MANUALE DI CONSERVAZIONE

DI SYSTEMS S.R.L.

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	01.05.2020	Riccardo Gottardi	Responsabile della funzione archivistica di conservazione
Verifica	01.06.2020	Michael Hellweger	Responsabile della sicurezza dei sistemi per la conservazione
Approvazione	01.06.2020	Hofer Lukas	Responsabile del servizio di conservazione

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
Versione 1.0	01.12.2015		
Versione 2.0	31.07.2018		
Versione 3.0	01.05.2020		
Versione 3.1	24.08.2020	Precisazioni su PdV e PdD	
Versione 3.2	01.04.2021	Aggiornato Incarico Ruolo Resp. Archivistica	Vedi DL-21-09884

INDICE

1. SCOPO ED AMBITO DEL DOCUMENTO

Il presente documento costituisce il manuale di conservazione di Systems Srl e ha l'obiettivo di descrivere la società, i processi e gli ambiti relativi al sistema di conservazione dei documenti informatici adottati dall'azienda. Il sistema di conservazione è denominato *Systems Business Suite* ed è fornito come servizio ai soggetti produttori in conformità con le disposizioni dell'art. 8 del DPCM 3 dicembre 2013 riguardo il sistema di conservazione.

Il presente Manuale è redatto come prescritto dall'articolo 8 del D.P.C.M. 3 dicembre 2013 "Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71 comma 1 del Codice dell'amministrazione digitale (CAD) di cui al decreto legislativo n. 82/05".
Il Manuale è un documento informatico che descrive il sistema di conservazione che Systems s.r.l. ha realizzato per fornire ai propri clienti il relativo servizio, ai sensi dell'articolo 44 comma 3 del CAD, che prevede che la conservazione dei documenti informatici possa essere affidata a soggetti terzi, pubblici e privati, che offrono idonee garanzie organizzative e tecnologiche.
Il presente documento è conservato nel sistema di conservazione di Systems Srl. Esso è sottoposto a revisione per aggiornamenti periodici e ogni versione è conservata nel sistema di conservazione di Systems Srl. Il manuale illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, il processo, le architetture e le 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.
Ogni aspetto particolare del servizio di conservazione quale ad esempio, i documenti coinvolti, i metadati scelti per la conservazione degli oggetti digitali, i formati, le modalità di trasferimento e riferimenti presso il produttore, viene concordato e descritto sia attraverso il contratto di affidamento del servizio di conservazione sottoscritto dalle parti, sia attraverso l'allegato tecnico del contratto nominato "MODULO A: CONSERVAZIONE A NORMA DI DOCUMENTI INFORMATICI", che identifica il singolo utente committente che assume il ruolo di produttore, specifica i dati identificativi del soggetto produttore stesso, dei soggetti che assumono il ruolo di utente e descrive le tipologie degli oggetti digitali sottoposti a conservazione, i rapporti con i soggetti produttori, le specifiche operative e le modalità di descrizione e versamento nel sistema di conservazione digitale delle tipologie documentarie e delle aggregazioni documentali informatiche oggetto di conservazione. Il presente documento sarà aggiornato qualora fosse necessario apportare modifiche sostanziali al sistema o qualora si dovessero cambiare le figure professionali coinvolte nell'espletamento del servizio.

Una copia del manuale di conservazione è presente presso il soggetto conservatore. Il soggetto produttore ha la possibilità di consultarlo/scaricarlo dal portale della *Systems Business Suite*.

Dati identificativi del soggetto conservatore

Denominazione	Systems Srl
Indirizzo	Via S. Lorenzo 34C - I-39031 Brunico
Legale Rappresentante	Gustav Rechenmacher
Referente tecnico (nome e cognome) cui rivolgersi in caso di problemi tecnico-operativi	Team di Service Desk
E-mail del referente tecnico	service@systems.bz
N° telefono/fax	848 694 655
Sito web istituzionale	www.systems.bz
E-mail istituzionale	info@systems.bz

Torna al sommario

2. TERMINOLOGIA (GLOSSARIO, ACRONIMI)

All'interno delle regole tecniche del DPCM 3 dicembre 2013 relative al sistema di conservazione è presente l'allegato 1, in cui sono riportate le definizioni afferenti al processo di conservazione a norma.

Qui di seguito si riporta un glossario con i significati dei termini utilizzati e degli acronimi ricorrenti nel presente documento.

2.1. Glossario dei termini

Termini	Descrizione
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	Documento che compone l'unità documentaria per integrare le informazioni contenute nel documento principale. È redatto contestualmente o precedentemente al documento principale. La sua presenza è facoltativa.
Application server	Tipologia di server che fornisce l'infrastruttura e le funzionalità di supporto, sviluppo ed esecuzione di applicazioni nonché altri componenti server in un contesto distribuito. Si tratta di un complesso di servizi orientati alla realizzazione di applicazioni ad architettura multilivello ed enterprise, con alto grado di complessità, spesso orientate per il web (applicazioni web).
Archivio	Complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività.

Attestazione di conformità	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico in modo da autenticare le eventuali copie per immagine su supporto informatico di un documento analogico
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.
Cluster	Insieme di dispositivi di elaborazione connessi in maniera più o meno stretta che operano insieme in modo tale da poter essere considerati un unico sistema.
Codice	Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni
Comunità di riferimento	Un gruppo ben individuato di potenziali Utenti che dovrebbero essere in grado di comprendere un particolare insieme di informazioni. La Comunità di riferimento può essere composta da più comunità di Utenti. [da OAIS]
Conservatore accreditato	Soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza.
Conservazione	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione.

Contenuto informativo	L'insieme delle informazioni che costituisce l'obiettivo originario della conservazione. E' composto dall'Oggetto-dati e dalle Informazioni di rappresentazione.
Data center	Struttura utilizzata per ospitare computer e componenti associati quali dispositivi di telecomunicazioni e di storage, in generale con adeguati livelli di prestazioni e di sicurezza.
Destinatario	Identifica il soggetto/sistema al quale il documento informatico è indirizzato
Disaster recovery	Insieme delle misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi di business per imprese, associazioni o enti, a fronte di gravi emergenze che ne intacchino la regolare attività.
Documento analogico	Rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti
Documento informatico	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Esibizione	Operazione che consente di visualizzare un documento conservato e di ottenerne copia
Evidenza informatica	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.
File di indice	Indice dell'AIP, file XML che contiene tutti gli elementi del pacchetto di archiviazione, derivati sia dalle informazioni contenute nel SIP (o nei SIP) trasmessi dal produttore, sia da quelle generate dal sistema di conservazione nel corso del processo di conservazione.
Firma digitale	Particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici

Formato	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
Funzione di hash	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
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 il periodo di conservazione dello stesso e ne garantisce la staticità nella conservazione
Impronta informatica	Sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash
Informazioni descrittive	Descrivono il pacchetto informativo e consentono di ricercarlo nel sistema di conservazione. In base alle caratteristiche della tipologia di oggetto contenuto nel Pacchetto, tali informazioni possono essere un sottoinsieme di quelle presenti nel pacchetto informativo, possono coincidere o possono anche essere diverse.
Informazioni sulla conservazione (PDI)	Informazioni necessarie a conservare il Contenuto informativo e garantiscono che lo stesso sia chiaramente identificato e che sia chiarito il contesto in cui è stato creato. Sono costituite da metadati che definiscono la provenienza, il contesto, l'identificazione e l'integrità del Contenuto informativo oggetto della conservazione. [da OAIS]
Informazioni sulla rappresentazione	Informazioni che associano un oggetto-dati a concetti più significativi.
Ingester	È un'entità funzionale del sistema di conservazione, descritta nel modello OAIS, che ha la funzione di accettare i SIP, preparare gli AIP per la memorizzazione e li memorizza assieme alle relative informazioni descrittive.
Metadati minimi	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	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
Marca temporale	Sequenza di caratteri che rappresentano una data e/o un orario per accertare l'effettivo avvenimento di un certo evento. La data è di solito presentata in un formato compatibile, in modo che sia facile da comparare con un'altra per stabilirne l'ordine temporale. La pratica dell'applicazione di tale marca temporale è detto timestamping.
Memorizzazione	Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici
Metadati	Insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 del DPCM 3 dicembre 2013
Modello organizzativo della conservazione	Modello organizzativo con cui opera il sistema di conservazione garantendo la sua distinzione logica dal sistema di gestione documentale. La conservazione può essere svolta: - all'interno della struttura organizzativa del soggetto produttore dei documenti informatici da conservare; - affidandola, in modo totale o parziale, ad altri soggetti, pubblici o privati che offrono idonee garanzie organizzative e tecnologiche, anche accreditati come conservatori presso l'Agenzia per l'Italia digitale.

Pacchetto di archiviazione	Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 delle Regole tecniche 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 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 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
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 SIP ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale.
Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal Produttore
Regole tecniche	DPCM 3 dicembre 2013 e relativi allegati "Regole tecniche in materia di sistema di conservazione"
Responsabile della conservazione	Soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 delle regole tecniche del sistema di conservazione
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 SIP ed effettua il trasferimento del suo contenuto nel sistema di conservazione.
Responsabile della sicurezza	Soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza.

Responsabile del servizio di conservazione	Persona fisica incaricata dal Conservatore di sovrintendere al sistema di conservazione svolgendo le attività descritte nel documento Agid “Profili professionali” previsti per i Conservatori accreditati
Responsabile del trattamento dei dati personali	Ai sensi del Regolamento 2016/679/UE persona fisica o giuridica, l’autorità pubblica, il servizio o un altro organismo che tratta dati personali per conto del titolare del trattamento.
Riferimento temporale	Informazione contenente la data e l’ora con riferimento al Tempo Universale Coordinato (UTC)
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	Unità archivistiche o unità documentarie ordinate secondo un sistema di classificazione o conservati insieme perché: - sono il risultato di un medesimo processo di sedimentazione o archiviazione o di una medesima attività; - appartengono ad una specifica tipologia documentaria; - a ragione di qualche altra relazione derivante dalle modalità della loro produzione, acquisizione o uso. (fonte: ISAD)
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’art. 44 del Codice
Sistema di gestione documentale	Data Management System (DMS) con cui il Cliente/Utente gestisce i propri documenti
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.
Soggetto produttore	Persona fisica o giuridica, la pubblica amministrazione o l’ente titolare dei documenti informatici da conservare.
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
Testo unico	Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni.
Titolare	Soggetto produttore, ossia la persona fisica o giuridica, la pubblica amministrazione o l’ente titolare dei documenti informatici da conservare.
Unità archivistica	Insieme organizzato di Unità documentarie o Documenti raggruppati dal Produttore per le esigenze della sua attività corrente in base al comune riferimento allo stesso oggetto, attività o fatto giuridico. Può rappresentare una unità elementare di una serie [da ISAD].

Unità documentaria	Unità minima, concettualmente non divisibile, di cui è composto un archivio, per esempio, una lettera, un memorandum, un rapporto, una fotografia, una registrazione sonora. [da ISAD (G)]
Utente	Persona fisica o giuridica, destinatario del servizio di conservazione. Può coincidere con il Cliente ma può anche essere un soggetto diverso a cui il Cliente ha rivenduto il servizio o a cui il Cliente consente l'utilizzo dello stesso
Versamento	Azione di trasferimento di SIP dal produttore al sistema di conservazione.
Versamento agli archivi di stato	Operazione con cui il responsabile della conservazione di un organo giudiziario o amministrativo dello Stato effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali.

2.2. Acronimi

AgID	Agenzia per l'Italia Digitale
AIP	Archival Information package (Pacchetto di archiviazione)
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
DIP	Dissemination Information Package (Pacchetto di distribuzione)
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
IR	Informazioni della rappresentazione
IRse	Informazioni semantiche sulla rappresentazione
IRsi	Informazioni sintattiche sulla rappresentazione
ISO	International Organization for Standardization
METS	Metadata Encoding and Transmission Standard
OAIS	Open Archival Information System
ISAD (G)	General International Standard Archival Description

PDI	Preservation description information (informazioni sulla conservazione)
PEC	Posta elettronica certificata
SAA	Sistema di autenticazione e accesso
SGD	Sistema di gestione Dati
SIP	Submission Information Package
SM	Sistema di memorizzazione
SP	Soggetto produttore
SV	Sistema di versamento
TSA	Time Stamping Autorithy, è il soggetto che eroga la marca temporale
UNI SinCRO	UNI 11386:2010 – Standard nazionale per il supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (SinCRO)

Torna al sommario

3. NORMATIVA E STANDARD DI RIFERIMENTO

3.1. Normativa di riferimento

Qui di seguito è riportata la principale normativa di riferimento che disciplina l'attività di conservazione dei documenti:

- Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- 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 s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82;
- DPCM 13 novembre 2014 - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005

- DM 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.
- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 “relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)”, applicabile in tutti gli Stati membri a partire dal 25 maggio 2018.

Torna al sommario

3.2. Standard di riferimento

La realizzazione e la gestione del sistema di conservazione rispettano i seguenti standard come indicato nell’allegato 3 alle Regole tecniche:

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

Torna al sommario

4. RUOLI E RESPONSABILITÀ

Di seguito saranno indicati i nominativi delle persone che ricoprono i ruoli necessari per la corretta gestione del processo di conservazione, come indicati nel documento 'Profili professionali richiamato dalla Circolare AgID n°65/2014.

Le relative attività proprie di ciascun ruolo sono definite nella tabella del capitolo 0 del presente documento.

Responsabile del servizio di conservazione (RSC)
Il responsabile del servizio di conservazione è Lukas Hofer.

Cronologia dei responsabili del servizio di conservazione:

Nominato	Data nomina	Data revoca
Hofer Lukas	**01.06.2020 a oggi**	**-**

Responsabile Sicurezza dei sistemi per la conservazione (RSSC)
Il responsabile della Sicurezza dei sistemi per la conservazione è Michael Hellweger. La nomina è stata formalizzata in data 26.05.2020. La nomina è stata firmata per accettazione dal responsabile designato.

Cronologia:

Nominato	Data nomina	Data revoca
Hellweger Michael	**01.06.2020 a oggi**	**-**

Responsabile funzione archivistica di conservazione (RFA)

Il responsabile della funzione archivistica di conservazione è Nicola Nardini. La nomina è stata formalizzata in data 26.05.2020. La nomina è stata firmata per accettazione dal responsabile designato.

Cronologia:

Nominato	Data nomina	Data revoca
Riccardo Gottardi	**01.06.2020**	**31.03.2021**
Nicola Nardini	**01.04.2021 a oggi**	

Responsabile trattamento dei dati personali (RTD)

Il responsabile del trattamento dei dati personali è Michael Hellweger.

Cronologia:

Nominato	Data nomina	Data revoca
Michel Hellweger	**01.06.2020 a oggi**	**-**

Responsabile dei sistemi informativi (RSI)

Il responsabile del trattamento dei sistemi informativi è Richard Tappeiner. La nomina è stata formalizzata in data 26.05.2020. La nomina è stata firmata per accettazione dal responsabile designato.

Cronologia:

Nominato	Data nomina	Data revoca
Richard Tappeiner	**01.06.2020 a oggi**	**-**

Responsabile sviluppo e manutenzione del sistema di conservazione (RSM)

Responsabile dello sviluppo e della manutenzione del sistema di conservazione è Christoph Piock Ellena. La nomina è stata formalizzata in data 26.05.2020. La nomina è stata firmata per accettazione dal responsabile designato.

Cronologia:

Nominato	Data nomina	Data revoca
Christoph Piock Ellena	**01.06.2020 a oggi**	**-**

Torna al sommario

5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

I ruoli sotto riportati sono coinvolti nel processo di conservazione con i compiti e responsabilità individuati nella seguente tabella, come da indicazioni del documento “Profili professionali” richiamato dalla Circolare n°65/2014 di AgID.

Ruolo	Nominativo	Principali attività di competenza	Periodo dell’incarico	Deleghe
Responsabile del servizio di conservazione	Lukas Hofer	Definizione e attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione; definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente; corretta erogazione del servizio di conservazione all’ente produttore; gestione delle convenzioni, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.	01.06.2020	
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Christoph Piock Ellena	Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione; pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione; monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione; interfaccia con l’ente produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all’evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche; gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.	01.06.2020	
Responsabile della sicurezza dei sistemi per la conservazione	Michael Hellweger	Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.	01.06.2020	
Responsabile dei sistemi informativi	Richard Tappeiner	Gestione dell’esercizio delle componenti hardware e software del sistema di conservazione; monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l’ente produttore; segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive; pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione; controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.	01.06.2020	
Responsabile del trattamento dei dati personali	Michael Hellweger	Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.	01.06.2020	

Responsabile della funzione archivistica di conservazione	Riccardo Gottardi	Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici; monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione; collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.	01.06.2020	

Torna al sommario

5.1. Organigramma

L'organigramma che segue descrive la struttura coinvolta nel servizio di conservazione. di cui Systems si avvale per erogare il servizio di conservazione.

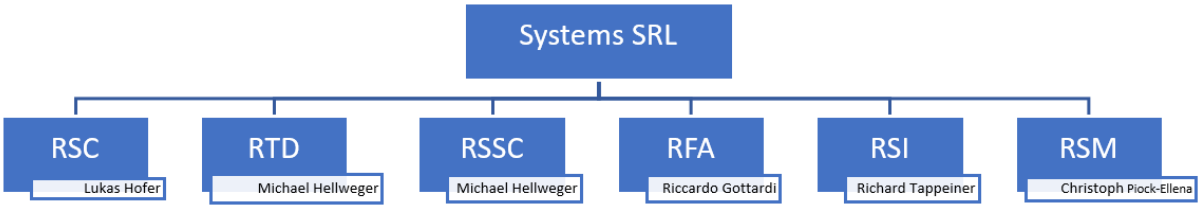

Figura 1: Organigramma funzionale e i nominativi delle figure preposte alla gestione del Sistema di Conservazione

Torna al sommario

5.2. Strutture organizzative

Il modello organizzativo utilizzato da Systems Srl per gestire il processo di conservazione, in qualità di soggetto conservatore, segue le regole definite nel DPCM 3 dicembre 2013 alla lettera b) comma 2 dell'articolo 5. Questo modello organizzativo tiene conto del modello di riferimento ISO 14721:2012 OAIS (Open Archival Information System), che definisce una struttura organizzata di persone e sistemi, che si assume la responsabilità di conservare le informazioni, rendendole fruibili nel tempo per una comunità di riferimento.

I ruoli principali che si possono identificare nel sistema di conservazione, rispettando quando defintio sia dalle regole tecniche del DPCM 3 dicembre 2013, sia dal modello di riferimento OAIS sono i seguenti: utente, produttore, responsabile del servizio di conservazione.

Per quanto riguarda poi le procedure organizzative, queste si basano sugli standard consolidati quali ISO/IEC 27001 e ISO 9001.

Produttore

Secondo il modello ISO 14721:2012 OAIS, il produttore è definito come un *"individuo, organizzazione, o sistema che deposita risorse digitali in un archivio OAIS per la conservazione nel lungo periodo. I produttori inviano a un archivio OAIS le risorse digitali da conservare e i relativi metadati attraverso un "processo di immissione".*

Questa definizione viene poi ripresa ed estesa anche nell'allegato 1 del DPCM 3 dicembre 2013 in cui viene definito come la persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento (SIP) ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione.

Come si evince dalla definizione sopra citata, il produttore non si identifica sempre con la persona che ha creato il documento, ma piuttosto con quel soggetto o ente che lo detiene, lo prepara, lo integra con eventuali informazioni aggiuntive per poi inviarlo al sistema di conservazione, sotto forma di pacchetto di versamento. Le informazioni di dettaglio sono esplicitate nel contratto di affidamento del servizio di conservazione. Il produttore è responsabile del contenuto del pacchetto di versamento ed è tenuto a trasmetterlo al soggetto conservatore, secondo quanto indicato nelle specifiche tecniche allegate al contratto di affidamento. Il produttore si impegna a depositare i documenti informatici e le loro aggregazioni documentali informatiche nei modi e nelle forme definite, garantendone l'autenticità e l'integrità nelle fasi di formazione e di archiviazione, effettuate nel rispetto delle norme sulla formazione e sui sistemi di gestione dei documenti informatici.

Il versamento dei documenti informatici e delle loro aggregazioni avviene nei modi e nelle forme definite nelle specifiche tecniche, garantendone l'autenticità e l'integrità nelle fasi di produzione e di archiviazione. In particolare, si garantisce che il trasferimento dei documenti informatici e delle loro aggregazioni venga realizzato utilizzando formati compatibili con la funzione di conservazione e sia rispondente a quanto previsto dalle specifiche tecniche allegate al contratto di affidamento, in cui si stabiliscono le tipologie documentarie, i metadati oggetto di conservazione, i formati e le modalità operative di versamento. Il soggetto produttore mantiene la titolarità e la proprietà dei documenti versati.

Il responsabile di riferimento del soggetto produttore, per le amministrazioni pubbliche, è di norma individuato nel responsabile della gestione documentale ovvero dal coordinatore della gestione documentale, ove nominato.

Il produttore ha accesso al sistema di conservazione direttamente dalla propria sede, tramite un accesso remoto da portale web dalla piattaforma *Systems Business Suite*.

Utente
L'utente del sistema, come da definizione riportata nell'allegato 1 del DPCM 3 dicembre 2013, viene identificato come *"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"*. Questi, come i soggetti produttori, possono essere interni od esterni al sistema di conservazione. L'utente può richiedere al sistema di conservazione l'accesso ai documenti informatici per acquisire le informazioni richieste nei limiti di legge. Il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto attraverso un portale web, ai documenti informatici conservati e consente la produzione e la richiesta di esibizione di un pacchetto di distribuzione. L'abilitazione e l'autenticazione degli utenti avviene in base alle procedure di gestione utenze indicate nel piano della sicurezza del sistema di conservazione ed in conformità alla legge italiana (D.Lgs 196/2003 s.m.i.) e dell'Unione Europea (Regolamento UE 2016/679).
Il modello OAIS la comunità degli utenti può essere definita come comunità di riferimento.

Responsabile del servizio di conservazione
Persona fisica nell'organizzazione del conservatore che svolge le attività di conservazione attraverso il servizio di conservazione, così come stabilito nel contratto di affidamento del servizio. Le responsabilità del responsabile del servizio di conservazione sono definite all'art. 7 del DPCM 3 dicembre 2013. Nel contratto di affidamento del servizio di conservazione, sottoscritto tra il soggetto produttore e il conservatore, vengono definite le attività e le responsabilità affidate al conservatore e quelle che rimangono a carico del soggetto produttore. Il conservatore è responsabile soltanto della conservazione dei pacchetti di versamento (SIP) accettati nel sistema di conservazione.

Organismo di tutela e vigilanza (in riferimento alle amministrazioni pubbliche)
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. La tutela e vigilanza sugli archivi di enti pubblici non statali è esercitata dal MiBACT, tramite le Soprintendenze archivistiche competenti per territorio. "Lo spostamento, anche temporaneo dei beni culturali mobili" compresi gli archivi storici e di deposito è soggetto ad autorizzazione della Soprintendenza archivistica (D. lgs 22 gen. 2004, n. 42, 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 22 gen. 2004, n. 42, art.21, c. 1, lettera e). La disposizione si applica anche:

- All' affidamento a terzi dell'Archivio (outsourcing), ai sensi del D. lgs 22 gen. 2004, n. 42, 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.

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. In base alle regole tecniche i sistemi di conservazione delle amministrazioni pubbliche e i sistemi di conservazione dei conservatori accreditati sono soggetti anche alla vigilanza di AgID.

Torna al sommario

6. OGGETTI SOTTOPOSTI A CONSERVAZIONE

Con il termine “oggetti digitali sottoposti a conservazione” si possono intendere: i documenti informatici, i documenti amministrativi informatici e i fascicoli informatici ed aggregazioni documentali informatiche, insieme alle relative informazioni, ovvero i metadati. Gli oggetti digitali con le relative informazioni vengono versati nel sistema di conservazione sotto forma di pacchetti informativi, successivamente, se i controlli vanno a buon fine, verranno conservati nel sistema di conservazione, sotto forma di pacchetti di archiviazione (AIP).
Sia in base alle regole tecniche del DPCM 3 dicembre 2013 sia in base al modello di riferimento OAIS, si distinguono tre tipi di pacchetti informativi: pacchetto di versamento (SIP), pacchetto di archiviazione (AIP) e pacchetto di distribuzione (DIP).
Di seguito, vengono illustrate le informazioni principali relative agli oggetti digitali trattati e alla loro gestione come pacchetti informativi.

La definizione dei formati supportati dal sistema di conservazione e la loro rappresentazione è parte integrante delle specifiche tecniche (allegato al contratto di affidamento del servizio).

6.1. Oggetti conservati

In sede di attivazione o successivamente ad essa, il soggetto produttore elenca quali oggetti digitali e quali metadati versare in conservazione, sulla base degli accordi stipulati all’atto della sottoscrizione del contratto di affidamento del servizio di conservazione. La definizione deitipi di documenti con i loro relativi metadati è presente nelle specifiche tecniche; il sistema gestisce gli oggetti digitali sottoposti a conservazione, distinti per ogni singolo soggetto produttore. I documenti sono versati nel sistema sotto forma di pacchetti di versamento comprensivi dei metadati che definiscono ciascun elemento con informazioni aggiuntive.

Ogni documento inviato dal soggetto produttore, viene classificato secondo delle regole ben precise, che permettono di configurare strutture e parametri adeguati ad ogni soggetto produttore definiti sulla base degli accordi stipulati all’atto della sottoscrizione del contratto di affidamento del servizio di conservazione. La classificazione dettagliata di tutte le tipologie di documento trattate dal sistema di conservazione si può trovare nell’allegato specifiche tecniche. Per ogni tipologia di documento inviato è necessario specificare i relativi metadati minimi, necessari per la sua conservazione. Ad ogni tipologia di documento sono associate delle validazioni, che vengono verificate all’accettazione del documento sulla base degli accordi presi con il soggetto produttore.
Tutti gli oggetti versati sono accompagnati da un set di informazioni minime, così come specificato e richiesto nel formato UNI 11386:2010 e da altre informazioni facoltative che vengono definite per ciascun tipo di documento. Tali regole ne identificano il comportamento e le informazioni minime richieste perché il documento venga accettato dal sistema per essere conservato.
Il sistema di conservazione, rispetta l’architettura OAIS: punto di ingresso dei documenti nel sistema è rappresentato dalla API, l’ingester secondo il modello di riferimento sopra indicato, che

acquisisce i documenti sotto forma di pacchetti di versamento e li valida, rispetto alle specifiche presenti nell'allegato tecnico.

Ogni documento conservato può essere collegato ad altri documenti. Questi collegamenti sono mantenuti e gestiti anche nel sistema di conservazione in modo da poter sempre risalire ad eventuali documenti collegati anche una volta archiviati. Esistono pertanto unità minime, come descritte nello standard ISO 23081-2, identificate e gestite come un'unica entità dal sistema di conservazione, nonostante siano costituite da più oggetti digitali: un esempio potrebbe essere un messaggio di posta elettronica contenente allegati: questo verrà conservato così come è, come email contenente allegati e non come documenti separati e collegati tra loro. Il dettaglio sulle relazioni gestite all'interno del sistema e delle unità minime è contenuta nell'allegato tecnico. Un altro raggruppamento di documenti eterogenei, che viene gestito dal sistema, è il fascicolo informatico. Grazie a questo possono essere conservati documenti "diversi" in un unico contenitore. Il fascicolo informatico è una tipologia di documento che deve essere gestito dal sistema di conservazione a norma, necessario per legge, ed è quindi anch'esso, corredato dai metadati richiesti.

Lo standard OAIS prevede che, ad ogni oggetto portato in conservazione, vengano associate un insieme di informazioni (metadati) che ne permettono in futuro una facile reperibilità e le informazioni sulla rappresentazione (IR), classificabili in sintattiche (IRsi) e semantiche (IRse), il cui obiettivo è fornire tutte le informazioni necessarie per poter leggere ed interpretare la sequenza di bit dell'oggetto conservato. È necessario, inoltre, ricordare che un sistema di conservazione che rispetti la normativa italiana, deve garantire il requisito di leggibilità degli oggetti dati conservati imposto dal comma 1 dell'art. 3 delle nuove regole tecniche e dal comma 1 dell'art. 44 del Codice dell'amministrazione digitale. Per soddisfare questi requisiti, prima di versare un qualsiasi oggetto digitale nel sistema di conservazione, è necessario che il responsabile del servizio di conservazione, in accordo con il soggetto produttore, proceda a conservare tutte le informazioni sulla rappresentazione, necessarie alla futura consultazione di tale oggetto. A questo proposito il sistema, al momento del versamento, rende possibile la ricezione dei soli documenti abilitati secondo quanto riportato nel contratto di affidamento del servizio tra ciascun soggetto produttore e Systems Srl.

Classifichiamo quindi le informazioni sulla rappresentazione in:

- Strumenti per la leggibilità: tipicamente legati al formato dell'oggetto conservato.
- Informazioni sulla rappresentazione sintattica: tipicamente legate al formato dell'oggetto conservato (per esempio il documento di specifiche tecniche del formato del file)

- Informazioni sulla rappresentazione semantica: tipicamente legate alla descrizione archivistica dell'oggetto conservato (per esempio come leggere il contenuto di un documento fiscale).

il sistema di conservazione garantisce la leggibilità nel tempo dei documenti, mantenendo anche i visualizzatori relativi ai formati gestiti, grazie all'identificazione del loro formato a partire dalla loro estensione. I visualizzatori si trovano anch'essi nel sistema di conservazione e vengono monitorati (verifica di leggibilità) e integrati nel caso venga richiesto un DIP. L'elenco dei visualizzatori e i formati dei file riconosciuti dal sistema si trova nell'allegato tecnico; di seguito riportiamo la lista dei formati standard riconosciuti dal sistema:

Formato	Proprietario	Estensione	Tipo	Aperto	Standard
PDF - PDF/A	Adobe Systems	pdf	application/pdf	Si	ISO32000-1ISO 19005-1:2005 (vers. PDF 1.4) ISO 19005-2:2011 (vers. PDF 1.7)
TIFF	Aldus Corporation in seguito acquistata da Adobe	.tif, .tiff	image/tiff	No	TIFF 6.0 del 1992 TIFF Supplement 2 del 2002
JPG	Joint Photographic Experts Group	.jpg, .jpeg	image/jpeg	Si	ISO/IEC 10918:1
MSG	Outlook mail message	.msg	application/vnd.ms-outlook	No	
XML Extensible Markup Language	W3C	.xml	application/xml text/xml	Si	
TXT	-	.txt .log	ASCII, UTF-8,UNICODE	Si	ISO 646, RFC 3629, ISO/IEC 10646
EML	-	.eml	MIME	No	RFC 2822/MIME
Office Open XML (OOXML)	Microsoft	.docx, .xlsx, .pptx	Derivato da XML	Si	ISO/IEC DIS 29500:2008
ODF Open Document Format	OASIS	.ods, .odp, .odg, .odb	application/vnd.oasis.opendocument.text	Si	ISO/IEC 26300:2006 UNI CEI ISO/IEC 26300

Il sistema è, tuttavia, in grado di supportare anche altri formati, che è possibile trovare nell'allegato tecnico del contratto di affidamento del servizio di conservazione.

Come stabilito dalla normativa di riferimento i documenti sono statici e non modificabili nel senso che non contengono macroistruzioni o codici eseguibili. Ciò è assicurato dal momento dell'invio dei documenti da parte del soggetto produttore al sistema di conservazione, che effettua, oltre alle varie validazioni e controlli di leggibilità, nonché la conformità dei rispettivi metadati rispetto a quanto riportato nell'allegato tecnico, anche la verifica di compatibilità dei file con i visualizzatori disponibili. La lista dei visualizzatori associati per formato di documento è definita nell'allegato tecnico, che sulla base di ciascuna estensione del file, associa il relativo mime-type e il

visualizzatore ad esso connesso. I metadati dell'utente vengono poi integrati con quelli del sistema, prima che il documento possa venire conservato, cosicché queste informazioni possano essere aggiunte, al corredo di informazioni inviate dall'utente per definirne meglio l'ambiente in cui il documento è stato prodotto. Le informazioni aggiuntive allegati ai documenti conservati, si possono trovare nell'allegato tecnico, in cui, per ogni tipologia di documento sono definiti i metadati obbligatori.

Queste informazioni sono intrinsecamente collegate alla tipologia di documento conservato e, al momento della richiesta di un DIP, verrà inglobato il visualizzatore relativo in modo da permettere al richiedente di poter consultare e accedere al file richiesto in maniera più completa, prima che esso venga distribuito alla comunità di riferimento.

Il requisito di leggibilità viene assicurato nel seguente modo: ad ogni invio di documenti nel sistema di conservazione, il produttore, oltre al bytestream del documento, ne fornisce anche l'hash. Tramite questo valore l'ingester elabora i documenti presenti nel pacchetto inviato e ne verifica la corrispondenza con l'hash generato a partire dal loro contenuto. Anche al momento della distribuzione dei documenti, questa corrispondenza viene controllata. In caso di errori in questo procedimento, il sistema di conservazione setta particolari stati che vengono intercettati dalle verifiche di integrità del sistema di conservazione, eseguite ad intervalli regolari. La verifica di integrità dei documenti conservati viene invece assicurata da un servizio, che scandaglia l'intero archivio nella ricerca di eventuali documenti che non rispettano la corrispondenza tra hash e contenuto del file.

Il pacchetto informativo che utilizziamo è lo stesso definito nello standard OAIS, che contiene tutte quelle informazioni che identificano il documento al momento della sua archiviazione. Questo è quindi costituito da due macro-categorie: le informazioni di contenuto (dall'OAIS "Content Information" – CI) e quelle descrittive di conservazione (Preservation Description Information – PDI). Le CI contengono a loro volta il file vero e proprio (dall'OAIS "Content Data Object" – CDO)

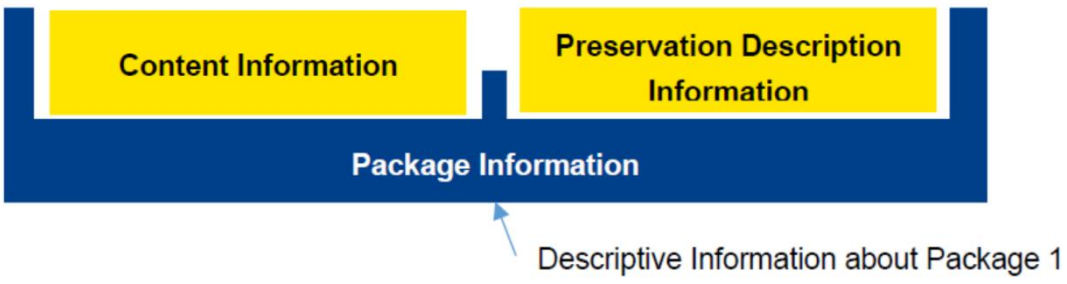

Figura 2 Struttura del pacchetto informativo secondo OAIS

e le sue informazioni di rappresentazione (dall'OAIS "Representation Information" – IR), che ne identificano la versione, il formato ed associano ad ogni documento un hash in modo che possa essere mantenuta la sua integrità e sia possibile assicurarne l'accesso tramite l'opportuno visualizzatore. Le informazioni descrittive di conservazione sono, invece, tutte quelle informazioni

che identificano il file all'interno del suo contesto e ne permettono la ricerca all'interno del sistema.

Torna al sommario

6.2. Pacchetto di versamento (SIP)

Gli oggetti digitali sottoposti a conservazione, siano essi aggregazioni documentali informatiche, documenti informatici, sono trasmessi dal produttore, conservati nel sistema di conservazione e distribuiti agli utenti sotto forma di pacchetti di distribuzione. Il pacchetto informativo, a seconda del suo utilizzo per versare, conservare o distribuire gli oggetti sottoposti a conservazione, assume la forma, rispettivamente, di SIP, AIP e DIP.

Facendo riferimento al modello OAIS e alle regole tecniche sul sistema di conservazione del DPCM 3 dicembre 2013, il sistema di conservazione di Systems Srl riprende il concetto di SIP come un contenitore del documento digitale stesso, o di un insieme di documenti, e di tutte quelle informazioni supplementari descrittive del documento (i metadati) inviate dal soggetto produttore al momento del versamento di un SIP nel sistema di conservazione.
Questo pacchetto informativo inviato dal soggetto produttore al sistema di conservazione è oggetto dell'accordo stipulato in occasione del contratto di affidamento del servizio di conservazione. Tutti i documenti presenti in un SIP vengono resi immodificabili solo al momento dell'accettazione effettiva del pacchetto da parte del sistema di conservazione, ovvero previa verifica che tutti i documenti del pacchetto siano presenti e siano stati scaricati correttamente. In termini di SIP, il contratto di affidamento del servizio di conservazione è finalizzato alla definizione degli accordi che sanciscono le modalità di trasferimento dei pacchetti stessi, la loro tempistica di trasferimento, la loro costituzione e composizione e tutte le componenti informative di cui il sistema di conservazione necessita per creare degli AIP coerenti e bene strutturati.

La fase relativa alla preparazione del SIP e il conseguente invio al sistema di conservazione può avvenire in modi diversi, essendo dipendente fortemente dalla situazione specifica del soggetto produttore e dagli accordi stipulati con il conservatore. Come anticipato, il sistema di conservazione dispone di due modi per sottoporre un SIP:

- Tramite API REST, con la possibilità di automatizzare le procedure da parte del produttore
- Tramite Interfaccia Web, con la possibilità di caricare singoli documenti manualmente

Il sistema mette a disposizione del soggetto produttore una serie di funzionalità di validazione che gli consentono, se necessario, di correggere la composizione dei pacchetti di versamento (SIP) prima del loro effettivo versamento nel sistema di conservazione. Al momento dell'invio del

SIP al sistema di conservazione, nel caso ci sia qualche documento erroneo, l'intero SIP verrà invalidato e sarà necessario un nuovo invio al sistema di conservazione.

In condizioni generali, il SIP, prodotto e trasferito dal produttore al sistema di conservazione, è costituito dall'insieme dei file che saranno oggetto di conservazione, accompagnati dai loro metadati.
Il file di indice dovrà contenere i metadati per ricercare i documenti all'interno del sistema. Le informazioni sono concordate con il conservatore e configurate nel sistema di conservazione per ciascuna descrizione archivistica, nella stessa configurazione saranno anche implementate le regole di validazione dei metadati, concordate sempre con il conservatore. Il formato del file indice utilizzato per il versamento rispetta lo standard UNI 11386:2010 Standard SInCRO, utilizzato anche per il salvataggio delle informazioni relativi ai documenti conservati.

Il sistema di conservazione permette di associare ad ogni soggetto produttore una molteplicità di tipologie documentali, ad ognuna delle quali è associato un insieme di informazioni minime nel rispetto dell'allegato 5 del DPCM del 3 dicembre 2013. Una volta che i SIP sono stati acquisiti, questi vengono trasformati in pacchetti di archiviazione (AIP) a seconda di regole di raggruppamento ben precise, definite nell'allegato tecnico.

Oltre ai metadati minimi, il soggetto produttore, in accordo con il responsabile della conservazione e con il responsabile del servizio di conservazione, può decidere di aggiungere ulteriori metadati di specializzazione del documento utilizzando la struttura "MoreInfo" (Standard UNI- SInCRO). Per ogni tipologia documentale accettata, i metadati di base e quelli facoltativi (EmbeddedMetadata) sono esplicitati nei relativi allegati del contratto di affidamento di servizio.

Alcuni di questi metadati vengono inviati direttamente dal soggetto produttore, altri vengono estrapolati ed integrati con le informazioni raccolte dal sistema di conservazione sulla base di analisi interne del documento, del suo formato e sulla base degli accordi presi con il soggetto produttore nel contratto di fornitura del servizio.

La gestione della privacy avviene tramite differenti limitazioni agli accessi, definite dal contratto di affidamento del servizio tra soggetto produttore e conservatore, rispetto alle tipologie di documenti inviati.

L'invio dei metadati da associare ad ogni documento avviene tramite il caricamento nel sistema di un file di tipo JSON, che rispecchia la stessa struttura dei metadati conservati nel file indice dell'AIP. Questo file è caricato nella prima fase della creazione del SIP, ovvero come descritto nella '"Modalità di acquisizione dei pacchetti di versamento per la loro presa in caricoAccettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico". Di risposta, nell'ultima fase, ovvero quella di "Accettazione dei pacchetti di

versamento e generazione del rapporto di versamento di presa in carico" viene restituito un rapporto di versamento sotto forma di file xml e contente i seguenti dati:

- Data di creazione del pacchetto di versamento (equivalente alla chiusura del pacchetto)
- Nome del file indice di versamento. Questo è un file XML generato dalla API che raccoglie tutte le informazioni inviate al sistema di conservazione in un unico file XML auto-esplicativo.
- Hash del file indice di versamento (il file XML precedentemente descritto)
- Il contenuto stesso del file indice xml, codificato in base64

In questo modo il produttore ha la possibilità di ricevere una conferma, che il pacchetto di versamento è andato a buon fine e con le informazioni ricevute sarà sempre possibile risalire al pacchetto originale inviato al sistema di conservazione.

Torna al sommario

6.3. Pacchetto di archiviazione (AIP)

La struttura dell'indice del pacchetto di archiviazione fa riferimento allo standard SInCRO – Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010), che è lo standard nazionale riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione.
Il sistema è costruito in modo da accettare e validare i SIP inviati dal soggetto produttore ed aggregarli in AIP, a seconda di regole definite all'interno del sistema di conservazione. Queste, devono assicurare la loro conservazione, sulla base delle scadenze legali e anche migliorare la loro consultazione e reperibilità. Un altro punto cardine della conservazione a norma di Systems Srl, consiste nel fatto che il sistema è intelligente, contiene cioè delle regole per archiviare i documenti in maniera ottimizzata, per ridurre i costi e massimizzare le performance dell'intero sistema.

In analogia allo standard SInCRO, la struttura di seguito descritta prevede una specifica articolazione per mezzo del linguaggio formale XML, per la cui applicazione pratica si rimanda allo standard stesso. Per completezza, si avverte che ciò che in questo documento è denominato IPdA (indice del pacchetto di archiviazione) nello standard SInCRO è indicato come IdC (indice di conservazione) e, analogamente, AIP è indicato come VdC (volume di conservazione).

L'IPdA è l'evidenza informatica associata ad ogni AIP contenente un insieme di informazioni, articolate come descritto nel seguito e deve essere corredato sia da un riferimento temporale sia dalla firma digitale o firma elettronica qualificata del soggetto che interviene nel processo di produzione dell'AIP.
Entrando nel dettaglio, all'interno dell'elemento IPdA si trovano le seguenti strutture:

- Informazioni generali relative all'indice del pacchetto di archiviazione: un identificatore dell'IPdA, il riferimento all'applicazione che l'ha creato, eventuali riferimenti ad altri IPdA da cui deriva il presente, e un eventuale elemento "MoreInfo" che consente di introdurre metadati soggettivi relativi all'IPdA liberamente definiti dall'utilizzatore con un proprio schema;
- Indicazione di uno o più raggruppamenti di uno o più file che sono contenuti nell'AIP. È possibile raggruppare file, nel file indice come nodo "FileGroup" dello standard UNI SInCRO, sulla base di criteri di ordine logico o tipologico ed assegnare ad ogni raggruppamento, o singolo file, le informazioni di base. In aggiunta a tali informazioni è possibile inserire un ulteriore elemento "MoreInfo", che consente di introdurre metadati aggiuntivi definiti nelle specifiche di contratto tra ente produttore e conservatore. Ogni elemento file contiene l'impronta attuale dello stesso, ottenuta con l'applicazione di un algoritmo di hash e un'eventuale impronta precedentemente associata ad esso, in questo modo ad esempio è

possibile gestire il passaggio da un algoritmo di hash diventato non più sicuro ad uno più robusto;

- Informazioni relative al processo di produzione dell'AIP, come: l'indicazione del nome e del ruolo dei soggetti che intervengono nel processo di produzione dell'AIP (es. responsabile del servizio di conservazione, delegato, pubblico ufficiale ecc.), il riferimento temporale adottato (generico riferimento temporale o marca temporale ed, infine, anche per il processo, un elemento "MoreInfo" che consente di aggiungere altre informazioni aggiuntive per descrivere meglio il processo.

All'atto della conservazione verrà composto l'AIP. In ottemperanza al modello 14721:2002 OAIS il pacchetto di archiviazione è identificato dalle informazioni sull'impacchettamento.

Si riporta di seguito la struttura dell'indice del pacchetto di archiviazione secondo lo standard UNI SInCRO. Questo pacchetto racchiude tutte le informazioni sopra citate, raggruppate in un file di formato XML con una struttura ben specifica. Questa struttura viene rappresentata dallo schema sottostante:

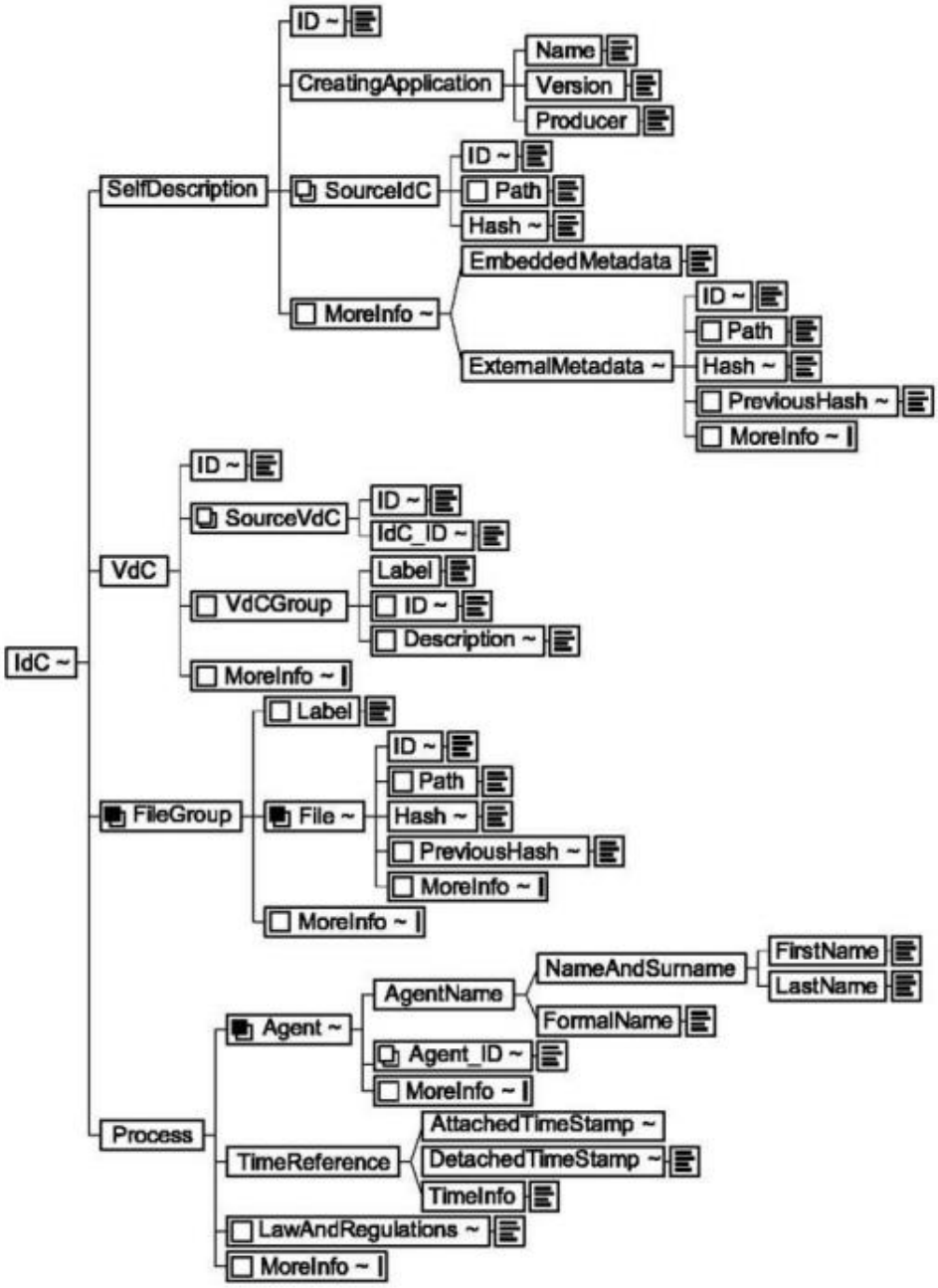

Figura 3: Struttura file indice Standard UNI SInCRO

L'AIP 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 del sistema di conservazione è quello di un'assoluta auto consistenza del pacchetto informativo nel momento in cui è costituito l'AIP stesso, 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 uno solo pacchetto informativo
- l'insieme delle relazioni di contesto che permettono la correlazione logica del pacchetto informativo agli altri pacchetti informativi e in generale ad un qualsiasi contesto di natura archivistico-gerarchica.

Quest'ultimo elemento è quello che ci permette di ricostruire il vincolo archivistico e quindi di ricondurre, ad esempio, ad una stessa pratica o ad uno stesso fascicolo tutti i documenti relativi ad una medesima attività, 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:

- l'oggetto digitale possibilmente in un formato standard non proprietario
- l'impronta del documento generata con funzione di hash
- il riferimento temporale (rappresentato dalla marca temporale o altro riferimento temporale opponibile a terzi, come la segnatura di protocollo)
- il set di metadati gestionali (UNI SinCRO)
- il set di metadati identificativi (per esempio possono essere utilizzati i metadati dello standard ISAD);
- il set di metadati descrittivi (per esempio possono essere utilizzati i metadati dello standard ISAD o METS);
- il set di metadati tecnologici (per esempio possono essere utilizzati i metadati dello standard METS).
- il viewer necessario per la visualizzazione del documento stesso
- la documentazione tecnica necessaria alla comprensione del viewer stesso

Pertanto la definizione dei metadati supplementari, non obbligatori per legge, viene definita nel dettaglio nell’allegato tecnico del contratto con ogni singolo produttore.

La forza innovativa del sistema di conservazione risiede, oltre che negli elementi informativi che sono stati descritti sopra e che permettono una perfetta conformità al modello OAIS, anche nel livello descrittivo adottato.
Si assume che il livello di descrizione minimo che garantisca una gestione efficace di tutti i dati e metadati necessari per la conservazione e che permette quella necessaria contestualizzazione archivistica del documento, è rappresentato dall’unità archivistica. Essa rappresenta un livello di aggregazione minimo nel quale racchiudere le informazioni comuni a più documenti e contenuti

digitali per relazionare i documenti afferenti al medesimo oggetto, pratica, procedimento o processo.
Tale livello diventa un file contenente i metadati identificativi e descrittivi, secondo il modello sopra proposto. Ovviamente esso non contiene un oggetto digitale, nella stretta accezione OAIS, ma diventa un container da conservare, un vero e proprio fascicolo informatico.
Oltre ai metadati tipici (ad esempio, denominazione del fascicolo ed estremi cronologici del fascicolo) esso potrà contenere uno o più puntatori agli oggetti digitali collegati: un documento può essere collegato ad uno o più documenti che ne estendano il significato. Questa informazione è riportata nel sistema di archiviazione come collegamento e viene mantenuta anche nel file indice dell'AIP e del DIP.
Il livello di descrizione sufficiente e necessario per una corretta conservazione della risorsa digitale è rappresentato proprio dall'unità archivistica. Tale livello, pertanto, diventa elemento conservato e incorporato (embedded) a tutti gli effetti all'AIP che contiene l'oggetto digitale che rappresenta il documento informatico da conservarsi a norma.
L'insieme, costituito dal data object, dai suoi metadati e dalle relazioni fra i documenti e fra questi e la struttura di archivio, costituisce il nucleo minimo e sufficiente della conservazione a lungo termine.
In concreto, una volta che i SIP sono stati accettati nel sistema, (e sono quindi stati oggetto di controlli sui metadati previsti dal contratto di servizio) essi sono pronti ad essere trasformati in AIP e quindi diventare l'oggetto della conservazione a lungo termine.

Lo schema seguente mostra sinteticamente come sarà costruito l'AIP:

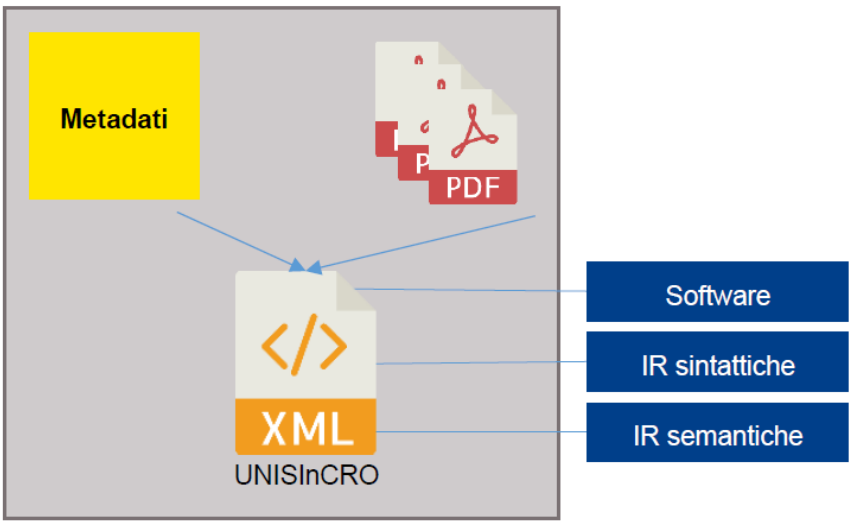

Figura 4: Struttura AIP (Archival Information Package)

Ogni oggetto versato nel sistema di conservazione verrà in automatico identificato e per ciascuno tipo di formato, viene associato un viewer al momento della richiesta di scaricamento tramite il DIP.

Torna al sommario

6.4. Pacchetto di distribuzione (DIP)

Nel modello OAIS, il DIP è strutturato nel modello dati, come l'AIP per assicurare l'accesso e la fruibilità degli oggetti digitali conservati nel sistema di conservazione. La differenza sta nella sua destinazione in quanto esso viene concepito per essere fruito ed utilizzato dall'utente finale (esibizione).

In questo caso, un DIP può anche non coincidere con un 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. Può anche verificarsi il caso di DIP che sono il frutto di più AIP che vengono "spacchettati" e rimpacchettati per un più fruibile utilizzo da parte dell'utente.

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

È possibile ricevere i dati utilizzando una particolare richiesta di interrogazione, rispettando le restrizioni di accesso esistenti. Grazie a questa è possibile "configurare" un DIP in modo che contenga le sole informazioni richieste.

Il sistema di conservazione 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 sono 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 i software necessari alla loro visualizzazione.

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

- i documenti richiesti nel formato previsto per la loro visualizzazione
- un'estrazione dei metadati associati ai documenti
- l'indice di conservazione firmato e marcato
- tutti gli indici di conservazione degli AIP corrispondenti ai documenti richiesti
- Indicazione dei 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 del modello OAIS.

La struttura del file restituito dal sistema come DIP è il seguente:

- File indice del DIP
- Directory con Guid del produttore/i
- Directory con Guid dell'AIP/ degli AIPs
- Documenti effettivi
- Directory contenente il file indice AIP
- File indice AIP

Torna al sommario

7. IL PROCESSO DI CONSERVAZIONE

Il processo di conservazione si attiva a seguito della sottoscrizione del contratto di affidamento del servizio di conservazione, le cui procedure vengono dettagliate nell'allegato, specifiche tecniche. Il sistema di conservazione erogato da Systems srl è regolato dai seguenti documenti:

- contratto di affidamento del servizio di conservazione
- Relativi allegati al contratto secondo i relativi moduli acquistati
- atto di nomina responsabile del servizio di conservazione
- nomine dei responsabili delle aree coinvolte nel processo di conservazione
- oggetti da sottoporre a conservazione (parte integrante delle specifiche tecniche, allegato del contratto di affidamento del servizio di conservazione)
- manuale operativo del software di conservazione, disponibile online sul nostro portale.

Il Responsabile del servizio di Conservazione, in conformità ai compiti previsti dall'art. 7 del DPCM 3 dicembre 2013, gestisce i servizi e le funzioni per l'operatività complessiva del sistema. Nel seguito viene rappresentato il processo di conservazione implementato nel sistema di conservazione in conformità all'art. 8 del DPCM 3 dicembre 2013.

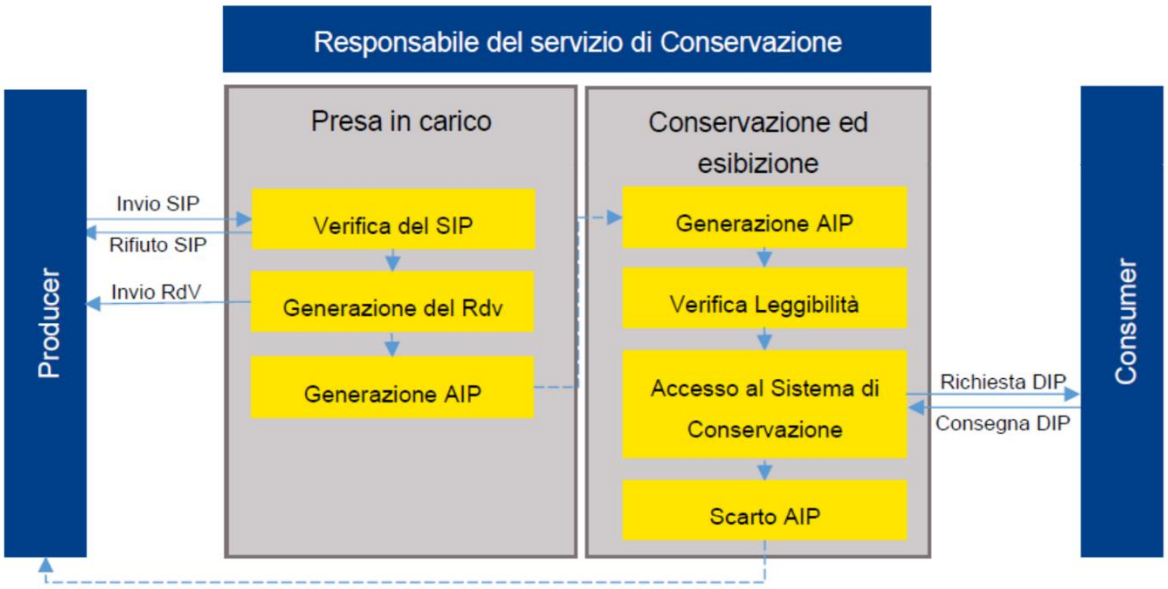

Figura 5: Processo di conservazione della Systems Business Suite

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

Torna al sommario

7.1. Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico

La prima fase è l'acquisizione del SIP nel sistema di conservazione. Il modello di trasmissione del SIP dal soggetto produttore al soggetto conservatore viene concordato in fase contrattuale e descritto nelle specifiche tecniche.
Il caricamento dei documenti alla *Systems Business Suite* può avvenire nelle seguenti modalità:

- Tramite REST API, con la possibilità di automatizzare le procedure da parte del produttore
- Tramite Interfaccia Web, con la possibilità di caricare singoli documenti manualmente

REST API - WebServices

In caso di caricamento tramite REST API il feedback avviene in maniera sincrona, quindi viene restituito immediatamente dopo ogni chiamata. Con la modalità Web Service l'applicativo chiamante del cliente, dopo l'autenticazione, avvia un processo di conservazione nel sistema durante il quale invia alla *Systems Business Suite* i pacchetti informativi e l'insieme dei metadati di ricerca a loro associati.
Il processo può essere suddiviso nelle seguenti passi:

- Apertura di un SIP: questa chiamata avviene con il trasferimento di tutti metadati. Viene restituito un errore in caso di metadati mancanti o nel caso che le validazioni definite nell'allegato tecnico del contratto non vadano a buon fine.
- Invio dei singoli documenti con impronta. Questa viene comparata con quella generata dal sistema di conservazione sulla base del contenuto ricevuto. Nel caso queste due impronte non corrispondano, il file inviato non verrebbe accettato e si riceverebbe una informazione del relativo errore. In questo caso l'utente ha la possibilità di caricare nuovamente tale file.
- Chiudere il SIP. Con questa chiamata si riceve come feedback il rapporto di versamento.

Se il processo non viene chiuso con successo ed in maniera attiva dall'utente abilitato, viene chiuso automaticamente dopo 24 ore e viene settato uno stato di errore. Tutti i pacchetti erronei non vengono mantenuti se non alcune informazioni minime, che ne permettono una loro tracciabilità in caso di necessità: il contenuto dei singoli file, viene quindi rimosso.
Il produttore può verificare lo stato della conservazione di un documento specifico con un'apposita chiamata API, per verificare se esso si trovi in un AIP o ancora solo in un SIP.

Interfaccia web

La modalità di trasferimento, via upload manuale, prevede che l'utente abilitato carichi da interfaccia web nel portale della *Systems Business Suite* il file da conservare ed evidenzii metadati ad esso associati. La procedura di upload nel dettaglio prevede:

- La selezione della descrizione archivistica a cui appartiene il documento che si sta caricando
- La selezione del file che dovrà essere caricato a sistema attraverso un browsing da file system
- L'imputazione manuale dei diversi metadati associati al singolo file, direttamente nei campi della maschera di input: a seconda della tipologia di file caricato verranno richieste informazioni supplementari per la corretta identificazione e ricerca del documento da conservare
- La selezione di eventuali allegati al documento principale attraverso un browsing da file system
- La conferma di caricamento del documento

Alla chiusura del SIP, tutti i documenti contenuti nel pacchetto sono resi immodificabili all'utente che li ha caricati. In caso di errore nel processo di creazione del SIP, è possibile visualizzare i pacchetti in errore dal portale della Systems Business Suite. Per ogni documento caricato è possibile capire se esso sia stato conservato in un AIP o si trovi ancora in un SIP. Tramite opportuni filtri nel portale è possibile eseguire delle ricerche efficaci sui documenti, per capire, ad esempio, se essi siano già stati conservati.

Torna al sommario

7.2. Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti

Il sistema di conservazione prevede la possibilità di eseguire verifiche sulla composizione del SIP, sull'integrità dei file e sull'insieme dei metadati forniti. Le validazioni si basano sulle normative vigenti e effettuano dei controlli sulla conformità di legge dei documenti inviati in conservazione. Il dettaglio sulle verifiche per ogni tipologia di documento, lo si può trovare nell'allegato tecnico allegato al contratto con il soggetto produttore.

Di seguito descriviamo i diversi tipi di validazione previsti, in caso uno di questi controlli fallisca il documento non potrà essere versato nel sistema di conservazione:

- Validazioni del SIP: il sistema di conservazione verifica la congruità delle informazioni contenute nell'indice dei metadati con il numero di documenti presenti

nel SIP: per superare la validazione il SIP deve contenere tutti i documenti elencati nell'indice di conservazione (controllo obbligatorio) Il sistema attende finché non tutti i documenti di un SIP siano stati inviati. Se questo non dovesse essere raggiunto dopo un tempo ben preciso, il pacchetto sarà scartato. Tutti questi dettagli sono definiti nell'allegato tecnico.

- Validazioni sul singolo documento: il sistema di conservazione permette di verificare che:
- L'estensione del documento in elaborazione appartenga ad alla lista dei formati per i quali il sistema può associarvi il viewer (ad eccezione di eventuali file criptati, dove la possibilità di visualizzazione viene demandata al produttore).
- Il file dei metadati, prodotto e versato dal SP, deve includere sempre un campo contenente l'impronta informatica di ciascun file, in modo che il sottosistema di validazione ricalcola l'impronta di ogni documento e lo confronta con quello dell'indice verificando l'integrità del file versato.
- In fase di acquisizione del SIP il sistema elabora i metadati e verifica che siano rispondenti alle caratteristiche configurate nella descrizione archivistica.
- Verifica che il soggetto che invia i documenti corrisponda effettivamente al produttore o sia responsabile per l'invio di un certo tipo di documenti da parte del produttore in questione. Questi controlli vengono fatti sulla base del token di autenticazione e sui metadati dei documenti inviati. Se questa corrispondenza fallisce per un qualsiasi documento, il pacchetto di versamento non viene chiuso correttamente e non verrà portato in conservazione.

All'atto della creazione del SIP, come in ogni fase del processo, il servizio crea un log che viene salvato come descritto nel piano di sicurezza. Le informazioni salvate sono le seguenti:

- Data e ora al secondo
- Livello di log
- Classe di attività
- Descrizione dell'accaduto, in cui è presente il servizio che ha svolto una certa attività, su che server, quando, il livello di log e una descrizione dell'evento

Tramite dei tool è possibile accedere a questi log per eseguire delle ricerche mirate per un determinato problema, permettendo al sistema di conservazione di essere molto preciso ed efficace.

Torna al sommario

7.3. Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico

Il sistema, superate le validazioni dei documenti del SIP, restituisce al produttore il rapporto di versamento. Per attestare l'avvenuta acquisizione e presa in carico del SIP, il sistema restituisce al produttore il rapporto di versamento relativo al pacchetto di versamento appena inviato, come previsto dalla DPCM del 03. dicembre 2013. All'interno del rapporto di versamento viene restituito un file indice che riassume tutti i documenti inviati con i relativi metadati ed un'evidenza informatica dello file stesso. Questo file viene salvato anche nella *Systems Business* Suite, per essere eventualmente scaricato dal portale web ed essere consultato dai nostri clienti.

Le operazioni principali, eseguite dal processo di conservazione, vengono registrate nel sistema di log. Per ogni singolo log è presente la seguente informazione:

- Timestamp = Riferimento temporale UTC dell'operazione
- Message / Custom Dimensonsions = Descrizione dettagliata dell'operazione eseguita con informazioni riferite all'oggetto della su cui è stata fatta l'operazione: ad esempio il Guid del pacchetto, del documento, l'identificativo utente o quello del produttore
- severityLevel = definisce la tipologia del log (se grave o meno grave)
- itemType = descrive se log di tipo trace, request, customEvents, exeption…
- operation_Name = nome dell'operazione eseguita
- operation_id = identificativo univoco della singola operazione per poter risalire ai vari passaggi inseriti nel log di una particolare operazione
- operation_ParentId = identificativo univoco del padre di ogni singola operazione per poter risalire ad una catena di operazioni
- application_Version = numero della versione dell'applicativo stesso
- Cloud_RoleIstance = definisce su quale server è stato eseguita l'operazione

Dipendentemente dalla chiamata API che si esegue, si possono trovare le seguenti informazioni all'interno dei log :

- Apertura di un SIP:
  - Nome della chiamata API ricevuta con, ad esempio, l'indicazione dei metadati ricevuti con l'apertura del pacchetto. In più sono presenti le informazioni sul produttore per cui è stato aperto il pacchetto e da quale utente è stata eseguita l'operazione
  - Apertura del Pacchetto stesso

- Verifica dei singoli documenti indicati nell'elenco dei documenti con i loro metadati (come indicato sotto capitolo 7.2 Verifiche effettuate sui pacchetti di versamento)
- Conferma del salvataggio del documento con i suoi metadati all'interno del database
- Conferma dell'associazione corretta tra documento e pacchetto

➢ Invio dei singoli documenti con impronta:

- Dettaglio della chiamata API ricevuta con, ad esempio, indicazione dell'impronta dichiarata da parte dell'utente.
- Conferma che il file è stato salvato correttamente nel sistema (avendo superato tutte le verifiche sul file proprio come descritto nel capitolo 7.2 Verifiche effettuate sui pacchetti di versamento)

➢ Chiusura del SIP:

- Dettaglio della chiamata API della richiesta ricevuta con l'identificativo univoco del pacchetto ed indicazione dell'utente che esegue l'operazione
- Verifica se il SIP può essere chiuso (quindi va verificato se tutti file sono presenti, con le impronte corrette e tutti i loro metadati sono presenti)
- Creazione del file indice, che contiene tutti i metadati ricevuti, le impronte dei file e il suo rapporto di versamento.

In caso di errori (vale per ogni passo descritto in precedenza), come ad esempio una verifica sui metadati non superata, viene anche loggato:

➢ Il tipo di verifica fallito

➢ La causa dell'errore

➢ Il modulo del codice sorgente su cui si è riscontrato l'errore. Questo in modo da risalire eventualmente anche all'errore nel codice sorgente da parte del team di sviluppo, se necessario.

➢ Il messaggio che viene restituito all'utente per poter capire meglio il problema.

Il rapporto di versamento consegnato al produttore contiene le seguenti informazioni:

Dato	Descrizione	Nome tecnico in API
Riferimento temporale	Riferimento al Tempo universale coordinato (UTC)	endDateUTC
Impronta	Impronta, calcolata sull'intero contenuto del pacchetto di versamento, quindi sul file indice fornito	fileHash
Nome file indice	Nome del file indice fornito	fileName
Contenuto file indice	File indice riassuntivo di tutti i documenti inviati con i relativi metadati ed un'evidenza informatica dello stesso	content
Identificativo Pacchetto	Identificativo univoco per identiticare il pacchetto di versamento	guid

Torna al sommario

7.4. Rifiuto del pacchetto di versamento e modalità di comunicazione delle anomalie

Il SIP viene sottoposto ad una serie di controlli. Qualora il SIP non abbia superato i controlli, il sistema notifica l'avvenuto errore e dettaglia nei log la motivazione dell'errore. Qualora il SIP inviato dal produttore non abbia superato tutti i controlli previsti, il sistema rifiuta l'intero pacchetto e restituisce un messaggio di errore al momento della chiusura del pacchetto, in modo che questi venga avvisato subito dell'errore e possa rielaborare prontamente i documenti per poterli riversare prima possibile: il produttore ha quindi una conferma istantanea dell'avvenuto versamento. Il responsabile del servizio di conservazione controlla regolarmente eventuali log o notifiche dal sistema di conservazione, per verificare che eventuali errori di sistema possano influire sul rifiuto dei pacchetti inviati. I pacchetti, che non abbiano superato correttamente l'esecuzione del processo di versamento, vengono segnalati con un flag, in modo da poterli comunque mantenere nel sistema, nel caso il produttore voglia confrontarsi con noi. Il produttore riceve una descrizione dell'errore che può segnalarlo all'Service Desk di Systems Srl attraverso l'identificativo interno del pacchetto di versamento che provvederà a comunicarlo al responsabile dello sviluppo e manutenzione del sistema di Conservazione.

Torna al sommario

7.5. Preparazione e gestione del pacchetto di archiviazione

La *Systems Business Suite* garantisce la conformità a questo requisito OAIS creando dei pacchetti di archiviazione contenenti tutti i file necessari alla loro ricostruzione e ricerca, collegando i documenti alle informazioni sulle rappresentazioni a loro associate e ai rispettivi viewer.

Un AIP contiene tutti i documenti conservati di un particolare soggetto produttore, organizzati per tipo di documento. Tale pacchetto viene creato in automatico dal sistema di conservazione a norma dopo corretta consegna di uno o più pacchetti di versamento entro i termini prescritti secondo allegato tecnico del contratto di affidamento del servizio.
La dimensione dell'AIP è variabile e dipende dal numero di documenti da elaborare presenti in un dato momento, raggruppati per produttore. Ogni file conservato è identificato da una serie di metadati che lo contraddistinguono e ne rendono possibile la sua ricerca all'interno del sistema di conservazione. La forma utilizzata nella costruzione degli AIP fa riferimento alla norma UNI 11386:2010 che è lo standard nazionale riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione. In concreto, l'AIP è un'entità logica contenuta in un'alberatura di file e cartelle e definita nel file indice UNI SinCRO generato nel corso del processo di conservazione e contenente tutte le informazioni inviate nel SIP o definite nel sistema di conservazione.

Gli oggetti conservati sono salvati nel file system in una struttura logica organizzata in modo che ogni file è nominato con l'identificativo univoco del file stesso come inserito anche nel file indice secondo il modello UNI SinCRO. La struttura delle cartelle nel file system è gestita dal sistema di conservazione per permettere delle ricerche performanti.
I riferimenti tra file fisico e relativo pacchetto (SIP, AIP, DIP) sono gestiti all'interno del database. Ogni documento salvato è corredato degli stessi metadati caricati inizialmente dal produttore, più quelli integrati dal sistema di conservazione durante la sua elaborazione. Questo ci permette una più veloce consultazione dei documenti e semplifica le verifiche automatizzate ed i controlli di integrità che effettuiamo sistematicamente sull'archivio di conservazione.

L'AIP è un pacchetto informativo auto-consistente, conforme alle specifiche fornite dal modello di riferimento OAIS e dal DPCM 3 dicembre 2013 in materia di conservazione; si compone:

- degli oggetti digitali sottoposti a conservazione,
- dalle informazioni sulla rappresentazione
- dalle informazioni sulla conservazione (metadati).

La conservazione si conclude con la firma digitale e la marca temporale dell'indice UNI SinCRO e termina con la messa a disposizione del cliente di questa evidenza di avvenuta conservazione (indice XML) da parte del responsabile del servizio di conservazione. Il sistema di conservazione

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

Anche attraverso la API il produttore può verificare lo stato della conservazione di un documento specifico con un'apposita chiamata. Inoltre è anche possibile visualizzare ogni pacchetto di archiviazione creato attraverso la piattaforma Web.

Torna al sommario

7.6. Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione

Gli utenti abilitati hanno la possibilità di richiedere l'accesso e la consultazione agli oggetti digitali conservati. Questo avviene tramite opportune richieste fatte al sistema di conservazione, che una volta raccolti tutti gli oggetti digitali con i relativi metadati, li restituisce sotto forma di DIP. La richiesta di DIP avviene direttamente dalla *Systems Business Suite* tramite la funzione di ricerca , la loro selezione e la confermaper la creazione del DIP. Il sistema di conservazione preparerà il DIP, che una volta terminato sarà reso disponibile per lo scaricamento nell'area riservata di un particolare cliente/produttore.

A questo proposito, possono essere create illimitate possibilità di creazione dei DIP, che non sono limitate ad un AIP ma possono contenere documenti di AIP differenti. Un DIP contiene quindi:

- Gli oggetti digitaliselezionati per la creazione del DIP
- un'estrazione delle informazioni di conservazione dei documenti e dei loro documenti collegati
- l'indice di conservazione firmato e marcato e le informazioni sulla conservazione associate ai fascicoli informatici di ogni documento presente nell'AIP (in caso di più documenti presenti nello stesso AIP il suo indice all'interno del DIP comparirà solo una volta)
- I riferimenti ai viewer necessari alla visualizzazione dei documenti del pacchetto e le informazioni sulla loro rappresentazione
- le informazioni sull'impacchettamento e le informazioni descrittive associate al pacchetto informativo.

In linea generale il DIP può essere erogato dal sistema di conservazione come unico file in formato ZIP. Ogni cliente con accesso alla *Systems Business Suite* ha la possibilità di richiedere al sistema di conservazione un particolare gruppo di documenti. Il sistema aiuta l'utente a preparare la query che poi viene inviata al sistema di conservazione per venire poi elaborata e restituire un DIP con i documenti e i metadati richiesti (esibizione). In caso di utilizzo diretto della API, il produttore deve conoscere la sintassi corretta, per poter eseguire la richiesta diretta al

sistema di conservazione. Questa sintassi è comunque specificata nel manuale di utilizzo per l'utente, allegato al contratto affidamento del servizio di conservazione.

La struttura dei file fisici all'interno del DIP e la seguente:

- Indice del DIP
- Indici AIP rispettivamente ai file presenti nel DIP
- directory di nome "Files" contenente tutti i file fisici
- riferimento nome "Viewers"

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

Il soggetto produttore può consultare i documenti informatici versati al sistema di conservazione tramite interfaccia web, collegandosi all'indirizzo comunicato dal soggetto conservatore con le proprie credenziali, oppure utilizzando gli appositi web services, ricercare i documenti informatici versati, effettuarne il download e acquisirne le prove delle attività di conservazione tramite la consultazione/scaricamento dei DIP, in cui contenuta tutta la catena di documentazione necessaria a rispondere alle esigenze dello standard OAIS.

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 conservatore, i propri delegati alla visualizzazione e al download dei documenti informatici originali ai fini dell'esibizione. Il conservatore genera gli account e il sistema invia le credenziali all'utente per accedere al portale del sistema di conservazione all'indirizzo https://bs.systems.bz. Il collegamento avviene tramite

connessione sicura SSL con certificato rilasciato da Certification Authority che si attiene a standard internazionali. Una volta accreditato, l'utente ha accesso ai servizi opportunamente profilati per la sua utenza, tra cui:

- Visualizzare i documenti informatici originali conservati da remoto
- Visualizzare le informazioni di conservazione associate all' AIP
- Scaricare i documenti informatici conservati (duplicati) e i file di evidenza della conservazione (indice di conservazione UNI SinCRO)
- Scaricare le informazioni sulla rappresentazione associate all'AIP
- Richiedere e scaricare i DIP da consegnare alle autorità competenti, in caso di necessità.

Sarà cura del soggetto produttore fornire un'eventuale copia conforme, richiedendo la presenza di un pubblico ufficiale. 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 la 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.

Il sistema di conservazione è stato progettato, anche in termini organizzativi e di preservation planning, proprio con l'obiettivo di prevenire l'obsolescenza dei formati gestiti: a questo scopo sono disponibili un sistema di gestione e tracciabilità delle informazioni sulla rappresentazione associate ai documenti, un sistema di esibizione degli strumenti di restituzione della rappresentazione dei documenti conservati, e infine un sistema di reportistica associato alle informazioni sulla rappresentazione. Tutte queste componenti permettono al Responsabile del Servizio di Conservazione l'aggiornamento delle informazioni sulla rappresentazione, nel tempo, con la relativa cristallizzazione, storicizzazione e tracciabilità. 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 soggetto produttore avrà cura di gestire tale scelta. Il conservatore rimanda la gestione di tale attività al soggetto produttore le cui modalità di intervento sono esplicitate nel contratto di affidamento. Il conservatore garantisce la messa a disposizione dell'originale informatico attraverso un DIP eventualmente firmato dal responsabile del servizio di conservazione

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 al meglio lo scarto del materiale documentario non destinato alla

conservazione permanente, ma caratterizzato invece da tempi di conservazione limitati e diversificati.
Il soggetto produttore, nei 90 giorni prima dell'effettivo scarto di un AIP, ha la possibilità di visualizzarlo e richiederne il prolungamento per iscritto al soggetto conservatore. In quest'ultimo caso, verrà avviata la procedura di prolungamento delle scadenze dei documenti presenti nel pacchetto, cosi come descritto nell'allegato tecnico.
Negli archivi correnti, gestiti secondo criteri aggiornati, è presente un metadato nel piano di classificazione e conservazione, definibile per ciascuna tipologia documentaria o fascicolo (descrizione archivistica), che stabilisce i tempi di conservazione.
Il responsabile del servizio di conservazione verifica, ad intervalli regolari, che non ci siano documenti scaduti, in questo caso ne esegue lo scarto, fatto salvo comunicazione esplicita del produttore dei dati.

In fase di creazione del pacchetto di archiviazione viene già definita la sua data di scarto, sulla base del documento che esso contiene, che deve essere conservato più a lungo. Vengono scartati quindi solo pacchetti interi, anche se alcuni documenti hanno già raggiunto la loro scadenza. Il motivo principale di questa decisione è quello di mantenere integro il pacchetto di archiviazione nel tempo fino allo suo scarto.
La data di scarto del pacchetto di archiviazione è visibile, al relativo utente abilitato, fin dall'inizio della sua creazione. In un'apposita sezione l'utente può visualizzare i suoi pacchetti che saranno scartati nell'arco dei prossimi 90 giorni da parte del responsabile del servizio di conservazione
Il caso non pervenga nessuna richiesta esplicita da parte del soggetto produttore, prima della scadenza della data di scarto, il responsabile del servizio di conservazione procede a scartare tale pacchetto.

Nei casi previsti dalla legge, nel caso di controlli da parte dell'agenzia delle entrate o da parte di un organo di vigilanza, come le soprintendenze archivistiche competenti per territorio, nel caso degli enti pubblici e degli archivi appartenenti a soggetti privati, considerati di particolare rilevanza storica (dichiarazione ex. art. 13 Decreto Legislativo 22 gennaio 2004, n. 42 Codice dei beni culturali e del paesaggio), la richiesta di scarto di uno o più pacchetti deve essere trasmesso dal soggetto produttore all'autorità di vigilanza che, in base alle norme vigenti, deve fornire il nulla-osta per lo scarto. Il soggetto produttore, una volta ricevuto il nulla-osta, provvede ad adeguare, se necessario, l'elenco dei pacchetti da scartare presenti sul sistema alle decisioni dell'autorità.
Una volta che l'elenco di scarto definitivo viene predisposto, il soggetto produttore può trasmetterlo a Systems Srl con la richiesta di procedere allo scarto. Dall'altra parte Systems Srl, verifica, all'interno del processo di scarto, se il pacchetto appartiene a tale categoria ed in questo caso attende la conferma da parte del soggetto produttore.

Solo dopo aver ricevuto l'autorizzazione, il conservatore provvederà alla cancellazione dei pacchetti di archiviazione contenuti nell'elenco di scarto.

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 si basi sullo standard OAIS, deve essere assicurata l'interoperabilità e la trasferibilità degli archivi informatici tra sistemi differenti. Visto che il presente sistema di conservazione si basa sullo standard OAIS, questo permette l'esportazione e l'importazione di DIP da altri sistemi.
Lo standard utilizzato ai fini dell'interoperabilità tra sistemi differenti è definito dall' UNI 11386:2010 Standard SInCRO, che è lo standard nazionale riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione.

L'importazione e l'esportazione dei DIP in un formato standard (UNI SInCRO) permette lo scambio di pacchetti e di documenti tra sistemi, agevolando l'interoperabilità degli stessi.

In caso di migrazione degli oggetti digitali da un conservatore ad un altro o da un conservatore ad un utente autorizzato, si utilizzano canali sicuri e criptati: per questo è necessario utilizzare connessioni sicure (https) nello scaricamento e upload direttamente tramite le interfacce di scaricamento fornite dai conservatori certificati.

La *Systems Business Suite* è in grado di importare dati di altri outsourcer qualora dette informazioni, precedentemente soggette a conservazione a norma, rispettino alcune caratteristiche. La verifica di dette caratteristiche è preventiva rispetto all'accettazione dei dati conservati da migrare. I contratti avranno pertanto una componente di valutazione preventiva della fattispecie.

In caso di importazione di piccoli pacchetti di distribuzione, provenienti da altri conservatori certificati, è possibile effettuare un'importazione manuale dei documenti e dei loro relativi metadati, in modo da abilitare la loro ricerca attraverso le procedure standard della Systems Business Suite. In caso di import più massicci, è preferibile utilizzare degli script che sfruttano le API oppure richiedere a Systems Srl una procedura ad hoc, per l'import di questi documenti.

Torna al sommario

7.10. Cessazione delle attività di conservazione.

Ai sensi dell'art. 37 del d.lgs. n. 82/2005 Codice dell'Amministrazione Digitale, nel caso in cui Systems Srl decidesse di cessare le proprie attività di conservazione a norma, la stessa è tenuta a comunicarlo al AgID per mezzo di un email certificata (PEC), almeno sessanta giorni prima della cessazione.

Allo stesso tempo, Systems Srl notificherà, sempre per mezzo di una PEC (o un' altra modalità concordata) all'indirizzo istituzionale del cliente (Soggetto Produttore), ovvero a quello indicato nell'affidamento del servizio, le seguenti informazioni:

- Data di cessazione del servizio di conservazione, secondo il preavviso concordato nel contratto di affidamento del servizio di conservazione
- Procedura di recupero degli archivi
- Intervallo di tempo disponibile ai soggetti produttori per il recupero.

Consegnati i dati, o superati i sessanta giorni successivi alla cessazione del servizio, Systems Srl è assolta 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 vengono rimossi dai sistemi di Systems Srl in modalità sicura.

Torna al sommario

8. IL SISTEMA DI CONSERVAZIONE

Il sistema è realizzato attraverso componenti logiche, componenti tecnologiche e componenti fisiche. Il rispetto del sistema allo standard ISO 14721: OAIS Open Archival Information System lo si può trovare nella distinzione e gestione di questi tre tipi di pacchetti informativi:

- SIP o pacchetto di versamento: è un contenitore costituito dal documento digitale o l'insieme dei documenti digitali, corredati da tutti i metadati descrittivi, versati dal soggetto produttore nel sistema di conservazione.
- AIP o pacchetto di archiviazione: è un pacchetto informativo derivato dal pacchetto di versamento (SIP o PdV), che può contenere al suo interno uno o più SIP. L'AIP ha un insieme completo di informazioni sulla conservazione che si aggiungono al file di metadati
- DIP o pacchetto di distribuzione: è la terza tipologia di pacchetto informativo, che può contenere al suo interno il singolo documento digitale o l'insieme di documenti digitali, corredati dai metadati previsti, inviati tramite SIP e conservati sotto forma di un AIP. Questo è finalizzato alla presentazione e alla distribuzione dei documenti conservati

In termini generali, il modello di riferimento OAIS definisce le componenti logiche comuni a tutti e tre i pacchetti informativi sopra descritti. Il modello dati utilizzato dal sistema di conservazione prevede una strettissima aderenza a tale modello concettuale rivisitandolo ed ampliandolo con elementi di contestualizzazione provenienti dalla tradizione archivistica italiana.
Inoltre l'obiettivo del sistema di conservazione è quello di garantire non solo la gestione e la conservazione dell'insieme informativo e descrittivo del singolo documento (o collezione di documenti, nell'accezione OAIS, in riferimento all' 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 informatico di riferimento.

L'attuale sistema di conservazione implementato da Systems Srl si basa sulla struttura dello standard ISO 14721: OAIS Open Archival, ma non solo: ad esso integra le regole tecniche del DPCM 3 dicembre 2013 per quanto riguarda un sistema inerente alla normativa sulla conservazione a norma, che conservi, oltre ai documenti ed ai fascicoli informatici anche i metadati e le informazioni sul contesto degli stessi, un fattore molto importante per permettere la ricostruzione del vincolo archivistico, cioè mantenere in conservazione tutte quelle relazioni tra documenti che vanno a formare l'archivio del soggetto produttore.

Il soggetto produttore invia i documenti all'"Ingest", rappresentato dalla nostra API e da servizi di elaborazione interna dei documenti. Questa li accetta, li valida, li elabora e li prepara per una loro memorizzazione. L'"Archival Storage" è l'elemento che si assicura che i files vengano

memorizzati correttamente e si preoccupa inoltre di gestire l'accesso ad essi. Questo assicura lo storage del file, effettuando dei controlli di integrità sul contenuto, prima di salvare il file su un supporto fisico. Il "Data Management", invece, è caratterizzato da tutte quelle informazioni di supporto, per la gestione e l'accesso ai documenti che sono salvate in un database.
"L'"Administration" ha come scopo principale quello di coordinare operativamente il funzionamento delle altre unità funzionali. Questo si preoccupa anche di definire policy di accesso ai dati e di effettuare dei report per le verifiche sul corretto funzionamento del sistema di conservazione. Il "Preservazion Planning", invece, è costituito da tutte quelle verifiche e tutti quei controlli, che abbiamo definito, atti a limitare al minimo possibile l'obsolescenza dei dati conservati nonché monitora i cambiamenti e i requisiti della Comunità Designata. L'"Access" è un insieme di servizi che rendono visibili i contenuti dell'archivio, quindi gestisce gli accessi per utenti e i gruppi al sistema di conservazione.

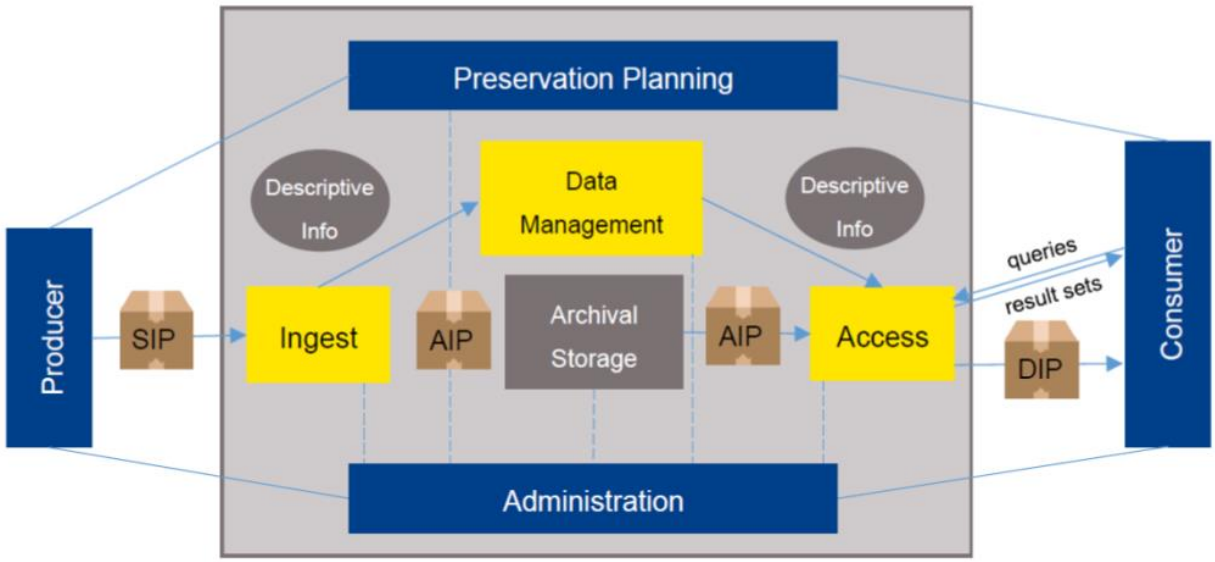

Figura 6: OAIS - Preservation planning schema

Torna al sommario

8.1. Componenti Logiche

L'architettura logica del sistema di conservazione è basata su componenti applicative distinte su quattro livelli principali:

- Sistema di versamento (SV)
- Sistema di gestione Dati (SGD)
- Sistema di memorizzazione (SM)
- Sistema di autenticazione e accesso (SAA).

Sistema di versamento (SV)

Il sistema di versamento rappresenta la porta con cui i documenti vengono immessi nel sistema. Questa componente ha il compito di raccogliere tutti i documenti da inviare in conservazione e verifica anche la loro aderenza al contratto di servizio di conservazione e ai requisiti di conservazione.

Le possibilità di caricamento avvengono tramite:

- Browser: il produttore usa il portale web della *Systems Business Suite* per inviare più documenti al sistema di versamento. Nell'interfaccia Web ha la possibilità di inserire manualmente per singolo documento i relativi metadati previsti secondo la definizione dei metadati a disposizione per singolo tipo documento. Inviando i documenti al sistema di conservazione si può poi in un secondo momento visualizzare il rapporto di versamento.
- API: è possibile inviare i documenti attraverso software terzi che utilizzano la *Systems Business Suite* REST-API. È possibile:
  - Aprire un SIP, indicando in formato Json tutti metadati dei singoli documenti (ricevendo una GUID del Pacchetto)
  - Inviare singoli file associati al SIP aperto (attraverso un collegamento GUID del pacchetto)
  - Chiudere un SIP (attraverso GUID del pacchetto), si ottiene il relativo rapporto di versamento, una volta che il sistema ha verificato il pacchetto ed ha effettuato gli opportuni controlli.

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

- le caratteristiche minime che la documentazione deve possedere per poter essere accettata in ingresso

- i metadati di ciascun "pacchetto di 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:

- tecnologiche: riferite ai singoli oggetti digitali
- archivistiche: che comprendono i metadati di contesto.

Le caratteristiche tecnologiche riguardano esclusivamente i documenti digitali e possono riferirsi, ad esempio, al formato con cui sono stati prodotti.
Le caratteristiche archivistiche possono riguardare, ad esempio, le interconnessioni di un documento con altri, come è stato inviato e come potrebbe essere raccolto all'interno di un fascicolo.
Una volta ricevuto, ogni singolo documento deve superare i controlli di qualità, assicurati dal processo di convalida, questo 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

Una volta che i documenti hanno superato i controlli di qualità previsti, sistema di versamento dovrà applicare le regole previste dal *preservation planning* per costruire i pacchetti di versamento a partire dai documenti inviati dal soggetto produttore.
L'accesso al documento informatico viene gestito sfruttando la gestione dei diritti associati al singolo utente che appartiene ad uno o più produttori (=Cliente).

Il sistema di versamento aggiunge ai dati ricevuti dal produttore una serie di dati aggiuntivi:

- Data e ora di ricezione del documento (per mostrare quando il produttore ha inviato al conservatore tale documento per avere con certezza la data da quale in poi è possibile per il conservatore conservare tale documento. Così si dà evidenza se un produttore invia al conservatore un documento informatico dove sono scaduti termini per legge, che questa mancanza è stata causata dal produttore dei dati.)
- Data di eliminazione del documento (viene calcolato attraverso la "data documento" ricevuto nei metadati da parte del produttore + il periodo di conservazione definito per tipo documento nell'allegato tecnico del contratto)
- Utente e Sistema Applicativo dell'utente (viene memorizzato quale utente con quale sistema applicativo ha inserito i relativi documenti)

Il risultato della convalida è riepilogato da un esito in formato Json, nominato “rapporto di versamento”. Tale rapporto di versamento contiene:

- Riferimento Tempo UTC
- Impronta del Pacchetto di Versamento (riferito al file indice allegato)
- File riassuntivo dei metadati dei documenti ricevuti (contiene anche tutti dati aggiunti in automatico dal sistema di versamento)
- Hash relativo al pacchetto di versamento

Nel caso questo rapporto sia generato e riconsegnato dal sistema di versamento, il processo termina correttamente. In caso di errore viene restituita la descrizione dello stesso, in modo che l’utente possa provvedere a sistemare i documenti in errore e rinviarli
Un SIP che contiene un errore, ad esempio su un singolo documento, non può essere terminato con successo ma va in errore e deve essere rinviato dal cliente. Se un SIP non viene chiuso correttamente in 24 ore dalla sua creazione, entra in uno stato di errore. Qualsiasi pacchetto ricevuto in errore, non sarà poi conservato.

Sistema di gestione dati (SGD)
Il sistema di gestione dati che ha il compito di gestire le informazioni legate al contesto archivistico e alle descrizioni dei documenti. Questo macro-componente è in pratica il collante dell'intero sistema, il motore su cui si basa tutto il processo della conservazione.
Il sistema di gestione dati è il cuore archivistico del sistema ed è la componente che consente di avere una visione unitaria dell'archivio e quindi consente di accedervi. Il sistema di gestione dati ha una duplice valenza: da una parte offre servizi al sistema di accesso per consentire le ricerche e la navigazione e, dall'altra, consente al soggetto 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 è ritenuta la componente essenziale per consentire ad un soggetto produttore di gestire al meglio il proprio deposito digitale. Il soggetto produttore attraverso questo modulo, potrà vedere l'archivio come il complesso sistema di relazioni che in effetti è e, tramite le funzionalità che esso offre, potrà compiere tutte quelle operazioni tipicamente archivistiche, necessarie per la gestione di un archivio (di deposito).
Per esempio, il sistema di gestione dati, grazie alla propria particolare concezione, permette di gestire al meglio lo scarto del materiale documentario non destinato alla conservazione permanente, ma caratterizzato invece da tempi di conservazione limitati e diversificati.

In caso di una PA, come soggetto produttore, questa è tenuta a verificare le proprie specifiche richieste sulla base dei propri strumenti archivistici (quali ad esempio il proprio piano di classificazione e di conservazione) attraverso i quali può identificare le forme di classificazione più inerenti alle proprie necessità. In caso di tipologie documentali non incluse nel sistema di

conservazione, sarà possibile effettuare una richiesta di conservazione per queste tipologie, o per nuovi formati, così come definito nell'allegato tecnico.

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 come la leggibilità, l'integrità, il valore legale, l'obsolescenza del formato e la possibilità di applicare la procedura di scarto dei documenti per cui ormai è stato superato il termine di conservazione. 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 rispettiva fase e, verificandone preventivamente l'affidabilità, provvederà a gestirne lo stoccaggio. 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.

Sistema di autenticazione e accesso (SAA)

Il modulo per la gestione degli accessi orchestra il flusso di informazioni e servizi necessari per fornire le funzionalità di accesso al cosiddetto "consumer" ovvero all'utente che ha la necessità di accedere ad un determinato documento. A seguito di una ricerca impostata dall'utente il modulo di gestione accesso richiede i risultati della ricerca al sistema di gestione dati che, organizzando le informazioni descrittive degli AIP, è in grado di rispondere alla richiesta; l'utente, una volta individuato il documento desiderato, (o i documenti, o addirittura un intero fascicolo o volume di conservazione) potrà inoltrare una richiesta di accesso ai dati, questa genererà la richiesta al modulo di generazione *Dissemination Information Package* (DIP)il quale interagendo sia con il sistema di gestione dati che con il sistema di memorizzazione recupererà le informazioni necessarie (AIP e informazioni descrittive) per produrre DIP corrispondente alla richiesta. Inoltre, il sistema di conservazione, 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 dal software di conservazione è regolato anche da un sottosistema di autorizzazione che permette di definire un numero illimitato di utenti, associabili a uno o più produttori. Per ogni utente, è possibile anche limitare l'accesso a un insieme limitato di tipi di documento. Con queste

combinazioni di accesso, è possibile controllare in maniera molto sottile, gli accessi ai documenti del sistema di conservazione.

Sistema di 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'indice di conservazione (UNI 11386) del AIP, 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 del software di utilizzare qualunque dispositivo di firma digitale, dato che le eventuali differenze nell'implementazione vengono mascherate dal sottosistema stesso. Resta l'obbligo che la firma digitale, in questo contesto relativa al responsabile del servizio di conservazione ed eventualmente anche ad un pubblico ufficiale (o ruolo equivalente), deve essere apposta utilizzando un dispositivo di firma di un tipo approvato da AgID ed un certificato rilasciato da una Certification Authority (CA) appartenente all'elenco dei certificatori accreditati presso AgID.
Il sistema di conservazione sfrutta il servizio di Certification Authority di Namirial.

Sistema per l'apposizione della 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 accreditato. In linea di massima le TSA coincidono con le Certification Authority e questo servizio è offerto on-line utilizzando protocolli di comunicazione standard. Il sistema è in grado di richiedere in modo automatico ed on-line la marca temporale alle TSA utilizzate nel sistema.
Per i servizi di marca temporale il soggetto conservatore si avvale di Namirial.

Torna al sommario

8.2. Componenti Tecnologiche

L'architettura del sistema di conservazione è basata su una soluzione multilivello a 3 livelli:

- Presentation layer
- Business layer
- Data layer.

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

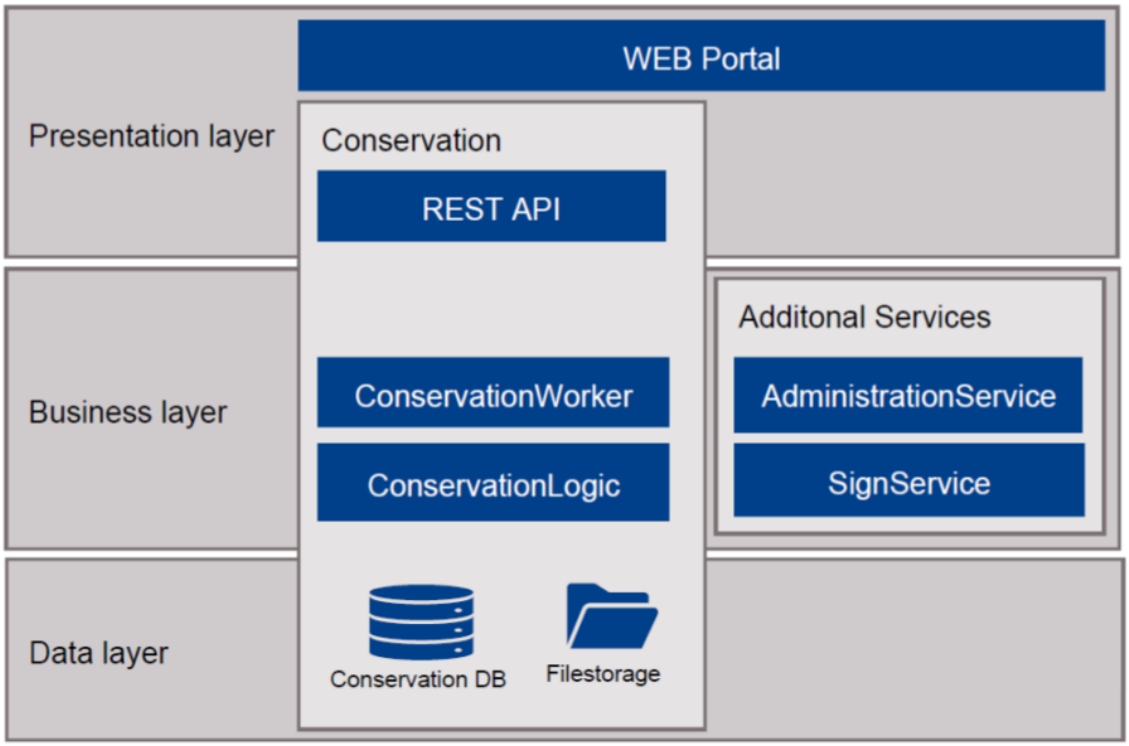

Figura 7: Architettura del Sistema di Conservazione

Presentation layer

- WEB Portal: è un'applicazione realizzata come single page application con framework Angular che garantisce la compatibilità con un larga parte degli attuali browser senza la necessità di installare ulteriori plug-in sul client. La parte di amministrazione delle utenze e produttori è fatta in tecnologia Webratio basata su Java-Server-Pages. Per scalare l'applicazione di frontend è installata su piú application server per rendere l'applicativo altamente disponibile. Il servizio è pubblicato per gli utenti solo attraverso protocolli sicuri https.
  I dati del frontend vengono popolati attraverso la REST API descritta di seguito.
- Conservation REST APIs: sono un insieme di servizi web che permettono, ad applicazioni di terze parti e al WEB Portal, di versare documenti nel sistema di

conservazione o di interrogarne lo stato. I dati vengono erogati in formato Json e solo a utenti autorizzati ed autenticati. Il servizio è pubblicato per gli utenti solo attraverso protocolli sicuri https.

Business layer

- ConservationWorker: è il motore che esegue la creazione e verifica dei vari pacchetti richiesti degli utenti o attraverso logiche automatiche usando la ConservationLogic.
- ConservationLogic: rappresenta il core della logica applicativa e l'interfaccia verso il data layer, il signservice e i vari servizi amministrativi a cui l'applicazione attinge, come descritto di seguito. La comunicazione con i servizi amministrativi e il sign service avviene attraverso Rest-API interni.
- AdministrationService: rappresenta diversi servizi d'aiuto, che servono per gestire l'autenticazione, l'autorizzazione e la configurazione del servizio di conservazione. Il servizio è pubblicato per gli utenti solo attraverso protocolli sicuri https.
- SignService: Questo servizio si occupa dell'applicazione della firma digitale del responsabile del sistema di conservazione, come firma automatica delegata, e marca temporale attraverso il servizio di Namirial SPA. Questo servizio è visibile solo internamente.

Data layer

- Conservazion DB: Database che contiene tutti i metadati sui pacchetti e i suoi documenti associati, e la connessione con il file storage. Oltre questo viene anche memorizzato il riferimento al produttore per singolo pacchetto e documento.
- File storage: archivio dei file fisici sottoposti alla conservazione a norma.

Torna al sommario

8.3. Componenti Fisiche

L'infrastruttura per il servizio di conservazione si basa su un sito operativo e due datacenter di Systems:

Collocazione	Descrizione
Sede Operativa di Systems	Si tratta del sito dove è operativo il Team di sviluppo software, gestione operativa del Team IT-Operation e del Team Service Desk
Sito Primario	Il datacenter primario virtuale eroga il servizio di conservazione e ospita tutti sistemi che sono necessari per il servizio. Il sistema e composto da tre macro-elementi che sono: ➢ Systema produttivo ➢ Systema di Test ➢ Frontend-Security-Services
Sito Secondario	Il datacenter secondario virtuale di disaster recovery è predisposto per erogare il servizio di conservazione e ospita tutti sistemi che per il servizio sono necessari, continuamente replicati dal sito primario, per essere attivati nel caso di un disastro. Questo sistema è composto da i due macro-elementi essenziali, che sono: ➢ Systema produttivo ➢ Frontend-Security-Services

Le figure sottostanti schematizzano l'infrastruttura virtuale ospitata nella server farm:

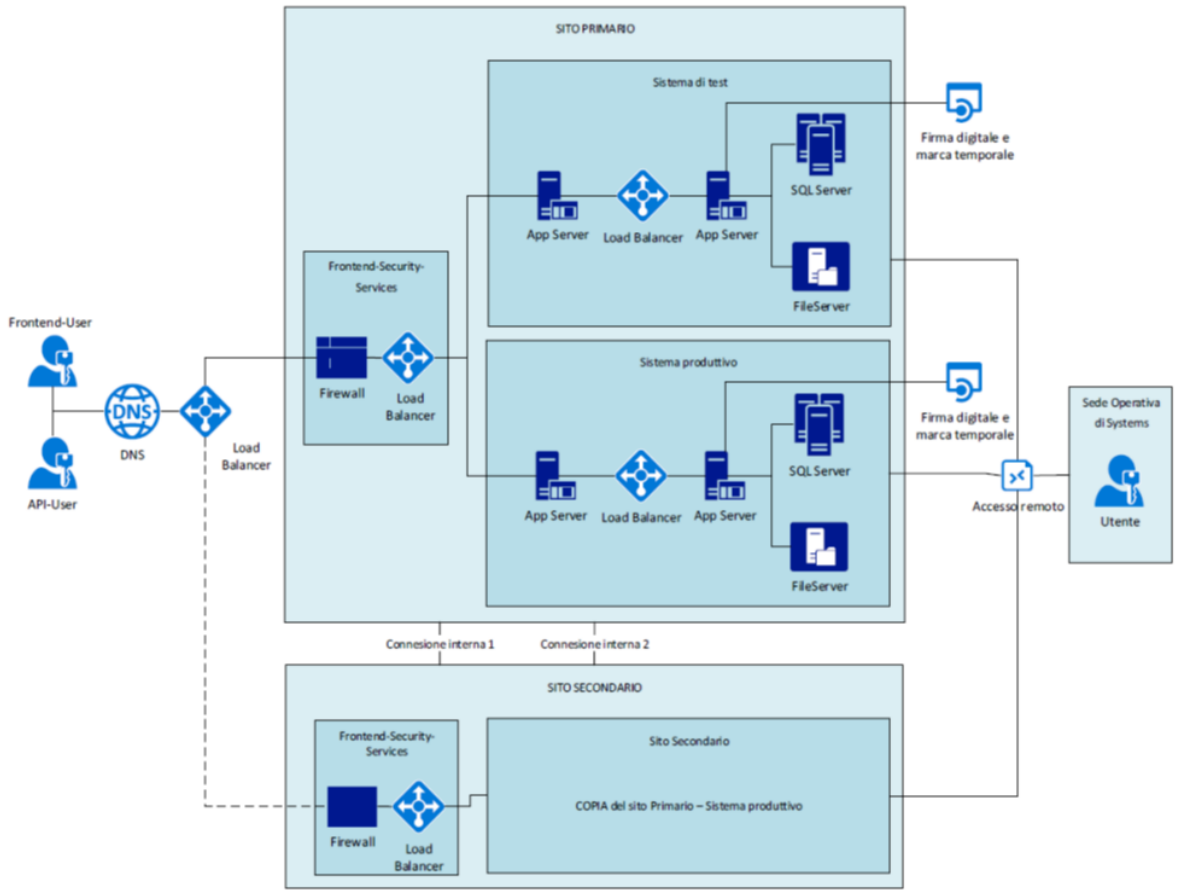

Figura 8: Schema dell'architettura del sistema di conservazione

L'architettura virtuale applicata, per quanto concerne la piattaforma Conservazione a norma, mediante duplicazione fisica e virtuale dei singoli componenti dell'infrastruttura, al fine di garantire la tolleranza ai guasti e l'eliminazione dei single point of failure, è strutturata a livelli e realizzata,

- con connessioni internet ridondanti per ogni sito, banda sufficiente per coprire anche elevati volumi e interconnessioni dedicati, high speed tra i due datacenter
- per proteggere i sistemi di front-end da Internet e dalle reti interne mediante l'utilizzo di una rete DMZ protetta da due livelli di firewalling distinti composta da sistemi ridondati di Loadbalancing, Enterprise Firewalling e Application-delivery-Controller
- l'infrastruttura virtuale è composta da virtual LAN dedicate, virtual Server, Database Server, File-Server, diversi Application Server, sistemi di security e Backup
- Il Management-System è composto da servizi di monitoring, management dei server e dei singoli servizi

Il sistema virtuale adottato è composto in maniera da garantire una scalabilità di ogni risorsa in funzione di aumenti del carico derivante dalla crescita del numero dei documenti e degli utenti da elaborare.

Per un maggior dettaglio dei sistemi di sito primario si rimanda alla copia del piano per la sicurezza.

Torna al sommario

8.4. Procedure di gestione e di evoluzione

Il change management del software e dell'hardware viene eseguito secondo la seguente descrizione. Qualsiasi change viene registrato negli appositi sistemi come previsto secondo il Piano della Sicurezza e le procedure aziendali dell' ISO 27001.
Systems, con il supporto di tutte le strutture aziendali ha provveduto ad implementare un sistema di governo con lo scopo di:

- Garantire la riservatezza, integrità e leggibilità dei documenti
- Garantire i requisiti del sistema in conformità alla normativa vigente
- Manutenzione del servizio
- Monitorare i livelli di sicurezza
- Gestire operativamente eventuali incidenti, prevenzione, gestione della comunicazione in emergenza

Manutenzione del sistema di conservazione

I requisiti di sicurezza per la manutenzione del sistema di conservazione, delle politiche di incident manamgent e della continuità operativa del servizio di conservazione sono specificati e riportati nel piano della sicurezza e nella documentazione del sistema di gestione della sicurezza.

Per la soluzione software della Systems Business Suite viene mantenuto un sistema di code-repository che permette di tornare in qualsiasi momento ad ogni versione software, alle info di che cosa è stato modificato nel codice sorgente, per quale motivo (=Change richiesto) e da chi è stato approvato e testata la modifica. Cosi viene garantito si riesca a risalire ad una qualsiasi condizione software nel passato, attiva nel momento della conservazione di un determinato documento.

Systems mette a disposizione per i soggetti produttori autorizzati, l'assistenza tramite team di Help Desk. Secondo i processi interni aziendali vengo presi in carico le richieste dei richiedenti ed elaborate secondo le relative responsabilità associate.

Gestione e conservazione dei Log

Il software della conservazione a norma tiene traccia di ogni operazione, chiamata, eventi del sistema. Nel dettaglio viene tenuto traccia di:

- Log degli accessi
- Log applicativi
- Log di processo
- Log di sicurezza
- Log del sistema di monitoraggio

I log del software sono disponibili nei livelli di gravità Fatal, Error, Warn e Info e vengono archiviati per un periodo di 3 mesi.
Oltre questo viene memorizzato su ogni tipo di pacchetto e singolo documento lo storico con i seguenti dati:

- In caso di processi eseguiti dall'utente:
  - Utente che ha salvato il relativo documento/pacchetto
  - Applicativo dell'utente che ha salvato il relativo documento/pacchetto
  - Riferimento temporale
  - Riferimento al Produttore come proprietario del dato
- In caso di processi automatici:
  - Stato del processo
  - Riferimento temporale
  - Riferimento al pacchetto elaborato
  - Tale informazione viene mantenuta per l'intero periodo di conservazione del singolo documento.

Monitoraggio del sistema di conservazione

Attraverso un applicativo staccato dal principale software di conservazione viene monitorato qualsiasi dettaglio in merito ai processi in corso, eventuali errori, problemi infrastrutturali attraverso numerosi sensori.
In caso di errori, tali problemi vengono segnalati al Responsabile del servizio di conservazione, attraverso un sistema di ticketing interno, che, attraverso il team dedicato al software di conservazione, opera secondo le relative priorità nel sistemare eventuali errori entro i tempi definiti.
Maggiori dettagli si possono trovare nel Piano di sicurezza e nel capitolo 9 del presente documento.

Change management

Il Change management del software è definito all'interno secondo la relativa procedura nell' ISO 27001. Un Software Change potrebbe avvenire da una richiesta di un utente (presa in carico attraverso sistema di ticketing) o attraverso esigenze interne.
Ogni esigenza viene documentata nel sistema di documentazione dei software Changes, sulla base del quale il team di sviluppo esegue le modifiche del codice. È possibile seguire il processo di software change a partire dalla singola richiesta fino all'effettivo rilancio.
In questo modo è garantito che ogni modifica nel codice sia tracciata e giustificabile attraverso il collegamento della sua richiesta descritta nel sistema di documentazione dei software Changes.

Verifica periodica di conformità normativa e standard di riferimento

Ogni semestre viene effettuato un riesame generale del sistema di conservazione a norma. Tale verifica viene effettuata dal Responsabile del servizio di Conservazione in collaborazione della squadra incaricata nell'organigramma per la conservazione.
In tale riesame vengono verificati:

- miglioramenti necessari causa richieste da legge o tecnologia
- miglioramenti necessari causa incidenti o disservizi gravi

Con periodicità almeno annuale il Responsabile del servizio di Conservazione pianifica degli audit interni che coinvolgono aspetti normativi, di processo, organizzazione e tecnologici.
Oltre questo vengono eseguiti degli audit per migliorare il sistema di monitoraggio automatico per garantire, ad esempio, la corretta funzione dei processi di conservazione, la gestione delle anagrafiche e dei diritti, nonché la corretta applicazione di firma e marca etc.

Torna al sommario

9. MONITORAGGIO E CONTROLLI

Sul sistema di conservazione viene effettuata la seguente attività di monitoraggio e controllo:

- monitoraggio sul funzionamento del software e dei virtual datacenter.
- verifica di integrità degli archivi
- verifica di leggibilità dei documenti

Dalla sede principale vengono svolte tutte le attività operative necessarie alla gestione, al mantenimento. Vengono eseguiti dei controlli automatici del sistema usato per garantire il corretto funzionamento del sistema di conservazione.
In caso di anomalia, il sistema usato per il monitoraggio informa, attraverso un processo definito, il responsabile di conservazione per fare in modo che possa intervenire ed definire delle soluzioni, sempre nell'ambito dei processi definiti all'interno del sistema di conservazione.
Per maggiori informazioni sul sistema di monitoraggio del sistema di conservazione, sui dispositivi e processi in uso rimandiamo al Piano della Sicurezza del sistema di conservazione di Systems.

Torna al sommario

9.1. Procedure di monitoraggio

Oltre al sistema di monitoraggio automatico, che informa i relativi responsabili attraverso il sistema di ticketing, l'amministratore ha una serie di ulteriori strumenti per verificare lo stato del sistema di conservazione, per gestire le anomalie ed eventuali errori riconosciuti. In ogni caso, se si dovessero presentare delle anomalie non riconosciute dal sistema di monitoraggio automatico, verrebbe applicato un processo di miglioramento per trovare delle strategie, per permettere che l'anomalia non si ripresenti più e se si dovesse ripresentare viene comunque esteso il sistema di monitoraggio per automatizzare la verifica di eventuale anomalie future.

Strumenti di verifica dedicati ad utenti amministrativi

Stato dei sensori del sistema di monitoraggio:

Un utente amministratore ha sempre la possibilità di verificare lo stato di tutti singoli sensori che verificano il corretto funzionamento dell'infrastruttura e dei processi per avere una panoramica generale sulla situazione del sistema di conservazione.

Monitoraggio dei log:

Un utente amministratore ha la possibilità di visualizzare la panoramica dei log con delle dashboard, per capire, ad esempio, la quantità di errori per periodo, la quantità di richieste al sistema di conservazione e la velocità media di elaborazione delle richieste.

Sulla base di un certo input (ad esempio utente finale richiede problematica su un singolo documento) si ha la possibilità di ricercare i log secondo questi parametri esemplificativi (nel dettaglio dipende ovviamente dal tipo di processo e operazione eseguita):

- Nome utente della richiesta
- Applicativo dell'utente richiedente
- Data e ora richiesta
- Tipo di operazione effettuata
- Dettagli sull'operazione (eventuale)
- Indicazioni su identificativo pacchetto e identificativo documento (eventuale)
- Indicazione dell'identificativo del processo (per poter ricostruire l'intero processo attraverso un singolo dato di log)

Stato dei processi:

Un utente amministratore ha la possibilità di verificare lo stato dei processi sui singoli pacchetti elaborati e quelli in elaborazione attraverso la piattaforma web. Si rende quindi disponibile, la possibilità di verificare eventuali situazioni non già segnalate dal sistema automatico di monitoraggio.

Torna al sommario

9.2. Verifica dell'integrità degli archivi

Nella fase di memorizzazione del file viene verificata la corrispondenza per ogni documento tra l'impronta ricevuta dal produttore e quella effettiva, ricalcolata al momento del controllo di integrità.
In caso di "non corrispondenza" l'intero pacchetto viene scartato con delle note specifiche, per permettere al produttore di sistemare queste anomalie.
Una volta salvato correttamente il documento, il sistema è in grado di ri-verificare questa corrispondenza attraverso dei processi automatizzati.
Gli intervalli del processo di verifica automatico sono dimensionati secondo il volume dei documenti presenti nel sistema di conservazione e la durata del processo stesso. Sulla base di questi risultati, il responsabile di conservazione verifica, con le persone di competenza, se la durata dei backup disponibili, per poter, in caso di anomalia, ritornare alla situazione precedente, sia sufficiente per ritornare allo stato in cui il file era ancora integro.
Su ogni documento presente nel sistema di conservazione viene effettuato almeno un controllo all'anno sulla sua integrità.
Per ogni verifica viene generato un log apposito nel sistema di conservazione, in modo da capire sempre quando è stata fatta l'ultima verifica da parte di un utente amministratore.

Torna al sommario

9.3. Soluzioni adottate in caso di anomalie

Systems metta a disposizione ai clienti un servizio di Service Desk disponibile tra lunedì a venerdì. Gli orari sono concordati nel contratto di affidamento del servizio.
Per ogni modalità di contatto (Mail, Telefono…) il team di Serivce Desk, presso la sede di Systems, genera un ticket con un numero univoco per tracciare sempre l'intera comunicazione in merito alla segnalazione dell'utente finale.
Le anomalie segnalate dal sistema di monitoraggio automatico vengono inviate al team di Service Desk tramite ticket con id univoco.

Anomalie dovute a bug del software

Una volta segnalata l'anomalia e valutata dal responsabile dell'area Software-Development - Supporto e Manutenzione, gestione Operativa, viene risolta con le priorità secondo la definizione di Software-Changes dell'ISO 27001.
Di seguito la definizione dei vari livelli di criticità dell'anomalia:

Criticità	Criterio	Presa in carico
Critical	Funzioni centrali del sistema sono totalmente bloccati. Più di 10 utenti saranno bloccati dall'anomalia entro lo stesso giorno	2 ore lavorative
High	Piú di 10 utenti sono bloccati o in contatto con l'anomalia nei prossimi 5 giorni	4 ore lavorative
Medium	Piú di 10 utenti sono bloccati o in contatto con l'anomalia nelle prossime due settimane o gli utenti non sono bloccati nelle funzioni principali del servizio di conservazione	8 ore lavorative
Low	Non piú di 10 utenti sono bloccati o in contatto con l'anomalia nei prossimi due mesi. O l'anomalia esiste solo nel sistema di Backend	16 ore lavorative

I numeri indicati nella colonna del "criterio" hanno solo compito di indicare al team di Service Desk un valore misurabile per classificare in maniera semplice il problema.

Anomalie dovute a malfunzionamento dell'impianto

Attività	Livelli di servizio	% di applicazione
Elaborazione dei pacchetti di versamento	Entro il giorno lavorativo successivo (festivi esclusi) dalla ricezione del pacchetto di versamento	99,5% dei pacchetti di versamento
Comunicazione di eventuali anomalie nei pacchetti di versamento ricevuti	Immediatamente dopo corretta ricezione dei del pacchetto di versamento	99,5% dei pacchetti di versamento
Invio ai clienti della segnalazione di errori che causano blocco della creazione dei pacchetti di archiviazione	Entro il giorno lavorativo successivo (festivi esclusi) dalla ricezione del pacchetto di versamento	99,5% dei pacchetti di versamento
Disponibilità del servizio di caricamento	Vedi condizioni contrattuali	-
Disponibilità del servizio di consultazione	Vedi condizioni contrattuali	-

Eventuali condizioni da parte del produttore e del conservatore qui non elencati sono riportati nel contratto di affidamento servizio.

Torna al sommario

10. INDICE DELLE FIGURE