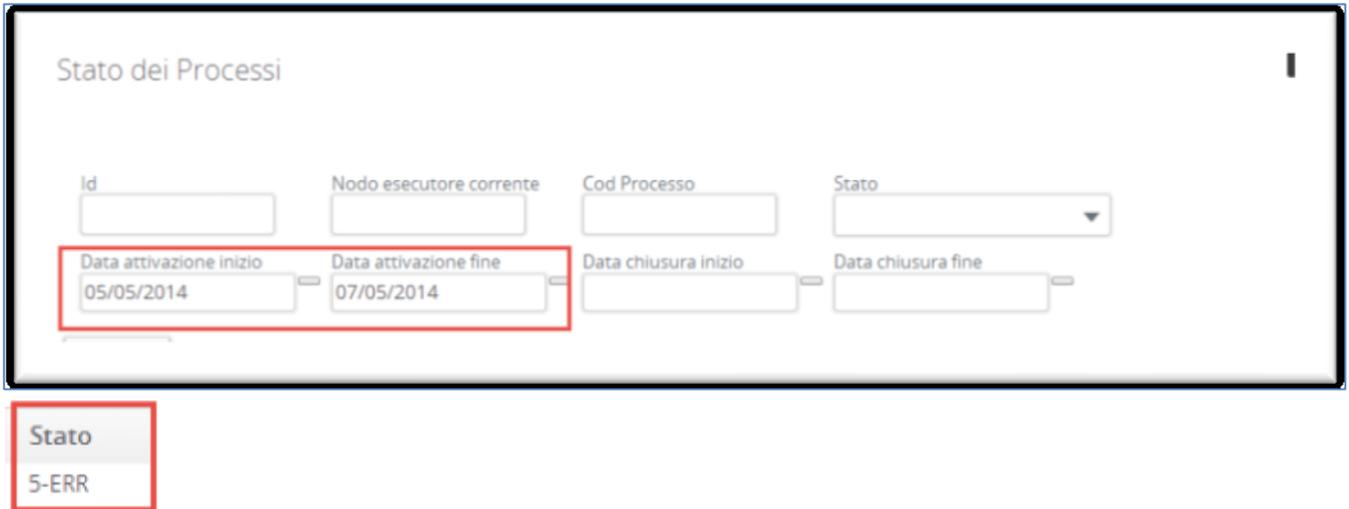


Figura 15:LegalArchive® Verifica Stato dei processi

In caso di errore, nel LOG del processo di conservazione viene registrato un messaggio che spiega cosa manca o quale processo è propedeutico per l'avanzamento del processo stesso., come sotto illustrato

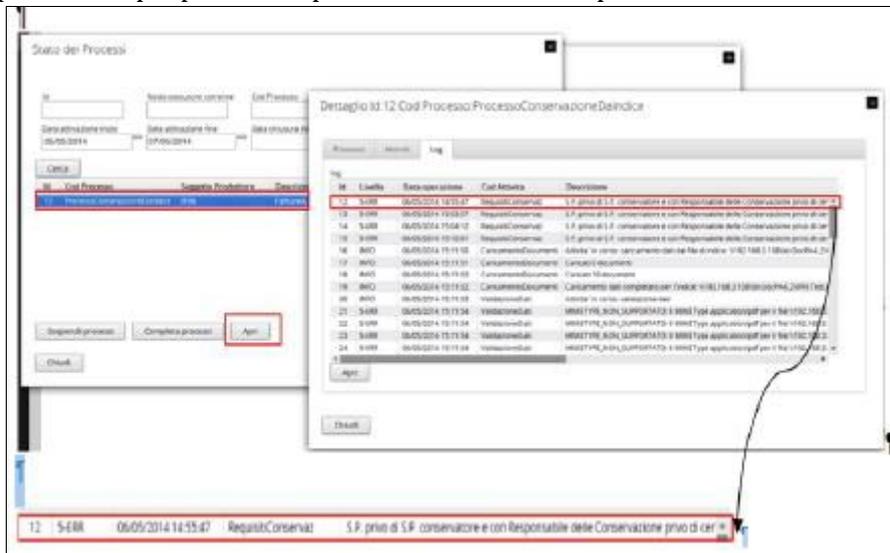


Figura 16:LegalArchive® Gestione anomalie

Nelle righe di log sono resi disponibili:

- <data e ora di esecuzione del processo>,
- <utente che ha richiesto il processo>,
- <tipo di processo richiesto>,
- <esito del processo>.

Le anomalie sono affrontate con diverse metodologie, secondo la natura dell'anomalia stessa e, la collocazione dell'evento che l'ha generata nel processo di conservazione: pertanto, oltre alle procedure



atte a garantire l'Integrità degli archivi, esistono anche procedure atte a risolvere anomalie in altre componenti del sistema.

Le caratteristiche comuni e le specificità delle procedure di risoluzione delle anomalie dipendono da diversi fattori organizzativi e tecnologici:

- tutte le funzionalità del sistema che inseriscono o modificano dati nel Data Base e file nell'area FTP o nel File System operano in modalità transazionale;
- il backup del Data Base assicura il restore all'ultima transazione completata correttamente;
- il File System e l'area FTP sono sottoposte a backup incrementale giornaliero e full settimanale a caldo;

[TORNA AL SOMMARIO](#)

7.5. [PREPARAZIONE E GESTIONE DEL PACCHETTO DI ARCHIVIAZIONE](#)

In un sistema OAIS si definisce pacchetto di archiviazione, un pacchetto informativo composto dall'insieme delle informazioni che costituiscono l'obiettivo originario della conservazione e dalle relative informazioni sulla conservazione. In un contesto OAIS il pacchetto di archiviazione deve essere auto-consistente, cioè, deve prevedere tutte le informazioni necessarie al recupero e alla ricostruzione dell'oggetto conservato e delle informazioni ad esso associate.

LegalArchive® garantisce la conformità a questo requisito OAIS creando dei pacchetti di archiviazione contenenti tutti i file necessari alla loro ricostruzione e ricerca (si veda anche il paragrafo 6.3)

[TORNA AL SOMMARIO](#)

7.6. [PREPARAZIONE E GESTIONE DEL PACCHETTO DI DISTRIBUZIONE AI FINI DELL'ESIBIZIONE](#)

La generazione di un pacchetto di distribuzione passa necessariamente per la ricerca di un pacchetto di archiviazione specifico.

L'Utente può consultare i documenti informatici versati al sistema di conservazione tramite interfaccia web, collegandosi all'indirizzo comunicato dal soggetto conservatore autenticandosi tramite autenticazione informatica (user-id/password). L'accesso web consente al soggetto produttore di ricercare i documenti informatici versati, di effettuarne il download e di acquisire le prove delle attività di conservazione. Il produttore può richiedere i documenti e fascicoli informatici versati e conservati anche utilizzando gli appositi web services, chiamati secondo le modalità indicate nelle specifiche tecniche.

L'utente che richiede l'esibizione potrà selezionare:

- Il formato di download;
- Formato ZIP;



- Formato ISO.
- Una delle seguenti possibilità:
 - Download delle informazioni sulla rappresentazione e viewer al momento della conservazione;
 - Scelta del viewer in base al sistema operativo.
- Richiesta Esibizione: Avvia la creazione di un file *.Zip o *.Iso contente:
 - Documenti richiesti.
 - Evidenza della firma.
 - Metadati associati.

Il sistema provvede quindi a notificare, tramite la mail associata alla persona legata al profilo in uso, il link tramite il quale sarà possibile scaricare il file.

Fino a quando l'utente non scarica il pacchetto di distribuzione, il sistema mantiene la richiesta in standby. Una volta scaricato il file il sistema cancella il pacchetto di distribuzione e chiude la procedura di esibizione.

Il sistema permette di richiedere, di generare e di scaricare i pacchetti di distribuzione (DIP), completi di Indice di conservazione e delle informazioni di rappresentazione collegate. Inoltre, nei DIP è contenuta tutta la catena di documentazione necessaria a rispondere alle esigenze dello standard OAIS.

SISTEMA DI CONSERVAZIONE EasyLegal®

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

Il sistema consente modalità multiple di presa in carico dei pacchetti di versamento tramite il modulo connector.

Questo modulo effettua una connessione ad una sorgente del cliente, che può essere un documentale o uno spazio ftp, all'interno della quale si trovano i documenti da versare e i relativi metadati. Dopodiché li trasferisce nel repository tramite il layer E-Archiver.

Il modulo si realizza come un unico applicativo:

- Un software che realizza un batch di polling da filesystem

Effettua le seguenti operazioni:

- Connessione alla sorgente
- Connessione al target (layer E-Archiver)



- Creazione del pacchetto di versamento sul repository (createSubmissionPackage)
- Trasferimento dei documenti e dei metadati dalla sorgente al target
- Commit della creazione del pacchetto di versamento. Che include la validazione del pacchetto ed il rilascio del semaforo per l'uso esclusivo delle risorse.
- In caso di successo un'email di notifica viene inviata ai destinatari descritti nel file di configurazione. Il corpo della mail conterrà l'elenco dei batchID dei pdv importati con un esito valido/non valido per ogni pacchetto
- In caso di errore, il pacchetto di versamento viene cancellato (vedi removeZombieFiles) e un'email di notifica viene inviata agli amministratori
- Tutte le azioni saranno registrate in un file di log

Configurabile con i seguenti parametri:

- Dati per la connessione alla sorgente
- Dati per la connessione al target
- Flag di cancellazione dei documenti trasferiti (decidere dove spostare i file per evitare che vengano processati successivamente)
- Flag di lettura ricorsiva delle cartelle della sorgente
- Tipologia documentale
- Mapping dei metadati tra sorgente e target
- Dati mail per invio notifica

In caso di filesystem è atteso un file indice che raccoglie tutti i metadati e il link logico al documento da importare. Il file di indice sarà l'unico ricercato per effettuare il polling e il path nel repository target sarà composto come il target path del file di configurazione più il path relativo contenuto nel file di indice. Ogni file di indice definisce un pacchetto di versamento. Il file di indice conterrà anche un campo che indica l'azione da compiere fra: insert-update o delete.

Ogni pacchetto di versamento sarà riconoscibile nel repository di conservazione da un ID univoco che sarà riportato in tutti i documenti. Il formato dell'ID sarà "versamento_yyyymmddhhmiss"

Modulo connector da filesystem

Il modulo si realizza mediante un programma standalone scritto in Java da eseguire automaticamente con cron o scheduler. L'input del programma Java è un file di configurazione che conterrà tutte le parametrizzazioni necessarie e sufficienti per la sua esecuzione personalizzata. Di seguito i parametri contenuti nel file di configurazione:

- path di polling (il polling avviene sui file di indice)
- mask di polling (regular expression per identificare gli indici da acquisire)
- flag di spostamento dal polling path (solo in caso di successo)
- path di spostamento
- tipologia del file di indice (csv)



- alias del tipo di document
- parametri di connessione all'E-Archiver (url, apiKey)
- Cliente

Il file di indice descritto in precedenza sarà disponibile in formato csv con una prima riga contenente l'header descrittivo dei campi. La struttura ammessa è descritta come segue:

- path relativo del documento a partire dalla cartella nella quale si trova il file di indice. Questo campo è opzionale ed in caso di valore vuoto si assume l'acquisizione di un record no-content. Questo campo nell'header si chiamerà "nome_file"
- elenco di campi custom del cliente. Questo elenco di campi permette il passaggio dei metadati obbligatori per legge o opzionali perché richiesti dal cliente, e saranno mappati uno a uno con quelli dichiarati dalla struttura dell'E-Archiver. I campi saranno soggetti a mappatura come da descrizione archivistica. Nell'header quindi, sarà fondamentale nominare i file in modo tale che la mappatura possa essere efficace e rispettata. Osserviamo che tutti i campi non mappati da configurazione non saranno riportati nell'E-Archiver.

Ogni file di indice che sarà identificato nel polling corrisponderà ad un pacchetto di versamento. Per ogni pacchetto di versamento sarà data notifica mediante email al destinatario riportato nella configurazione di EasyLegal Archiver, sia in caso di successo sia in caso di insuccesso. In caso di successo alla comunicazione via email sarà allegato anche il rapporto di versamento.

Per evitare conflitti e sovrapposizione nell'esecuzione dei batch, ogni file di indice, appena preso in carico per il versamento, viene rinominato apponendo un suffisso (es. ".lock") che indica che è in corso di lavorazione.

Di seguito una descrizione del flusso di versamento:

- try
 - o Repository.createSubmissionPackage(cliente, type)
 - o while(each document)
 - getContentID(...)
 - createContent(contentID, submitted, streamBase64, JSONMetadati, SHA1, checkSignature=yes, checkMarkup=yes)
 - o commitSubmittedBatchID(batchID)
 - o if (isValidSubmittedBatchID(batchID))
 - gestisce il file indice (in base al file di configurazione)
 - o else
 - segnala l'anomalia nel versamento al destinatario
- catch
 - o removeZombieFiles(batchID, submission)
 - o marca il file indice come errato
 - o email agli amministratori



[TORNA AL SOMMARIO](#)

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

Il Sistema di versamento prevede:

- La verifica dell'identificazione certa del Soggetto Produttore;
- La verifica che il Soggetto Produttore non sia bloccato;
- La verifica del raggiungimento dei limiti di contratto;
- La verifica che sia stato definito almeno un certificato di Firma;
- La verifica che sia stato definito un responsabile della conservazione per il Soggetto Produttore;
- La verifica che sia stato definito un account di marca temporale per la descrizione archivistica;
- La verifica che siano state definite informazioni di rappresentazioni valide;
- La normalizzazione del file di metadati del pacchetto di versamento;
- Il caricamento nel database dei metadati del pacchetto di versamento;
- La validazione dei metadati secondo le specifiche concordate con il Soggetto Produttore.

Easylegal® prevede la generazione di log nei quali sono riportate le seguenti informazioni:

- <data e ora di esecuzione del processo>,
- <utente che ha richiesto il processo>,
- <tipo di processo richiesto>,
- <esito del processo>

[TORNA AL SOMMARIO](#)

7.9. ACCETTAZIONE DEI PACCHETTI DI VERSAMENTO E GENERAZIONE DEL RAPPORTO DI VERSAMENTO

Per attestare l'avvenuta acquisizione e presa in carico del pacchetto di versamento (SIP), per ogni pacchetto accettato, il Sistema genera un Rapporto di versamento che è memorizzato nel database e associato logicamente al pacchetto di archiviazione cui si riferisce.

Il Rapporto di versamento contiene:

- l'Identificativo univoco del Rapporto, ovvero l'identificativo univoco del processo che l'ha generato;
- il Riferimento temporale relativo alla sua creazione (specificato con riferimento al tempo UTC);
- gli identificativi univoci dei documenti versati;
- gli identificativi univoci dei file versati;



- le Impronte degli Oggetti-dati che ne fanno parte;
- la lista dei metadati versati suddivisi per documento.

L'esito restituito, contiene, in un file in formato XML, la lista dei file, il relativo hash e l'identificativo univoco che è stato assegnato al file dal sistema di conservazione e che potrà essere utilizzato per accedere al file.

Nell'impostazione della singola descrizione archivistica, il sistema EasyLegal® consente di definire l'apposizione della firma digitale e la marca temporale al rapporto di versamento generato dal sistema, che avverrà in modalità automatica.

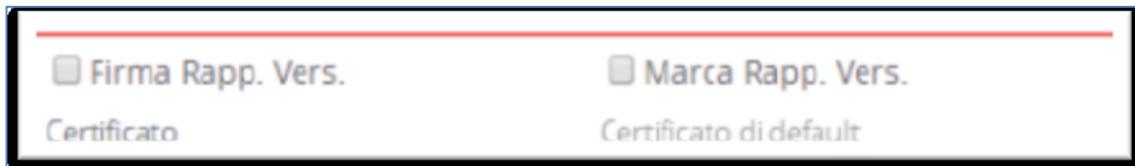


Figura 17: EasyLegal®: definizione apposizione firma e marca temporale sul rapporto di versamento

Il Riferimento temporale può essere apposto anche mediante marca temporale secondo le specifiche tecniche concordate con il soggetto produttore.

Il Rapporto di versamento è reso disponibile al soggetto Produttore in varie modalità:

- è trasmesso in risposta al Versamento del SIP;
- può essere richiesto utilizzando un apposito web service;
- può essere visualizzato e scaricato dall'interfaccia web del Sistema di conservazione dagli utenti abilitati utilizzando le apposite funzionalità del Sistema.

Il sistema prevede la presenza di log dei pacchetti di versamento ricevuti e verifica (si rimanda al paragrafo 8.4 Log di sistema) nei quali sono riportate le seguenti informazioni:

- <data e ora di esecuzione del processo>,
- <utente che ha richiesto il processo>,
- <tipo di processo richiesto>,
- <esito del processo>

[TORNA AL SOMMARIO](#)

7.10. [RIFIUTO DEI PACCHETTI DI VERSAMENTO E MODALITÀ DI COMUNICAZIONE DELLE ANOMALIE](#)



Sui documenti versati nel sistema di conservazione è possibile avviare un'attività di validazione sia dei file che dei metadati rispetto alle regole ed agli standard previsti dalle descrizioni archivistiche di appartenenza. I risultati della convalida possono essere allegati al documento oggetto della convalida per essere eventualmente portati in conservazione insieme al documento. (cfr anche paragrafo 8.2.1 Sistema di versamento)

Il processo di convalida include:

- la verifica dell'integrità del documento memorizzato sul supporto rispetto all'impronta associata allo stesso;
- la verifica che il formato del contenuto binario sia coerente con quanto dichiarato nei suoi metadati, oppure, si potrebbe consentire l'invio di formati di file non adatti alla conservazione;
- la verifica delle eventuali firme digitali apposte su di esso, comprensiva di convalida del certificato rispetto ad uno "store" locale ed alle liste di revoca on-line;
- l'eventuale verifica della presenza in archivio di un documento identico (i.e.: stessa impronta e/o metadati);
- la compilazione metadati: alcuni metadati potrebbero essere compilati in questa fase in maniera automatica (ad esempio potrebbero essere aggiunte le informazioni relative all'utente che ha effettuato il versamento e la data di versamento).

Il sistema EasyLegal® consente di definire l'invio di notifiche relativi ad eventi associati alle conservazioni specificando campi quali:

- Descrizione Archivistica.
- Gruppo Notificato.
- Tipo Notifica: Notifica via Email e/o Notifica via Web (nella pagina di accesso).
- Evento Notifica:
- In fase di esecuzione.
- Eseguito senza errori.
- Sospeso/Da non terminare.
- Eseguito con segnalazioni.
- Eseguito con errori
- In attesa/Da terminare.
- In attesa di conclusione conservazione.
- Errore di validazione.
- Annullato dall'utente.
- Cancellato

E' possibile aggiungere alla notifica mail:

- L'oggetto della mail.
- Testo della mail



CORVALLIS DM

EN/ISO 14001:2004 IE-0915-05
ISO/IEC 27001:2013 IIS-1014-01
ISO 9001 IQ-1015-02



Dasa-Rägister

00-CDM-Manuale Conservazione-Rev-1-13-del-15-gennaio-2019.docx

L'oggetto ed il testo della mail sono personalizzabili in termini di:

- Testo libero
- [ID_Volumes] : identificativi dei volumi di conservazione
- [SP_ALIAS]: alias del Soggetto produttore
- **[DATA], [MESSAGE] data e messaggio della notifica**
- [PRO_ID], [PRO-DATE],[PRO_STATUS]: identificativi del processo

Le notifiche via e-mail saranno inviate da un server propedeuticamente definito da cui il sistema EasyLegal® invierà le comunicazioni di sistema.

Le notifiche di cui sopra non sono firmate digitalmente



Nella tabella sottostante si riportano le anomalie che determinano il rifiuto del pacchetto di versamento e relativa modalità di gestione

Tipo Anomalia	Descrizione	Gestione
Mancata risposta al versamento	L'unità documentaria è correttamente versata, ma per svariati motivi, la risposta di avvenuta ricezione non è pervenuta al produttore, che di conseguenza, erroneamente, la considera non versata.	Il soggetto produttore deve versare nuovamente: il sistema di conservazione restituirà una risposta di esito negativo con l'indicazione che l'unità documentaria risulta già versata. Tale risposta deve essere usata dal produttore come attestazione di avvenuto versamento e l'unità documentaria deve risultare come versata.
Errori temporanei	È il caso di errori dovuti a problemi temporanei che pregiudicano il versamento, ma si presume non si ripresentino a un successivo tentativo di Versamento. Il caso più frequente è l'impossibilità temporanea di accedere alle CRL degli enti certificatori. In questi casi il sistema di conservazione dopo aver riprovato 10 volte, genera un messaggio di errore perché non riesce a completare le verifiche previste sulla validità della firma e il versamento viene quindi rifiutato impostando il processo in stato ERRV.	Il soggetto produttore deve provvedere a rinviare l'unità documentaria in un momento successivo. L'operazione potrebbe dover essere ripetuta più volte qualora il problema, seppur temporaneo, dovesse protrarsi nel tempo.
Versamenti non conformi alle regole concordate	È il caso in cui il versamento non viene accettato perché non conforme alle regole concordate (firma non valida, Formato file non previsto, file corrotto, mancanza di Metadati obbligatori, ecc.).	Il soggetto conservatore invia via e-mail una segnalazione dell'anomalia ai referenti del soggetto produttore, con i quali viene concordata la soluzione del problema.
Errori interni o dovuti a casistiche non previste o non gestite	In alcuni casi è possibile che il sistema di Conservazione risponda con un messaggio di errore generico che non indica le cause dell'anomalia riscontrata in quanto dovuta a un errore interno o perché legata a una casistica non prevista, non gestita o non gestibile dal sistema di conservazione.	I referenti del soggetto produttore segnalano il problema via e-mail al soggetto conservatore, che si attiverà per la sua risoluzione



In caso di errore, nel LOG del processo di conservazione viene registrato un messaggio che spiega cosa manca o quale processo è propedeutico per l'avanzamento del processo stesso., come sotto illustrato
Nelle righe di log sono resi disponibili:

- <data e ora di esecuzione del processo>,
- <utente che ha richiesto il processo>,
- <tipo di processo richiesto>,
- <esito del processo>.

Le anomalie sono affrontate con diverse metodologie, secondo la natura dell'anomalia stessa e, la collocazione dell'evento che l'ha generata nel processo di conservazione: pertanto, oltre alle procedure atte a garantire l'Integrità degli archivi, esistono anche procedure atte a risolvere anomalie in altre componenti del sistema.

Le caratteristiche comuni e le specificità delle procedure di risoluzione delle anomalie dipendono da diversi fattori organizzativi e tecnologici:

- tutte le funzionalità del sistema che inseriscono o modificano dati nel Data Base e file nell'area FTP o nel File System operano in modalità transazionale;
- il backup del Data Base assicura il restore all'ultima transazione completata correttamente;
- il File System e l'area FTP sono sottoposte a backup incrementale giornaliero e full settimanale a caldo;

[TORNA AL SOMMARIO](#)

7.11. [PREPARAZIONE E GESTIONE DEL PACCHETTO DI ARCHIVIAZIONE](#)

In un sistema OAIS si definisce pacchetto di archiviazione, un pacchetto informativo composto dall'insieme delle informazioni che costituiscono l'obiettivo originario della conservazione e dalle relative informazioni sulla conservazione. In un contesto OAIS il pacchetto di archiviazione deve essere auto-consistente, cioè, deve prevedere tutte le informazioni necessarie al recupero e alla ricostruzione dell'oggetto conservato e delle informazioni ad esso associate.

EasyLegal® garantisce la conformità a questo requisito OAIS creando dei pacchetti di archiviazione contenenti tutti i file necessari alla loro ricostruzione e ricerca (si veda anche il paragrafo 6.3)

[TORNA AL SOMMARIO](#)



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

La generazione di un pacchetto di distribuzione passa necessariamente per la ricerca di un pacchetto di archiviazione specifico.

L'Utente può consultare i documenti informatici versati al sistema di conservazione tramite interfaccia web, collegandosi all'indirizzo comunicato dal soggetto conservatore autenticandosi tramite autenticazione informatica (user-id/password). L'accesso web consente al soggetto produttore di ricercare i documenti informatici versati, di effettuarne il download e di acquisire le prove delle attività di conservazione. Il produttore può richiedere i documenti e fascicoli informatici versati e conservati anche utilizzando gli appositi web services, chiamati secondo le modalità indicate nelle specifiche tecniche.

L'utente che richiede l'esibizione potrà selezionare:

- Il formato di download:
- Formato ZIP;
 - Formato ISO.
- Una delle seguenti possibilità:
 - Download delle informazioni sulla rappresentazione e viewer al momento della conservazione;
 - Scelta del viewer in base al sistema operativo.
- Richiesta Esibizione: Avvia la creazione di un file *.Zip o *.Iso contente:
 - Documenti richiesti.
 - Evidenza della firma.
 - Metadati associati.

Il sistema provvede quindi a notificare, tramite la mail associata alla persona legata al profilo in uso, il link tramite il quale sarà possibile scaricare il file.

Fino a quando l'utente non scarica il pacchetto di distribuzione, il sistema mantiene la richiesta in standby. Una volta scaricato il file il sistema cancella il pacchetto di distribuzione e chiude la procedura di esibizione.

Il sistema permette di richiedere, di generare e di scaricare i pacchetti di distribuzione (DIP), completi di Indice di conservazione e delle informazioni di rappresentazione collegate. Inoltre, nei DIP è contenuta tutta la catena di documentazione necessaria a rispondere alle esigenze dello standard OAIS.

[TORNA AL SOMMARIO](#)



7.12.1. PROCEDURE DI SUPPORTO IN CASO DI ANOMALIE DEI DUE SISTEMI

L'organizzazione Corvallis Document Management mette a disposizione la sua infrastruttura Hardware / Software ed Organizzativa afferente all'infrastruttura IT al fine di supportare la fruibilità dei servizi legati all'utenza finale del servizio di conservazione.

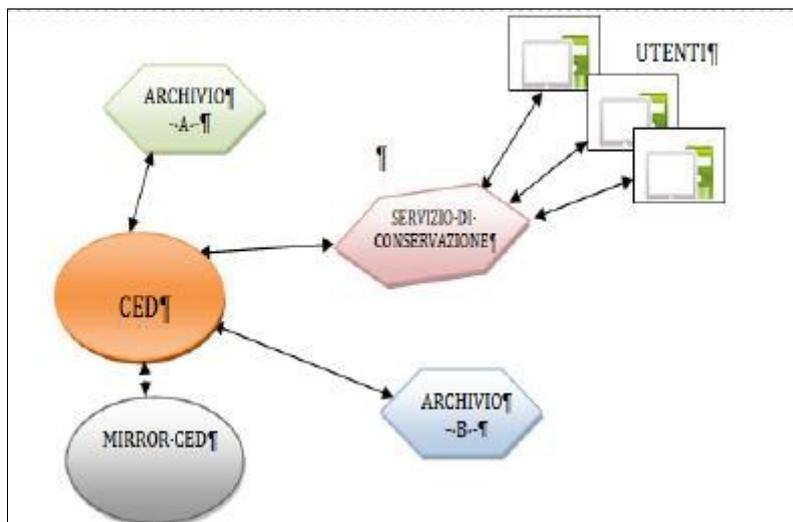


Figura 18:Schema infrastruttura di rete di Corvallis DM

La platea di utenti del servizio di conservazione erogato dall'organizzazione aziendale è suddivisa nelle seguenti macro categorie:

CLASSI DI UTENZA	DESCRIZIONE
UTENTI OPERATIVI	Utenti definiti ed autorizzati dai produttori dei documenti
UTENTI AMMINISTRATIVI	Assegnati ai singoli uffici della sede amministrativa;
UTENTI CON RESPONSABILITÀ	Personale che governa l'organizzazione del produttore dei documenti
	Personale che governa l'organizzazione del Conservatore dei documenti
UTENTI DELL'AREA IT	Personale che ricopre diversi ruoli all'interno dell'area IT

Per ogni utente autorizzato ad operare sul sistema di conservazione, è creata una scheda identificativa gestita in collaborazione fra il Responsabile del Trattamento dei Dati ed responsabile della sicurezza del sistema di conservazione. La scheda raccoglie anche gli estremi dell'autorizzazione ad operare sul sistema di conservazione per conto del produttore / conservatore. Ogni utente del sistema di conservazione può usufruire del servizio di Help Desk attivato da Corvallis Document Management.



L'Area IT si è dotata di un applicativo gestionale "SERVICE DESK" per la gestione di tutte le richieste di assistenza che gli utenti del sistema di conservazione hanno necessità di inoltrare.

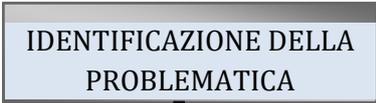
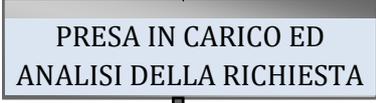
Le richieste non inoltrate tramite l'applicativo "SERVICE DESK" verranno rilevate come non conformità a carico della direzione di appartenenza dell'utente richiedente.

Livelli di Urgenza della Richiesta

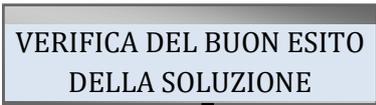
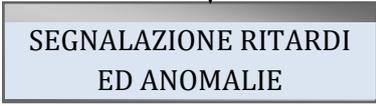
Le richieste urgenti possono riguardare le seguenti tipologie di anomalia:

- Impossibilità ad accedere alle applicazioni web based;
- Impossibilità ad usufruire dei servizi di ricerca;
- Errori di trasmissione dei pacchetti
- Messaggi di anomalia che inducono a pensare a minacce informatiche;
- Evidenze di violazione del proprio account;
- Evidenze di violazione del proprio hardware;
- Smarrimento del proprio hardware;
- Blocco / sospensione di un account;
- Blocco o smarrimento delle proprie credenziali

FLUSSO DI GESTIONE DELLA RICHIESTA DI ASSISTENZA

FASE DELLA RICHIESTA	DESCRIZIONE ATTIVITA'	RESPONSABILITÀ
 ↓	L'utente dei servizi di conservazione deve circoscrivere la problematica che si trova ad affrontare prima di richiedere aiuto.	UTENTE
 ↓	La richiesta di aiuto / assistenza deve essere inviata esclusivamente tramite l'applicativo "SERVICE DESK".	UTENTE
 ↓	La richiesta viene inviata in automatico dal sistema una volta confermata la compilazione del ticket.	UTENTE
 ↓	Il gruppo di operatori dell'AREA IT riceve notifica della creazione del nuovo TICKET aperto.	AREA IT
 ↓	Gli operatori che prendono in carico il TICKET analizzano i log del sistema di conservazione per individuare la causa, descrivono le attività messe in atto per la	AREA IT



FASE DELLA RICIESTA	DESCRIZIONE ATTIVITA'	RESPONSABILITÀ
	soluzione del TICKET e ne descrivono le cause	
 ↓	L'UTENTE che riceve notifica di chiusura del TICKET deve verificare l'effettivo superamento della difficoltà segnalata ed in caso contrario aprire un nuovo TICKET collegandolo al precedente.	AREA IT
 ↓	Il sistema "SERVICE DESK" riporta per ogni TICKET i tempi di lavorazione. Il responsabile AREA IT periodicamente analizza i dati della gestione del servizio.	AREA IT
	L'UTENTE che non dovesse essere soddisfatto del servizio offerto può inviare una e-mail al Responsabile del servizio di conservazione che approfondirà il reale sviluppo del TICKET.	UTENTE

[TORNA AL SOMMARIO](#)

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

Nell'ambito del servizio di conservazione l'attività sarà di competenza del Soggetto Produttore così come richiedere ,ove previsto, l'intervento del pubblico ufficiale.

Il Codice dell'amministrazione digitale definisce duplicati e copie informatiche di documenti informatici quali

Copia informatica di documento informatico: il documento informatico avente contenuto identico a quello del documento dai cui è tratto su supporto informatico con diversa sequenza di valori binari.

Duplicato informatico: il documento informatico ottenuto mediante la memorizzazione , sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario.



Il DPCM 13 novembre 2014 definisce i criteri di generazione di quanto sopra

Articolo 5

1. Il duplicato informatico di un documento informatico di cui all'art. 23-bis, comma 1, del Codice e' prodotto mediante processi e strumenti che assicurino che il documento informatico ottenuto sullo stesso sistema di memorizzazione, o su un sistema diverso, contenga la stessa sequenza di bit del documento informatico di origine.

Articolo 6

1. La copia e gli estratti informatici di un documento informatico di cui all'art. 23-bis, comma 2, del Codice sono prodotti attraverso l'utilizzo di uno dei formati idonei di cui all'allegato 2 al presente decreto, mediante processi e strumenti che assicurino la corrispondenza del contenuto della copia o dell'estratto informatico alle informazioni del documento informatico di origine previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza del contenuto dell'originale e della copia.

Il processo di duplicazione avverrà tramite la creazione di copie di backup di un AIP ovvero, qualora in scadenza la sottoscrizione, si apponga una nuova firma digitale ed apposizione della marca temporale ai file contenuti nel pacchetto.

Il processo di creazione di copie, che determina la modificazione della sequenza dei valori binari del documento informatico originale, avverrà con strumenti e modalità per cui sarà assicurata la rispondenza del contenuto della copia all'originale informatico, Il processo terminerà con l'apposizione della firma digitale del Responsabile della Conservazione e della marca temporale sull'insieme dei documenti o su una evidenza informatica contenente una o più impronte dei documenti , salvo i casi (natura dell'attività, documento analogico unico ai sensi del DPCM 21 marzo 2013) in cui sia necessaria la presenza e l'attestazione di conformità da parte di un Pubblico Ufficiale ovvero di un notaio.

[TORNA AL SOMMARIO](#)

7.14. [SCARTO DEI PACCHETTI DI ARCHIVIAZIONE](#)

Il TU 445/2000 definisce la Gestione dei documenti quale:



“insieme delle attività finalizzate alla registrazione di protocollo e alla classificazione, organizzazione, assegnazione e reperimento dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato; essa è effettuata mediante sistemi informativi automatizzati”

e come compito precipuo del servizio per la gestione dei flussi documentali e degli archivi l'elaborazione e l'aggiornamento del

piano di conservazione degli archivi, integrato con il sistema di classificazione, per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione permanente dei documenti, nel rispetto delle vigenti disposizioni contenute in materia di tutela dei beni culturali e successive modificazioni ed integrazioni

Da quanto sopra emerge chiaramente la funzione della classificazione d'archivio (titolario) quale strumento di organizzazione logica dell'archivio quale universitas rerum. La classificazione definisce il criterio con cui i documenti sono organicamente prodotti e fascicolati in relazione alle funzioni, alle competenze ed alle modalità operative di ogni soggetto produttore. Il piano di classificazione, pertanto, in quanto atto di organizzazione è lo strumento primo di organizzazione gerarchico - funzionale di un complesso documentale e ne permette il corretto evolversi. Il dettato normativo rende altresì esplicito il legame fondamentale fra il piano di classificazione ed il piano di conservazione e scarto, qualificandoli come strumenti primi per la corretta gestione e sedimentazione di un archivio.

Il processo dello scarto, o meglio della selezione dei documenti destinati alla conservazione perenne, è uno dei momenti di maggior criticità nell'attività archivistica, poiché deve essere svolta in modo da

- Non compromettere l'unitarietà dell'archivio;
- Eliminare solo documenti strumentali;
- Valorizzare ed assicurare pro futuro l'intelligibilità delle funzioni del soggetto produttore e del relativo operato amministrativo;
- Tutelare i diritti degli utenti interni ed esterni del Soggetto Produttore.

Lo scarto è, pertanto, la realizzazione di un'esigenza funzionale del soggetto produttore, che deve rispondere a criteri di economicità e di discriminazione degli elementi qualificanti la sua attività: nel caso precipuo di archivi di soggetti pubblici ovvero privati, per i quali sia intervenuta la dichiarazione



di interesse culturale, si richiede la necessaria e propedeutica autorizzazione da parte del Ministero dei beni e delle attività culturali e del turismo³.

Il DPCM 03/12/2013 prevede come parte integrante del processo di conservazione

Lo scarto del pacchetto di archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dalla norma, dandone informativa al produttore.

EasyLegal® è un software di conservazione, che consente di gestire e configurare un piano di classificazione permettendo di configurare Titoli, Classi, Classi Documentali. Il sistema prevede la possibilità di definire uno specifico metadato per la gestione dei tempi di conservazione, che consentirà la generazione di notifiche sui pacchetti che possono essere sottoposti al processo di scarto, quindi, il sistema produrrà un apposito elenco che sarà sottoposto al Soggetto produttore, che potrà validarlo o rifiutarlo.

In caso affermativo, il processo di selezione e scarto provvederà ad eliminare fisicamente i file presenti nel file system e a cancellare tutti i riferimenti nel database, mantenendo però l'indice di conservazione (in quanto contiene la lista dei file scartati). Il sistema genera una nota che indichi il fatto che il pacchetto è stato sottoposto a processo di scarto, includendo data e ora di esecuzione.

[TORNA AL SOMMARIO](#)

³ Cfr Dlgs 42/2004 art. 21 comma 1 lettera d)



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

I sistemi di conservazione sono in grado di esportare, secondo lo standard OAIS, i singoli pacchetti di archiviazione; gli stessi pacchetti possono essere importati senza problemi in seguito da un qualsiasi altro sistema che sia compatibile OAIS.

[TORNA AL SOMMARIO](#)

8. IL SISTEMA DI CONSERVAZIONE

Il modello dei dati che viene utilizzato come base per l'implementazione dei due sistemi di conservazione EasyLegal® e LegalArchive® è lo standard ISO 14721: OAIS Open Archival Information System esplicito nella gestione di tre differenti tipologie di pacchetti informativi secondo lo schema sotto riportato:

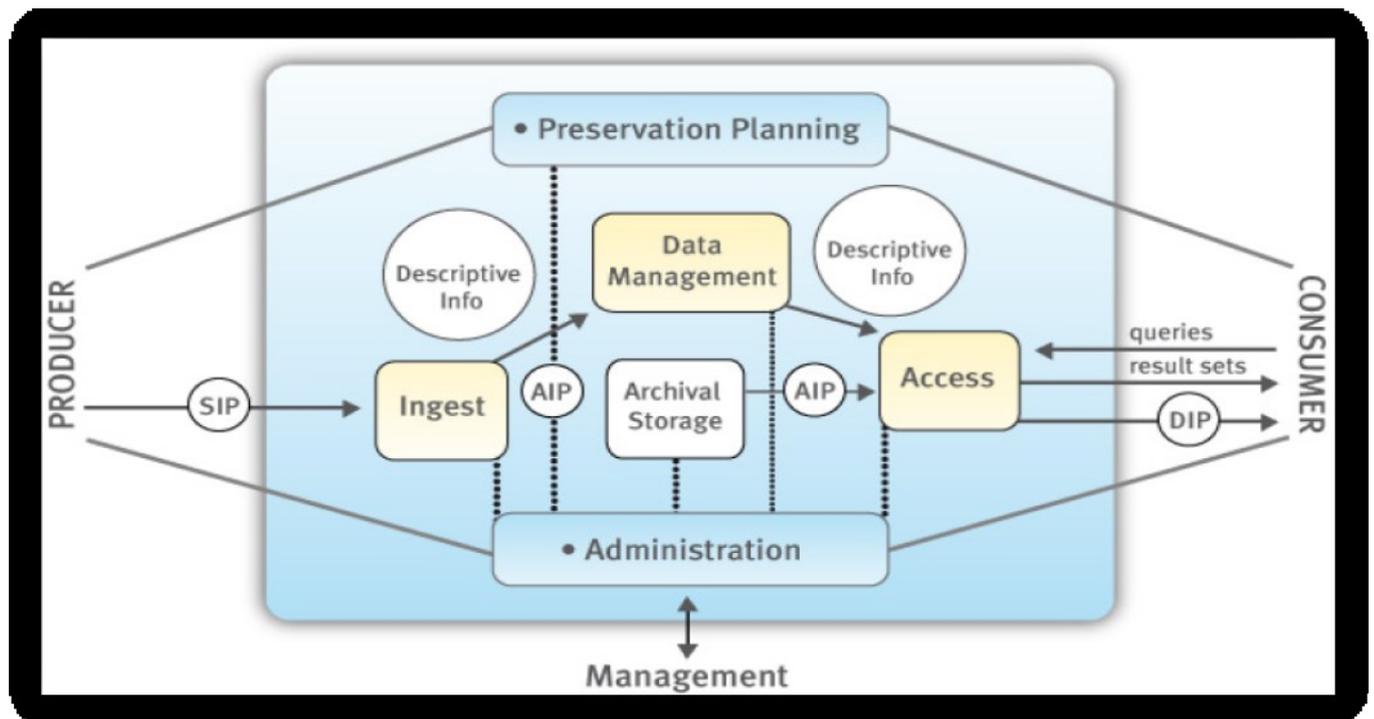


Figura 19: Modello OAIS di riferimento

- **Pacchetto di versamento. (SIP):** documento digitale o l'insieme dei documenti digitali, corredati da tutti i metadati descrittivi, versati dal Soggetto Produttore nel sistema di conservazione



CORVALLIS DM

00-CDM-Manuale Conservazione-Rev-1-13-del-15-gennaio-2019.docx

- **Pacchetto di archiviazione (AIP):** uno o più SIP sono trasformati in pacchetto di archiviazione per la conservazione. L'AIP ha un insieme completo di informazioni sulla conservazione che si aggiungono al file di metadati versato dal Soggetto Produttore
- **Pacchetto di distribuzione (DIP)** il documento digitale o l'insieme dei documenti digitali, corredati da tutti o da parte dei metadati previsti nell'AIP, finalizzati alla presentazione e distribuzione dei documenti conservati.

In termini generali, il modello OAIS definisce le componenti logiche comuni a tutti e tre i pacchetti informativi sopra descritti. Il modello dati utilizzato da EasyLegal® e LegalArchive® prevede una strettissima aderenza a tale modello concettuale rivisitandolo ed ampliandolo con elementi di contestualizzazione provenienti dalla tradizione archivistica italiana. Inoltre l'obiettivo dei sistemi di conservazione implementati da CORVALLIS DM, è quello di garantire non solo la gestione e la conservazione dell'insieme informativo e descrittivo del singolo documento (o collezione di documenti, nell'accezione OAIS, in riferimento a AIC, Archival Information Collection), ma anche di tutte le informazioni di contesto dei metadati e, soprattutto, delle relazioni fra i documenti che servono per la ricostruzione del vincolo archivistico e, quindi, del fascicolo digitale di riferimento. Nella figura successiva si mostra come EasyLegal® e LegalArchive® aderiscono al modello OAIS. Si può notare come l'amministrazione e il preservation planning siano distribuiti sui vari sistemi in quanto ognuno di essi metterà a disposizione una serie di funzionalità che ne consentiranno la configurazione (preservation planning) e la gestione (amministrazione).

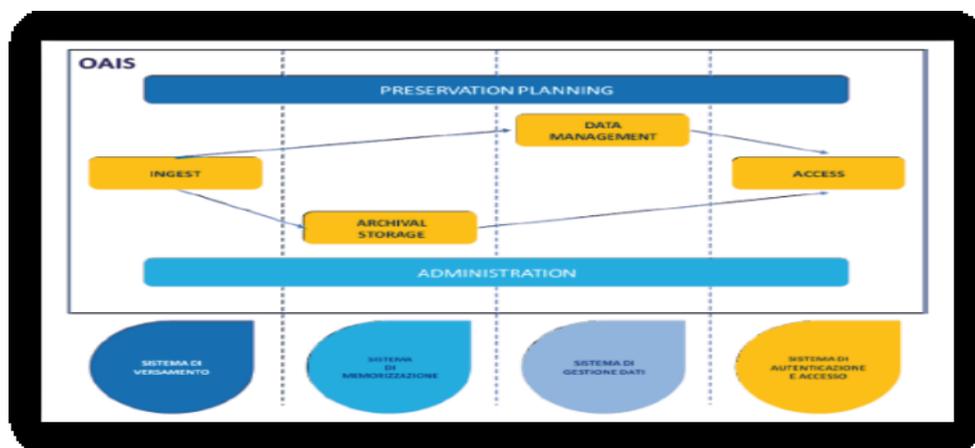


Figura 20: LealgArchive® - LegalArchive® & OAIS

[TORNA AL SOMMARIO](#)

8.1. [CARATTERISTICHE OAIS DEL SISTEMA DI CONSERVAZIONE](#)

Lo standard OAIS prevede che, ad ogni oggetto portato in conservazione, vengano associate:

- un insieme di informazioni (metadati) che ne permetta in futuro una facile reperibilità;
- le informazioni sulla rappresentazione (IR), classificabili a loro volta in sintattiche (IRsi) e semantiche (IRse).



il cui obiettivo è fornire tutte le informazioni necessarie per poter leggere ed interpretare la sequenza di bit dell'oggetto conservato. È necessario, inoltre, ricordare che un sistema di conservazione che rispetti la normativa italiana, deve garantire il requisito di leggibilità degli oggetti dati conservati imposto dal comma 1 dell'art. 3 delle nuove regole tecniche e dal comma 1 dell'art. 44 del Codice dell'Amministrazione Digitale. Per soddisfare questi requisiti, prima di versare un qualsiasi oggetto digitale nel sistema di conservazione, è necessario che il responsabile della conservazione, in accordo con il Soggetto Produttore, proceda a conservare tutte le informazioni sulla rappresentazione necessarie alla futura consultazione dell'oggetto stesso.

Si classificano, quindi, le informazioni sulla rappresentazione in:

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

Per soddisfare l'eventuale necessità di una disponibilità immediata dell'oggetto conservato, il sistema di conservazione deve avere, almeno, conservati gli strumenti per la leggibilità (visualizzatori) degli oggetti dati da conservare. Le informazioni sulla rappresentazione, semantiche e sintattiche, e i visualizzatori potranno essere inglobate nel pacchetto di distribuzione assieme ai documenti richiesti garantendo così la piena leggibilità nel lunghissimo periodo del documento conservato. Sarà compito dei sistemi di conservazione EasyLegal® e LegalArchive® creare il pacchetto di distribuzione aggiungendo per ciascun file le corrette informazioni sulla rappresentazione ad esso correlate, e sarà compito del responsabile della conservazione di CORVALLIS DM configurare correttamente i due software e mantenere aggiornate le informazioni per la loro rappresentazione. All'atto della conservazione verrà composto il pacchetto di archiviazione (PdA).

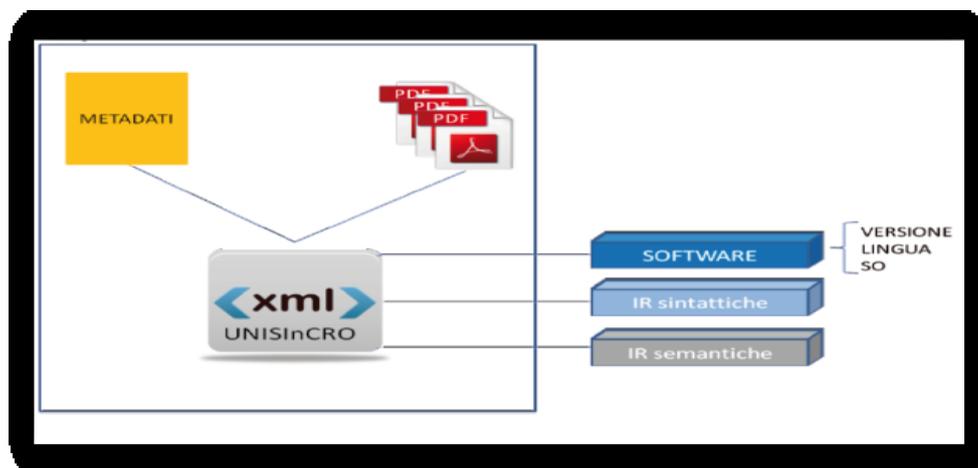


Figura 21: Schema di conservazione per EasyLegal® e LegalArchive®

Lo schema sopra riportato mostra come sarà costruito il PdA.



Ad ogni oggetto versato nel sistema di conservazione sarà associato:

- l'UID del software per la visualizzazione;
- l'UID del fascicolo delle informazioni sulla rappresentazione sintattica;
- l'UID del fascicolo delle informazioni sulla rappresentazione semantica.

a questi associato.

[TORNA AL SOMMARIO](#)

8.2. [COMPONENTI LOGICHE](#)

EasyLegal® e LegalArchive® sono stati progettati, così come richiesto dalla normativa, avendo come riferimento il modello OAIS (ISO 14721), cercando di ottimizzare il rapporto tra l'aderenza al modello teorico e le esigenze pratiche dei soggetti produttori.

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

- **Sistema di Versamento (SV).**
- **Sistema di Gestione Dati (SGD).**
- **Sistema di Memorizzazione (SM).**
- **Sistema di Autenticazione e Accesso (SAA).**

[TORNA AL SOMMARIO](#)

8.2.1. [SISTEMA DI VERSAMENTO](#)

Il sistema di versamento, è la porta di ingresso dell'intero sistema di conservazione ed ha il compito di:

- ricevere i pacchetti di versamento da parte dei soggetti produttori e verificarne l'aderenza al contratto di servizio di conservazione e ai requisiti di conservazione;
- preparare i pacchetti di archiviazione ed infine di inviare ai sistemi opportuni, le informazioni e i dati per garantire la conservazione a norma dei documenti informatici ricevuti.

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

- le caratteristiche minime che la documentazione deve possedere per poter essere accettata in ingresso;
- i tempi di versamento della documentazione dotata di tali caratteristiche;
- e modalità di versamento;
- i metadati di ciascun "versamento" che dovranno anch'essi essere conservati dal sistema.

In particolare, per quanto riguarda il primo punto, il sistema può gestire due ordini di caratteristiche:

- caratteristiche tecnologiche, riferite ai singoli oggetti digitali;
- caratteristiche archivistiche, ossia la presenza di alcuni metadati di contesto.



Le caratteristiche archivistiche possono riguardare, ad esempio, l'appartenenza di ciascun documento, ad un fascicolo, o la possibilità di ricondurre un fascicolo all'attività di un determinato ufficio.

Le caratteristiche tecnologiche riguardano esclusivamente i documenti digitali, e possono riferirsi al formato con cui sono stati prodotti, alla validità della firma, e/o della marca temporale. Poiché i documenti informatici potrebbero giungere al sistema dopo un considerevole arco di tempo dalla loro formazione, a causa dei tempi di chiusura delle relative pratiche, è quanto mai opportuno che il sistema si incarichi di verificare la sussistenza dei requisiti di base per la conservazione. Una volta che la documentazione avrà superato i controlli di qualità previsti, il sistema di versamento dovrà applicare le regole previste dal preservation planning per costruire i pacchetti di archiviazione a partire dai SIP inviati dal soggetto produttore. Innanzitutto sarà generata la cosiddetta "descrizione del pacchetto" che consiste in una serie di informazioni descrittive (descrizioni associate) che consentirà l'accesso al documento informatico da parte dell'utente. Infatti, sulla base di queste descrizioni, è possibile effettuare delle ricerche ed è, a partire da queste descrizioni che verranno costruiti i Dissemination Information Package (DIP) differenti a seconda delle necessità dell'utente.

[TORNA AL SOMMARIO](#)

8.2.2. SISTEMA DI GESTIONE DATI

Il sistema di gestione dati ha il compito di gestire le informazioni legate al contesto archivistico e alle descrizioni dei documenti, funge quindi da collante dell'intero sistema. Il sistema di gestione dati è il cuore archivistico dei due sistemi adottati da CORVALLIS DM ed è la componente che consente di avere una visione unitaria dell'archivio e quindi consente di accedervi. Il sistema di gestione dati ha una duplice valenza:

- da una parte offre servizi al sistema di accesso per consentire le ricerche e la navigazione
- dall'altra consente all'ente produttore di gestire il proprio deposito digitale secondo canoni archivistici, offrendo funzionalità come la descrizione e il riordino, la selezione e lo scarto, la ricollocazione del materiale non digitale, ecc.

Il Soggetto Produttore attraverso questo modulo, potrà vedere l'archivio come il complesso sistema di relazioni che in effetti è, tramite le funzionalità che esso offre, potrà compiere tutte quelle operazioni tipicamente archivistiche, necessarie per la gestione di un archivio: come ad esempio gestire al meglio lo scarto del materiale documentario non destinato alla conservazione permanente, ma caratterizzato invece da tempi di conservazione limitati e diversificati.

[TORNA AL SOMMARIO](#)

8.2.3. SISTEMA DI MEMORIZZAZIONE

Il sistema di memorizzazione ha lo scopo di gestire in modo semplice e sicuro la conservazione a lungo termine dei documenti informatici integrando una serie di servizi specifici di monitoraggio dello stato fisico e logico dell'archivio ed effettuando, per ogni documento conservato, una continua verifica di



caratteristiche come la leggibilità, l'integrità, il valore legale, l'obsolescenza del formato e la possibilità di applicare la procedura di scarto d'archivio.

Nell'ambito del sistema complessivo, quindi, il sistema di memorizzazione ha il compito di garantire il mantenimento della validità nel tempo dei singoli "documenti digitali", preoccupandosi di aspetti quali l'affidabilità, l'autenticità e l'accessibilità.

Il sistema di memorizzazione, in primo luogo acquisisce quanto inviato dal sistema di versamento durante la fase di versamento e, verificandone preventivamente l'affidabilità, provvederà a gestirne lo storage.

Sui documenti conservati con EasyLegal® e LegalArchive® verranno applicate opportune politiche di gestione atte a garantire, non solo la catena ininterrotta della custodia dei documenti, ma anche la piena tracciabilità delle azioni conservative finalizzate a garantire nel tempo la salvaguardia della fonte.

[TORNA AL SOMMARIO](#)

8.2.4. SISTEMA DI AUTENTICAZIONE E ACCESSO AI DATI

Il modulo per la gestione degli accessi orchestra il flusso di informazioni e servizi necessari per fornire le funzionalità di accesso al cosiddetto "consumer" cioè all'utente, che ha la necessità di accedere ad un determinato documento.

A seguito di una ricerca impostata dall'utente, il modulo di gestione accesso richiede i risultati della ricerca al sistema di gestione dati che, organizzando le informazioni descrittive degli AIP, è in grado di rispondere alla richiesta.

Quindi verrà inoltrata una richiesta di accesso ai dati, con richiesta di generazione del DIP, il quale interagendo sia con il sistema di gestione dati che con il sistema di memorizzazione recupererà le informazioni necessarie (AIP e informazioni descrittive) per produrre il Dissemination Information Package (DIP) corrispondente alla richiesta. Inoltre, il sistema di conservazione, consente anche ricerche trasversali tra tipologie documentarie differenti.

Le funzionalità di ricerca sono implementate dal sistema di gestione dati di EasyLegal® e di LegalArchive®, mentre il sistema di accesso fornirà le interfacce per l'interrogazione e per la ricezione e visualizzazione dei risultati.

Le modalità di accesso, in generale, permettono quindi di poter ricercare il documento singolo o le aggregazioni di documenti, mediante tutti i criteri derivabili dai metadati ad esso direttamente associati, per poi risalire al suo contesto archivistico.



L'accesso alle funzionalità offerte dal software di conservazione è regolato anche da un sottosistema di autorizzazione, che permette di suddividere l'utenza applicativa in gruppi ai quali è possibile assegnare permessi di esecuzione di specifiche operazioni.

Grazie ai "profili d'uso", definibili autonomamente dall'amministratore delle due applicazioni, ogni utente potrà accedere ad uno o più soggetti produttori e avere visibilità su uno o più descrizioni archivistiche, nonché è possibile assegnare visualizzazioni di singoli pulsanti e/o menù.

[TORNA AL SOMMARIO](#)

8.2.5. SISTEMA PER LA FIRMA DIGITALE

L'architettura dei sistemi di conservazione EasyLegal® e LegalArchive® prevede di demandare ad un apposito sottosistema il compito di interfacciarsi con essi. Ciò consente al sistema di memorizzazione dei software di utilizzare qualunque dispositivo di firma digitale, dato che le eventuali differenze nell'implementazione vengono mascherate dal sottosistema stesso.

Resta l'obbligo che la firma digitale, in questo contesto relativa al responsabile del servizio di conservazione ed eventualmente anche ad un pubblico ufficiale (o ruolo equivalente), deve essere apposta utilizzando un dispositivo di firma di un tipo approvato da AgID ed un certificato rilasciato da una Certification Authority (CA) appartenente all'elenco dei certificatori accreditati presso AgID.

Il sistema di conservazione è compatibile con i seguenti dispositivi di firma digitale:

- SmartCard.
- Token USB.
- HSM (Hardware Security Module) o servizi di Certification Authority:
- Aruba Sign Box.
- Aruba Remote Sign System.
- Actalis BBF.
- Intesi Group PKBOX.
- Intesa-IBM.

I sistemi di conservazione EasyLegal® e LegalArchive® sono in grado di applicare la firma digitale utilizzando certificati rilasciati da tutte le Certification Authority accreditate presso AgID.

[TORNA AL SOMMARIO](#)

8.2.6. COMPONENTE PER LA MARCA TEMPORALE

La Marca Temporale (ulteriore firma digitale apposta da un soggetto esterno :Time Stamping Authority) è un servizio offerto da un Certificatore Accreditato, che permette di associare data e ora certe e legalmente valide ad un documento informatico, consentendo quindi di associare una validazione temporale opponibile a terzi. (cfr. Art. 20, comma 3 Codice dell'Amministrazione Digitale DLgs 82/2005). L'apposizione di una Marca Temporale a un documento firmato digitalmente ne garantisce la validità nel tempo.



EasyLegal® e LegalArchive® sono in grado di richiedere in modo automatico ed on-line la marca temporale alle TSA (Time Stamping Authority) utilizzate nel sistema.

[TORNA AL SOMMARIO](#)

8.2.7. CERTIFICATORE UTILIZZATO

CORVALLIS DM per il servizio di marca temporale e firma digitale si avvale di ACTALIS (<https://www.actalis.it/>)

[TORNA AL SOMMARIO](#)

8.2.8. PROCEDURE PER LA CONTINUITÀ OPERATIVA

Per le procedure di Business Continuity e di Disaster Recovery si rimanda al piano di sicurezza allegato al presente documento

[TORNA AL SOMMARIO](#)

8.3. COMPONENTI TECNOLOGICHE

8.3.1. ARCHITETTURE

- L'architettura di EasyLegal® è basata su una soluzione multi-tier a 3 livelli:
 - Presentation layer;
 - Business logic (o application) layer;
 - Database layer.

L'estrema elasticità di EasyLegal® permette di sostituire, eseguire l'upgrade a caldo oppure di aggiungere a piacere applicazioni in uno o più nuovi nodi di un eventuale cluster.

- L'architettura di LegalArchive® è basata su una soluzione multi-tier a 3 livelli:
 - Presentation layer;
 - Business logic (o application) layer;
 - Database layer.

L'estrema elasticità di LegalArchive® permette di sostituire, upgradare a caldo oppure di aggiungere a piacere applicazioni in uno o più nuovi nodi di un eventuale cluster:



- **Back End (Services):** rappresenta il core della logica applicativa e l'interfaccia verso le basi dati (Microsoft SQL 2012 oppure Oracle 11g) a cui l'applicazione attinge. Il Back End ha in carico la gestione e la distribuzione dei processi tra i vari nodi del cluster. E' implementato tramite Spring ed espone le sue funzionalità remotamente via protocollo HTTP/HttpInvoker. Non si necessita di un container J2EE ma è sufficiente l'utilizzo di un Servlet Container quale Apache Tomcat 6 per il deploy dello stesso.
- **Engine:** è il motore di conservazione.
- **Front End (Interfaccia Web):** è un'applicazione J2EE stateful Spring 3 realizzata attraverso l'uso di pagine web dinamiche costruite secondo il design pattern MVVM e la tecnologia Vaadin 7. Attraverso Front End gli utenti potranno accedere per configurare e monitorare il sistema.

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

Di seguito la lista dei browser dichiarati compatibili:

- Android 2.3 o superiore.
- Google Chrome 23 o superiore.
- Internet Explorer 8 o superiore.
- OS 5 o superiore.
- Mozilla Firefox 17 o superiore.
- Opera 12 o superiore.
- Safari 6 o superiore.

L'applicazione è pensata per essere scalabile, aumentando il numero dei Web container, attraverso una logica di server clustering gestita automaticamente dal sistema, che, a seconda del livello di carico di ciascun server, distribuirà al meglio le richieste dei client.

- **Full-text Engine:** è l'applicazione che abilita le funzionalità di full-text.
- **Web Services:** sono un insieme di servizi web che permettono, ad applicazioni di terze parti, di versare documenti nel sistema di conservazione o di interrogare lo stesso sullo stato di un documento.

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

[TORNA AL SOMMARIO](#)

8.3.2. [SCALABILITÀ VOLUMI](#)

La conservazione dei documenti, rispetto ai volumi, è soggetto a due variabili:

- **Crescita dei documenti;**



— **Crescita dei dati.**

La crescita dei documenti, vista la dimensione fisica degli oggetti è sicuramente la parte più critica in termini di scalabilità. Per questo motivo EasyLegal® e LegalArchive® sono stati entrambi sviluppati per essere indipendenti dal sistema hardware che conserva i file. Oltre ad essere svincolati dal sistema hardware, i software sono in grado di distribuire i documenti da conservare su più storage in funzione di regole impostate in base alla tipologia documentaria o alla disponibilità di risorse. Per questo motivo, al crescere dei volumi, è possibile affiancare a quegli esistenti altri storage con caratteristiche tecnologiche anche differenti rispetto a quelli già in uso.

[TORNA AL SOMMARIO](#)

8.3.3. SCALABILITÀ UTENTI

In EasyLegal® e LegalArchive® è possibile definire un numero illimitato di utenti che dovranno essere assegnati ad un gruppo dal quale ereditano profilo e capabilities. Con l'utente si definisce una credenziale di autenticazione costituita dalla coppia username-password che in abbinamento consente l'accesso a EasyLegal® o a LegalArchive®. La credenziale potrà essere assegnata ad una persona o ad un'applicazione. Una volta che l'utente sarà connesso al sistema, qualsiasi operazione egli faccia da interfaccia grafica sarà registrata in appositi file di log che saranno conservati automaticamente.

Il sistema di autenticazione supportato da EasyLegal® e LegalArchive® può gestire tre diverse tipologie di accounting:

- **Definizione degli utenti nell'applicazione;**
- **Interfacciamento ai sistemi Microsoft Active Directory;**
- **Interfacciamento a Open LDAP.**

Inoltre, per garantire la massima sicurezza e rendere i sistemi adattabili agli ambienti bancari /finanziari, EasyLegal® e LegalArchive® supportano forme di Strong Authentication aggiuntive quali Pin Code o One Time Password.

Come detto i Sistemi di Conservazione adottati da CORVALLIS DM sono stati progettati per supportare numeri elevati di utenti che vi accedono per consultare documenti in esso conservati. In ogni caso, trattandosi di un applicativo sviluppato a tre livelli ed impiegando le più moderne tecnologie di implementazione software, è possibile far crescere la componente Interfaccia Web in funzione del numero di utenti. Anche la componente database è assolutamente scalabile in funzione del numero di utenti.

Riepilogando, le seguenti necessità dei sistemi EasyLegal® e LegalArchive® sono monitorati per assicurare continuità e qualità del servizio:

- Necessità di maggiore capacità elaborativa sui Database e Repository/Content Server implica l'aggiunta di ulteriori server ai rispettivi cluster e/o core e RAM;



- Necessità di archiviare un maggior volume di dati implica l'aggiunta di nuovi dispositivi di storage;
- Necessità di ulteriore spazio su disco alla saturazione di uno storage per aggiungerne un altro;
- Necessità di maggiore banda fra il sito principale e il sito di disaster recovery: la presenza di accessi in Fibra Ottica sulle due sedi consente di ampliare agevolmente la banda disponibile per il collegamento.

[TORNA AL SOMMARIO](#)

8.3.4. DATA BASE

Il database su cui si basa EasyLegal® è PostgreSQL;

Il database su cui si basa LegalArchive® è Microsoft SQL Server 2012 R2 edizione standard che include Clustering di failover a due nodi, log shipping e replica peer-to-peer.

[TORNA AL SOMMARIO](#)

8.3.5. STORAGE

Lo storage utilizzato per entrambe le installazioni è un EMC CLARION CX4-120 per la parte database e un nas synology RS2414+ per la parte relativa al file system.

[TORNA AL SOMMARIO](#)

8.4. LOG DI SISTEMA

Le diverse componenti logiche che soddisfano i diversi aspetti funzionali dei due sistemi EasyLegal® e LegalArchive®, tracciano su log informazioni idonee all'analisi e al monitoraggio di sistema utilizzate per la gestione del sistema di conservazione.

Nel log relativo alla componente Back End vengono tracciate le informazioni associate alle diverse interrogazioni al sistema.

Per ciascuna di esse sono rese disponibili:

- <indirizzo da cui proviene la richiesta>,
- <data e ora della richiesta>,
- <utente>,
- <tipo di operazione richiesta>,
- <dettaglio dell'operazione richiesta> (eventuale).

Si riportano le richieste tracciate e relative risposte:

- Login --> user id.
- Dettaglio soggetto produttore --> l'alias del soggetto produttore.
- Dettaglio persona fisica --> codice fiscale della persona.



- Dettaglio username --> username.
- Dettaglio certificato --> codice fiscale.
- Dettaglio volume di conservazione --> numero volume di conservazione.
- Dettaglio documento/fascicolo --> UID + lista metadati separati da pipe.
- Download --> UID + lista metadati separati da pipe

— LOG COMPONENTE ENGINE

La componente di Engine dei due sistemi di conservazione è demandata all'elaborazione dei processi di conservazione e tracciata nel proprio log per soggetto produttore le informazioni associate.

Nelle righe di log sono resi disponibili:

- <data e ora di esecuzione del processo>,
- <utente che ha richiesto il processo>,
- <tipo di processo richiesto>,
- <esito del processo>.

Tutti i log dei sistemi EasyLegal® e LegalArchive® vengono registrati e conservati nello specifico sistema di conservazione.

[TORNA AL SOMMARIO](#)

8.5. COMPONENTI FISICHE

Per quanto riguarda le componenti fisiche utilizzate per i sistemi EasyLegal® e LegalArchive® si basano su un sistema di virtualizzazione. La tecnologia usata è quella di virtualizzazione di Redhat KVM. che consente una modularità ed una scalabilità in termini assoluti.

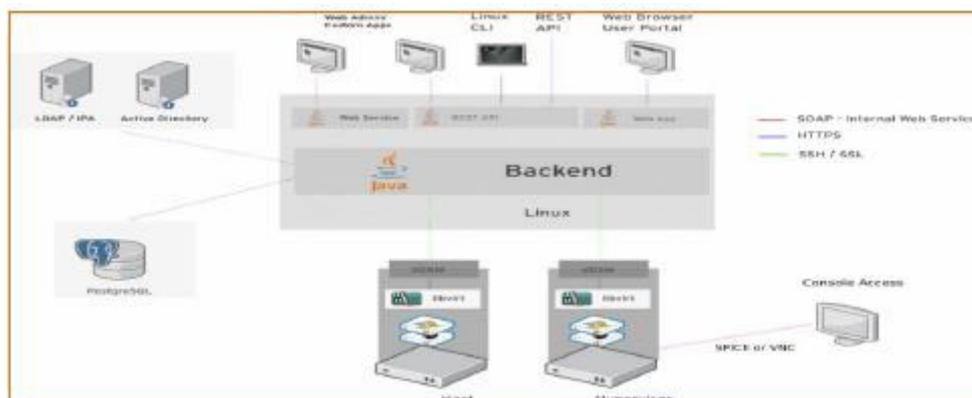


Figura 22: EasyLegal® e LegalArchive® (componenti fisiche)



L'alta disponibilità di risorse è assicurata dall'utilizzo di ovirt 3.5.1. per la virtualizzazione dei servizi (Private Cloud). Esso consente la gestione centralizzata delle macchine virtuali e delle immagini attraverso un portale web che fornisce funzionalità di ricerca, gestione delle risorse, live migration e provisioning , High availability e utilizzo degli snapshot per ripristinare le VM ad uno stato precedente dei due sistemi EasyLegal® e LegalArchive®.

La gestione delle macchine virtuali tramite Ovirt di RedHat integrato in RHEV ne migliora la scalabilità, l'interfaccia di gestione e l'amministrazione dei due sistemi EasyLegal® e LegalArchive® da parte dell'utente, oltre a controllare le funzionalità di networking, storage e virtual desktop. Consente inoltre una scalabilità delle macchine virtuali 'guest', che permette di supportare fino a 160 Cpu logiche e fino a 2 Terabyte di memoria, per ogni macchina virtuale. Incorpora Security Enhanced Linux, che isola le macchine virtuali da attacchi esterni e permette tramite un sottoportale per gli utenti, la gestione autonoma e separata delle risorse di virtualizzazione.

Gli host utilizzati ove girano gli hypervisor sono HP Proliant DL380 G8

La soluzione tecnologica dove sono inglobati i due sistemi di conservazione si distinguono come una architettura sovradimensionata rispetto alle esigenze attuali ed altamente scalabili in quanto:

- completamente virtualizzata,
- orchestrata da un gestore di Private Cloud di classe enterprise
- ospitata in un data center completamente ridondato,
- collegata in Fibra Ottica con supporto diretto della Telco fornitrice,
- rilocabile in Data Center di DR (BCP) in caso di eventi catastrofici con RPO ed RTO estremamente contenuti,
- monitorata costantemente in tutte le sue componenti HW/SW,
- Costantemente aggiornata sulla base degli standard di mercato dei major vendor del segmento (HP/CISCO/REDHAT)

[TORNA AL SOMMARIO](#)



9. MONITORAGGIO E CONTROLLI

[TORNA AL SOMMARIO](#)

9.1. PROCEDURE DI MONITORAGGIO

Il sistema è presidiato dalle 8:00 alle 18:00 almeno da un sistemista senior DBA che garantisce il supporto in caso di malfunzionamento del S.O e del database e si occupa dell'eventuale patching dei sistemi.

Per anticipare anomalie e disservizi e monitorare le performance del sistema viene utilizzato il sistema di monitoraggio Nagios, la soluzione Open Source in grado di controllare infrastrutture IT complesse.

Lo scopo principale dell'utilizzo di Nagios è il raggiungimento della massima disponibilità dei sistemi presenti nell'intera infrastruttura informatica. La soluzione comprende funzionalità che permettono di intervenire in modo proattivo per impedire un calo di performance o un disservizio.

Nel caso si verificasse una riduzione del grado di qualità prevista dagli standard, lo staff informatico sarebbe prontamente allertato prevenendo il rischio che si verificassero dei seri problemi.

Il sistema di Monitoraggio è in grado di aprire dei ticket in automatico in service desk per lo staff informatico qualora si verificasse un malfunzionamento.

Più specificatamente vengono monitorati i file system, i tempi di risposta del database ed il funzionamento dei vari processi che compongono il sistema, compreso quello di ricezione e trasmissione file.

[TORNA AL SOMMARIO](#)

9.2. VERIFICA DELL'INTEGRITÀ DEGLI ARCHIVI

Si tratta di un processo che permette di verificare le conservazioni almeno una volta ogni cinque anni.

Ogni conservazione presenta un link a tutte le verifiche che sono state effettuate, inoltre è possibile visualizzare data di verifica ed esito. In caso di errore, l'anomalia viene registrata nel registro annotazioni. Ogni volta che viene schedato un processo di verifica massiva vanno definiti tre parametri:

- Nr pacchetti per schedulazione: il numero di pacchetti da verificare nella schedulazione;
- Nr pacchetti per processo: il numero dei pacchetti da verificare per un singolo processo;
- Età del pacchetto(d: giorni, m: mesi, y: anni, una sola unità): tempo trascorso dall'ultima verifica effettuata.



Un processo di verifica massiva è suddiviso in quattro attività:

- Check Performance: che stabilisce se sia ancora presente un processo di verifica massiva e segnala con un "Warning" una errata schedulazione o un problema di performance;
- Book Volumes: che, facendo uso dei contatori delle verifiche massive, prenota un blocco di pacchetti di dimensioni chunk e sposta il contatore a contatore+chunk+1;
- Verifica files: scarta i pacchetti che non corrispondono ai requisiti (azienda diversa/verifica troppo recente) ed esegue la verifica vera e propria sull'evidenza e su tutti i suoi file contenuti e decrementa il parametro nr pacchetti per la schedulazione;
- Reschedule: usando il parametro nr pacchetti per la schedulazione (se > 0) crea un nuovo processo di VM con chunk prefissata.

Nel caso non ci siano più pacchetti da verificare che soddisfano i parametri in ingresso il processo si fermerà anche se non è stata raggiunta la quota nr pacchetti per schedulazione

[TORNA AL SOMMARIO](#)

9.3. [SOLUZIONI ADOTTATE IN CASO DI ANOMALIE](#)

Le anomalie che si possono verificare nella gestione del sistema informatico sono:

- Guasto hardware sugli apparati (server/storage)
- Compromissione del sistema informatico
- Guasto al dispositivo di firma
- Indisponibilità della Certification Authority

Di seguito vengono descritte le modalità operative adottate per far fronte ai rischi precedentemente elencati:

Guasto Hardware apparati

Il sistema di conservazione si compone di software e hardware in grado di erogare le funzionalità richieste anche in presenza di guasti.

Ciò è stato ottenuto rimuovendo dal disegno logico-architetturale tutti i "single point of failure" o eventualmente ridondandoli in modo da garantire "back-up" e "virtual clustering" e in analisi ricorrendo a servizi di "pure clustering" e "fail over".

Nel caso in cui si verificasse un guasto hardware lo stesso potrà essere riparato senza pregiudicare il funzionamento del sistema.

Compromissione del sistema software

La struttura del sistema informatico risponde ai requisiti di alta affidabilità e ridondanza in modo da garantire la continuità di esercizio.



CORVALLIS DM

EN/ISO 14001:2004 IE-0915-05
ISO/IEC 27001:2013 IIS-1014-01
ISO 9001 IQ-1015-02



Dasa-Rägister

00-CDM-Manuale Conservazione-Rev-1-13-del-15-gennaio-2019.docx

In caso di compromissione di questa struttura, la versione in esercizio può essere ripristinata in tempo reale utilizzando gli apparati ridondanti a disposizione del sistema.

Nel caso di compromissione dell'intera struttura si potrà ripristinare la situazione attraverso le copie di sicurezza effettuate giornalmente fino all'ultimo punto di ripristino funzionante.

Guasto al dispositivo di firma

Il dispositivo di firma è un servizio esterno con delle SLA molto restringenti con tempi di ripristino molto brevi.

Indisponibilità della certification authority

E' un evento particolarmente improbabile in quanto anche lì sono implementate politiche di erogazione del servizio con SLA di altissimo livello

[TORNA AL SOMMARIO](#)