

Manuale di Conservazione

di Microdata Service S.r.l. Unipersonale

Emissione del documento

Azione	Data	Nominativo	Funzione
Redazione	15/11/2019		-
		Davide Miragoli	-
		Massimiliano Pessina e Maurizio Delcuratolo	Responsabile dei sistemi informativi e della sicurezza dei sistemi per la conservazione
		Flora Santorelli	Responsabile della funzione archivistica
Verifica	18/11/2019	Carolina Cortellini	Responsabile del trattamento dei dati personali
Approvazione	18/11/2019	Alfredo Lupi	Responsabile del servizio di conservazione

Registro delle versioni

N° Versione	Data emissione	Modifiche apportate	Osservazioni
1.0	02/10/2014	Prima stesura.	
1.1	04/01/2016	Manuale adattato in base all'indice fornito da AgID v.2, inclusa modifica della sede legale della società.	La presente versione non è stata pubblicata in AgID e non è stata conservata
1.2	10/03/2016	Aggiunto testo alternativo nelle figure.	
1.3	16/03/2017	Aggiornamento sede operativa, componenti fisiche e tecnologiche e gestione anomalie causa trasferimento.	La presente versione non è stata pubblicata in AgID e non è stata conservata
1.4	27/07/2017	<ul style="list-style-type: none"> • Aggiornamento cap.3: aggiunto il DMEF del 17/06/2014 . • Aggiornamento cap. 4: ridefinite le attività associate a ciascun Responsabile ad eccezione del Responsabile del trattamento dei dati personali; modifica al Responsabile della funzione archivistica; modificati i riferimenti contrattuali. • Aggiornamento cap.5: aggiunta l'Agenzia delle Entrate tra gli organismi di tutela e di vigilanza; ridefinita la struttura organizzativa. • Aggiornamento cap.7: revisione del processo di conservazione. 	La presente versione non è stata pubblicata in AgID e non è stata conservata
1.5	21/12/2017	<ul style="list-style-type: none"> • Sostituito il termine volume/i con pacchetto/i di archiviazione. • Aggiunti riferimenti normativi. • Definiti in modo più chiaro i seguenti ruoli: Soggetto produttore, Responsabile della conservazione, Responsabile del servizio di conservazione e organi di vigilanza. • Fatti alcuni inserimenti e/o modifiche nel testo. 	Esclusi i casi in cui si fa riferimento al VdC UNI SInCRO
1.6	06/03/2018	<ul style="list-style-type: none"> • Sostituito o eliminato il termine volume/i (terminologia dell'abrogata delibera CNIPA 11/2004) ai seguenti paragrafi: <ul style="list-style-type: none"> - Par. 6.3 - Il Pacchetto di Archiviazione; - Par. 8.1 - Le componenti logiche. 	Esclusi i casi in cui si fa riferimento al VdC UNI SInCRO
1.7	03/06/2019	<ul style="list-style-type: none"> • Introdotta nel paragrafo 9.1 quanto definito delle procedure interne in merito al monitoraggio normativo; • Modificato lo schema di rete 	La presente versione non è stata pubblicata in AgID e non è stata conservata
1.8	05/09/2019	<ul style="list-style-type: none"> • Aggiornato normativo in riferimento al nuovo regolamento in materia di protezione dei dati personali. • Aggiunto standard ISO 15489:2016 e ISO 	

		<p>23081-1:2017.</p> <ul style="list-style-type: none"> • Aggiunto documento contrattuale: Atto di nomina Responsabile del servizio di conservazione. • Revisione capitolo "Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione". • Revisione capitolo "Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del Pubblico Ufficiale nei casi previsti". • Aggiunto capitolo "Cessazione dell'attività di conservazione"; • Modificata gestione degli errori temporanei descritta nel paragrafo 9.3.; • Aggiornata Figura 10. 	
1.9	15/11/2019	<ul style="list-style-type: none"> • Aggiornamento nominativo Responsabile dei sistemi informativi • Aggiornamento nominativo Responsabile della sicurezza dei sistemi per la conservazione 	

INDICE

1. SCOPO E AMBITO DEL DOCUMENTO	5
2. TERMINOLOGIA	7
3. NORMATIVA E STANDARD DI RIFERIMENTO.....	14
3.1 NORMATIVA DI RIFERIMENTO.....	14
3.2 STANDARD DI RIFERIMENTO.....	15
3.3 PROGETTI DI STUDIO.....	16
4. RUOLI E RESPONSABILITÀ	17
5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE	20
5.1 ORGANIGRAMMA.....	20
5.2 STRUTTURA ORGANIZZATIVA	20
6. OGGETTI SOTTOPOSTI A CONSERVAZIONE	24
6.1 OGGETTI CONSERVATI	24
6.2 IL PACCHETTO DI VERSAMENTO (PDV)	33
6.3 IL PACCHETTO DI ARCHIVIAZIONE (PDA)	34
6.4 IL PACCHETTO DI DISTRIBUZIONE (PDD)	37
7. IL PROCESSO DI CONSERVAZIONE	39
7.1 MODALITÀ DI ACQUISIZIONE DEI PACCHETTI DI VERSAMENTO PER LA LORO PRESA IN CARICO	39
7.2 VERIFICHE EFFETTUATE SUI PACCHETTI DI VERSAMENTO E SUGLI OGGETTI IN ESSI CONTENUTI.....	41
7.3 ACCETTAZIONE DEI PACCHETTI DI VERSAMENTO E GENERAZIONE DEL RAPPORTO DI VERSAMENTO DI PRESA IN CARICO.....	41
7.4 RIFIUTO DEI PACCHETTI DI VERSAMENTO E MODALITÀ DI COMUNICAZIONE DELLE ANOMALIE.....	42
7.5 PREPARAZIONE E GESTIONE DEL PACCHETTO DI ARCHIVIAZIONE	42
7.6 PREPARAZIONE E GESTIONE DEL PACCHETTO DI DISTRIBUZIONE AI FINI DELL'ESIBIZIONE.....	42
7.7 PRODUZIONE DI DUPLICATI E COPIE INFORMATICHE E DESCRIZIONE DELL'EVENTUALE INTERVENTO DEL PUBBLICO UFFICIALE NEI CASI PREVISTI.....	43
7.8 SCARTO DEI PACCHETTI DI ARCHIVIAZIONE.....	45
7.9 PREDISPOSIZIONE DI MISURE A GARANZIA DELL'INTEROPERABILITÀ E TRASFERIBILITÀ AD ALTRI CONSERVATORI	46
7.10 CESSAZIONE DELL'ATTIVITÀ' DI CONSERVAZIONE	46
8. IL SISTEMA DI CONSERVAZIONE	47
8.1 COMPONENTI LOGICHE.....	48
8.2 COMPONENTI FISICHE E TECNOLOGICHE	55
8.3 PROCEDURE DI GESTIONE E DI EVOLUZIONE.....	60
9. MONITORAGGIO E CONTROLLI.....	61
9.1 PROCEDURE DI MONITORAGGIO	61
9.2 VERIFICA INTEGRITÀ DEGLI ARCHIVI	61
9.3 GESTIONE DELLE ANOMALIE.....	62

1. SCOPO E AMBITO DEL DOCUMENTO

Il presente documento ha lo scopo di descrivere il sistema di conservazione dei documenti informatici e la gestione dei relativi processi adottati e previsti dal conservatore accreditato Microdata Service S.r.l..

L'art. 44-bis del D.lgs. 7 marzo 2005, n. 82 (Codice dell'Amministrazione digitale, di seguito CAD) attribuisce all'Agenzia per l'Italia Digitale il compito di accreditare *“i soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici e di certificazione dei relativi processi anche per conto di terzi e intendono conseguire il riconoscimento dei requisiti del livello più elevato, in termini di qualità e sicurezza [..]”*.

Con il DPCM del 3 dicembre 2013 (G.U. n. 59 del 12 marzo 2014 - S.O. 20) sono state emanate le regole tecniche in materia di sistema di conservazione dei documenti informatici ai sensi degli artt. 20, commi 3 e 5 bis, 23 ter, comma 4, 43, commi 1 e 3 44, 44 bis e 71, comma 1 del CAD, in vigore dall'11 aprile 2014 (art. 14 comma 1).

Il manuale della conservazione di Microdata, in linea con l'art. 8 del DPCM 3 dicembre 2013 ha lo scopo di descrivere:

- L'organizzazione della struttura che realizza il processo di conservazione, definendo i soggetti coinvolti e i ruoli svolti dagli stessi;
- Il modello di funzionamento, la descrizione delle architetture e delle infrastrutture utilizzate;
- Le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.

In merito alle tipologie degli oggetti sottoposti a conservazione e ai rapporti con i soggetti produttori il presente Manuale deve essere integrato con le specifiche tecniche (o allegato tecnico), documento allegato al contratto di affidamento del servizio di conservazione, redatto con ogni soggetto produttore, che definisce le specifiche operative e le modalità di descrizione e di Versamento nel Sistema di conservazione digitale delle Tipologie documentarie e Aggregazioni documentali informatiche oggetto di conservazione.

Nell'erogazione del servizio di conservazione, Microdata utilizza il **software Legal Archive®** di proprietà di Ifin Sistemi S.r.l. a socio unico (di seguito Ifin Sistemi), in grado di gestire l'intero processo di conservazione dei documenti informatici in conformità alla normativa vigente.

Il sistema Legal Archive® si configura come un servizio a disposizione di qualsivoglia piattaforma, applicativo e Sistema di Document Management (DMS).

All'interno di questo sistema articolato, il soggetto produttore, cui spetta il compito di nominare un Responsabile della conservazione interno, nomina **Microdata Service S.r.l.**, nella persona di **Alfredo Lupi** in qualità di suo legale rappresentante, **Responsabile del servizio di conservazione:**

Denominazione	Microdata Service S.r.l. Unipersonale
Indirizzo sede legale	Via Porlezza n.16 - 20123, Milano
Indirizzo sede operativa	Via Dell'Innovazione Digitale, 3 - 26100, Cremona
Indirizzo sede secondaria	Via delle Economie 9/11 - 26030 Gadesco (Cr)
Legale Rappresentante	Alfredo Lupi
Referente tecnico cui rivolgersi in caso di problemi tecnico-operativi	Davide Lorenzo Miragoli
E-mail del referente tecnico	staff_conservazioneditale@microdatagroup.it
N° telefono/fax	0372805100 / 0372590344
Sito web istituzionale	www.microdatagroup.it
E-mail istituzionale	info@microdatagroup.it

Nel corso degli anni non è stato nominato altro Responsabile del servizio di conservazione.
Il presente manuale è un documento informatico conservato nel sistema di conservazione.

[Torna al sommario](#)

2. TERMINOLOGIA

GLOSSARIO

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

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' Agenzia per l'Italia digitale , del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza, ad un soggetto pubblico o privato che svolge attività di conservazione o di certificazione del processo di conservazione.
affidabilità	caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico.
aggregazione documentale informatica	aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente.
allegato	componente dell'unità documentaria, costituita da un documento unito a un altro documento principale per integrarne le informazioni, redatto contestualmente o precedentemente al documento principale stesso.
annesso	componente dell'unità documentaria, costituita da un documento, generalmente prodotto e inserito nell'unità documentaria in un momento successivo, a integrazione e corredo del documento principale.
archivio	complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o acquisiti da un soggetto produttore durante lo svolgimento dell'attività.
archivio informatico	archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico.
area organizzativa omogenea	un insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445.
attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.
autenticità	caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico.
base di dati	collezione di dati registrati e correlati tra loro.
certificatore accreditato	soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, dall' Agenzia per l'Italia digitale , il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza.

ciclo di gestione	arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo.
classificazione	attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati.
Codice	decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni (CAD).
codice eseguibile	insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici.
comunità di riferimento	con riferimento al modello OAIS, è costituita da un gruppo ben individuato di potenziali utenti che dovrebbero essere in grado di comprendere l'informazione conservata. La comunità di riferimento può essere composta da più comunità di utenti.
conservatore accreditato	soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, dall' Agenzia per l'Italia digitale .
conservazione	insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione.
contenuto informativo	con riferimento al modello OAIS, è costituito dall'oggetto-dati e dalle informazioni sulla rappresentazione.
coordinatore della gestione documentale	responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 nei casi di amministrazioni che abbiano istituito più Aree Organizzative Omogenee.
copia analogica del documento informatico	documento analogico avente contenuto identico a quello del documento informatico da cui è tratto.
copia di sicurezza	copia di <i>backup</i> degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 delle presenti regole tecniche per il sistema di conservazione.
destinatario	identifica il soggetto/sistema al quale il documento informatico è indirizzato.
disaster recovery	con riferimento all'art. 50bis del CAD, l'insieme delle misure tecniche e organizzative adottate per assicurare all'organizzazione il funzionamento del centro elaborazione dati e delle procedure e applicazioni informatiche dell'organizzazione stessa, in siti alternativi a quelli primari/di produzione, a fronte di eventi che provochino, o possano provocare, indisponibilità prolungate.
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.
formato	modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.

funzionalità aggiuntive	le ulteriori componenti del sistema di protocollo informatico necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni.
funzionalità interoperative	le componenti del sistema di protocollo informatico finalizzate a rispondere almeno ai requisiti di interconnessione di cui all'articolo 60 del D.P.R. 28 dicembre 2000, n. 445.
funzionalità minima	la componente del sistema di protocollo informatico che rispetta i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445.
funzione di hash	una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
generazione automatica di documento informatico	formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni.
identificativo univoco	sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione.
immodificabilità	caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso.
impronta	la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di <i>hash</i> .
insieme minimo di metadati del documento informatico	complesso dei metadati, la cui struttura è descritta nell'allegato 5 del presente decreto, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta.
integrità	insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato.
interoperabilità	capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi.
leggibilità	insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti.
log di sistema	registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati.
manuale di conservazione	strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 delle regole tecniche del sistema di conservazione.
manuale di gestione	strumento che descrive il sistema di gestione informatica dei documenti (di cui all'articolo 5 delle regole tecniche del protocollo informatico) ai sensi delle regole tecniche per il protocollo informatico D.P.C.M. 31 ottobre 2000 e successive modificazioni e integrazioni.
memorizzazione	processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici.
metadati	insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica, per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 del presente decreto.

pacchetto di archiviazione	pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del presente decreto e secondo le modalità riportate nel manuale di conservazione.
pacchetto di distribuzione	pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta.
pacchetto di versamento	pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione.
pacchetto informativo	contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare.
piano della sicurezza del sistema di conservazione	documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza.
piano della sicurezza del sistema di gestione informatica dei documenti	documento, che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi nell'ambito dell'organizzazione di appartenenza.
piano di conservazione	strumento, integrato con il sistema di classificazione per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445.
piano generale della sicurezza	documento per la pianificazione delle attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza.
presa in carico	accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione.
processo di conservazione	insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 10 delle regole tecniche del sistema di conservazione.
produttore	persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni tale figura si identifica con il 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.
repertorio informatico	registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche con cui si formano altri atti e documenti o indici di atti e documenti secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica.

responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi	dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico-archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione.
responsabile della conservazione	soggetto responsabile dell'insieme delle attività elencate nell'articolo 7, comma 1 delle regole tecniche del sistema di conservazione.
responsabile del trattamento dei dati	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.
responsabile della 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.
serie	secondo la definizione di ISAD (G), all'interno di un archivio o fondo, si definisce serie un insieme di documenti ordinati secondo un sistema di archiviazione comune o conservati unitariamente perché sono il risultato di un medesimo processo di sedimentazione o di una stessa attività; vi è cioè tra essi una qualche forma di relazione originaria derivante dalle modalità della loro produzione, acquisizione o uso.
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 (ACID) delle modifiche della base di dati.
Testo Unico	Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (TUDA), 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.
unità archivistica	insieme di unità documentarie unite secondo un nesso di collegamento organico; unità elementare della serie.
unità documentaria	unità elementare di cui è composto un archivio rappresentata da un aggregato logico costituito da uno o più elementi da trattare in modo unitario
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	operazione con la quale il produttore trasferisce al sistema di conservazione un pacchetto di versamento.

versamento agli Archivi di Stato	operazione con cui il Responsabile della conservazione di un organo centrale o periferico 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 (D.lgs. 22 gennaio 2004, n. 42, art. 41).
web service	Sistema software progettato per supportare l'interoperabilità tra diversi computer su di una medesima rete o in un contesto distribuito.

[Torna al sommario](#)

ACRONIMI

ACRONIMO	DEFINIZIONE
AgID	Agenzia per l'Italia Digitale.
CA	Certification Authority.
CAD	Codice dell'amministrazione digitale.
CRL	Certificate Revocation List, è la lista dei certificati revocati o sospesi, ovvero lista di certificati che sono stati resi non validi prima della loro naturale scadenza.
HSM	Hardware Security Module, è l'insieme di hardware e software che realizza dispositivi sicuri per la generazione delle firme in grado di gestire in modo sicuro una o più coppie di chiavi crittografiche.
IdC	Indice di conservazione realizzato secondo le specifiche dello standard UNI SinCRO.
IdV	Indice di versamento.
IR	Informazioni sulla rappresentazione.
IRse	Informazioni sulla rappresentazione semantica.
IRsi	Informazioni sulla rappresentazione sintattica.
ISAD	Information Standard Archival Description.
ISAAR	Information Standard Archival Authority Record.
ISO	International Organization for Standardization.
OAIS	ISO 14721: 2012: Space data and information transfer systems – Open archival information system. ISO 14721:2012 definisce il modello di riferimento per un <i>open archival information system</i> (OAIS), un sistema archivistico inteso come struttura organizzata di persone e sistemi che hanno accolto la responsabilità di preservare documenti e metadati di uno o più soggetti produttori, rendendoli disponibili per una comunità di riferimento.
PdA	Pacchetto di Archiviazione.
PdD	Pacchetto di Distribuzione.
PdV	Pacchetto di Versamento.
PDI	Preservation Description Information (informazioni sulla conservazione).
PEC	Posta Elettronica Certificata.
RdC	Responsabile della conservazione.
RdSC	Responsabile del servizio di conservazione.
SFTP	Secure File Transfer Protocol.
SMTP	Simple Mail Transfer Protocol (SMTP) è il protocollo standard per la trasmissione via internet di e-mail.
SNMP	Simple Network Management Protocol.
SP	Soggetto produttore.
TSA	Time Stamping Authority, è il soggetto che eroga la marca temporale.
UID	Unique Identifier
UNI SinCRO	UNI 11386:2010 - Supporto all'interoperabilità nella conservazione e nel recupero degli oggetti digitali.
URL	Uniform Resource Locator
VdC	Volume di conservazione.

[Torna al sommario](#)

3. **NORMATIVA E STANDARD DI RIFERIMENTO**

3.1 **NORMATIVA DI RIFERIMENTO**

- **Codice Civile** -Libro Quinto del Lavoro, Titolo II del lavoro nell'impresa, Capo III delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili, art. 2215 bis - Documentazione informatica;
- **Legge del 7 agosto 1990, n. 241 e s.m.i.** - Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- **Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445** - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (TUDA);
- **Decreto legislativo 30 giugno 2003, n. 196 e s.m.i** - Codice in materia di protezione dei dati personali;
- **Decreto legislativo 22 gennaio 2004, n. 42 e successive modificazioni** - Codice dei beni Culturali e del Paesaggio;
- **Decreto legislativo 7 marzo 2005, n. 82 e s.m.i.** - Codice dell'Amministrazione digitale (CAD);
- **Circolare AGID del 23 gennaio 2013, n.60** - Formato e definizioni dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le pubbliche amministrazioni;
- **Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013** - Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;
- **Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013** - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del CAD;
- **Circolare AGID del 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 CAD;
- **Decreto del Ministero delle Economie e delle Finanze del 17 giugno 2014-** "Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005" (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 CAD (GU Serie Generale n. 8 del 12-01-2015);
- **Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016** - Regolamento 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) (Testo rilevante ai fini del SEE);

- **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.

[Torna al sommario](#)

3.2 STANDARD DI RIFERIMENTO

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

- **ISAD (G) 1999-02**, General Information Standard Archival Description;
- **ISAAR (CPF) 2003-02**, International Standard Archival Authority Records for Corporate Bodies, Persons and Families;
- **PAIMAS - ISO 20652:2006**, Space data and information transfer systems- Producer - Archive Interface - Methodology Abstract Standard;
- **ISO 15836:2009 Information and documentation**, The Dublin Core Metadata Element Set;
- **UNI 11386:2010 Standard SInCRO**, Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- **ISO 23081-1:2006. -02:2011**, Metadata for records;**ISO 16363:2012**, Space Data and Information Transfer Systems - Trustworthy Repositories Audit & Certification (TRAC);
- **ISO 14721:2012**, OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- **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;
- **ISO/IEC 27001:2013**, Information technology - Security techniques - Information security management systems - Requirements, Requisiti di un ISMS (Information Security Management System);
- **ISO 15489-1:2016**, Information and documentation -- Records management Concepts and principles;
- **ISO 23081-1:2017**, Information and documentation -- Records management processes -- Metadata for records.

[Torna al sommario](#)

3.3 PROGETTI DI STUDIO

Si segnalano alcuni dei principali progetti di studio internazionali sul tema della conservazione in ambito digitale e sui principi di valutazione dei depositi di conservazione:

- APARSEN (*Alliance for Permanent Access to the Records of Science in Europe Network*)
- DRAMBORA (*Digital Repository Audit Method Based on Risk Assessment*)
- InterPARES Project (*The International Research on Permanent Authentic Records in Electronic Systems*)
- MoReq2 (*Model Requirements for the Management of Electronic Records*)
- TRAC (*Trusted Repositories Audit & Certification*).

[Torna al sommario](#)

4. RUOLI E RESPONSABILITÀ

Nel presente capitolo si elencano i nominativi, i ruoli e i compiti svolti dai responsabili che interagiscono nel sistema di conservazione

CRONOLOGIA DEI RESPONSABILI

NOME COGNOME	FUNZIONE	CONTRATTO DI ASSUNZIONE	DATA NOMINA	DATA REVOCA
Alfredo Lupi	Responsabile del servizio di conservazione	-----	-----	-----
Carolina Cortellini	Responsabile per il trattamento dei dati personali	-----	-----	-----
Alfredo Luigi Martini	Responsabile dei sistemi informativi e della sicurezza dei sistemi per la conservazione	Contratto a tempo indeterminato	30/09/2014	30/09/2019
Massimiliano Pessina	Responsabile dei sistemi informativi per la conservazione	Contratto a tempo indeterminato	01/10/2019	-----
Maurizio Delcuratolo	Responsabile della sicurezza dei sistemi per la conservazione	Contratto a tempo indeterminato	01/10/2019	-----
Massimiliano Pessina	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Contratto a tempo indeterminato	30/09/2014	-----
Valeria Leoni	Responsabile della funzione archivistica	Contratto di lavoro autonomo della durata di 36 mesi (tre anni) rinnovabile	10/10/2014	30/06/2017
Flora Santorelli			01/09/2017	-----

[Torna al sommario](#)

RUOLI E RESPONSABILITÀ

Ruolo	Nominativo	Attività di competenza	Periodo nel ruolo ¹	Eventuali deleghe
Responsabile del servizio di conservazione	Lupi Alfredo	Definisce le politiche complessive del sistema di conservazione nonché del governo della gestione del sistema di conservazione. In particolare, definisce: - le caratteristiche e i requisiti del sistema di conservazione in conformità alla normativa vigente; - le modalità operative di erogazione dei servizi di conservazione; - gli aspetti tecnici di erogazione del servizio di conservazione. Approva il manuale di conservazione digitale.	Dal 2005	

¹ Occorre precisare che ciascun Responsabile svolge il ruolo di cui è stato incaricato a partire dalla data di assunzione ma la nomina è stata formalizzata dopo la pubblicazione della Circolare 65 del 10 aprile 2014. Tale Circolare ha infatti decretato l'obbligatorietà delle figure professionali descritte nella presente tabella.

Responsabile del trattamento dei dati personali	Cortellini Carolina	Garantisce il rispetto delle vigenti disposizioni in materia di trattamento dei dati personali e si assicura che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.	Dal 2005	
Responsabile della sicurezza dei sistemi per la conservazione	Delcuratolo Maurizio	Garantisce il rispetto e assicura il monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; segnala eventuali difformità al Responsabile del servizio di conservazione e individua e pianifica le necessarie azioni correttive.	Dal 2016	
Responsabile dei sistemi informativi per la conservazione	Pessina Massimiliano	Gestisce l'esercizio delle componenti hardware e software del sistema di conservazione; monitora il mantenimento dei livelli di servizio (SLA) dei sistemi informativi concordati con l'Azienda; segnala le eventuali difformità degli SLA al Responsabile del servizio di conservazione e individua e pianifica le necessarie azioni correttive; pianifica lo sviluppo delle infrastrutture tecnologiche del sistema di conservazione; controlla e verifica i livelli di servizio erogati dai fornitori con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.	Dal 2012	
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Pessina Massimiliano	Coordina lo sviluppo e la manutenzione delle componenti software del sistema di conservazione; pianifica e monitora i progetti di sviluppo del sistema di conservazione; monitora gli SLA relativi alla manutenzione del sistema di conservazione, gestisce le eventuali migrazioni verso nuove piattaforme tecnologiche e lo sviluppo di siti web e portali connessi al servizio di conservazione.	Dal 2012	
Responsabile della funzione archivistica di conservazione	Santorelli Flora	Definisce e gestisce gli aspetti archivistici relativi al processo di conservazione. Effettua le attività di analisi documentale connesse allo svolgimento del servizio di conservazione per il settore pubblico; per le aziende private soltanto su richiesta. Nel settore pubblico assume un ruolo consulenziale nella gestione del processo di conservazione, in particolare può definire le modalità di trasferimento del documento, il set di metadati di conservazione dei documenti e dei fascicoli informatici; monitora gli aspetti archivistici del processo di conservazione. Cura i rapporti con il Ministero dei Beni e delle attività culturali per quanto di competenza.	Dal 2017	

[Torna al sommario](#)

RIFERIMENTI CONTRATTUALI

Il servizio di conservazione erogato da Microdata è regolato dai seguenti documenti:

- Contratto di affidamento del servizio di conservazione.
- Allegato tecnico: contenente le specifiche tecniche.
- Atto di nomina Responsabile del servizio di conservazione.

[Torna al sommario](#)

5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 ORGANIGRAMMA

Si riporta di seguito l'organigramma della struttura coinvolta nel servizio di conservazione.

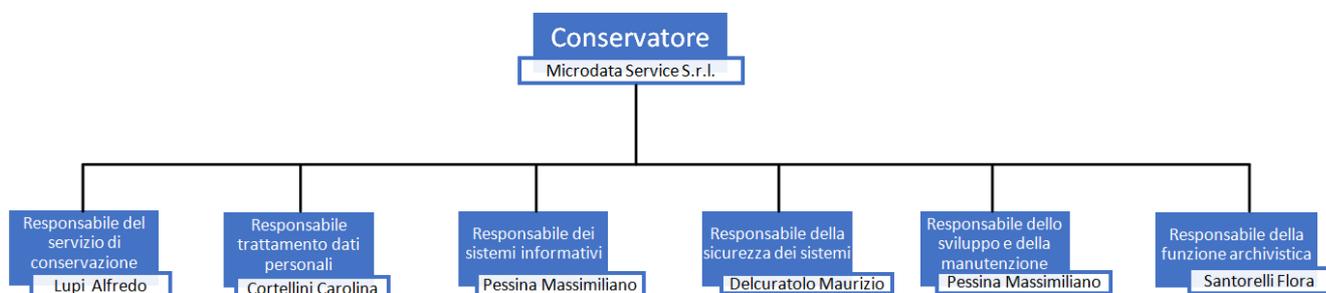


Figura 1: Struttura organizzativa Microdata Service S.r.l.

[Torna al sommario](#)

5.2 STRUTTURA ORGANIZZATIVA

MODELLO ORGANIZZATIVO DELLA CONSERVAZIONE

Nell'erogazione del servizio di conservazione, Microdata ha adottato un modello organizzativo strutturato secondo quanto stabilito dalle vigenti regole tecniche, DPCM 3 dicembre 2013 alla lettera b) comma 2 dell'articolo 5 nonché tenendo conto del modello OAIS (Open Archival Information System), ovvero di una struttura organizzata di persone e sistemi che accetti la responsabilità di conservare l'informazione e di renderla disponibile per una comunità di riferimento.

Seguendo quanto indicato dalle Regole tecniche vigenti e, sulla base dello stesso modello OAIS, si possono identificare i seguenti ruoli fondamentali:

- **PRODUTTORE**

È il soggetto che affida la conservazione dei propri Documenti informatici e delle Aggregazioni di Documenti Informatici a Microdata così come denominato nel **contratto di affidamento del servizio di conservazione**. Secondo lo standard OAIS, il produttore versa gli oggetti digitali e le relative informazioni sulla rappresentazione da conservare a norma.

I rapporti tra Microdata e il soggetto produttore sono concordati mediante un accordo formale (specifiche tecniche allegate al contratto di affidamento) che stabilisce le tipologie documentarie, i metadati oggetto di conservazione, i formati e le modalità operative di versamento.

Il responsabile di riferimento del soggetto produttore è di norma individuato nel responsabile della gestione documentale. **Il soggetto produttore è responsabile del contenuto del pacchetto di versamento** (d'ora in poi PdV) ed è tenuto a trasmetterlo al soggetto conservatore secondo quanto indicato nelle specifiche tecniche allegate al contratto di affidamento.

Il modello organizzativo fa riferimento al modello Open Archival Information System (OAIS), certificato standard ISO 14721 nel 2003 e recentemente aggiornato (ISO 14721:2012).

Il soggetto produttore ha accesso al sistema di conservazione direttamente dalla propria sede, tramite accesso web. Il soggetto produttore, secondo quanto previsto nel contratto di affidamento del servizio di conservazione, si impegna a depositare i documenti informatici e le loro aggregazioni nei modi e nelle forme definite nelle specifiche tecniche, garantendone l'autenticità e l'integrità nelle fasi di produzione e di archiviazione. In particolare, garantisce che il trasferimento dei documenti informatici venga realizzato utilizzando formati compatibili con la funzione di conservazione e rispondenti a quanto previsto dalla normativa vigente.

Il produttore mantiene la titolarità e la proprietà dei documenti depositati.

- **UTENTE**

Le vigenti regole tecniche identificano l'utente come una persona, ente o sistema che interagisce con i servizi di un sistema per la conservazione di documenti informatici.

L'utente richiede al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge. Il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, ai documenti informatici conservati e consente la produzione di un pacchetto di distribuzione (d'ora in poi PdD) direttamente acquisibile dai soggetti autorizzati. In termini OAIS la comunità degli Utenti può essere definita come Comunità di riferimento.

Nelle Specifiche Tecniche, documento allegato al contratto di affidamento del servizio di conservazione, vengono indicati quei soggetti abilitati dal soggetto produttore che possono accedere ai documenti versati dal produttore al conservatore. L'abilitazione e l'autenticazione degli utenti avviene in base alle procedure di gestione utenze indicate nel Piano della sicurezza del sistema di conservazione e nel rispetto delle misure di sicurezza previste negli articoli da 31 a 36 del D.lgs. 30 giugno 2003, n. 196, in particolare di quelle indicate all'art. 34 comma 1 e dal Disciplinare tecnico di cui all'allegato B del medesimo decreto.

- **RESPONSABILE DELLA CONSERVAZIONE**

Il Responsabile della conservazione è una persona fisica i cui compiti sono definiti nel DPCM 3 dicembre 2013, art. 7. Il Responsabile della conservazione ha il compito di definire e attuare le politiche complessive del sistema di conservazione, di governarne la gestione con piena responsabilità e autonomia in relazione al modello organizzativo adottato e in conformità agli standard previsti dalla normativa.

Nelle pubbliche amministrazioni, **il ruolo del responsabile della conservazione è svolto da un dirigente o da un funzionario formalmente designato**; tale ruolo può essere svolto dal responsabile della gestione documentale ovvero dal coordinatore della gestione documentale, ove nominato.

Nei soggetti privati, in mancanza di una nomina formalizzata, **il Responsabile della conservazione è individuato nel Rappresentante Legale del soggetto produttore.**

- **RESPONSABILE DEL SERVIZIO DI CONSERVAZIONE**

Il Responsabile del servizio di conservazione è la persona fisica, interna all'organizzazione del soggetto conservatore, che svolge le attività così come definite nel contratto di affidamento del servizio. I compiti del Responsabile del servizio di conservazione sono definiti all'art. 7 del DPCM 3 dicembre 2013. Nel contratto di affidamento del servizio di conservazione sono definite le attività e le responsabilità affidate al responsabile del servizio di conservazione e quelle che rimangono a carico del produttore.

Ai sensi dell'art. 6 del suddetto DPCM il soggetto esterno a cui è affidato il servizio di conservazione assume il ruolo di Responsabile del trattamento dei dati personali come previsto dal Codice in materia di protezione dei dati personali.

• **ORGANISMO DI TUTELA E VIGILANZA**

La funzione di vigilanza e tutela sugli archivi informatici affidati a servizi di conservazione esterni spetta ad AgID (dall'art. 14-bis, comma 2, lettera i del CAD) che accredita i soggetti conservatori previa valutazione dei requisiti di qualità e di sicurezza in merito all'infrastruttura, ai processi e all'organizzazione (art. 44 bis del CAD).

Il Ministero per i beni e le attività culturali e del turismo (MiBACT) esercita funzioni di tutela e vigilanza dei sistemi di conservazione degli archivi di enti pubblici o di enti privati dichiarati di interesse storico particolarmente importante e autorizza le operazioni di scarto e trasferimento della documentazione conservata ai sensi del D.lgs. 42/2004 (artt. 21, 30).

La tutela e vigilanza sugli archivi di enti pubblici non statali è esercitata dal MiBACT, tramite le Soprintendenze archivistiche competenti per territorio (D.lgs. 42/2004, art. 18).

"Lo spostamento, anche temporaneo dei beni culturali mobili" compresi gli archivi storici e di deposito è soggetto ad autorizzazione della Soprintendenza archivistica (D.lgs. 42/2004, art. 21, c. 1, lettera b).

Anche "Il trasferimento ad altre persone giuridiche di complessi organici di documentazione di Archivi pubblici, nonché di Archivi di privati per i quali sia intervenuta la dichiarazione ai sensi dell'articolo 13", sia che comporti o non comporti uno spostamento, rientra tra gli interventi soggetti ad autorizzazione della Soprintendenza archivistica (D.lgs. 42/2004, art.21, c. 1, lettera e).

La disposizione si applica anche:

- all'affidamento a terzi dell'archivio (outsourcing), ai sensi del D.lgs. 42/2004, art.21, c. 1, lettera e)
- al trasferimento di Archivi informatici ad altri soggetti giuridici, nell'ottica della Conservazione permanente sia del documento sia del contesto archivistico (art.44 bis del CAD).

La Soprintendenza può, in seguito a preavviso, effettuare ispezioni per accertare lo stato di conservazione e custodia degli archivi e può emettere prescrizioni per la tutela degli archivi.

Sono considerati organismi di tutela e vigilanza anche l'Istituto per la Vigilanza sulle Assicurazioni (IVASS) che ha compiti di vigilanza nei settori finanziario e assicurativo e l'Agenzia delle Entrate.

[Torna al sommario](#)

FIGURE PROFESSIONALI RESPONSABILI DEL SERVIZIO DI CONSERVAZIONE

Il gruppo di lavoro del **servizio di conservazione** dei documenti, al fine di garantire la corretta esecuzione del servizio relativamente a tutte le problematiche tecnico-organizzative peculiari, è formato dalle figure professionali sopra descritte.

Le procedure organizzative si basano sui mandatory standards ISO 27001 e ISO 9001.

Di seguito sono riportate le tabelle contenenti i ruoli e le attività di ciascun profilo professionale previsto dalla Circolare AgID 65/2014: **Microdata Service Srl, designata dal soggetto produttore Responsabile del servizio di conservazione, non sottopone a nessun trattamento di verifica il contenuto dei documenti che le sono inviati per sottoporli al processo di conservazione.**

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

[Torna al sommario](#)

6. OGGETTI SOTTOPOSTI A CONSERVAZIONE

6.1 OGGETTI CONSERVATI

Le specificità del processo di conservazione adottate per ciascuna tipologia documentaria sono descritte nell'allegato tecnico al contratto e condivise con il soggetto produttore.

In generale è possibile affermare che il sistema di conservazione installato è in grado di gestire e conservare i seguenti elementi:

[Torna al sommario](#)

DOCUMENTI INFORMATICI E AGGREGAZIONI DOCUMENTALI INFORMATICHE

Il sistema di conservazione gestito da Microdata conserva documenti informatici, in particolare documenti amministrativi informatici, con i metadati descrittivi ad essi associati e le loro aggregazioni documentali informatiche (allegati e/o annessi). Il sistema prevede anche la conservazione di fascicoli, cioè di aggregazioni di più unità documentarie legati insieme da un vincolo logico.

Tale modello riprende la struttura gerarchica di ordinamento di un archivio, illustrato nella Figura 2, derivata dallo schema dello standard ISAD (G).

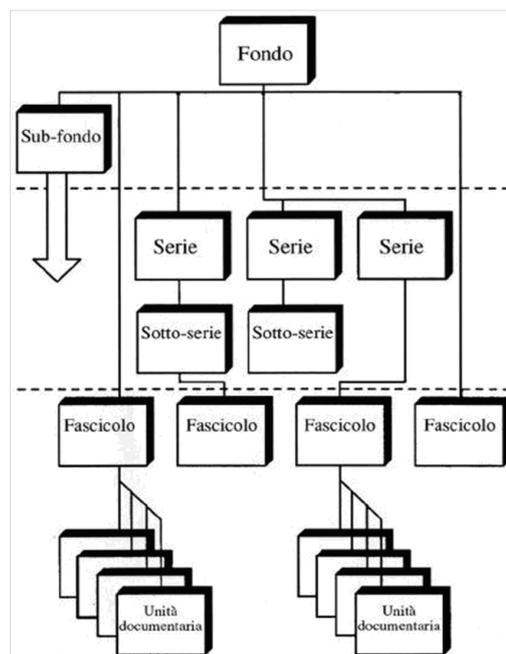


Figura 2: Gerarchia di un archivio

I documenti informatici e le loro aggregazioni di tipo fascicolo sono trattati nel sistema nella forma di unità documentarie e fascicolo, specificamente descritte nel paragrafo 7.1.2, e sono inviati in Conservazione sotto forma di Pacchetti di versamento (PdV), che contengono anche i relativi metadati.

Il sistema gestisce gli oggetti sottoposti a conservazione distinti per ogni singolo soggetto produttore anche per singola struttura (generalmente corrispondenti alle Aree Organizzative Omogenee), consentendo di definire configurazioni e parametri ad hoc per ogni soggetto

produttore, in base agli accordi stipulati all'atto della sottoscrizione del contratto di affidamento del servizio di conservazione.

Per mantenere anche nel sistema le informazioni relative alla struttura dell'archivio e dei relativi vincoli archivistici, le unità documentarie possono essere versate corredate di un set di metadati di profilo archivistico che include gli elementi identificativi e descrittivi del fascicolo, con riferimento alla voce di classificazione e l'eventuale articolazione in sottofascicoli. Inoltre, è gestita la presenza di classificazioni, fascicoli e fascicoli secondari (sottofascicoli) con collegamenti tra le diverse unità archivistiche e documentarie presenti nel sistema.

Le serie e i fascicoli possono essere versati nel sistema quando sono completi e dichiarati chiusi, descritti da un set di metadati che include obbligatoriamente, oltre alle informazioni di identificazione, classificazione e descrizione, anche il tempo di conservazione previsto. Nel caso delle serie la chiusura può avvenire a cadenza annuale o comunque secondo una definizione temporale stabilita dal soggetto produttore.

I documenti informatici (unità documentarie) e i fascicoli informatici possono essere suddivisi secondo un piano di classificazione, che identifica gruppi documentali omogenei per natura e/o funzione giuridica (titolo, classe, sottoclasse), modalità di registrazione o di produzione.

Le tipologie documentarie (suddivise in titoli, classi e sottoclassi) trattate e i loro specifici metadati e articolazioni sono indicate nell'allegato di servizio concordato con ogni soggetto produttore e riportate nelle funzionalità di amministrazione del Sistema.

[Torna al sommario](#)

UNITÀ DOCUMENTARIA

L'unità documentaria rappresenta l'unità minima elementare di riferimento di cui è composto un archivio, pertanto rappresenta il riferimento principale per la costruzione dei Pacchetti informativi secondo lo standard OAIS.

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

All'unità documentaria e agli elementi che la compongono sono associati set di metadati che li identificano e li descrivono, secondo le logiche e le articolazioni esposte al paragrafo 7.3.

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

[Torna al sommario](#)

INFORMAZIONE SULLA RAPPRESENTAZIONE

Lo standard OAIS prevede che ad ogni oggetto portato in conservazione siano associate una serie di informazioni (c.d. metadati) in grado di descrivere le caratteristiche estrinseche e intrinseche dell'oggetto e di garantirne nel futuro una facile reperibilità. Tra queste le informazioni sulla rappresentazione (IR), classificabili in sintattiche (IRsi) e semantiche (IRse), hanno l'obiettivo di

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 conservati imposto dal comma 1 dell'art. 3 delle nuove regole tecniche e dal comma 1 dell'art. 44 del CAD.

Risulta necessario affrontare tre tematiche importanti:

- La prima riguarda “cosa” associare ad un oggetto destinato alla conservazione in merito alle informazioni sulla rappresentazione e “come”;
- la seconda si riferisce al “come” rispettare il requisito di leggibilità;
- la terza si riferisce a “cosa” fornire nel momento in cui quell'oggetto deve essere distribuito agli utenti e “come”.

Per soddisfare questi requisiti, è indispensabile che il Responsabile del servizio di conservazione, in accordo con il soggetto produttore, sottoponga a conservazione tutte le informazioni sulla rappresentazione associate a un qualsiasi oggetto digitale da versare nel sistema necessarie alla futura consultazione di tale oggetto.

Classifichiamo quindi le informazioni sulla rappresentazione in:

- 1. Strumenti per la leggibilità:** tipicamente legati al formato dell'oggetto conservato (Viewer);
- 2. Informazioni sulla rappresentazione sintattica:** tipicamente legate al formato dell'oggetto conservato (per esempio il documento di specifiche tecniche del formato del file);
- 3. Informazioni sulla rappresentazione semantica:** tipicamente legate alla descrizione archivistica dell'oggetto conservato (per esempio come leggere il contenuto di una fattura) o a caratteristiche intrinseche del documento (quali la lingua o il codice utilizzati).

Sebbene le informazioni sulla rappresentazione sintattica (tipo 2) possano essere considerate le basi su cui poggiare le successive conservazioni di oggetti di uno specifico formato, poiché sono le informazioni necessarie a produrre/creare gli strumenti che ne permettono la leggibilità (tipo 1), resta fondamentale fornire fin dal principio, insieme all'oggetto conservato, gli strumenti necessari per poterlo leggere e utilizzare.

Concludendo, per soddisfare l'eventuale necessità di una disponibilità immediata dell'oggetto conservato, possiamo affermare che il sistema di conservazione deve avere almeno conservato gli strumenti per la leggibilità (visualizzatori) degli oggetti dati in conservazione.

Le informazioni sulla rappresentazione, sintattiche e semantiche, e i visualizzatori potranno essere inglobati nel PdD insieme ai documenti richiesti garantendo così la piena leggibilità nel lunghissimo periodo del documento conservato.

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

Si ritiene pertanto necessaria la capacità del software di generare, per ogni soggetto produttore, un insieme di descrizioni di tipo archivistico e diplomatistico “speciali” che diano modo al Responsabile del servizio di conservazione di conservare le tre tipologie di informazioni sulla rappresentazione.

In Legal Archive® distinguiamo tre descrizioni archivistiche speciali:

1. *“Viewer”* relativo a *“Unità documentaria”* con file di indice di tipo multi-indice.
2. *“Informazioni sulla rappresentazione”* relative a *“Unità Documentaria”* con file di indice di tipo indice singolo.
3. *“Fascicolo Informazioni sulla rappresentazione”* relativo a *“Fascicolo”*.

Le descrizioni archivistiche speciali sono descrizioni archivistiche prime in quanto non hanno nessuna diretta associazione con le informazioni sulla rappresentazione dei documenti informatici conservati.

La prima descrizione archivistica speciale (il *“Viewer”*) è obbligatoria, e oltre ai classici metadati Dublin Core, deve permettere di associare ad ogni documento informatico conservato (eseguibile del visualizzatore) la versione del visualizzatore, la lingua del visualizzatore e il sistema operativo di riferimento (versione, bit, lingua). Le operazioni per il suo versamento possono essere effettuate sia attraverso un PdV (file di metadati di tipo multi-indice) che manualmente da interfaccia web.

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

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

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

Le descrizioni archivistiche speciali sono di norma conservate per il conservatore (che diventa SP Padre) ed ereditate da tutti gli altri SP. In generale l'ereditarietà delle Informazioni sulla rappresentazione si sviluppa come nel classico schema di ereditarietà:

soggetto produttore → soggetto produttore padre → ... → soggetto produttore padre → soggetto conservatore → soggetto conservatore licenziatario.

[Torna al sommario](#)

VIEWER

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

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

Visto che questa n-pla permette di avere diversi strumenti per uno stesso Mime type, il sistema di conservazione deve permettere ad un Responsabile del servizio di conservazione di impostare a livello di soggetto produttore e/o a livello di descrizione archivistica (di tipo documento), quali siano gli strumenti per la leggibilità di un formato da collegare all'atto della conservazione e all'atto dell'esibizione.

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

soggetto produttore → soggetto produttore padre → ... → soggetto produttore padre → soggetto conservatore → soggetto conservatore licenziatario.

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

[Torna al sommario](#)

INFORMAZIONE SULLA RAPPRESENTAZIONE SINTATTICA

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

- formato (Mime type)
- eventuale versione del formato.

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

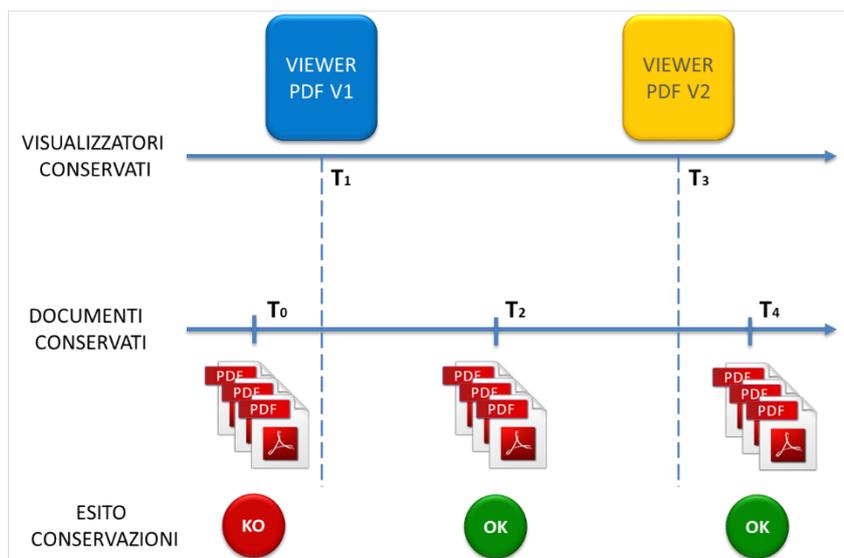


Figura 3: La conservazione delle informazioni sulla rappresentazione sintattica

[Torna al sommario](#)

INFORMAZIONE SULLA RAPPRESENTAZIONE SEMANTICA

Per quanto riguarda le informazioni sulla rappresentazione semantica, essendo anche queste legate ad una particolare versione di una descrizione archivistica, è necessario che ogni oggetto nel PdA si riferisca ad uno o più UID/ID che permettano di risalire all'ID della descrizione archivistica.

[Torna al sommario](#)

FORMATI

Il sistema di conservazione utilizza come formati di conservazione quelli elencati al punto 5 dell'allegato 2 alle Regole Tecniche e, inoltre, è in grado di gestire, su richiesta del soggetto produttore, anche Formati non compresi nel suddetto elenco ma che il soggetto produttore utilizza nei propri sistemi e che ritiene di dover conservare.

Tutti i Formati gestiti sono elencati e descritti in un registro interno al sistema di conservazione "Registro dei Formati" in cui ogni Formato è corredato da Informazioni descrittive relative alla eventuale versione, e al Mime type.

Con ciascun soggetto produttore è concordato un elenco di Formati ammessi, che individua i Formati che il Sistema può accettare da ogni produttore e per ogni tipologia documentaria gestita. L'elenco dei Formati ammessi è riportato (e gestito) nelle funzionalità "Amministrazione strutture versanti" del Sistema ed è aggiornato continuamente in base alle esigenze del produttore. Le modalità con cui si procede a tale aggiornamento sono concordate con ogni Produttore e riportate nelle specifiche tecniche. Il Sistema identifica i Formati al momento della ricezione del PdV mediante l'analisi dei magic numbers o del contenuto del file, in modo tale da consentire l'individuazione dello specifico Mime type. L'informazione sul Formato è parte dei metadati dei componenti dell'unità documentaria e costituisce un elemento delle Informazioni sulla rappresentazione.

[Torna al sommario](#)

I METADATI

I metadati degli oggetti sottoposti a conservazione sono parte integrante delle specifiche tecniche (allegato al contratto di affidamento del servizio di conservazione).

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

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

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

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

Una prima fonte autorevole di indicazioni sui requisiti dei metadati di un sistema ERMS (Electronic Resource Management System) è fornito dal MoReq² della Commissione Europea al cap. 12.

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

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

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

1. dei documenti (ISAD);
2. delle regole, gli indirizzi, le policies e altri requisiti per la formazione e gestione dei records;
3. dei soggetti produttori (ISAAR);
4. delle attività e processi di lavoro (ISAAR);

² http://ec.europa.eu/archival-policy/moreq/doc/moreq_it.pdf

5. dei processi di "records management" (ISAD).

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

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

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

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

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

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

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

Calando la terminologia OAIS su Legal Archive® possiamo affermare che: il sistema riceve in ingresso un PdV la cui struttura informativa deve essere concordata con il soggetto produttore, ed avrà come fine ultimo la produzione di un PdA che soddisfi i requisiti minimi definiti nell'ambito del progetto per l'archiviazione dei documenti.

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

Il modello OAIS, in virtù delle caratteristiche di generalità sulla cui base è concepito, non definisce uno specifico insieme di metadati, ma un modello, informativo e funzionale, che consente di adottare insiemi di metadati mirati di volta in volta all'ambito di riferimento. D'altro canto, la comunità archivistica ha da tempo raggiunto un accordo su quali debbano essere gli elementi

descrittivi che caratterizzano i complessi documentari, definendo lo standard ISAD (per la descrizione archivistica vera e propria) e ISAAR (per la descrizione del contesto di produzione).

A tali standard di carattere generale si sono nel tempo affiancati due schemi di metadati, EAD³ (Encoded Archival Description) ed EAC⁴ (Encoded Archival Context), che traducono in una codifica XML gli elementi descrittivi necessari a delineare un archivio, nelle sue componenti archivistiche e documentarie, nelle relazioni essenziali interne all'archivio e relative al contesto amministrativo, giuridico, archivistico.

EAD, in particolare, consente di spingere la descrizione gerarchica di un complesso documentario fino a livello del fascicolo archivistico e, ove possibile, collegare ad esso la rappresentazione elettronica dei documenti digitali in esso contenuti. Tali standard possono essere utilizzati come riferimento per rappresentare Content Information e Preservation Description Information del modello OAIS e sono certamente preferibili alla definizione ex novo di insiemi di metadati che comunque dovrebbero garantire la conformità ad ISAD e ISAAR.

Inoltre, per completare il quadro degli standard di riferimento per la caratterizzazione dei metadati dei documenti digitali, è importante fare riferimento a METS⁵ (Metadata Encoding and Transmission Standard) come ad uno schema per la codifica dei metadati necessari alla gestione degli oggetti contenuti in un deposito digitale. La compatibilità di METS con il modello OAIS consente di immaginare il suo utilizzo in tutte le fasi del processo conservativo, e può includere metadati desunti da altri schemi legati a domini specifici, quali ad esempio EAD ed EAC per l'ambito archivistico.

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

In Legal Archive® 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

³ www.loc.gov/ead/

⁴ <http://www3.iath.virginia.edu/eac/>;

http://media.regesta.com/dm_0/regesta/regestacms/generic/documentazione/Barbanti-EADEAC2005.pdf.

⁵ www.loc.gov/standards/mets/

- 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, Legal Archive®, 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:

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

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

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

Elenchiamo di seguito una tabella riepilogativa:

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

[Torna al sommario](#)

6.2 IL PACCHETTO DI VERSAMENTO (PDV)

Si tratta del pacchetto informativo inviato dal soggetto produttore al soggetto conservatore; è oggetto dell'accordo stipulato in occasione del Contratto di affidamento del servizio di conservazione.

In generale il PdV è costituito dall'insieme dei file che sono oggetto di conservazione accompagnati da un file indice contenente i metadati per ricercare i documenti all'interno del sistema.

Il Contratto di affidamento del servizio di conservazione è finalizzato alla definizione di tutte le componenti informative che il sistema di conservazione necessita per creare PdA coerenti e ben strutturati.

Legal Archive® accetta pacchetti di versamento che rispondono alle caratteristiche tecnologiche e informative previste nelle rispettive Specifiche Tecniche, documento allegato al contratto di affidamento.

Legal Archive® supporta PdV nel formato definito nell'allegato 2 delle nuove regole tecniche accompagnati da un indice nel formato txt oppure nel formato CSV in tre varianti:

1. formato CSV normale;
2. formato CSV con indirizzamento di output;
3. formato CSV con offset.

Il sistema di versamento mette a disposizione del 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 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 PdV.

[Torna al sommario](#)

6.3 IL PACCHETTO DI ARCHIVIAZIONE (PdA)

È l'elemento fondamentale del sistema di conservazione, è il pacchetto informativo che racchiude in sé tutti gli elementi sufficienti e necessari per una conservazione a lungo termine.

Il principio su cui si basa l'architettura del modello dati di Legal Archive® è quello di un'assoluta auto-consistenza del pacchetto informativo nel momento in cui è costituito il PdA; tale obiettivo viene raggiunto grazie all'aderenza al modello funzionale e al modello-dati previsto in OAIS.

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

- l'insieme delle informazioni statiche che prevedono un set complesso di metadati che descrivono in maniera "piatta" tutti gli elementi identificativi, descrittivi, gestionali, tecnologici, etc., relativi ad uno e 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.

Quest'ultimo elemento è quello che ci permette di ricostruire il vincolo archivistico e quindi di ricondurre, ad esempio, ad una stessa pratica o ad uno stesso fascicolo tutti i documenti relativi ad un medesimo affare o procedimento amministrativo.

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

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

- b. metadati descrittivi (per esempio possono essere utilizzati i metadati dello standard ISAD);
 - c. metadati gestionali (UNI SinCRO);
 - d. metadati tecnologici (per esempio possono essere utilizzati i metadati dello standard METS);
 - e. Dublin Core Metadata Element Set;
5. il viewer necessario per la visualizzazione del documento stesso o, in alternativa si inserisce il puntatore/riferimento al viewer comune a più pacchetti informativi per quel formato di file del documento;
 6. 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.

Concretamente tali informazioni compongono l'indice di conservazione (d'ora in poi IdC); l'IdC rispetta lo standard UNISinCRO, non contiene un oggetto digitale, nella stretta accezione OAIS, ma diventa un container da conservare. Oltre ai metadati tipici (ad esempio, denominazione del fascicolo, estremi cronologici del fascicolo, riferimenti al procedimento amministrativo associato) esso conterrà due puntatori fondamentali:

- uno o più puntatori agli oggetti digitali contenuti nel fascicolo (un fascicolo può contenere uno o più data object);
- uno o più puntatori alla struttura archivistica di riferimento (quindi alla serie/sottoserie della rappresentazione attuale dell'archivio); in altre parole un fascicolo potrà riferirsi ad una o più serie archivistiche.

In concreto, una volta che i PdV sono stati accettati nel sistema, (e sono quindi stati oggetto di controlli sui metadati previsti dal Contratto di servizio) essi sono pronti ad essere trasformati in PdA e quindi diventare l'oggetto della conservazione a lungo termine.

Qui di seguito si riporta la struttura dell'IdC del PdA:

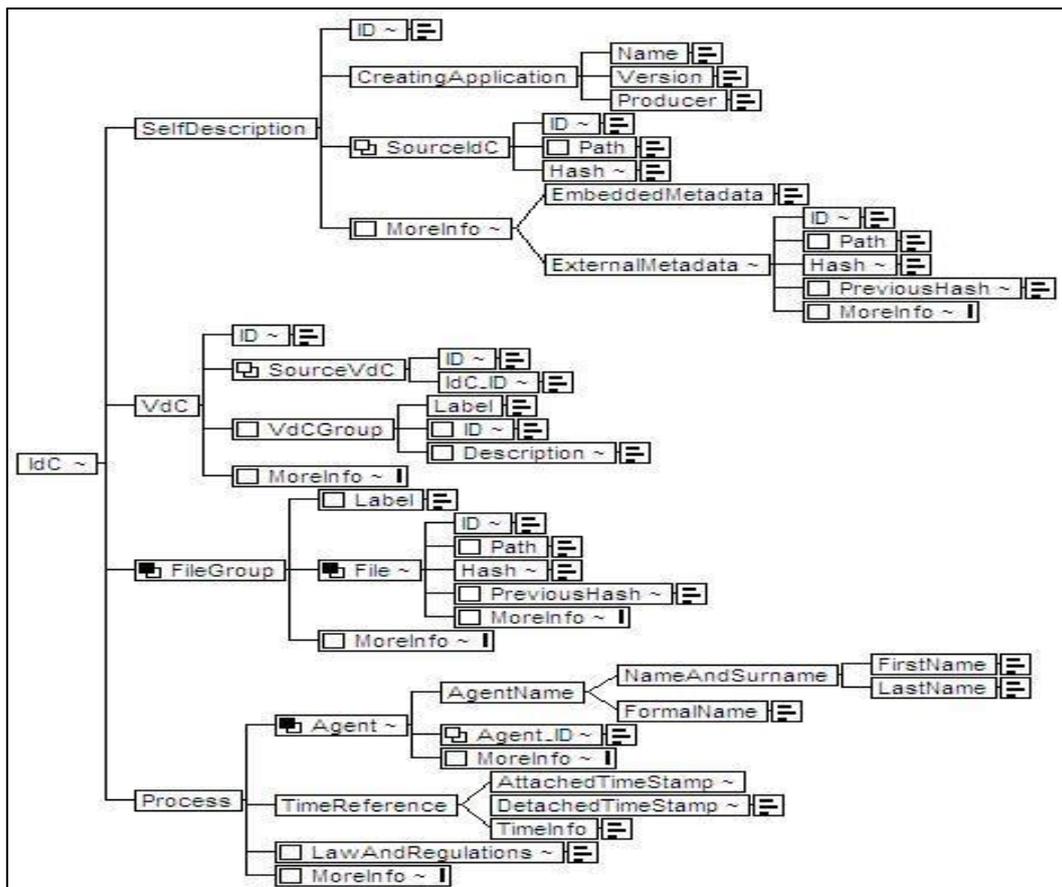


Figura 4: Schema dell'IdC

Il documento informatico, così trattato, sarà arricchito dei metadati previsti nel Contratto di servizio, ma anche di tutti quei metadati tecnologici, relativi al documento stesso e al viewer, necessari per superare l'obsolescenza tecnologica. Il pacchetto, così formato, sarà pronto per essere associato ai volumi di conservazione (VdC) previsti dallo standard SInCRO UNI 11386:2010. Ogni VdC sarà associato ai PdA relativi ad un medesimo fascicolo digitale, le relazioni fra loro e il PdA descrittivo del fascicolo stesso, nonché le relazioni fra il fascicolo e la struttura logica d'archivio. In tale maniera, si ritroveranno collegati allo stesso VdC tutti gli elementi necessari e sufficienti per la corretta interpretazione del singolo PdA.

All'atto della conservazione verrà composto il PdA. Lo schema seguente mostra sinteticamente come sarà costruito il PdA.

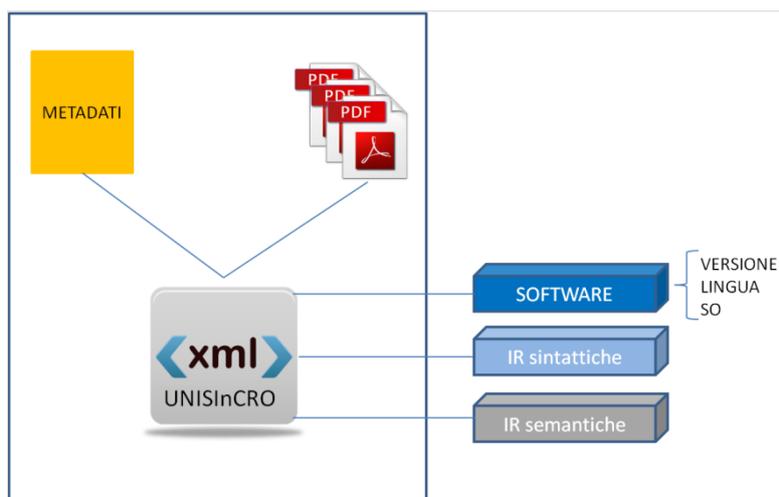


Figura 5 - Schema dell'PdA e dei collegamenti con le informazioni sulla rappresentazione

Ad ogni oggetto versato nel sistema di conservazione verrà associato:

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

[Torna al sommario](#)

6.4 IL PACCHETTO DI DISTRIBUZIONE (PdD)

Per maggiori informazioni si rimanda al manuale operativo Legal Archive® V08 al capitolo 20.

Nel modello OAIS, il pacchetto di distribuzione (PdD) è strutturato nel modello dati come il pacchetto di archiviazione (PdA). La differenza sta nella sua destinazione in quanto esso viene concepito per essere fruito ed utilizzato dall'utente finale (esibizione).

In questo caso, un PdD 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 PdD che sono il frutto di più PdA 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 PdD. 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.

Legal Archive® gestisce un archivio dei software eseguibili ciascuno dei quali utile a visualizzare un determinato formato file cui appartengono i documenti conservati.

I software dell'archivio possono essere associati ad una 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 PdD che nel caso più completo conterrà:

- i documenti richiesti nel formato previsto per la loro visualizzazione

- un'estrazione dei metadati associati ai documenti
- l' IdC firmato e marcato
- i viewer necessari alla visualizzazione dei documenti del pacchetto.

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

[Torna al sommario](#)

7. IL PROCESSO DI CONSERVAZIONE

Il servizio di conservazione è regolato dai seguenti documenti:

- Contratto di affidamento del servizio di conservazione
- Allegato tecnico
- Atto di nomina a Responsabile del servizio di conservazione
- Oggetti digitali sottoposti a conservazione: tale documento è parte integrante dell'allegato tecnico
- Scheda cliente
- Manuale utente Legal Archive

Il processo di conservazione designato ad hoc sulla base delle richieste del soggetto produttore e della tipologia documentaria conservata, in linea con la normativa vigente, è descritto nell'allegato tecnico del contratto.

[Torna al sommario](#)

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

La trasmissione del pacchetto informativo (PdV) dal soggetto produttore al soggetto conservatore viene concordato in fase contrattuale e descritto nelle specifiche tecniche.

Il PdV può essere trasferito dal soggetto produttore al soggetto conservatore tramite:

- SFTP - caricamento via file system
- Web services
- Interfaccia Web
- Pec

Microdata non prevede il trasferimento di PdV tramite mail e supporti rimovibili.

Il sistema di conservazione prevede tre modalità di versamento:

1) Versamento automatico:

con la modalità Web Service l'applicativo chiamante istanzia un processo di conservazione nel sistema durante il quale invia a Legal Archive® pacchetti informativi comprendenti i file e l'insieme dei metadati di ricerca a loro associati.

2) Versamento semiautomatico:

la modalità di versamento via file system prevede che il soggetto produttore trasferisca il PdV tramite SFTP. Il soggetto conservatore prende in carica i documenti trasferiti e, dopo il buon esito delle verifiche concordate, sposta il PdV in una posizione, all'interno del file system, accessibile al sistema di conservazione. Tale posizione deve essere prestabilita e preconfigurata nel setting della descrizione archivistica. A cadenza prestabilita, il software di conservazione fa un polling sulla cartella assegnata prendendo in carico il file indice presente insieme ai file ad esso associati.

In linea generale il file di indice può essere composto secondo le seguenti regole:

- a) Il file deve contenere tante righe quanti sono gli oggetti che costituiscono il PdV.
- b) Ciascuna riga contiene i metadati descrittivi di ciascuno oggetto.
- c) Ciascun metadato è separato dal successivo da un carattere separatore che può essere “|” o “;”.
- d) In ciascuna riga i metadati si susseguono in maniera ordinata: in ciascuna riga lo stesso tipo di dato sarà sempre nella stessa posizione.
- e) La prima colonna è sempre il percorso al file.

Nel caso in cui sia riportato il nome del file senza il percorso, Legal Archive® assume che il file referenziato si trovi sempre nella stessa cartella del file di indice.

Esempio operativo:

Il PdV è costituito da un insieme di n file (Unità Documentarie) tra loro indipendenti accompagnati dal relativo file dei metadati. Tutti gli n file appartengono alla stessa descrizione archivistica. Il file di indice sarà costituito quindi da n righe (1 riga di metadati per ciascun file), ciascuna riga contiene n campi separati tra loro dal carattere “|” contenente il valore di ciascun metadato.

- f) Il carattere “+” ad inizio riga indica al sistema di conservazione che il file descritto è un allegato/annesso al documento referenziato nella riga superiore precedente contenente nome file e metadati.

Esempio operativo:

Il PdV è costituito da un insieme di n file (Unità Documentarie) di cui alcuni sono allegati. Ciascun file principale è accompagnato dai relativi metadati. I file principali appartengono tutti alla stessa descrizione archivistica. Il file di indice avrà quindi n righe per n file. Ciascuna riga relazionata ai file principali contiene n campi separati tra loro dal carattere “|” contenente il valore di ciascun metadato, mentre x righe relionate agli allegati contengono solo path e nome file.

- g) Nel caso di versamento di un fascicolo è indispensabile acquisire i metadati descrittivi dell’aggregazione documentale utili anche a definire la gerarchia dei documenti.

Esempio operativo:

Il PdV contiene fascicoli di documenti diversi ma afferenti allo stesso contesto di provenienza. I diversi oggetti vengono relazionati tra loro in funzione di alcuni metadati che fungono da nessi logici necessari, autonomi e determinati.

3) Versamento manuale

il sistema di conservazione dispone di un’interfaccia di upload attraverso la quale l’utente può versare i documenti direttamente nel sistema di conservazione. In questo caso occorre:

- Selezionare la descrizione archivistica cui si riferiscono i documenti da versare.
- Indicare il percorso file che sarà caricato a sistema attraverso un browsing da file system.
- Imputare manualmente i diversi metadati associati al singolo file.
- Confermare il versamento del pacchetto.

Microdata considera il servizio di conservazione come l'attività conclusiva del ciclo di vita di un documento, per questo motivo può essere prevista un'attività di document management precedente al servizio di conservazione, le cui specifiche non costituiscono oggetto del servizio di conservazione digitale.

[Torna al sommario](#)

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

Il sistema di conservazione prevede controlli sulla composizione del PdV; in particolare verifica la congruità tra l'indice e gli oggetti da conservare sia per quanto attiene al numero dei documenti sia per quanto riguarda la validità dei metadati forniti nonché l'integrità dei documenti.

Nello specifico, sul singolo file sono effettuate le seguenti verifiche:

- il Mime type del documento in elaborazione deve appartenere alla lista dei Mime type per i quali il sistema conserva i viewer;
- il Mime type di un file deve corrispondere a quanto dichiarato;
- la validità della firma (impostabile solo nel caso p7m o pdf);
- la validità della marca temporale (impostabile solo nel caso tsd o p7m);
- nel caso in cui il file dei metadati, prodotto e versato dal SP, includa anche un campo contenente l'hash di ciascun file, il sottosistema di validazione ricalcola l'hash di ogni documento e lo confronta con quello dell'indice verificando l'integrità del file versato.

Le validazioni sono concordate con il soggetto produttore nell'allegato tecnico. Le validazioni vengono configurate per ciascuna descrizione archivistica.

Il sistema, superate le validazioni dei documenti del PdV, restituisce al SP il rapporto di versamento che rimane a disposizione anche direttamente nel sistema di conservazione.

[Torna al sommario](#)

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

Per attestare l'avvenuta acquisizione e presa in carico del PdV, per ogni pacchetto accettato il sistema genera un rapporto di versamento che viene memorizzato nel database e associato logicamente al PdA cui si riferisce.

Il rapporto di versamento contiene:

- l'Identificativo univoco del rapporto di versamento, 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.

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:

- può essere trasmesso via SFTP;
- 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.

[Torna al sommario](#)

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

Il rifiuto del PdV rappresenta un'anomalia del sistema di conservazione; per la sua gestione si rimanda al paragrafo 9.3 Gestione delle Anomalie.

La gestione delle anomalie costituisce comunque oggetto di specifici accordi descritti nell'allegato tecnico al contratto di affidamento del servizio.

[Torna al sommario](#)

7.5 PREPARAZIONE E GESTIONE DEL PACCHETTO DI ARCHIVIAZIONE

I PdV che superano le verifiche descritte nel paragrafo precedente sono trasformati in PdA.

I PdA contengono i documenti collegati alle informazioni sulla rappresentazione ad esse associate e i viewer necessari al fine di rendere possibile la ricostruzione dell'archivio e le funzioni di ricerca.

Un PdA viene salvato nella risorsa Archivio configurata a sistema.

Le informazioni di conservazione sono salvate nel file system, in una sottocartella della directory indicata come radice nel pannello di configurazione dell'Archivio.

Il PdA è salvato in una posizione associata a:

- soggetto produttore
- anno
- ID volume di conservazione

Il PdA contiene:

- Indice_<N° del pacchetto>.xml: file xml con la descrizione del PdA.
- Tutti i file XML e XSD necessari per l'eventuale ricostruzione dell'archivio.

[Torna al sommario](#)

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

L'esibizione è un atto da svolgersi in ottemperanza di quanto previsto dall'ultimo comma dell'art. 2220 del Codice Civile, ribadito nell'art. 10 del DPCM del 3 dicembre 2013. Essa consiste nel rendere leggibili con mezzi e strumenti idonei tutte le scritture e i documenti conservati. L'art. 10 del DPCM del 3 dicembre 2013 ribadisce le norme vigenti e specifica che ai fini dell'esibizione il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, al documento informatico conservato, attraverso la produzione di un PdD selettiva secondo le modalità descritte nel manuale di conservazione.

Dalla norma ne deriva che, in un momento successivo alla generazione dei PdA, utenti autorizzati dal soggetto produttore possono accedere al sistema di conservazione e interrogarlo per ottenere pacchetti di distribuzione configurati in diversi modi:

- PdD coincidente con il PdA, che contiene:
 - tutti gli elementi presenti nel PdA;
 - i documenti del PdA richiesto;
 - un'estrazione delle informazioni di conservazione dei documenti e dei fascicoli;
 - l'IdC firmato e marcato e le informazioni sulla conservazione associate ai fascicoli;
 - i viewer necessari alla visualizzazione dei documenti del pacchetto e le informazioni sulla rappresentazione;
 - le informazioni sull'impacchettamento e le informazioni descrittive associate al pacchetto informativo.
- PdD dell'unità documentaria che contiene gli oggetti che la compongono e i dati relativi.

In linea generale il PdD può essere erogato dal sistema di conservazione come unico file in formato ZIP e in formato ISO a seconda della richiesta dell'utente.

Va sottolineato che l'esibizione degli oggetti digitali conservati deve avvenire in modo che le autorità competenti possano verificare la coerenza della firma digitale e della marca temporale apposte durante il processo di conservazione. Tale procedura, non potendo essere effettuata stampando l'evidenza firmata della conservazione, deve necessariamente prevedere un supporto informatico.

[Torna al sommario](#)

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

In fase di attivazione del servizio, il soggetto produttore segnala al soggetto conservatore, su apposita documentazione allegata al contratto, gli utenti designati alla visualizzazione e al download dei documenti informatici originali ai fini dell'esibizione.

Gli utenti possono consultare i documenti informatici versati nel sistema di conservazione tramite interfaccia web, utilizzando le credenziali di accesso inviate dal soggetto conservatore tramite e-mail. L'accesso web permette all'utente di ricercare e visualizzare i documenti informatici originali conservati, scaricare i documenti informatici conservati (duplicati) e i file di evidenza della conservazione, richiedere e consegnare il PdD alle autorità competenti e in caso di necessità produrre eventualmente una copia conforme richiedendo la presenza di un pubblico ufficiale. Si

sottolinea che, il PdD scaricato risulta completo di IdC e delle relative informazioni sulla rappresentazione. Inoltre, nel PdD è contenuta tutta la catena di documentazione necessaria a rispondere alle esigenze dello standard OAIS, nonché le informazioni sul sistema operativo in grado di supportare l'applicazione.

Il titolare dell'utenza è responsabile dell'utilizzo della stessa.

Sul soggetto produttore permane l'onere di valutare la fondatezza giuridica della domanda di accesso, di far pervenire il documento (o sua eventuale copia cartacea conforme) al soggetto richiedente la consultazione e di comunicare al soggetto conservatore l'eventuale revoca o modifica dei diritti di accesso.

[Torna al sommario](#)

PRODUZIONE DI COPIE E DUPLICATI

Non è previsto da parte del soggetto conservatore il rilascio di copie cartacee conformi agli originali digitali conservati. Sarà cura del soggetto produttore produrre le copie conformi e richiedere, quando necessario, la presenza di un pubblico ufficiale.

[Torna al sommario](#)

PUBBLICO UFFICIALE

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

[Torna al sommario](#)

7.8 SCARTO DEI PACCHETTI DI ARCHIVIAZIONE

L'art. 9 comma 2, lett. K del DPCM 3 dicembre 2013 stabilisce che deve essere effettuato lo scarto dal sistema di conservazione, alla scadenza dei termini di conservazione previsti dalla norma, dandone informativa al soggetto produttore. Il sistema di gestione dati, grazie alla propria concezione, permette di gestire lo scarto del materiale documentario non destinato alla conservazione permanente, ma caratterizzato invece da tempi di conservazione limitati e diversificati. Negli archivi correnti gestiti secondo criteri aggiornati è presente, nel piano di classificazione e conservazione, un metadato, definibile per ciascuna tipologia di documento o fascicolo (descrizione archivistica), che stabilisce i tempi di conservazione. Sarà dunque il sistema di gestione dati (SGD) ad incaricarsi di avvisare il Responsabile del servizio di conservazione attraverso una o più notifiche impostabili, circa la scadenza dei tempi di conservazione dei documenti, a supportarlo nell'effettuazione materiale dello scarto, e a mantenere al proprio interno, ove richiesto, i metadati della documentazione fisicamente scartata.

Il sistema di conservazione produrrà quotidianamente un **elenco** dei pacchetti di archiviazione che hanno superato il tempo di conservazione, così come definito dal massimario di selezione e scarto. Tale elenco di scarto, dopo una verifica da parte di Microdata, viene comunicato al soggetto produttore che, utilizzando apposite funzionalità del sistema, può rifiutarlo (perché non intende procedere allo scarto) o validarlo.

Nei casi previsti dalla legge, l'elenco di scarto così validato viene trasmesso dal soggetto produttore all'Autorità di vigilanza o all'organismo di tutela che, in base alle norme vigenti, deve fornire il nulla-osta per lo scarto. Il soggetto produttore, una volta ricevuto il nulla-osta (che può essere concesso anche solo su una parte dell'elenco proposto), provvede ad adeguare, se necessario, l'elenco di scarto presente sul sistema alle decisioni dell'Autorità. Una volta che l'elenco di scarto definitivo viene predisposto, il soggetto produttore lo valida e trasmette a Microdata la richiesta di procedere allo scarto. Solo dopo aver ricevuto l'autorizzazione il conservatore provvederà alla cancellazione dei pacchetti di archiviazione contenuti nell'elenco di scarto.

Il sistema di conservazione è quindi dotato di un processo di scarto che si occupa di controllare quotidianamente se esistono pacchetti di archiviazione che devono essere scartati. Alla presenza di uno o più pacchetti, il processo avvisa il soggetto conservatore che avrà a disposizione una interfaccia che gli permetterà di decidere se scartare o meno i documenti. In caso affermativo, il processo di selezione e scarto provvederà ad eliminare fisicamente i file presenti nel file system e a cancellare tutti i riferimenti nel database, mantenendo però l'IdC (in quanto contiene la lista dei file scartati) e aggiungendo automaticamente ai metadati dei PdA una nota che indichi il fatto che i PdA sono stati sottoposti a scarto, includendo data e ora di esecuzione.

[Torna al sommario](#)

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

Per una corretta erogazione di un servizio di conservazione a norma che risponda alle caratteristiche richieste dallo standard OAIS, una qualsiasi applicazione di conservazione deve essere in grado di esportare i documenti informatici conservati in un formato che garantisca l'integrità della conservazione stessa.

L'applicazione Legal Archive® essendo progettata secondo lo standard OAIS è in grado di esportare i singoli pacchetti di archiviazione generati durante gli anni, seguendo le regole che permettono successivamente di importare i pacchetti in un altro sistema OAIS compliant.

L'esportazione dei PdA può essere effettuata su supporto elettronico in formato ZIP oppure in formato ISO. Tali file saranno messi a disposizione del cliente su server SFTP oppure memorizzati su supporto fisico e consegnati da personale autorizzato Microdata. Per rispondere ai requisiti richiesti dalla norma ISO27001, in quest'ultimo caso i file memorizzati su supporto fisico trasportabile saranno criptati.

[Torna al sommario](#)

7.10 CESSAZIONE DELL'ATTIVITÀ DI CONSERVAZIONE

Nel caso in cui Microdata Service Srl decidesse di cessare le proprie attività di conservazione a norma, la stessa è tenuta a comunicarlo ad AgID a mezzo PEC, almeno **sessanta giorni**⁶ prima della cessazione. Allo stesso modo procederà a comunicare ai suoi Clienti, a mezzo PEC

- la data di cessazione del servizio di conservazione,
- la procedura di recupero degli archivi,
- l'intervallo di tempo disponibile per il recupero dei dati come specificato all'interno del contratto.

Una volta consegnati tutti i PdD e decorsi i tempi stabiliti all'interno del contratto per l'attività di validazione da parte del Cliente, Microdata Service Srl è liberata dall'obbligo di conservazione nonché dagli obblighi derivanti dall'art. 7 comma 1 del DPCM 03/12/2013.

Al termine delle operazioni di restituzione i dati saranno rimossi.

[Torna al sommario](#)

⁶ art. 37 del d.lgs. n. 82/2005 Codice dell'Amministrazione Digitale

8. IL SISTEMA DI CONSERVAZIONE

Tutte le procedure operative sono ampiamente descritte nel manuale operativo Legal Archive.

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

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

L'intera soluzione è stata progettata per essere in grado di gestire l'elaborazione di grandi volumi di dati. A tale scopo, Legal Archive® può essere scalato sia verticalmente che orizzontalmente e le singole componenti possono essere distribuite su più server. La compatibilità con la virtualizzazione e il cloud computing è garantita previa raggiungibilità dei certificati di firma.

Di seguito riportiamo in Figura 6 uno schema in rappresentazione delle componenti del sistema di conservazione che possono essere installate su server distinti.



Figura 6: Componenti scalabili del sistema

Le modalità di interazione possibili tra Microdata e i Clienti sono:

- Invio e ricezione Flussi dati via FTP-SFTP-FTPS (Flat file, XML, AFP) o attraverso l'utilizzo di software dedicati;
- Invio, ricezione ed elaborazione di documenti e file via Web Services, di e-mail ed allegati (standard e PEC) o fax, upload e lavorazione di documenti via Web;
- Consultazione Web via browser con connettività attraverso Rete internet ad accesso pubblico, con limitazione degli indirizzi sorgenti, attraverso VPN su Internet o linee dedicate.

[Torna al sommario](#)

8.1 COMPONENTI LOGICHE

IL MODELLO DATI OAIS IN LEGAL ARCHIVE®

Il modello dei dati che viene utilizzato come base per l'implementazione del software di conservazione Legal Archive® è lo standard ISO 14721: OAIS Open Archival Information System, esplicitato nella gestione di tre differenti tipologie di pacchetti informativi (Figura 7):

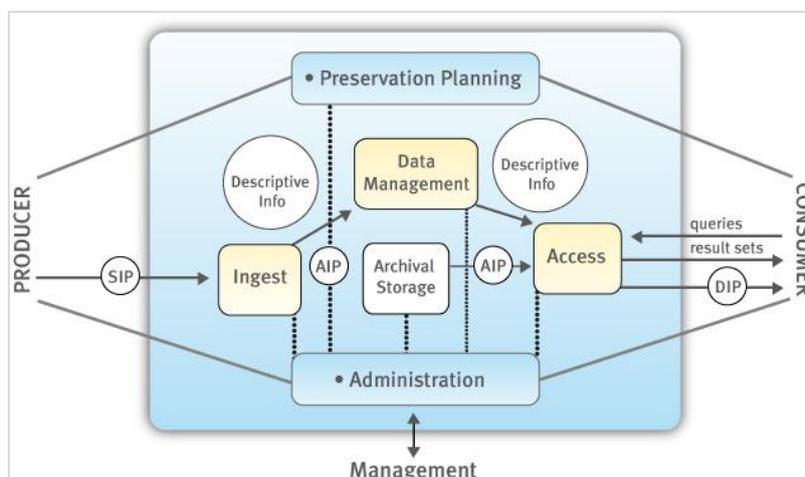


Figura 7: Il modello OAIS

- PdV: il documento digitale o l'insieme dei documenti digitali, corredati da tutti i metadati descrittivi, versati dal soggetto produttore nel sistema di conservazione.
- PdA: uno o più PdV sono trasformati in PdA per la conservazione. Il PdA ha un insieme completo di informazioni sulla conservazione che si aggiungono al file di metadati.
- PdD: il documento digitale o l'insieme dei documenti digitali, corredati da tutti o da parte dei metadati previsti nel PdA, finalizzati alla presentazione e distribuzione dei documenti informatici originali conservati a norma.

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 Legal Archive® prevede una strettissima aderenza a tale modello concettuale rivisitandolo ed ampliandolo con elementi di contestualizzazione provenienti dalla tradizione archivistica italiana.

Inoltre, l'obiettivo del sistema di conservazione è quello di garantire non solo la gestione e la conservazione dell'insieme informativo e descrittivo del singolo documento (o collezione di documenti, nell'accezione OAIS, in riferimento a AIC, Archival Information Collection), ma anche di tutte le informazioni di contesto dei metadati e, soprattutto, delle relazioni fra i documenti che servono per la ricostruzione del vincolo archivistico e, quindi, del fascicolo digitale di riferimento.

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

Nel rispetto dello standard OAIS, il sistema è formato da 4 macro-componenti funzionali (Figura 8):

1. sistema di versamento (SV).
2. sistema di gestione dati (SGD).
3. sistema di memorizzazione (SM).
4. sistema di autenticazione e accesso (SAA).

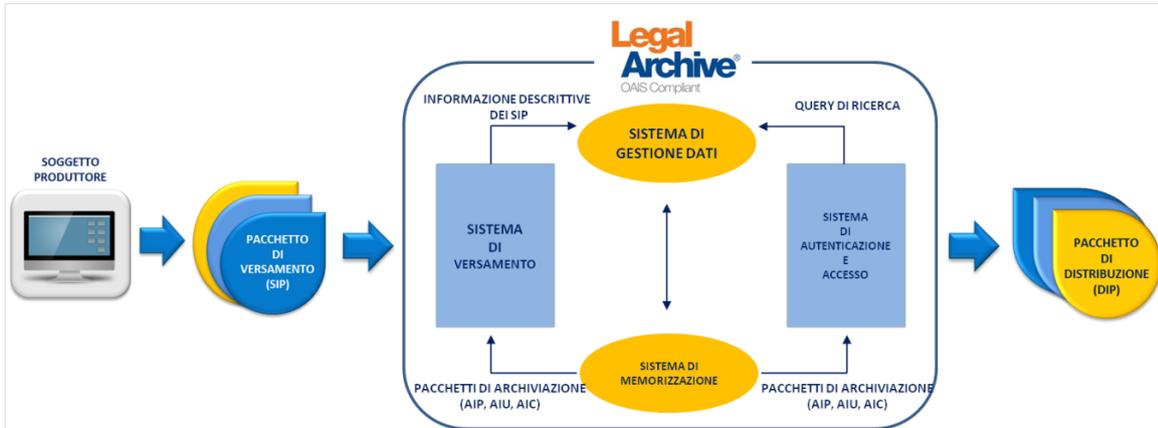


Figura 8: Il Sistema di Conservazione

Legal Archive® ha come obiettivo quello di interpretare nel modo più fedele possibile il modello OAIS traducendolo in un sistema reale. Nella Figura 9 si mostra come Legal Archive® aderisca al modello OAIS; da 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).

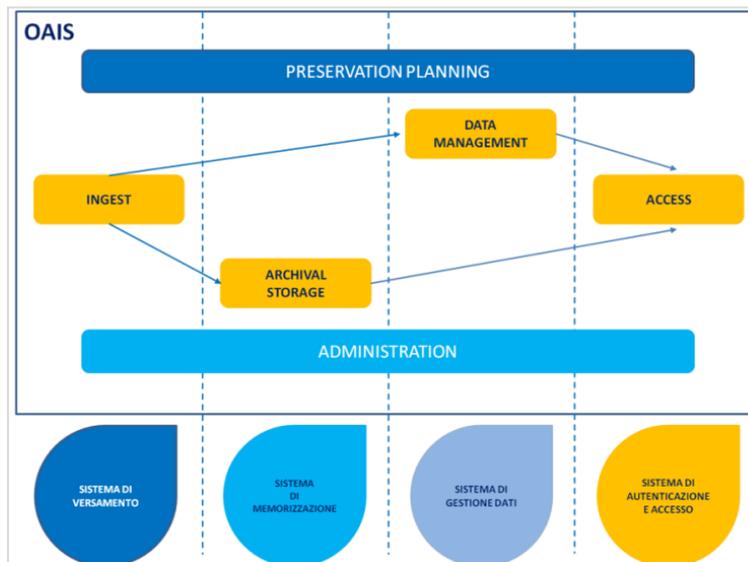


Figura 9: L'adesione allo standard OAIS

[Torna al sommario](#)

SISTEMA DI VERSAMENTO (SV)

Il sistema di versamento è la porta di ingresso dell'intero sistema e ha il compito di ricevere i Pacchetti di versamento da parte dei soggetti produttori, di verificarne l'aderenza al contratto di servizio e ai requisiti di conservazione, di preparare i pacchetti di archiviazione ed infine di inviare

ai sistemi opportuni le informazioni e i dati per garantire la conservazione a norma dei documenti ricevuti.

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

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

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

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

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

Le caratteristiche tecnologiche riguardano esclusivamente i documenti digitali e possono riferirsi al formato con cui sono stati prodotti, alla validità della firma, e/o della marca temporale. Poiché i documenti digitali potrebbero giungere al sistema dopo un considerevole lasso di tempo dalla loro formazione, a causa dei tempi di chiusura delle relative pratiche, è quanto mai opportuno che il sistema si incarichi di verificare la sussistenza dei requisiti di base per la conservazione.

Una volta che la documentazione avrà superato i controlli di qualità previsti, il sistema di versamento dovrà applicare le regole previste dal preservation planning per costruire i PdA a partire dai PdV inviati dal soggetto produttore.

Innanzitutto, viene generata la cosiddetta "Descrizione del pacchetto" che consiste in una serie di informazioni descrittive (descrizioni associate) che consentirà l'accesso al documento 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 PdD differenti a seconda delle necessità dell'utente.

Sui documenti versati nel sistema di conservazione è possibile quindi avviare un'attività di validazione sia dei file che dei metadati rispetto alle regole ed agli standard previsti dalle descrizioni archivistiche di appartenenza. I risultati della convalida possono essere allegati al documento oggetto della convalida per essere eventualmente portati in conservazione insieme al documento. Il processo di convalida include:

- la verifica dell'integrità del documento memorizzato sul supporto rispetto all'impronta associata allo stesso;
- la verifica che il formato del contenuto binario sia coerente con quanto dichiarato nei suoi metadati; diversamente 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 online;
- l’eventuale verifica della presenza in archivio di un documento identico (i.e.: stessa impronta e/o metadati).
- compilazione metadati: alcuni metadati potrebbero essere compilati in questa fase in maniera automatica (ad esempio potrebbero essere aggiunte le informazioni relative all'utente che ha effettuato il versamento e la data di versamento).

Il risultato della convalida è riepilogato da un esito in formato XML (rapporto di versamento) che può essere positivo o negativo. I documenti, per i quali l’esito della convalida è risultato positivo, possono quindi essere associati ad un volume di conservazione.

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

Un aspetto importante da sottolineare è che la fase relativa alla preparazione del PdV e il seguente invio al sistema di conservazione può avvenire in molti modi essendo dipendente fortemente dalla situazione specifica del soggetto produttore; pertanto Legal Archive® dispone di 3 modi per sottoporre un PdV:

1. via web service;
2. via file system;
3. via interfaccia web attraverso una operazione manuale di upload dei documenti.

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

Una volta che i PdV sono stati acquisiti, questi vengono trasformati in pacchetti di archiviazione (AIP) e memorizzati nel sistema di memorizzazione; nella fase di generazione dei PdA vengono anche estratte le informazioni descrittive, necessarie al funzionamento del sistema di gestione dati, a cui sono inviate anche tutte le informazioni di contesto eventualmente fornite o messe a disposizione dal soggetto produttore.

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

Le operazioni di accesso sono effettuate tramite l'apposito sistema, che grazie ai servizi messi a disposizione dal sistema di gestione dati e dal sistema di memorizzazione è in grado di consentire agli utenti abilitati di ricercare con varie modalità la documentazione conservata.

[Torna al sommario](#)

SISTEMA DI GESTIONE DATI (SGD)

Completata l'architettura, il sistema di gestione dati ha il compito di gestire le informazioni legate al contesto archivistico e alle descrizioni dei documenti; questa macro-componente è in pratica

l'elemento di coesione dell'intero sistema. Il sistema di gestione dati è il cuore archivistico del sistema ed è la componente che consente di avere una visione unitaria dell'archivio e quindi di accedervi. Il sistema di gestione dati ha una duplice valenza: da una parte offre servizi al sistema di accesso per consentire le ricerche e la navigazione e, dall'altra, consente all'ente produttore di gestire il proprio deposito digitale secondo canoni archivistici, offrendo funzionalità come la descrizione e il riordino, la selezione e lo scarto, la ricollocazione del materiale non digitale, ecc. Il sistema di gestione dati rappresenta il collante archivistico dell'intero sistema di conservazione e per questo lo riteniamo componente essenziale per consentire ad un soggetto produttore di gestire al meglio il proprio deposito digitale.

Attraverso questo modulo il soggetto produttore potrà vedere l'archivio come il complesso sistema di relazioni che in effetti è e, tramite le funzionalità che esso offre, potrà compiere tutte quelle operazioni tipicamente archivistiche, necessarie per la gestione di un archivio (di deposito). Per esempio, il sistema di gestione dati, grazie alla propria particolare concezione, permette di gestire al meglio lo scarto del materiale documentario non destinato alla conservazione permanente, ma caratterizzato invece da tempi di conservazione limitati e diversificati.

Per la corretta formazione della struttura di archivio, Microdata acquisisce gli strumenti archivistici del soggetto produttore (Titolario o Piano di classificazione, Piano di conservazione, ecc.). L'aggiornamento del piano di conservazione memorizzato in Legal Archive® può essere demandato ad utenti dell'ente produttore.

[Torna al sommario](#)

SISTEMA DI MEMORIZZAZIONE (SM)

Il sistema di memorizzazione ha lo scopo di gestire in modo semplice e sicuro la conservazione a lungo termine dei documenti informatici, integrando una serie di servizi specifici di monitoraggio dello stato fisico e logico dell'archivio ed effettuando, per ogni documento conservato, una continua verifica di caratteristiche come la leggibilità, l'integrità, il valore legale, l'obsolescenza del formato e la possibilità di applicare la procedura di scarto d'archivio.

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

Il sistema di memorizzazione in primo luogo acquisisce quanto inviato dal sistema di versamento durante la fase di versamento e, verificandone preventivamente l'affidabilità, provvederà a gestirne lo storage. Sui documenti conservati verranno applicate opportune politiche di gestione atte a garantire non solo la catena ininterrotta della custodia dei documenti, ma anche la piena tracciabilità delle azioni conservative finalizzate a garantire nel tempo la salvaguardia della fonte.

[Torna al sommario](#)

SISTEMA DI ACCESSO

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

A seguito di una ricerca impostata dall'utente il modulo di Gestione Accesso richiede i risultati della ricerca al sistema di gestione dati che, organizzando le informazioni descrittive dei PdA, è in grado di rispondere alla richiesta; l'utente, una volta individuato il documento desiderato (o i documenti, o addirittura un intero fascicolo o un pacchetto di conservazione) potrà inoltrare una richiesta di accesso ai dati; questa inoltrerà la richiesta al modulo di generazione PdD il quale, interagendo sia con il sistema di gestione dati che con il sistema di memorizzazione, recupererà le informazioni necessarie (PdA e informazioni descrittive) per produrre il PdD corrispondente alla richiesta.

Inoltre, Legal Archive® consente anche ricerche trasversali tra tipologie documentarie differenti. Le funzionalità di ricerca saranno implementate dal sistema di gestione dati, mentre il sistema di accesso fornirà le interfacce per l'interrogazione e per la ricezione e visualizzazione dei risultati. Le modalità 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 da Legal Archive® è regolato 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. In Legal Archive® è possibile definire un numero illimitato di ruoli attraverso la definizione di profili d'uso.

I singoli permessi (capabilities) sono assegnabili ad un gruppo tramite la definizione di "Profilo d'uso". Grazie ai "profili d'uso", definibili autonomamente dall'amministratore dell'applicazione, ogni utente potrà accedere ad uno o più Soggetti Produttori e avere visibilità su uno o più descrizioni archivistiche; è inoltre possibile assegnare visualizzazioni di singoli pulsanti e/o menù.

[Torna al sommario](#)

COMPONENTE PER LA FIRMA DIGITALE

Il sottosistema per la firma digitale nel contesto della conservazione digitale si configura come elemento fondamentale per consentire di attuare la conservazione a norma dei documenti di un preciso flusso di lavoro. Il processo essenziale per completare la procedura consiste nella firma dell'IdC (UNI 11386) del volume, nonché nell'apposizione di una marca temporale su tale file.

Essendo presenti diversi dispositivi in grado di fornire queste funzionalità, l'architettura del sistema di conservazione prevede di demandare ad un apposito sottosistema il compito di interfacciarsi con essi. Ciò consente al sistema di memorizzazione di Legal Archive® 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 Legal Archive® 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.

Microdata ha scelto di utilizzare due dispositivi di firma HSM.

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

[Torna al sommario](#)

COMPONENTE PER LA MARCA TEMPORALE

La marca temporale consiste in un'ulteriore firma digitale apposta da un soggetto esterno, Time Stamping Authority (TSA), il quale registra e memorizza, presso la propria struttura organizzativa, l'impronta del file e la relativa data di firma. In questo caso il soggetto esterno non è, dunque, una persona fisica, ma un Ente certificatore.

In linea di massima le TSA coincidono con le Certification Authorities. Questo servizio è offerto online utilizzando protocolli di comunicazione standard.

Il sistema è in grado di richiedere in modo automatico ed online la marca temporale alle TSA utilizzate nel sistema.

[Torna al sommario](#)

CERTIFICATORE ACCREDITATO UTILIZZATO

Per i servizi di firma digitale e marca temporale il soggetto conservatore si avvale di ACTALIS.

PROCEDURE PER LA CONTINUITÀ OPERATIVA

In conformità ai requisiti della certificazione ISO 27001:2005 conseguita nel 2013, e aggiornata nel 2015 alla 27001:2013. Microdata ha elaborato procedure di Business Continuity e Disaster Recovery volte a garantire la continuità operativa in risposta alla valutazione dei rischi per la sicurezza delle informazioni caratteristica per le proprie attività.

[Torna al sommario](#)

8.2 COMPONENTI FISICHE E TECNOLOGICHE

Il seguente paragrafo ha l'obiettivo di descrivere le infrastrutture dati, la struttura dei server, gli ambienti operativi e di test che concorrono a determinare il sistema di conservazione di Microdata.

INFRASTRUTTURE DATI

Le infrastrutture dati sono basate su macchine HP con contratti di manutenzione 24x7x4 gestiti direttamente dalle case madri.

Le infrastrutture dati di produzione sono installate su un sistema iperconvergente con nodi in ognuna delle sedi operative, primaria e secondaria, sincronizzate in tempo reale su rete GBE privata composta da 2 collegamenti su percorsi diversi, ciascuno a 10 Gbit/s.

L'infrastruttura virtualizzata è realizzata con sistema VMWare VSphere Enterprise 6.0.

Entrambe le sedi Operative di Microdata sono attive per una parte delle lavorazioni ed erogazione di servizi ai clienti.

[Torna al sommario](#)

SERVER

I singoli Server sono configurati con sistema operativo Microsoft Windows 2008 R2 e Web Server IIS 7, il database è MS SQL 2012.

Nell'ambiente virtualizzato con VMWare i server hanno dimensioni e caratteristiche (CPU), memoria e spazio disco modificabili a seconda delle necessità senza dare interruzioni di servizio.

[Torna al sommario](#)

AMBIENTI OPERATIVI, PRODUZIONE E DR

L'infrastruttura dati iperconvergenti consente il mantenimento in entrambe le sedi di tutti i dati e sistemi necessari alla conservazione, con una sincronizzazione in tempo reale, che di fatto permette di superare il concetto di Disaster Recovery.

In caso di necessità, l'infrastruttura dati nella sede rimasta operativa si attiva in modo automatico con l'aggiornamento dei sistemi in tempo reale fino al momento in cui la sede da sostituire è rimasta attiva, realizzando di fatto un RPO (*Recovery Point Objective*) pari a Zero ed un RTO (*Recovery Time Objective*) reale inferiore a 10 minuti.

A ulteriore garanzia della continuità operativa, dal punto di vista dell'utente finale non sono necessarie operazioni o modifiche di comportamento, il sistema di conservazione è sempre

raggiungibile allo stesso indirizzo indipendentemente dal fatto che sia attiva la sede principale o quella secondaria, ciò perché Microdata è un Autonomous System (AS 48382) univocamente identificato in internet con propri indirizzi, raggiungibile attraverso provider di connettività ridondati e AS diversi.

Per ogni cliente o servizio sono implementate una DMZ Web e DMZ Server su VLAN e interfacce fisiche dei firewall diverse.

Sui singoli server vengono installati un Antivirus e, a richiesta, un firewall Software.

[Torna al sommario](#)

SVILUPPO E TEST

Gli ambienti di sviluppo e test sono realizzati su una infrastruttura dati dedicata e sono collegati su DMZ e VLAN riservate.

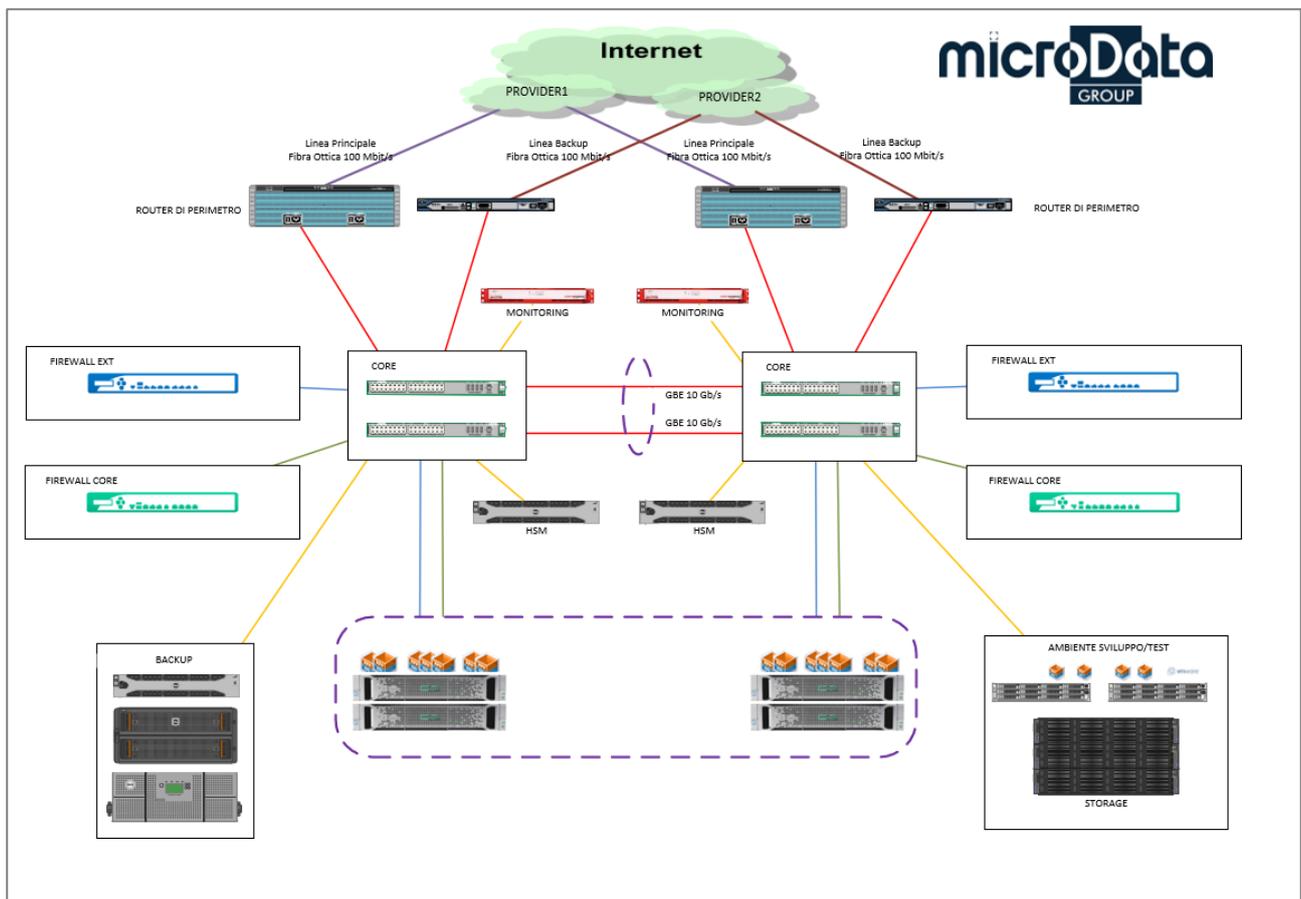


Figura 10: Schema di rete di Microdata

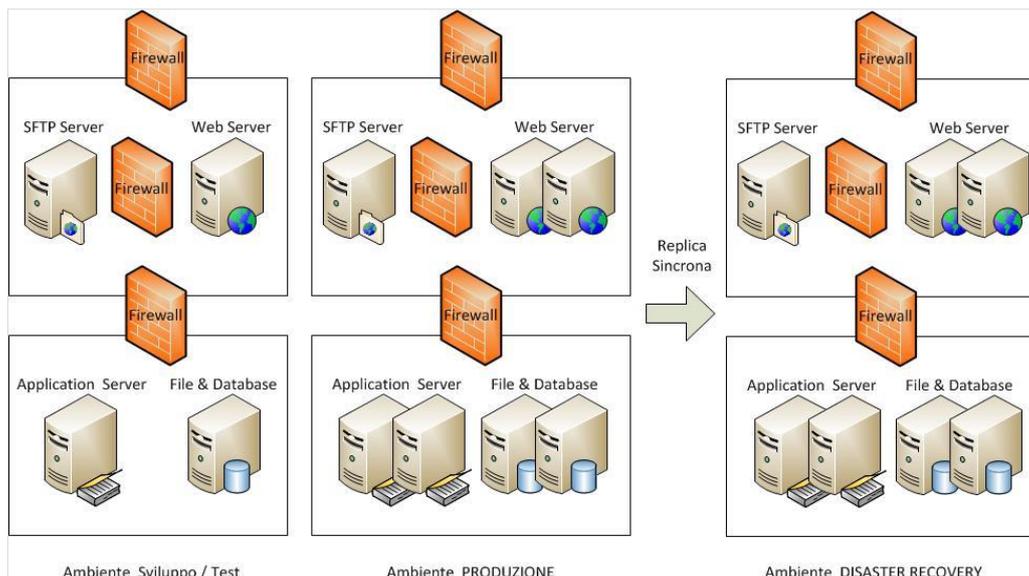


Figura 11: Schema di connessione tra le componenti del sistema

[Torna al sommario](#)

COMPONENTE LEGAL ARCHIVE®

L'architettura di Legal Archive® è basata su una soluzione multi-tier a 3 livelli:

- Presentation layer;
- Business logic (o application) layer;
- Database layer.

L'estrema elasticità di Legal Archive® 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. È 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 una larga parte degli attuali browser senza la necessità di installare ulteriori plug-in sul client. Di seguito la lista dei browser dichiarati compatibili:
 - ✓ Android 2.3 o superiore.
 - ✓ Google Chrome 23 o superiore.
 - ✓ Internet Explorer 8 o superiore.
 - ✓ iOS 5 o superiore.
 - ✓ Mozilla Firefox 17 o superiore.

- ✓ Opera 12 o superiore.
- ✓ Safari 6 o superiore.

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

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

In un'ottica di installazione su ambienti virtuali, Legal Archive® 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](#)

SCALABILITÀ SUI VOLUMI

La conservazione dei documenti, rispetto ai volumi, è soggetta 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 Legal Archive® è stato sviluppato per essere indipendente dal sistema hardware che conserva i file. Oltre ad essere svincolato dal sistema hardware, il software è in grado di distribuire i documenti da conservare su più storage in funzione di criteri che dipendono dalla tipologia documentaria o dalla disponibilità di risorse. Per questo motivo, al crescere dei volumi, è possibile affiancare agli esistenti altri storage con caratteristiche tecnologiche anche differenti rispetto ai presenti.

[Torna al sommario](#)

SCALABILITÀ SUGLI UTENTI

Il sistema di conservazione è stato progettato per supportare numeri elevati di utenti che vi accedono per consultare documenti in esso conservati. In ogni caso, trattandosi di un applicativo sviluppato a tre livelli ed impiegando le più moderne tecnologie di implementazione software, è possibile far crescere la componente Interfaccia Web in funzione del numero di utenti. Anche la componente database è assolutamente scalabile in funzione del numero di utenti.

Riepilogando:

- La necessità di maggiore capacità elaborativa implica l'aggiunta di application server e/o core e RAM;
- La 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;

- La necessità di archiviare un maggior volume di dati implica l'aggiunta di nuovi nodi nell'infrastruttura;
- Alla saturazione di uno storage se ne aggiunge un altro;
- La necessità di maggiore banda fra il sito principale e il sito di disaster recovery: la presenza di accessi in Fibra Ottica ed il collegamento in fibra ottica ad uso esclusivo tra le due sedi operative di Microdata consente di ampliare agevolmente la banda disponibile per il collegamento.

[Torna al sommario](#)

COMPONENTE DATABASE

Il database utilizzato per la soluzione Legal Archive è SQL 2012, completamente dedicato ed installato su un server virtuale le cui caratteristiche e funzionalità sono sotto monitoraggio costante e le cui risorse (CPU, memoria e spazio disco) sono modificabili a seconda delle necessità in tempo reale e senza dare interruzioni di servizio.

[Torna al sommario](#)

COMPONENTE STORAGE

L'infrastruttura Dati è una Federazione di nodi iperconvergenti Simplivity realizzata su hardware DELL. La Federazione di nodi replica i dati e realizza il suo funzionamento grazie al collegamento in fibra ottica ad uso esclusivo tra le due sedi operative di Microdata e garantisce in caso di guasti o disaster recovery un RTO reale inferiore a 10 minuti (è comunque dichiarato un RTO di 4 h per situazioni di disastro) ed un RPO ZERO

[Torna al sommario](#)

ALTRE COMPONENTI

Networking pubblico

Microdata è un Autonomous System con indirizzamento pubblico internet dedicato.

L'infrastruttura di Rete prevede per ognuna delle sedi un accesso a internet in Fibra ottica Gigabit Ethernet con banda di 100Mbit/s attraverso un provider e su backup in fibra attraverso un provider diverso gestito con protocollo BGP (Border Gateway Protocol).

Networking Microdata

Tra i Data Center la connettività è garantita da Fibre ottiche 10 Gigabit Ethernet e Fibre Channel ad uso esclusivo e da VPN su rete pubblica per ridondanza per la connettività delle reti Microdata.

Backup

I Sistemi di Backup sono realizzati nella modalità Disk To Disk To Tape direttamente dall'infrastruttura dati.

Ogni ora viene effettuato un backup incrementale attraverso uno snapshot dei sistemi, quotidianamente viene effettuato un backup su disco, settimanalmente viene invece effettuato un backup full. I dati sono scritti su server esterni dedicati al backup.

In seguito alla scrittura su disco, i dati sono trasferiti su nastro.

8.3 PROCEDURE DI GESTIONE E DI EVOLUZIONE

Il sistema è progettato e realizzato in maniera da fornire un'elevata continuità di servizio, garantire l'Integrità degli oggetti conservati, gestire grandi volumi di dati, mantenere performance stabili indipendentemente dai volumi di attività ed assicurare la riservatezza degli accessi.

È pertanto necessario prestare attenzione ai seguenti punti:

- **conduzione e manutenzione del sistema di conservazione:**
il sistema di conservazione fa parte dell'infrastruttura dati aziendale, ne eredita i criteri di conduzione e manutenzione, descritti nelle procedure operative IT del sistema ISO27001 di Microdata. Tali attività riguardano la supervisione tecnica e funzionale da parte del sistema di monitoring aziendale, la gestione delle segnalazioni ed incidenti, le repliche ed i backup e la gestione del Capacity Management in termini di strumenti, azioni e processi;
- **gestione e conservazione dei log (anche in accordo con l'ente Produttore):**
il sistema di conservazione esegue la conservazione dei log ed è descritto nel manuale operativo di Legal Archive. I sistemi hardware generano un file di log di sistema che viene inviato ad un syslog server aziendale il quale codifica e firma quotidianamente ogni file garantendone la non alterazione nel tempo. I file di log sono conservati per 6 mesi a norma di legge;
- **monitoraggio del sistema di conservazione:**
la supervisione tecnica e funzionale da parte del sistema di monitoring aziendale fa parte dell'operatività normale di Microdata ed è descritta nelle procedure operative IT del sistema ISO27001 di Microdata;
- **change management:**
Il change management fa parte dell'operatività normale di Microdata ed è descritta nelle procedure operative IT del sistema ISO27001 di Microdata;
- **verifica periodica di conformità a normativa e standard di riferimento:**
tale attività è svolta in collaborazione con lfin Sistemi, attraverso gli aggiornamenti normativi e tecnici effettuati dal personale.

[Torna al sommario](#)

9. MONITORAGGIO E CONTROLLI

Le procedure di monitoraggio e controllo del sistema di conservazione, comprensive dei relativi report e log, sono ampiamente descritte nel manuale operativo Legal Archive.

[Torna al sommario](#)

9.1 PROCEDURE DI MONITORAGGIO

Il monitoraggio del sistema e delle sue componenti avviene come descritto nelle procedure operative IT del sistema ISO27001 di Microdata.

La rilevazione di qualsiasi anomalia viene registrata e successivamente risolta dal personale autorizzato.

Riguardo agli interventi e alle evoluzioni dell'applicativo, non c'è necessariamente una pianificazione periodica, ma le azioni sono concordate in base alla necessità di intervento da parte del produttore, autorizzato dal Responsabile dei sistemi informativi con il presidio del personale operativo e/o Sistemi di Microdata.

Oltre ad un monitoraggio software e hardware, Microdata effettua anche un monitoraggio normativo secondo quanto disposto dal suo ordinamento interno.

[Torna al sommario](#)

9.2 VERIFICA INTEGRITÀ DEGLI ARCHIVI

La funzionalità di verifica di integrità degli archivi permette di verificare l'integrità del documento dal momento della sua conservazione, confrontando l'impronta attuale con quella contenuta nell'IdC. Tale funzionalità viene applicata durante il processo di conservazione subito dopo la fase di memorizzazione nel file system, e risulta poi utile, nell'assolvimento dei requisiti di verifica periodica della leggibilità dei documenti, come richiesto dalla normativa.

Questa funzionalità è presente in Legal Archive® come processo schedulabile, ed è pianificato dal soggetto conservatore.

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

[Torna al sommario](#)

9.3 GESTIONE DELLE ANOMALIE

Le anomalie che possono riscontrarsi nell'operatività del servizio in fase di versamento sono gestite in generale secondo il seguente schema.

Tipo anomalia	Descrizione	Modalità di gestione
Mancata risposta al Versamento	È il caso in cui l'unità documentaria viene correttamente versata ma, per vari motivi, la risposta di avvenuta ricezione non perviene al produttore, che pertanto, erroneamente, la reputa non versata.	Il soggetto produttore deve trasmettere nuovamente e il sistema di conservazione restituisce una risposta di esito negativo con l'indicazione che l'unità documentaria risulta già versata. Tale risposta deve essere usata dal produttore come attestazione di avvenuto versamento e l'unità documentaria deve risultare come versata.
Errori temporanei	È il caso di errori dovuti a problemi temporanei che pregiudicano il versamento, ma si presume non si ripresentino a un successivo tentativo di Versamento. Il caso più frequente è l'impossibilità temporanea di accedere alle CRL degli enti certificatori. In questi casi il sistema di conservazione dopo aver riprovato 10 volte genera un messaggio di errore perché non riesce a completare le verifiche previste sulla validità della firma e il versamento viene quindi rifiutato impostando il processo in stato ERRV.	Qualora il processo di conservazione avvenga attraverso un versamento manuale ad opera del soggetto produttore, allora lo stesso 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. Qualora il processo di conservazione avvenga tramite versamento automatico o semiautomatico, il soggetto conservatore si fa carico di risolvere l'anomalia e di riversare i documenti nel sistema di conservazione e se necessario, informare il Soggetto Produttore tramite mail.
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.

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

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

- tutte le funzionalità del sistema che inseriscono o modificano dati nel Data Base e file nell'area 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 SFTP sono sottoposti a backup incrementale giornaliero e full settimanale a caldo;
- Non è quindi possibile far fronte a tutte le possibili anomalie con le stesse procedure, ma sono necessarie procedure specifiche secondo la natura dell'anomalia stessa.

La tabella seguente illustra le misure adottate per risolvere eventuali anomalie, classificate in ragione della collocazione delle informazioni nell'ambito del sistema nel momento in cui si è verificata l'anomalia:

File System	Si effettua la restore tramite le funzioni standard del file server per tutti i file inseriti nel File system fino all'ultimo backup (effettuato ogni ora); per i file inseriti successivamente all'ultimo back up si eseguono opportune procedure di quadratura tra Data Base e File system, che provvedono a riportare il sistema in stato di congruenza.
Database	Si effettua la restore tramite le funzioni standard di SQL.
Area SFTP	Si richiede al soggetto produttore la ritrasmissione dei PDV.

[Torna al sommario](#)