Allegato 5

MANUALE DI CONSERVAZIONE

REGISTRO DELLE VERSIONI

N° VERSIONE	DATA	NOMINATIVO	MODIFICHE APPORTATE	VERIFICATO	APPROVATO	DATA
1	20/12/2020	Laura Degani	Redazione	Emanuela Del Ross	Decreto del Direttore Generale n. 254/2021	Prot. n. 18414 del.20/12/2021

SOMMARIO

1. SCOPO E AMBITO DEL DOCUMENTO

Il manuale di conservazione dei documenti digitali, come previsto dal documento AgID 2020 “Linee Guida sulla formazione, gestione e conservazione dei documenti informatici”, è uno strumento operativo che descrive e disciplina il modello organizzativo della conservazione adottato e descrive i criteri adottati dall’INRIM per la conservazione di:

- documenti informatici;
- documenti amministrativi informatici con i metadati ad essi associati;
- fascicoli con i metadati ad essi associati;
- aggregazioni documentali informatiche con i metadati ad essi associati.

A questi documenti vengono garantiti le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità come indicato dal d.lgs. 07/03/2005 n° 82 -Codice dell'amministrazione digitale (CAD)- nel quale, per la predisposizione di un sistema di conservazione per documenti informatici, vengono stabiliti i seguenti requisiti:

a) Identificazione certa del soggetto che ha formato il documento e dell'amministrazione o dell'area organizzativa omogenea di provenienza;

b) Integrità del documento;

c) Leggibilità ed agevole reperibilità dei documenti e delle informazioni identificative, inclusi i dati di registrazione e di classificazione originari.

Il rispetto delle misure di sicurezza dei dati, contenuti nei documenti conservati, sono adeguate ai sensi del decreto legislativo 30 giugno 2003, n. 196, integrato con le modifiche introdotte dal D. lgs. 10 agosto 2018, n. 101, recante “Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)” (in G.U. 4 settembre 2018 n.205) e dal disciplinare tecnico pubblicato nell’allegato B al d.lgs. del 07/03/2005 n.82.

Il processo di conservazione dell’INRiM, descritto nel presente manuale, è organizzato in conformità alle regole tecniche per la predisposizione e la gestione di un sistema di conservazione nel quale vengono definiti:

- i dati dei soggetti che nel tempo hanno assunto la responsabilità del sistema di conservazione
- la struttura organizzativa dei diversi soggetti che intervengono nel processo di conservazione ed i ruoli
- la descrizione delle tipologie degli oggetti digitali sottoposti a conservazione, comprensiva dell’indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di oggetti
- la descrizione delle modalità di presa in carico di uno o più pacchetti di versamento, e della predisposizione del rapporto di versamento

- la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione
- la modalità di svolgimento del processo di esibizione e la produzione del pacchetto di distribuzione
- la descrizione del sistema di conservazione, comprensivo di tutte le componenti tecnologiche, fisiche e logiche
- la descrizione delle architetture ed infrastrutture utilizzate, delle misure di sicurezza adottate e delle procedure di monitoraggio della funzionalità del sistema di conservazione
- la descrizione delle procedure per la produzione di duplicati o copie, le modalità con cui viene richiesta la presenza di un pubblico ufficiale, le normative in vigore nei luoghi dove sono conservati gli oggetti digitali.

Il presente Manuale di Conservazione è stato revisionato e verificato dal Responsabile della gestione documentale (che all'INRiM è coincidente con il Responsabile della Conservazione) e descrive 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, organizzato conformemente alle regole emanate da AgID, seguendo lo schema distributivo dal *Modello di Manuale di Conservazione* – versione 1.0 del 9 marzo 2017 – redatto dal Gruppo di lavoro Procedamus.

La redazione del Manuale di conservazione contempera l'assolvimento dell'obbligo normativo con le esigenze concrete dell'Ente (Produttore dei dati) che ha stipulato un accordo con il Consorzio Interuniversitario CINECA (Conservatore dei dati) per l'affidamento in outsourcing del processo di conservazione, previsto con gli accordi: "Convenzione relativa ai servizi informatici inerenti a sistemi informativi per l'Istituto Nazionale di Ricerca Metrologica: aree funzionali Contabilità, Risorse umane, Gestione documentale, Ricerca, Pianificazione e controllo", prot. n. 0002525 del 05/07/2016.

Le attività del processo di conservazione sono descritte facendo riferimento al manuale di conservazione del conservatore, in accordo alle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici emanate dall'AgID.

2. TERMINOLOGIA

Di seguito si riporta il glossario dei termini contenuti nelle regole tecniche di cui all'articolo 71 del d.lgs. 07/03/2005 n° 82 e delle sue successive modificazioni e integrazioni in materia di documento informatico e sistema di conservazione dei documenti informatici che si aggiungono alle definizione del citato decreto ed a quelle del decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445 e successive modificazioni e integrazioni.

2.1. Glossario

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

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

Affidabilità: caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico.

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

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

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

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

Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico: dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.

Base di dati: collezione di dati registrati e correlati tra loro.

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

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

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

Codice: decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni.

Codice eseguibile: insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici.

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

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

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

Copia analogica del documento informatico: documento analogico avente contenuto identico a quello del documento informatico da cui e tratto.

Destinatario: identifica il soggetto/sistema al quale il documento informatico e indirizzato.

Disponibilità richiesta: tempo in cui il sistema deve essere utilizzabile in conformità alle funzionalità previste, esclusi i tempi programmati per la manutenzione, rispetto alle ore concordate per l'esercizio.

Duplicazione dei documenti informatici: produzione di duplicati informatici.

Esibizione: operazione che consente di visualizzare un documento conservato e di ottenerne copia.

Estratto per riassunto: documento nel quale si attestano in maniera sintetica ma esaustiva fatti, stati o qualità desunti da dati o documenti in possesso di soggetti pubblici.

Evidenza informatica: una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.

Formato: modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente e identificato attraverso l'estensione del file.

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

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

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

Funzione di hash: una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.

Generazione automatica di documento informatico: formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni.

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

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

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

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

Insieme minimo di metadati del documento informatico: complesso dei metadati, la cui struttura è descritta nell'allegato al DPR 37/2001, atti a identificarne provenienza e natura e a garantirne la tenuta.

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

Interoperabilità: capacita di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi

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

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

Manuale di Conservazione: strumento che descrive il sistema di conservazione dei documenti informatici, come prescritto dal § 4.6 del documento AgID - Linee Guida sulla formazione, gestione e conservazione dei documenti informatici-.

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

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

Metadati: insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme e descritto nell'Allegato 5 del documento AgID 2020 - Linee Guida sulla formazione, gestione e conservazione dei documenti informatici-.

Obiettivo temporale di recupero (Recovery Point Objective): indica la perdita dati tollerata: rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di un evento imprevisto.

Pacchetto di archiviazione: pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nelle norme UNI 11386 - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali-.

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

Pacchetto di versamento: pacchetto informativo inviato dal Produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione.

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

Periodo criticità servizio: data/periodo in cui il dato o il servizio deve essere tassativamente erogato per esigenze specifiche del business, quali scadenze o presentazione dei dati.

Piano della sicurezza del sistema di conservazione: documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza.

Piano di conservazione: strumento, integrato con il sistema di classificazione per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R 28 dicembre 200, n.445.

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

Presa in carico: accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione.

Processo di conservazione: insieme delle attività finalizzate alla conservazione dei documenti informatici di cui al documento AgID 2020 - Linee Guida sulla formazione, gestione e conservazione dei documenti informatici-.

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

Rapporto di versamento: documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal Produttore.

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

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

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

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

Responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi: dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre n. 445, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione.

Responsabile della conservazione: dirigente o funzionario interno alla PA, il responsabile della conservazione opera secondo quanto previsto dall'art. 44, comma 1-quater del CAD e mette in atto le attività elencate nel §4.5 del documento AgID 2020 - Linee Guida sulla formazione, gestione e conservazione dei documenti informatici-.

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

Responsabile della sicurezza: soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza.

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

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

Sistema di classificazione: strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata

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

Sistema di gestione informatica dei documenti: nell'ambito della pubblica amministrazione e il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445; per i privati e il sistema che consente la tenuta di un documento informatico.

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

Tempo ripristino richiesto (Recovery Time Objective): tempo entro il quale un processo informatico ovvero il sistema informativo primario deve essere ripristinato dopo un disastro o una condizione di emergenza (o interruzione), al fine di evitare conseguenze inaccettabili.

Transazione informatica: particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche della base di dati.

Testo unico: decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni

Titolare del trattamento (data controller): è "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali" (art. 4. par. 1, n. 7 GDPR)

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

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

Versamento agli archivi di stato: operazione con cui il Responsabile della conservazione di una PA 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.Abbreviazioni

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

AIPA: Agenzia per l'Informatica nella Pubblica Amministrazione

ASP: Application Service Provider

CA: Certification Authority

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

CAS: Content-Addressed Storage

DLGS: Decreto Legislativo

DM: Decreto Ministeriale

DPCM: Decreto del Presidente del Consiglio dei Ministri

DPR: Decreto del Presidente della Repubblica

FE: Firma Elettronica

FEA: Firma Elettronica Avanzata

FEQ: Firma Elettronica Qualificata

FD: Firma Digitale

GU: Gazzetta Ufficiale della Repubblica Italiana

MEF: Ministero dell'Economia e delle Finanze

PA: Pubblica Amministrazione

3. Normativa e standard di riferimento

3.1. Contesto Normativo

Il sistema di conservazione digitale è stato redatto secondo le normative vigenti sulla conservazione dei documenti informatici:

- **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** – "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi"

- **DPR 28 dicembre 2000, n. 445**, e successive modificazioni - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa- (TUDA)

- **Decreto legislativo 30 giugno 2003, n. 196**, e successive modificazioni, recante -Codice in materia di protezione dei dati personali- **Decreto legislativo 22 gennaio 2004, n. 42**, e successive modificazioni, recante "Codice dei beni culturali e del paesaggio"

- **DPR 11 febbraio 2005, n. 68** - Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3

- **Decreto legislativo 7 marzo 2005, n. 82** - Codice dell'amministrazione digitale o CAD

- **Circolare n. 5/d Agenzia delle dogane del 25 gennaio 2005** - D.M. 23/1/2004 recante "Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di supporto"

- **Circolare dell'Agenzia delle Entrate n. 45/E del 19 ottobre 2005** - Decreto legislativo 20 febbraio 2004, n. 52; attuazione della direttiva 2001/115/CE che semplifica ed armonizza le modalità di fatturazione in materia di IVA

- **Circolare dell'Agenzia delle Entrate n. 36/E del 6 dicembre** 2006 - Decreto ministeriale 23 gennaio 2004; Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici e alla loro riproduzione in diversi tipi di supporto

- **Risoluzione Agenzia delle entrate n. 298 del 18 ottobre 2007** - Istanza di interpello, articolo 11 legge 27 luglio 2002, n. 212, - Conservazione su supporti informatici delle copie delle dichiarazioni da parte dei CAF - Adempimenti correlati e termine per l'invio dell'impronta dell'archivio informatico

- **Risoluzione n. 349 Agenzia delle entrate del 28 novembre 2007** - IVA - biglietto di trasporto elettronico - articolo 1 del decreto ministeriale 30 giugno 1992 Istanza di interpello -ART.11, legge 27 luglio 2000, n. 212

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

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

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

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

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

- **Regolamento ISVAP n. 27 del 14 ottobre 2008** -Tenuta dei registri assicurativi

- **Provvedimento Agenzia delle entrate del 25 ottobre 2010** - Provvedimento attuativo ella comunicazione dell'impronta relativa ai documenti informatici rilevanti ai fini tributari, ai sensi dell'articolo 5 del decreto 23 gennaio 2004

- **L. 22 dicembre 2011, n. 214.** Conversione in legge, con modificazioni, del decreto-legge 6 dicembre 2011, n. 201, recante disposizioni urgenti per la crescita, l'equità e il consolidamento dei conti pubblici

- **Decreto legge 24 gennaio 2012, n. 1** - Estratto – Dematerializzazione Contrassegni Assicurativi

- **Circolare n. 5/E Agenzia delle entrate del 29 febbraio 2012** - Quesiti riguardanti la comunicazione dell'impronta relativa ai documenti informatici rilevanti ai fini tributari, ai sensi dell'articolo 5 del decreto 23 gennaio 2004 e del provvedimento del Direttore dell'Agenzia delle Entrate del 25 ottobre 2010

- **Decreto del Ministro dell'Economia e delle Finanze 3 aprile 2013, n. 55**, Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'art. 1, commi da 209 a 213, della legge 24 dicembre 2007, n. 244

- **Decreto Legge 22 giugno 2012, n. 83**, convertito con Legge 7 agosto 2012, n. 134, Misure urgenti per la crescita del Paese

- **Decreto del Presidente del Consiglio dei Ministri 21 marzo 2013**, Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da

altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni

- **Circolare MEF del 31 marzo 2014 n. 1/DF** – Circolare interpretativa del DECRETO 3 aprile 2013, n. 55 - Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'articolo 1, commi da 209 a 213, della legge 24 dicembre 2007, n. 244

- **Decreto del Ministero dell'Economia e delle Finanze del 17 giugno 2014** – Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto – articolo 21, comma 5, del decreto legislativo n. 82/2005. (Ministero dell'economia e delle finanze) – in vigore dal 27.06.2014

- **Circolare Agenzia delle Entrate del 24 giugno 2014 n. 18/E** - OGGETTO: IVA. Ulteriori istruzioni in tema di fatturazione

- **Regolamento UE n. 910/2014 -** eIDAS Regulation - Identification and trusted services for electronic transactions in the internal market

- **Circolare AGID 10 aprile 2014, n. 65** - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82

- **Decreto del Ministro dell'Economia e delle Finanze 17 giugno 2014**, Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - art. 21, comma 5, del decreto legislativo n. 82/2005

- **Circolare dell'Agenzia delle Entrate 24 giugno 2014, n. 18/E**, IVA. Ulteriori istruzioni in tema di fatturazione

- **Decreto Legislativo 5 agosto 2015, n. 127**- Trasmissione telematica delle operazioni IVA e di controllo delle cessioni di beni effettuate attraverso distributori automatici, in attuazione dell'art. 9, comma 1, lettere d) e g), della legge 11 marzo 2014, n. 23

- **Risoluzione dell'Agenzia delle Entrate 25 settembre 2015, n.81/E, Interpello - ART.11, legge 27 luglio 2000, n. 212** – Comunicazione del luogo di conservazione in modalità elettronica dei documenti rilevanti ai fini tributari, art. 5 D.M. 17 giugno 2014

- **Decreto Legislativo 7 gennaio 2016, n. 2 -** Attuazione della **direttiva 2014/60/UE** relativa alla restituzione dei beni culturali usciti illecitamente dal territorio di uno Stato membro e che modifica il regolamento (UE) n. 1024/2012

- **Regolamento dell'Unione Europea (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 ditali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

- **Direttiva dell'Unione Europea (UE) 2016/680 del Parlamento Europeo e del Consiglio del 27 aprile 2016** relativa alla Protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio

- **Decreto Legislativo 12 maggio 2016, n. 90**, Completamento della riforma della struttura del bilancio dello Stato, in attuazione dell'art. 40, comma 1, della legge 31 dicembre 2009, n. 196

- **Decreto Legislativo 26 agosto 2016, n. 179**, Modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'art. 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche

- **Linee Guida dell'Agenzia per l'Italia Digitale – AgID - 9 settembre 2020 -** Linee Guida sulla formazione, gestione e conservazione dei documenti informatici

3.2. Riferimenti tecnici

Il sistema di conservazione digitale fa riferimento ai sottoelencati decreti ministeriali:

- **DPR del 28 dicembre 2000, n. 445** – Disposizioni legislative in materia di documentazione amministrativa

- **Decreto del 2 novembre 2005 – MIT** – Regole tecniche per la formazione, la trasmissione e la validazione anche temporale della posta elettronica certificata

- **DPR 633/1972** art.39 in vigore dal 1 gennaio 2013 –Modificato da: Legge del 24/12/2012 n. 228

  Art. 1 – Le fatture elettroniche in formato elettronico e quelle cartacee possono essere conservate elettronicamente

- **DPCM del 22 febbraio 2013** - Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali

- **DPCM del 3 dicembre 2013** - Regole tecniche per il protocollo informatico (limitatamente a: art. 2 comma 1; art. 6; art. 9; art. 18 commi 1 e 5; art. 20; art. 21)

- **D.lgs. del 7 marzo 2005, n.82** e successive modificazioni (14 settembre 2016) – Codice dell'Amministrazione Digitale (CAD)

3.3. Istruzioni, Linee Guida e documentazione informativa

- **Istruzioni dell'Agenzia per l'Italia Digitale – AgID - marzo 2015**, Produzione e conservazione del registro giornaliero di protocollo

- **Linee Guida dell'Agenzia per l'Italia Digitale – AgID - dicembre 2015,** Linee Guida sulla conservazione dei documenti informatici

- **Linee Guida dell'Agenzia per l'Italia Digitale – AgID - 26 aprile 2016**, Linee Guida per la sicurezza ICT delle Pubbliche Amministrazioni – Misure minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del Presidente del Consiglio dei Ministri 1° agosto 2015)

- **European Commission, working party on the protection of individuals with regard to the processing of personal data set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,** Guidelines on Data Protection Officers ('DPOs') Adopted on 13 December 2016

- **European Commission, working party on the protection of individuals with regard to the processing of personal data set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995**, Guidelines on the right to data portability Adopted on 13 December 2016

- **Linee Guida del Garante per la protezione dei dati personali 2 marzo 2011, n. 088 del registro dei provvedimenti,** Linee Guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web

- **Linee Guida del Garante per la protezione dei dati personali, 4 aprile 2013, n. 161 del registro dei provvedimenti**, Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach)

- **Linee Guida del Garante per la protezione dei dati personali, 15 maggio 2014 n. 243 del registro dei provvedimenti**, Linee Guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati

- **Scheda informativa del Garante per la protezione dei dati personali, 17 marzo 2016**, Scheda informativa sulla figura del Responsabile della protezione dei dati personali (Data Protection Officer)

- **Guida informativa del Garante per la protezione dei dati personali, giugno 2016**, Prima guida informativa al Regolamento europeo 2016/679 in materia di protezione dei dati personali

3.4. Standard di Riferimento

Il sistema di conservazione digitale dell'INRiM è stato realizzato in conformità agli standard di riferimento, di seguito riportati, elencati nell'Allegato 4 al documento AgiD 2020 - Linee Guida sulla formazione, gestione e conservazione dei documenti informatici.

Per la gestione documentale

- **UNI ISO 15489-1** - Informazione e documentazione - Gestione dei documenti di archivio - Principi generali sul record management

- **UNI ISO 15489-2** -Informazione e documentazione - Gestione dei documenti di archivio – Linee Guida sul record management

- **ISO/TS 23081-1** - Information and documentation - Records management processes – Metadata for records – Part 1 – Principles, Quadro di riferimento per lo sviluppo di un sistema di metadati per la gestione documentale

- **ISO/TS 23081-2** - Information and documentation - Records management processes – Metadata for records – Part 2 – Conceptual and implementation issues, Guida pratica per l'implementazione

- **ISO 16175-1** - (ICA) Information and documentation -- Principles and functional requirements for records in electronic office environments -- Part 1: Overview and statement of principles

- **ISO 16175-2** - (ICA) Information and documentation -- Principles and functional requirements for records in electronic office environments -- Part 2: Guidelines and functional requirements for digital records management systems

- **ISO 16175-3** - (ICA) Information and documentation -- Principles and functional requirements for records in electronic office environments -- Part 3: Guidelines and functional requirements for records in business system

- **ISO 15836** - Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core

- **ISO 9001** – Sistemi di gestione per la qualità – Requisiti

- **ISO 30300:2011** Information and documentation - Management systems for records - Fundamentals and vocabulary

- **ISO 30301:2011** Information and documentation - Management systems for records – Requirements

- **ISO 30302:2015** Information and documentation - Management systems for records - Guidelines for implementation

- **ISO/TR 23081-3 -** Information and documentation — Managing metadata for records — Part 3: Self-assessment method

- **MoReq 2001** Model requirements for the management of electronic records

- **MoReq 2** Specification 2008 Model requirements for the management of electronic records – che individua i requisiti funzionali della gestione documentale

- **MoReq2010** Modular requirements for records systems

3.5 Normativa per la conservazione digitale

- **UNI 11386** - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali

- **ISO 14721** - OAIS (Open Archival Information System), Sistema informativo aperto per l’archiviazione

- **ISO 15836** - Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core
- **ISO/TR 18492** - Long-term preservation of electronic document-based information
- **ISO 20652** - Space data and information transfer systems - Producer-Archive interface Methodology abstract standard
- **ISO 20104** - Space data and information transfer systems — Producer-Archive Interface Specification (PAIS)
- **ISO/CD TR 26102** - Requirements for long-term preservation of electronic records
- **SIARD** Software Independent Archiving of Relational Databases 2.0
- **Ministère de la culture et de la communication**, Service interministériel des Archives de France, Standard d'échange de donnéès pour l'archivage. Transfert – Communication – Élimination – Restitution - Modification, ver. 2.1, 2018
- **METS -** Metadata Encoding and Transmission Standard
- **PREMIS –** PREservation Metadata: Implementation Strategies
- **EAD (3)/ISAD (G)**
- **EAC (CPF)/ISAAR (CPF)/NIERA (CPF)**
- **SCONS2/EAG/ISDIAH**

3.6 Affidabilità (certificazione/valutazione e autovalutazione)

- **ISO 16363** - Space data and information transfer systems -- Audit and certification of trustworthy digital repositories
- **ISO 16919** - Space data and information trans:fer systems -- Requirements for bodies providing audit and certification of candidate trustworthy digital repositories
- **ISO 17068** - Information and documentation -- Trusted third party repository for digital records 2.1 per Sicurezza informatica
- **ISO/IEC 27001** - Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- **ISO/IEC 27017** - Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services;

- **ISO/IEC 27018** - Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors;

- **ETSI TS 101 533-1 V1.2.1** - 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 V1.2.1** - 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.

4. MODELLO ORGANIZZATIVO PER IL SISTEMA DI CONSERVAZIONE: RUOLI E RESPONSABILITÀ

4.1 Il modello organizzativo

Il sistema di conservazione delle unità documentarie informatiche e delle unità archivistiche Informatiche, prevede la collaborazione tra unità organizzative dell'Ente e il Consorzio Interuniversitario CINECA, quale soggetto esterno cui INRiM ha affidato il coordinamento del processo di conservazione in base all'accordo indicato al Capitolo 1, nel quale sono definite le condizioni generali di fornitura dei servizi; il documento è integrato dagli *Accordi di versamento* nel quale sono descritte le tipologie documentali, i tempi di versamento e conservazione, i formati e i metadati descrittivi utili a garantire una corretta interazione tra Produttore e Conservatore.

In virtù di tale affidamento del servizio di conservazione, il Conservatore si impegna alla conservazione dei documenti trasferiti e ne assume la funzione di Responsabile del servizio di conservazione ai sensi della normativa vigente, garantendo il rispetto dei requisiti previsti dalle norme in vigore nel tempo per i Sistemi di conservazione, che opera secondo quanto previsto dall'art. 44, comma 1-quater, del CAD[1] e svolge l'insieme delle attività individuate ed elencate nel paragrafo 4.5 del documento AgID « Linee Guida sulla formazione, gestione e conservazione dei documenti informatici».

Il versamento in conservazione dei documenti informatici gestiti dalle articolazioni amministrative dell'INRiM è effettuato con procedura automatizzata, su impostazione del Responsabile della gestione documentale e della conservazione; tale modalità di invio non preclude la possibilità di invio manuale delle tipologie documentali oggetto degli accordi.

[1] L'art. 44, comma 1-quater, del CAD prevede che: "Il responsabile della conservazione, che opera d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei sistemi informativi, può affidare, ai sensi dell'articolo 34, comma 1-bis, lettera b), la conservazione dei documenti informatici ad ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative, e tecnologiche e di protezione dei dati personali.

4.2. Organigramma

Nella Figura 1 sono rappresentate le Unità Organizzative dell'INRiM; nella Figura 2 è rappresentato l'organigramma per il sistema di conservazione del Consorzio Interuniversitario CINECA [2]

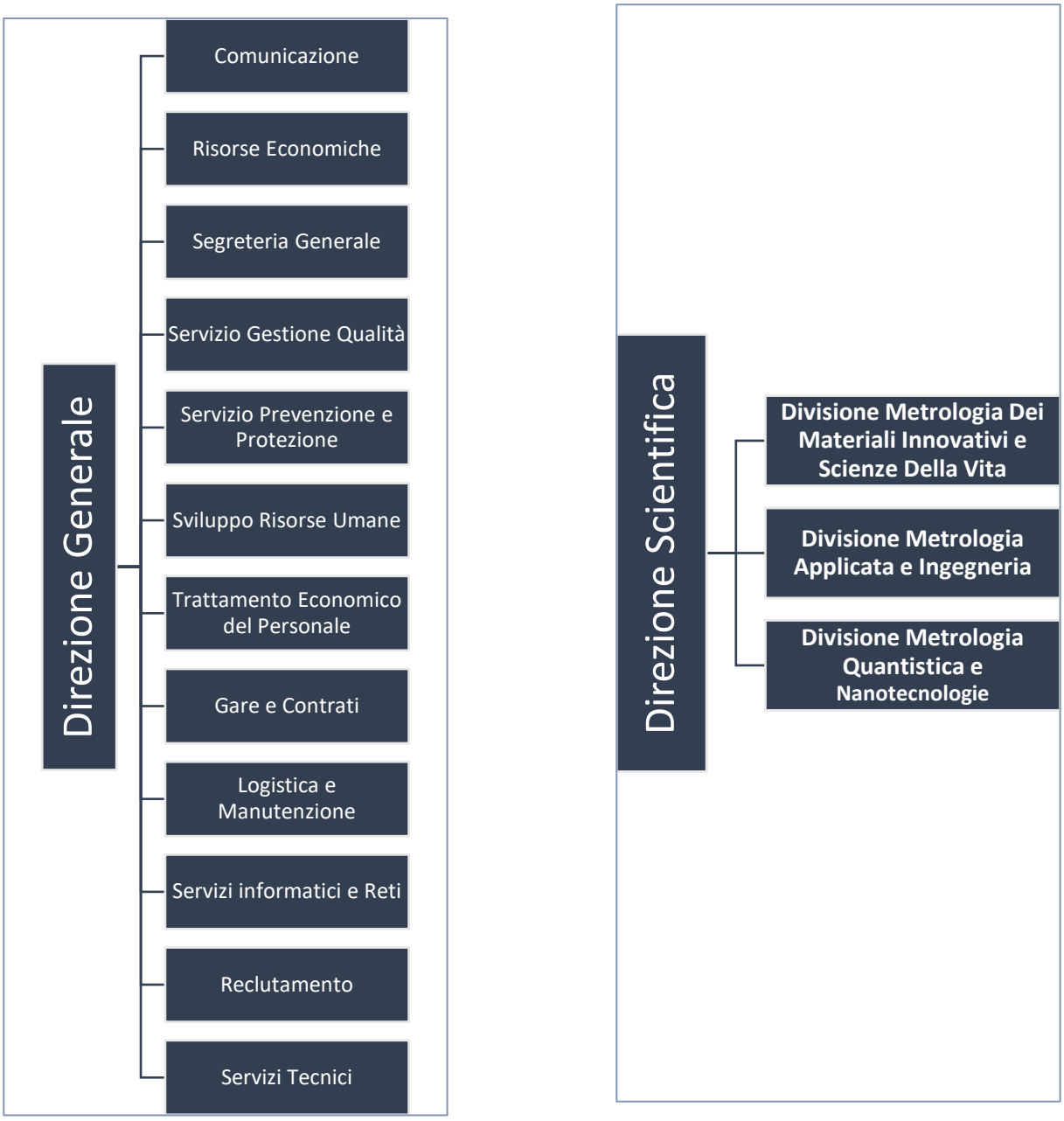

Figura 1. Organigramma delle unità organizzative dell'INRiM

[2] file:///C:/Users/Utente/Desktop/INRIM%20lavoro/Manuale%20di%20conservazione/Normativa/manualediconservazione-cineca_rev1_9pdfsigned.pdf

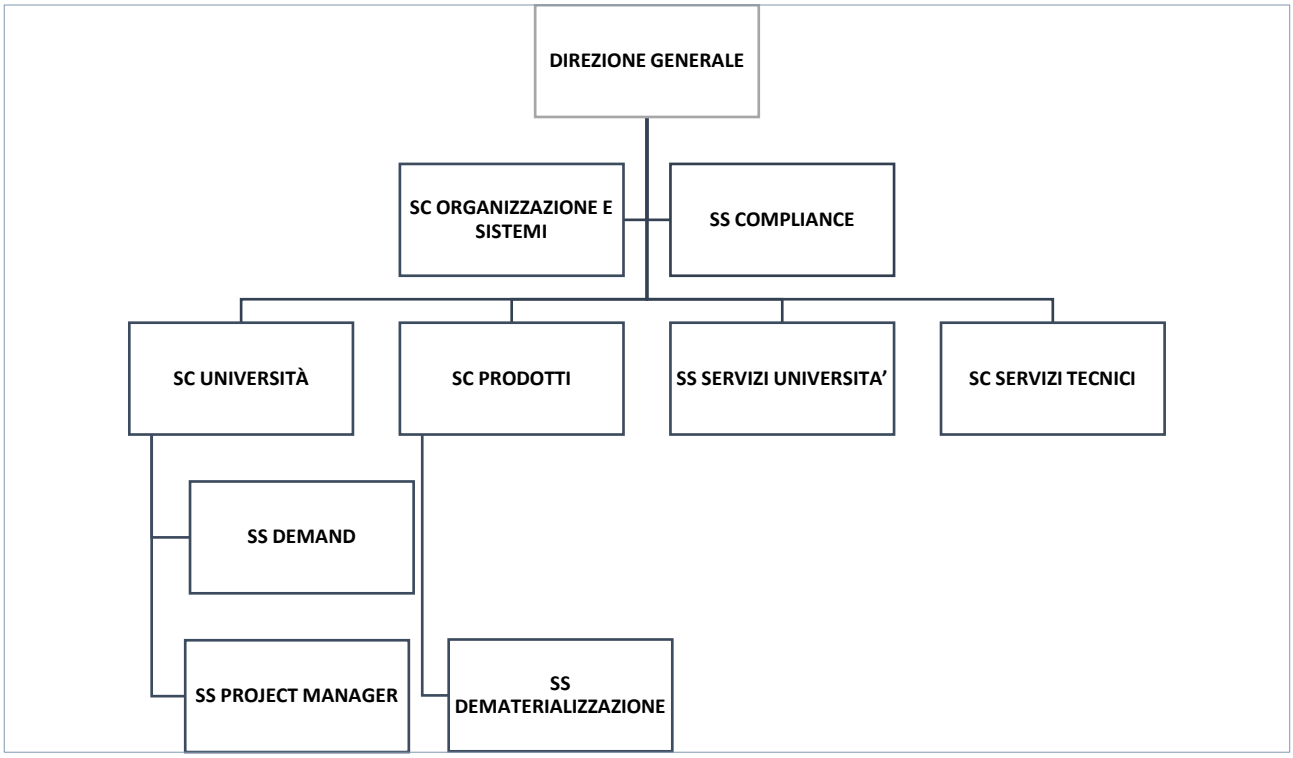

Figura 2 Organigramma Aziendale per il sistema di conservazione del Consorzio Interuniversitario CINECA, a cui l'Ente affida il servizio di conservazione. L'Immagine è tratta da: file:///C:/Users/Utente/Desktop/INRIM%20lavoro/Manuale%20di%20conservazione/Normativa/manualediconservazione-cineca_rev1_9pdfsigned.pdf

4.3. Ruoli e Responsabilità

Il documento AgID 2020 *Linee Guida sulla formazione, gestione e conservazione dei documenti informatici* individua i ruoli coinvolti nel processo di conservazione, di seguito descritti.

4.3.1. Produttore del pacchetto di versamento (PdV) e utente abilitato.

Nelle Pubbliche Amministrazioni il Responsabile della gestione documentale o il Coordinatore della gestione documentale, ove nominato, svolge il ruolo di Produttore di PdV; è persona interna alla struttura organizzativa e assicura la trasmissione del pacchetto di versamento al sistema di conservazione nelle modalità e con i formati concordati con il conservatore.

Il Produttore di PdV provvede, inoltre, a verificare il buon esito della operazione di trasferimento al sistema di conservazione tramite la presa visione del rapporto di versamento prodotto dal sistema di conservazione stesso.

L'utente abilitato, in particolare può richiedere al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge e nelle modalità previste dal manuale di conservazione.

4.3.2. Responsabile della Conservazione

Il responsabile della conservazione opera secondo quanto previsto dall'art. 44, comma 1-quater, del CAD[3].

Nella Pubblica Amministrazione, il Responsabile della conservazione:

a) è un ruolo previsto dall'organigramma del Titolare dell'oggetto di conservazione;

b) è un dirigente o un funzionario interno formalmente designato e in possesso di idonee competenze giuridiche, informatiche ed archivistiche;

c) può essere svolto dal responsabile della gestione documentale o dal coordinatore della gestione documentale, ove nominato.

Il Responsabile della conservazione definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.

Il Responsabile della conservazione, sotto la propria responsabilità, può delegare lo svolgimento delle proprie attività o parte di esse a uno o più soggetti che, all'interno della struttura organizzativa, abbiano specifiche competenze ed esperienze.

Tale delega deve individuare le specifiche funzioni e competenze delegate.

In particolare, il Responsabile della conservazione:

a) definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;

b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;

c) genera e sottoscrive il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;

d) genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;

e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;

[3] L'art. 44, comma 1-quater, del CAD prevede che: "Il responsabile della conservazione, che opera d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei sistemi informativi, può affidare, ai sensi dell'articolo 34, comma 1-bis, lettera b), la conservazione dei documenti informatici ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative, e tecnologiche e di protezione dei dati personali. Il responsabile della conservazione della pubblica amministrazione, che opera d'intesa, oltre che con i responsabili di cui al comma 1-bis, anche con il responsabile della gestione documentale, effettua la conservazione dei documenti informatici secondo quanto previsto all'articolo 34, comma 1-bis".

f) effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;

g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;

h) provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;

i) predispone le misure necessarie per la sicurezza fisica e logica del sistema di conservazione;

j) assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;

k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;

l) provvede per le amministrazioni statali centrali e periferiche a versare i documenti

4.3.3. Responsabilità del servizio di conservazione

Il Responsabile del servizio di conservazione si occupa delle politiche complessive del Sistema di conservazione e ne determina l'ambito di sviluppo e le competenze.

Il Conservatore, Consorzio Interuniversitario CINECA, quale erogatore del sistema di conservazione, in virtù dell'incarico descritto al Cap.1 e al §4.1, individua all'interno della propria struttura organizzativa i seguenti profili professionali:

- Responsabile del servizio di conservazione;
- Responsabile della funzione archivistica di conservazione;
- Responsabile della protezione dei dati personali;
- Responsabile della sicurezza dei sistemi per la conservazione;
- Responsabile dei sistemi informativi per la conservazione;
- Responsabile dello sviluppo e della manutenzione del sistema di conservazione

In particolare, secondo la Convenzione in atto, il Consorzio Interuniversitario Cineca, quale Conservatore esterno dei dati, si impegna a:

- nominare gli incaricati del trattamento e gli eventuali amministratori di sistema, di database e di software complesso e fornire loro dettagliate istruzioni operative;

- verificare, almeno annualmente, la sussistenza delle condizioni per la conservazione dei profili di autorizzazione assegnati agli incaricati del trattamento;

- conservare e mantenere aggiornato, in base a quanto prescritto nel provvedimento del 27/11/2008 del Garante (Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni della funzioni di amministratore di sistema) e successive modifiche, gli estremi identificativi (nome, cognome, area organizzativa di appartenenza) delle persone fisiche preposte quali amministratori di sistema/database /software complesso;

- verificare l'operato degli amministratori di sistema/database/software complessi nominati con una cadenza almeno annuale, al fine di controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali;

- comunicare all'INRiM, quale Titolare del trattamento, i nominativi degli incaricati e degli amministratori di sistema/database/software complesso;

- assicurare la predisposizione e aggiornamento di un sistema di sicurezza dei dati, in conformità con le misure minime prescritte nel D.lgs. 196/2003 e successivi

4.3.4. Organismi di tutela e di vigilanza

Gli archivi e i singoli documenti prodotti dagli enti pubblici sono considerati beni culturali e sottoposti, pertanto, alle disposizioni di tutela previste dal Codice dei beni culturali e del paesaggio, Decreto Legislativo 22 gennaio 2004, n. 42, art. 10, comma 2, lett. b).

Garantire la tutela di archivi e singoli documenti si concreta negli obblighi conservativi previsti nell'art. 30 del predetto Decreto Legislativo che comporta, infatti, "l'obbligo di conservare i propri archivi nella loro organicità e di ordinarli. I soggetti medesimi hanno altresì l'obbligo di inventariare i propri archivi storici"

Il rispetto delle disposizioni in ordine alla corretta conservazione è in capo al Ministero dei Beni e delle Attività Culturali e del Turismo, attraverso la Direzione generale archivi e, in particolare, alla Soprintendenza archivistica e bibliografica del Piemonte e della Valle d'Aosta. Tale ente, infatti, è investito del potere di vigilanza e ispezione ai sensi degli artt. 18 e 19 del Codice dei beni culturali e del paesaggio.

Per quanto riguarda il sistema di conservazione di dei documenti sottoposti a tutela, la Soprintendenza Archivistica e Bibliografica del Piemonte e della Valle d'Aosta verifica, in particolare, che il processo di conservazione avvenga in modo conforme alla normativa e ai principi di corretta e ininterrotta custodia.

L'importanza della corretta conservazione degli archivi che si intende adottare comprende, altresì la conservazione dell'ordine di aggregazione dei documenti (per non perdere l'organizzazione e il carattere di complesso unitario dell'archivio) e l'elencazione degli interventi soggetti ad autorizzazione, lo spostamento degli stessi, sia temporaneo che di eventuale "trasferimento ad altre persone giuridiche di complessi organici di documentazione di archivi pubblici".

Il sistema di conservazione CONSERVA di Cineca, descritto nel Capitolo 7, è sottoposto alla vigilanza di AgID che prevede la materiale conservazione dei dati e delle copie di sicurezza sul territorio nazionale e l'accesso ai dati presso la sede del Produttore.

4.3.5. Gestione del sistema di conservazione

Si rimanda al manuale di Conservazione, Consorzio Interuniversitario Cineca, reperibile sul sito AgID[4], dove sono dettagliati l'organigramma e la struttura organizzativa del Conservatore.

4.3.6. Pubblico ufficiale

Il Responsabile della conservazione assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento (cfr.§ 6.3.1), garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;

[4] https://www.agid.gov.it/sites/default/files/repository_files/manualediconservazione-cineca_rev1_9pdfsigned.pdf

4.3.7. Registro dei Responsabili

Vengono qui riportati i nominativi che rivestono i ruoli previsti dalla normativa in merito al servizio di conservazione.

Registro dei Responsabili del Consorzio Interuniversitario CINECA:

Nomine 2016	Ruolo
	Responsabile dello sviluppo e della manutenzione del sistema di
	Responsabile della funzione archivistica di conservazione
	Responsabile del servizio di conservazione
	Responsabile dei sistemi informativi per la conservazione
	Responsabile del trattamento dei dati personali
	Responsabile della sicurezza dei sistemi per la conservazione

Nomine 2018	Ruolo
Massimiliano Valente	Responsabile dello sviluppo e della manutenzione del sistema di
Laura Federica Nisi	Responsabile della funzione archivistica di conservazione
Riccardo Righi	Responsabile del servizio di conservazione
Angelo Neri	Responsabile dei sistemi informativi per la conservazione
David Vannozzi	Responsabile del trattamento dei dati personali
Paola Tentoni	Responsabile della sicurezza dei sistemi per la conservazione

Nomine	Ruolo
	Responsabile dello sviluppo e della manutenzione del sistema di
	Responsabile della funzione archivistica di conservazione
	Responsabile del servizio di conservazione
	Responsabile dei sistemi informativi per la conservazione
	Responsabile del trattamento dei dati personali
	Responsabile della sicurezza dei sistemi per la conservazione

Nomine	Ruolo
	Responsabile dello sviluppo e della manutenzione del sistema di
	Responsabile della funzione archivistica di conservazione
	Responsabile del servizio di conservazione
	Responsabile dei sistemi informativi per la conservazione
	Responsabile del trattamento dei dati personali
	Responsabile della sicurezza dei sistemi per la conservazione

Registro dei Responsabili INRiM:

Nominativo	Periodo nel ruolo	Ruolo	Deleghe	Ambiti oggetto della delega
		Responsabile della gestione documentale		
Paola Casale	Dal 2016 al 2020	Responsabile della Conservazione	Rosella Corsi	Operare nell'Archivio di deposito CONSERVA
Anna Galletti	Dal 2016	Responsabile della protezione dei dati personali		

Nominativo	Periodo nel ruolo	Ruolo	Deleghe	Ambiti oggetto della delega
	Dal 2020	Responsabile della gestione documentale	Laura Degani	Redazione del Manuale di gestione e dei suoi allegati.
Emanuela Del Ross	Dal 2020	Responsabile della Conservazione	Rosella Corsi, Laura Degani	Operare nell'Archivio di deposito CONSERVA
Silvia Misirocchi	Dal 18 nov. 2021	Responsabile della Protezione Dati (Data Protection Officer)		

Nominativo	Periodo nel ruolo	Ruolo	Deleghe	Ambiti oggetto della delega
		Responsabile della gestione documentale		
		Responsabile della Conservazione		
		Responsabile della Protezione Dati (Data Protection Officer)		

Nominativo	Periodo nel ruolo	Ruolo	Eventuali deleghe	Ambiti oggetto della delega
		Responsabile della gestione documentale		
		Responsabile della Conservazione		
		Responsabile della Protezione Dati (Data Protection Officer)		

5. OGGETTI SOTTOPOSTI A CONSERVAZIONE

5.1. Documenti informatici e aggregazioni documentali

Le aggregazioni di documenti informatici o di fascicoli informatici sono l'insieme definito e qualificato di documenti 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.

Il sistema di conservazione acquisisce, gestisce, organizza e conserva documenti informatici, in particolare documenti amministrativi informatici e le loro aggregazioni documentali informatiche sotto forma di fascicoli e serie, descritti nei seguenti paragrafi.

Il passaggio del documento dal sistema di gestione al sistema di conservazione consente il mantenimento delle caratteristiche del documento di immodificabilità, integrità e staticità, così come deve essere mantenuto il legame significante del documento con il fascicolo, al fine di preservare e tramandare per il periodo necessario il valore giuridico probatorio, amministrativo e storico, così come definito dal Codice dell'amministrazione digitale all'art. 1, lettera p); l'art 23 ter del CAD specifica la particolare categoria di documento informatico rappresentata dal documento amministrativo informatico ribadendone la natura di informazione primaria e originale. Lo stesso art. 23-ter riassume le azioni che è possibile effettuare sul documento amministrativo informatico con uno specifico richiamo alle regole tecniche previste all'art. 71[5].

Il sistema di gestione informatica dei documenti opera sui documenti amministrativi con le modalità descritte nel *Manuale di gestione dei flussi documentali e del protocollo informatico* dell'INRiM.

5.1.1 Documenti informatici

Il documento amministrativo informatico è prodotto e memorizzato su di un supporto elettronico durante lo svolgimento di un'attività di carattere amministrativo e, grazie al Sistema di gestione corrente, in cui è stato inserito al momento dell'acquisizione, possiede le opportune caratteristiche di immodificabilità, integrità e staticità, come previsto dalla normativa vigente; infatti, una volta inserito nel Sistema di gestione, il documento è sottoposto a una serie di azioni (es. protocollazione o registrazione a sistema, classificazione, attribuzione al Responsabile del procedimento, attribuzione al fascicolo etc.) che ne determinano la

[5] Le regole tecniche sono raccolte nel documento AgID 2020 "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, che sostituisce:

- il DPCM 13 novembre 2014, contenente "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici";
- la circolare n. 60 del 23 gennaio 2013 dell'AgID in materia di "Formato e definizione dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le Pubbliche Amministrazioni"
- il DPCM 3 dicembre 2013, contenente "Regole tecniche in materia di sistema di conservazione".
- il DPCM 3 dicembre 2013, contenente "Regole tecniche per il protocollo informatico", fatte salve le seguenti:
  - art. 2 comma 1, Oggetto e ambito di applicazione;
  - art. 6, Funzionalità;
  - art. 9, Formato della segnatura di protocollo;
  - art. 18 commi 1 e 5, Modalità di registrazione dei documenti informatici; • art. 20, Segnatura di protocollo dei documenti trasmessi;
  - art. 21, Informazioni da includere nella segnatura.

posizione logica all'interno dell'archivio così come l'identità: la particolarità e unicità del documento è caratterizzata proprio dalla specifica funzione che esso riveste nello svolgimento dell'attività del Produttore.

5.1.2. I fascicoli

I fascicoli sono aggregazioni di documenti suddivisi dal sistema di gestione; possono contenere documenti omogenei per procedimento, suddivisi per formato, natura, contenuto giuridico.

In alternativa, i fascicoli possono altresì contenere documenti della stessa tipologia o qualità o forma, raggruppati in base a criteri estrinseci, e riguardanti contenuti disomogenei.

In particolare è possibile distinguere tra differenti tipologie di fascicoli: fascicolo di persona, fascicolo di affare, fascicolo di attività, fascicolo procedimentale, fascicolo di fabbricato e fascicolo edilizio.

La distinzione tipologica dei fascicoli deriva dal particolare iter di produzione della documentazione per cui la catena delle azioni che pongono in essere un insieme di documenti determina anche le modalità con cui i documenti vengono organizzati e archiviati e dà luogo, nel medio e lungo periodo, al cosiddetto processo di sedimentazione.

Il fascicolo contiene la storia del procedimento; le azioni a cui il documento è soggetto nel corso della propria esistenza sono strettamente determinate dall'appartenenza ad un determinato fascicolo; in tal senso risulta fondamentale l'appartenenza del documento al fascicolo.

La fascicolazione, oltre a essere un obbligo previsto dalla normativa, è il requisito indispensabile per la corretta gestione del documento all'interno del contesto relazionale che ne determina il significato e l'identità; fascicolare significa esplicitare la posizione logica e fisica del singolo documento all'interno dell'archivio, quindi stabilire esattamente la funzione che il documento svolge.

Da un punto di vista normativo, il fascicolo informatico viene introdotto dal CAD all'art. 41, in relazione al procedimento amministrativo e, nel comma 2 ter del predetto articolo, vengono elencate le indicazioni di cui il fascicolo deve essere provvisto per la corretta identificazione e gestione.

Il successivo art. 44, esplicitando i requisiti per la gestione e conservazione dei documenti informatici, dichiara che annualmente devono essere trasferiti al sistema di conservazione "i fascicoli e le serie documentarie anche relative a procedimenti conclusi".

I fascicoli informatici sono altresì predisposti secondo il piano di classificazione e relativo piano di fascicolazione ai sensi dell'art. 64 del TUDA, in modo da consentirne il rapido reperimento e i dati ad esso associati, quali il procedimento ed il relativo responsabile, nonché la gestione delle fasi del procedimento;

La gestione del fascicolo e delle aggregazioni documentali viene affrontata anche dalle regole tecniche di cui alle Linee Guida AGiD 2020.

5.1.3 Le serie

I fascicoli, così come particolari tipologie di documenti, creano ulteriori aggregazioni documentali definite serie.

Si tratta di articolazioni interne all'archivio createsi sulla base del processo di sedimentazione reso esplicito dall'applicazione del titolario di classificazione, costituito da un quadro alfanumerico di riferimento per l'archiviazione, la conservazione e l'individuazione dei documenti che rappresenta la logica in base a cui è costruito e ordinato l'archivio.

Le serie, ed eventualmente le sotto-serie, sono funzionali all'individuazione di caratteristiche comuni per documenti o fascicoli e consentono di conseguenza un'efficiente gestione dei dati oltre a rappresentare un elemento indispensabile della struttura dell'archivio.

Le serie di fascicoli sono costituite da fascicoli accorpati per ragioni funzionali in base alla classe di riferimento o alla tipologia di fascicoli. I fascicoli appartenenti a serie diverse possono essere collegati tra loro. Le serie di fascicoli rispettano l'articolazione del titolario di classificazione sulla base del quale i singoli fascicoli vengono classificati e inseriti nel repertorio dei fascicoli.

Oltre che da fascicoli, le serie possono essere costituite da una aggregazione di specifiche tipologie documentali, le quali, quindi, condividono un insieme di caratteristiche omogenee, tradotte in ambito informatico in un set di metadati.

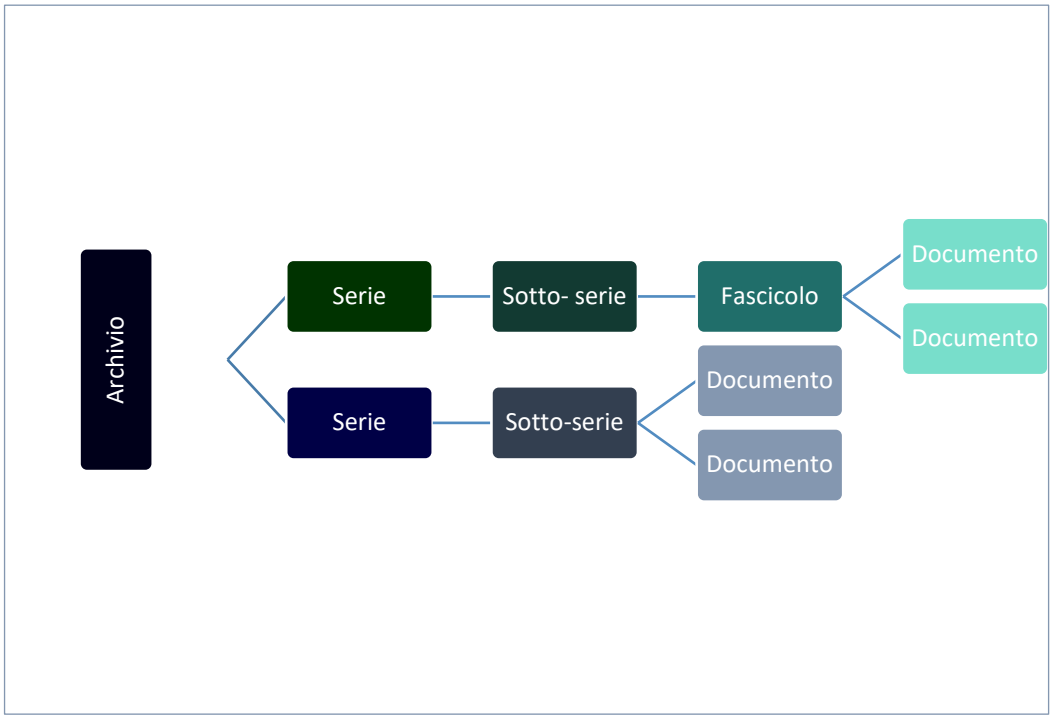

Figura 3 Schema gerarchico delle aggregazioni documentali descritte nel testo

5.1.4. Unità archivistiche e unità documentarie

Il rapporto tra unità archivistiche e unità documentarie subisce in ambito informatico una traslazione rispetto alla tradizione archivistica e ciò è dovuto a esigenze gestionali legate alla specificità dei supporti con cui vengono veicolate le unità informative in ambito informatico.

L'unità archivistica in ambito analogico è l'unità base costituita dall'insieme di documenti che condividono determinate caratteristiche identificative, risultato di un processo di produzione, che fanno dell'unità un'aggregazione qualificata e non casuale.

In tal senso, l'unità archivistica è il livello di definizione e descrizione dell'aggregazione documentale oltre il quale non è possibile procedere: i documenti che la costituiscono, infatti, sono elementi che non possiedono un'identità propria se tolti, ad esempio, dal fascicolo, cioè se decontestualizzati.

L'unità archivistica nella maggior parte dei casi corrisponde al fascicolo, quindi ad un insieme di documenti, ma può corrispondere anche al singolo documento.

In ambito informatico tale rapporto, benché mantenga il rispetto dei principi archivistici, risulta più complesso, poiché l'unità documentaria diventa a sua volta un contenitore la cui natura è pre-strutturata sulla base della tipologia di informazioni che deve contenere: si articola in documenti principali, allegati, componenti.

Le unità informative principali costituiscono il nucleo dell'unità documentaria e determinano la struttura e i metadati di riferimento.

L'Ente, in qualità di Produttore, determina la relazione di appartenenza tra i documenti che costituiscono l'unità documentaria e l'unità archivistica, mentre il Conservatore, in un secondo momento, si fa carico di mantenere stabili, consultabili e contestualizzate nel tempo tali informazioni, secondo i parametri definiti nel manuale di conservazione del Conservatore[6]

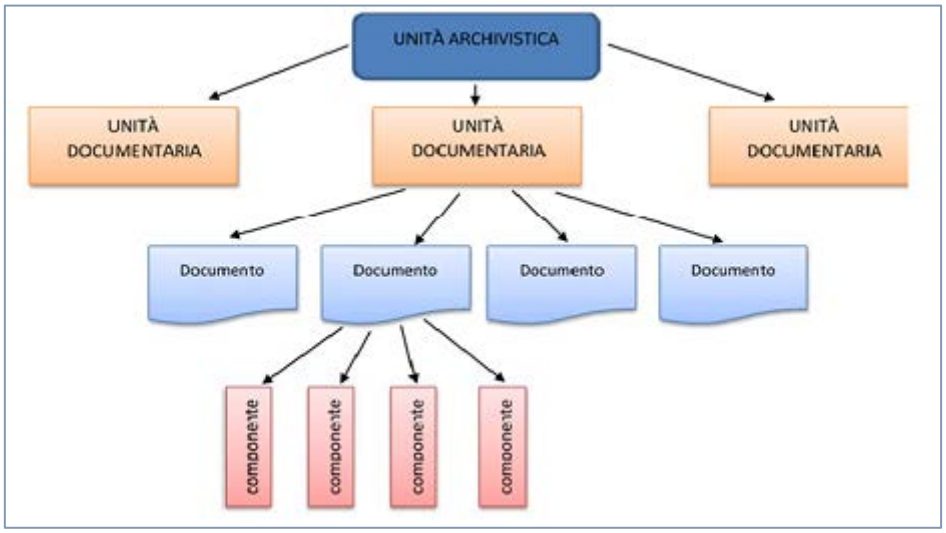

Figura 4 Schema delle relazioni di appartenenza esistenti tra le diverse componenti dell'Unità Archivistica *Da:* Modello di Manuale di Conservazione *redatto dal Gruppo di lavoro Procedamus (versione 1.0 9/3/17).*

5.3. Le unità documentarie soggette a conservazione e le soluzioni di conservazione adottate

Si riporta nelle seguenti tabelle la tipologia di documenti che vergono versati nel sistema di conservazione.

[6] https://www.agid.gov.it/sites/default/files/repository_files/manualediconservazione-cineca_rev1_9pdfsigned.pdf

Documentazione	Trasmissione	Conservazione
Registro giornaliero di protocollo	Sistema di registrazione Titulus	Illimitata
Fatture elettroniche attive verso PA	Sistema di registrazione Titulus tramite Sistema di interscambio	10 anni[7]
Fatture elettroniche passive/parcelle (compresi anche documenti di acconto/anticipo su fattura o parcella, note di credito e nota di debito)	Sistema di registrazione Titulus/UGOV- CONTABILITA'	10 anni[11]
Registro IVA	Sistema di registrazione Titulus	10 anni
Bandi di gara	UBUY Gara	Illimitata
Verbali di gare	UBUY Gara	Illimitata
Documentazione a fine procedura	UBUY Gara	10 anni
Richieste, risposte e comunicazioni verso operatori	UBUY Gara	10 anni
Richieste e risposte ricevute da operatore	UBUY Gara	10 anni

[7] Ai sensi dell''art. 2220 del codice civile. Per lo stesso periodo devono conservarsi le fatture, le lettere e i telegrammi ricevuti e le copie delle fatture, delle lettere e dei telegrammi spediti.
Nel caso di istanze di ispezione e di esibizione delle scritture contabili provenienti dall'Amministrazione finanziaria, la parte è tenuta a conservare la documentazione richiesta fino al momento in cui il giudice non abbia definitivamente e negativamente provveduto sull'istanza stessa; in tale ipotesi, il termine di prescrizione decennale di cui all'art. 2220 del codice civile può essere derogato (Corte di cassazione: 7 marzo 1997, n. 2086 e 19 novembre 1994, n. 9839).
In ambito fiscale, la conservazione di scritture e documenti contabili è disciplinata dall'art. 22 del DPR n. 600/1973, a cui peraltro fa riferimento anche l'art. 39 del DPR n. 633/1972 relativamente alla tenuta e conservazione dei registri e dei documenti rilevanti ai fini dell'IVA.
L'articolo 39 disciplina la tenuta e conservazione dei registri e dei documenti.
L'articolo 22 del DPR n. 600/1973 stabilisce che, fatto salvo quanto previsto dalla normativa civilistica, le scritture contabili obbligatorie e la relativa documentazione devono essere conservate fino a quando non siano definiti gli accertamenti relativi al corrispondente periodo d'imposta.
In caso di accertamenti in corso, notificati nei termini, la conservazione delle scritture contabili è dunque, obbligatoria, come detto, fino alla definizione dei medesimi, eventualmente anche oltre il termine massimo di dieci anni stabilito dall'articolo 2220 del codice civile.
L'obbligo di conservazione, negli stessi termini, si estende anche agli originali delle lettere, dei telegrammi e delle fatture ricevute e le copie delle lettere e dei telegrammi spediti e delle fatture emesse.

Documentazione	Trasmissione	Conservazione
Pubblicazioni elenco	UBUY EO	Illimitata
Documentazione a fine procedura	UBUY EO	10 anni
Risposte e comunicazioni verso operatori	UBUY EO	10 anni
Richieste, istanze d'iscrizione/rinnovo, integrazioni documenti	UBUY EO	10 anni
Avvisi	UBUY Avvisi	10 anni
Documentazione a fine procedura	UBUY Avvisi	10 anni
Risposte e comunicazioni verso operatori	UBUY Avvisi	10 anni
Richieste e risposte ricevute da operatori	UBUY Avvisi	10 anni

Per le altre tipologie di documenti e per le altre tipologie di fascicoli prodotti nativi digitali, sintetizzati nella seguente tabella, non sono ancora stati sottoscritti accordi di versamento con il conservatore.

Documentazione	Trasmissione	Conservazione
Statuto	Sistema di registrazione Titulus	Illimitata
Regolamenti	Sistema di registrazione Titulus	Illimitata
Verbali del Consiglio di amministrazione	Sistema di registrazione Titulus	Illimitata
Verbali del Nucleo di valutazione	Sistema di registrazione Titulus	Illimitata
Verbali dei Revisori dei conti	Sistema di registrazione Titulus	Illimitata

Documentazione	Trasmissione	Conservazione
Deliberazioni del Consiglio di amministrazione	Sistema di registrazione Titulus	Illimitata
Decreti - Provvedimenti	Sistema di registrazione Titulus	Illimitata
Relazioni annuali del Nucleo di valutazione	Sistema di registrazione Titulus	Illimitata
Contratti di lavoro	Sistema di registrazione Titulus	10 anni
Contratti e convenzioni soggetti a registrazione	Sistema di registrazione Titulus	10 anni
Contratti in forma pubblica amministrativa	Sistema di registrazione Titulus	10 anni
Protocollo particolare	Sistema di registrazione Titulus	Illimitata
Decreti - Provvedimenti	Sistema di registrazione Titulus	Illimitata
Fascicoli di procedimento amministrativo	Sistema di registrazione Titulus	Come da *Massimario di selezione e scarto* (Allegato 4)
Fascicoli di affare	Sistema di registrazione Titulus	
Fascicoli di natura giuridico-legale e contenzioso	Sistema di registrazione Titulus	
Fascicoli edilizi/fascicoli di fabbricato	Sistema di registrazione Titulus	
Fascicoli del personale	Sistema di registrazione Titulus	
Fascicoli di persona fisica e giuridica	Sistema di registrazione Titulus	

5.4 Formati dei documenti inviati in conservazione:

La leggibilità di un documento informatico dipende dalla possibilità e dalla capacità di interpretare ed elaborare correttamente i dati binari che costituiscono il documento, secondo le regole stabilite dal formato con cui esso è stato rappresentato.

La corretta conservazione dei documenti nel tempo è determinata anche dalla scelta dei formati idonei a tale scopo; tenendo in considerazione il problema della rapida obsolescenza dei formati, la scelta dei formati prende in esame le garanzie che i formati disponibili offrono in termini di conservazione a lungo termine ma anche la possibilità di migliore garanzie di leggibilità e reperibilità del documento informatico nel suo ciclo di vita.

La scelta tra i formati dipende dalle peculiarità proprie del formato e dei programmi che lo gestiscono; la norma raccomanda di considerare, nella scelta, le seguenti caratteristiche:

1. L'apertura. Un formato si dice "aperto" quando è conforme a specifiche pubbliche, cioè disponibili a chiunque abbia interesse ad utilizzare quel formato.
La disponibilità delle specifiche del formato rende sempre possibile la decodifica dei documenti rappresentati in conformità con dette specifiche, anche in assenza di prodotti che effettuino tale operazione automaticamente.
La normativa privilegia i formati già approvati dagli Organismi di standardizzazione internazionali quali ISO e ETSI.

2. La sicurezza. La sicurezza di un formato dipende da due elementi: il grado di modificabilità del contenuto del file e la capacità di essere immune dall'inserimento di codice maligno.

3. La portabilità, ovvero la facilità con cui i formati possano essere usati su piattaforme diverse, sia dal punto di vista dell'hardware che del software, inteso come sistema operativo. Di fatto è indotta dall'impiego fedele di standard documentati e accessibili.

4. La funzionalità, intesa come la possibilità da parte di un formato di essere gestito da prodotti informatici che prevedono una varietà di funzioni messe a disposizione dell'utente per la formazione e gestione del documento informatico.

5. Il supporto allo sviluppo: E' la modalità con cui si mettono a disposizione le risorse necessarie alla manutenzione e sviluppo del formato e i prodotti informatici che lo gestiscono (organismi preposti alla definizione di specifiche tecniche e standard, società, comunità di sviluppatori, ecc.).

6. La diffusione dell'impiego di uno specifico formato influisce sulla probabilità che esso venga supportato nel tempo.

7. La garanzia data in termini di interoperabilità tra i sistemi di gestione documentale e conservazione, valutata sulla base delle tipologie documentali.

Altre caratteristiche importanti sono l'efficienza in termini di occupazione di spazio fisico, valutando anche gli eventuali livelli di compressione utilizzabili e la possibilità di gestire il maggior numero possibile di metadati, compresi i riferimenti a modifiche o aggiunte intervenute sul documento

L'Allegato 2 alle Linee Guida AgID - *Formati di File e Riversamento-*, documento che verrà periodicamente aggiornato sulla base dell'evoluzione tecnologica e dell'obsolescenza dei formati, fornisce le indicazioni iniziali sui formati dei documenti informatici che per le loro caratteristiche sono da ritenersi coerenti con le regole tecniche del documento informatico, del sistema di conservazione e del protocollo informatico.

Il sistema di conservazione si avvale di librerie open source per il riconoscimento dei formati dei file ricevuti all'interno dei pacchetti di versamento.

Queste librerie non si limitano a verificare l'estensione dei file, ma ne verificano il contenuto, dando quindi un livello di sicurezza superiore rispetto al reale formato dei file giunti in conservazione.

I formati attualmente utilizzati dall'INRiM nella formazione dei documenti sono:

Tipo di file	*Estensione*	*Visualizzatore*
XML o XML (XADES)	*.xml*	*Mozilla, Chrome, altri browser o altro software specifico*
pdf o pdf/a o pdf(PADES)	*.pdf*	*Acrobat Reader o altro software specifico*
P7M	*.p7m*	*Dike o software specifico per la verifica delle firme digitali*

5.5 I metadati aggiuntivi associati alle diverse tipologie documentali inviate in conservazione

I metadati sono informazioni associate ai dati primari creati e trattati: sono a loro volta dati che descrivono, spiegano, localizzano una risorsa informativa rendendo più semplice il suo recupero, utilizzo e gestione.

Le caratteristiche proprie del documento vengono tradotte in ambito elettronico in metadati: informazioni connesse al documento che consentono all'interno del sistema l'identificazione, la descrizione, la gestione e la conservazione.

Ai fini della conservazione del documento amministrativo informatico, l'insieme dei metadati previsti per la registrazione di protocollo sono descritti dall'art 53 del TUDA[8]; a questi si aggiungono i metadati relativi alla classificazione, ai sensi dell'articolo 56 del TUDA[9], quelli relativi ai tempi di conservazione, in coerenza con il

[8] L'art. 53, comma 1, del TUDA prevede che "La registrazione di protocollo per ogni documento ricevuto o spedito dalle pubbliche amministrazioni è effettuata mediante la memorizzazione delle seguenti informazioni: a) numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile; b) data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile; c) mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile; d) oggetto del documento, registrato in forma non modificabile; e) data e protocollo del documento ricevuto, se disponibili; f) l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile".

[9] L'art. 56 del TUDA prevede che "Le operazioni di registrazione indicate all'articolo 53 e le operazioni di segnatura di protocollo di cui all'articolo 55 nonché le operazioni di classificazione costituiscono operazioni necessarie e sufficienti per la tenuta del sistema di gestione informatica dei documenti da parte delle pubbliche amministrazioni"

piano di conservazione, e quelli relativi alla relazione con l'aggregazione documentale informatica d'appartenenza.
Inoltre, nell'Allegato 5 al documento *" Linee Guida sulla modalità di formazione, gestione e conservazione dei documenti informatici",* emesso dall'AgID, sono descritti i metadati atti a fornire le informazioni relative alla modalità di formazione e alla tipologia del documento, alla presenza di allegati, alla riservatezza dello stesso, alle informazioni per identificare il formato, alla versione, e, infine, all'esito delle verifiche a cui il documento viene sottoposto; nello stesso documento AgID sono evidenziati i metadati da associare ai fascicoli informatici e alle aggregazioni documentali.

La descrizione dei metadati previsti dalla normativa per i documenti e le aggregazioni archivistiche è stata adottata dall'INRiM ed illustrata alle sezioni 3.8 e 4.9 del *Manuale di Gestione dei flussi documentali e del protocollo informatico*, di cui questo documento è parte integrante.

Ancora, al documento amministrativo informatico possono essere associati eventuali ulteriori metadati rilevanti ai fini amministrativi o per finalità gestionali, definiti, per ogni tipologia di documento, nell'ambito del contesto a cui esso si riferisce.

Il sistema di conservazione di Cineca, strutturato sul modello OAIS, è predisposto per conservare queste differenti tipologie di metadati in luoghi diversi e si avvale di una caratteristica propria dei metadati per cui essi possono far parte del dato stesso o possono essere archiviati come oggetti esterni e organizzati in gerarchie, ontologie o schemi.

Ad esempio, i dati e i metadati relativi all'oggetto informativo e alle informazioni sulla rappresentazione costituiscono un'unità denominata *contenuto informativo* e in tale forma viene conservata al fine di assicurare la fruibilità e la comprensibilità nel lungo periodo; i metadati descrittivi, invece, che descrivono e identificano le informazioni archiviate, vengono conservate separatamente in appositi database.

Le seguenti tabelle riportano i metadati aggiuntivi associati alle tipologie documentali, così come è riportato negli accordi di versamento stipulati tra INRiM e Cineca.

FATTURE ELETTRONICHE PASSIVE **Informazioni sulla conservazione**[10]	
Identificativi	• Un identificativo del sistema di provenienza • Il numero fattura • Il riferimento alla serie documentale • Un iD univoco assegnato dal sistema di conservazione • I metadati di segnatura di protocollo (nel caso di documento protocollato)
Informazioni sulla provenienza	• Firma digitale, attestante la paternità del documento convalidata secondo un riferimento temporale opponibile a terzi (data PEC ricevuta, data segnatura di protocollo o processo di conservazione) • Descrizione del processo di fatturazione elettronica • Ulteriori eventi che coinvolgono il documento, dalla ricezione in Titulus fino al versamento nel sistema di conservazione Conserva.
Informazioni sul contesto	• La classificazione • Il riferimento al fascicolo ove fosse presente • Il riferimento alla serie documentale • Collegamenti con altre fatture in caso di annullamento • Le ricevute di comunicazione via PEC con il Sistema di Interscambio.
Informazioni sull'integrità	• La firma digitale sul documento • L'impronta del documento
Informazioni sull'accesso	• I permessi di accesso

[10] Per ogni istanza del documento viene generato un set di metadati che integrano quelli indicati dalla normativa.

FATTURE ELETTRONICHE PASSIVE **Informazioni descrittive**[11]	
Default	• Id sistema (id delle fatture passive/lotto di Conserva) • Id provenienza (id delle fatture passive/lotto di Titulus)
Dati identificativi	• Tipo documento (fattura singola/lotto) • Codice Area Organizzativa Omogenea • Numero Protocollo • Data protocollo da…al… (ricerca per intervalli di date) • Nome Repertorio (se presente) • Numero Repertorio (se presente) • Data repertorio da…al… (per ricerca di intervalli di date) • Oggetto
Dati gestionali	• Classificazione • Unità Organizzativa • Persona
Dati Fattura elettronica	**Dati generali** • Numero • Data da…al… (ricerca per intervalli di date) • Causale • Sezionale • CodiceCIG • CodiceCUP **Cedente Prestatore** • Denominazione • Nome • Cognome • Partita IVA • Codice fiscale

[11] Chiavi di ricerca tramite le quali è possibile recuperare il documento, il fascicolo o la serie di interesse; Per quanto riguarda la ricerca della tipologia dei lotti è possibile ricercarlo per tutti i campi eccetto quelli relativi ai Dati Fattura elettronica.

FATTURE ELETTRONICHE ATTIVE **Informazioni sulla conservazione**[12]	
Informazioni sull'identificazione	• Identificativo del sistema di provenienza; • Il numero fattura che la identifica; • Il riferimento alla serie documentale che si forma per sezionale e per anno senza soluzione di continuità; • Un id univoco assegnato dal sistema di conservazione Conserva; • La registrazione di protocollo (in caso di documento protocollato,
Informazioni sulla provenienza	• La firma digitale, attestante la paternità del documento, convalidata secondo un riferimento temporale opponibile a terzi (data PEC ricevuta, data segnatura di protocollo o processo di conservazione); • La descrizione del processo di fatturazione • Gli ulteriori eventi che coinvolgono il documento, dalla generazione in UGOV fino al versamento nel sistema di conservazione Conserva.
Informazioni sul contesto	• La classificazione; • Il riferimento al fascicolo o ai fascicoli in cui viene collocata la fattura (ove presente); • Il sezionale nel cui ambito si crea una serie documentale; • Collegamenti con altre fatture in caso di annullamento.
Informazioni sull'integrità	• La firma digitale sul documento; • L'impronta del documento
Informazioni sull'accesso	• I permessi di accesso

[12] Per ogni istanza del documento viene generato un set di metadati che integrano quelli indicati dalla normativa.

FATTURE ELETTRONICHE ATTIVE **Informazioni descrittive[13]**	
Dati identificativi	• Codice Area Organizzativa Omogenea • Numero Protocollo • Data protocollo • Nome Repertorio • Numero Repertorio • Destinatario (da sistema di gestione documentale Titulus, coincide con la denominazione del cessionario committente) • Oggetto
Dati gestionali	• Classificazione • Unità Organizzativa • Persona
Dati Fattura elettronica	**Dati generali** • Numero • Data • Causale • Sezionale • CodiceCIG • CodiceCUP **Cessionario Committente** • Denominazione (nel caso di persona giuridica) • Nome (nel caso di persona fisica) • Cognome (nel caso di persona fisica) • Partita IVA • Codice fiscale

[13] Chiavi di ricerca tramite le quali è possibile recuperare il documento, il fascicolo o la serie di interesse; Per quanto riguarda la ricerca della tipologia dei lotti è possibile ricercarlo per tutti i campi eccetto quelli relativi ai Dati Fattura elettronica.

REGISTRI IVA **Informazioni sulla conservazione**[14]	
Identificativi	• Un proprio identificativo del sistema di provenienza • Un id univoco assegnato dal sistema di conservazione; • Il numero di registro di protocollo; • Il riferimento alla serie documentale della tipologia dei registri IVA cui appartiene il documento (numero di repertorio assegnato da Titulus)
Informazioni sulla provenienza	• La firma digitale, attestante la paternità del documento convalidata secondo un riferimento temporale opponibile a terzi (data PEC ricevuta, data segnatura di protocollo o processo di conservazione) • La descrizione del processo di produzione del registro IVA • Gli ulteriori eventi che coinvolgono il documento, dalla generazione in UGOV CO fino al versamento nel sistema di conservazione.
Informazioni sul contesto	• La classificazione relativa alla funzione dell'ente a cui il documento attiene; • Il riferimento alla serie documentale dei registri IVA cui appartiene il documento (numero di repertorio assegnato da Titulus)
Informazioni sull'integrità	• La firma digitale sul documento • L'impronta del documento
Informazioni sull'accesso	• I permessi di accesso

[14] Per ogni istanza del documento viene generato un set di metadati che integrano quelli indicati dalla normativa.

REGISTRI IVA **INFORMAZIONI DESCRITTIVE**[15]	
Default	• Id provenienza (id dei registri IVA di Titulus) • Id sistema (id dei registri IVA di Conserva)
Dati identificativi	• Codice Area Organizzativa Omogenea • Numero Protocollo • Data protocollo da…al…(ricerca per intervalli di date) • Nome Repertorio • Numero Repertorio • Data repertorio da…al… (ricerca per intervalli di date) • Oggetto
Dati gestionali	• Classificazione • Unità Organizzativa • Persona
Dati Registro IVA	• Tipo registro • Tipo attività • Sezionale

[15] Chiavi di ricerca tramite le quali è possibile recuperare il documento, il fascicolo o la serie di interesse;

UBUY.GARA E AVVISI **INFORMAZIONI SULLA CONSERVAZIONE**[16]	
Identificativi	• Un proprio identificativo del sistema di provenienza • Il riferimento alla serie documentale di appartenenza; • Un iD univoco assegnato dal sistema di conservazione Conserva; • I metadati di segnatura di protocollo (nel caso di documento protocollato)
Informazioni sulla provenienza	• La firma digitale, ove presente, attestante la paternità del documento, convalidata secondo un riferimento temporale opponibile a terzi • La descrizione del processo di formazione del documento • Gli ulteriori eventi che coinvolgono il documento, dalla generazione nei moduli UBUY fino al versamento nel sistema di conservazione Conserva.
Informazioni sul contesto	• La classificazione; • Il riferimento al fascicolo o ai fascicoli in cui viene collocato il documento (ove presente).
Informazioni sull'integrità	• La firma digitale, ove presente • L'impronta del documento • La registrazione sul sistema di gestione documentale.
Informazioni sull'accesso	• I permessi di accesso.

[16] Per ogni istanza del documento viene generato un set di metadati che integrano quelli indicati dalla normativa.

UBUY.GARA E AVVISI INFORMAZIONI DESCRITTIVE[17]	
Default	• Id sistema • Id provenienza
Dati identificativi	• Codice Area Organizzativa Omogenea • Numero protocollo • Data protocollo • Nome repertorio (se presente) • Numero repertorio (se presente) • Data repertorio (se presente) • Oggetto
Dati gestionali	• Voce di indice • Classificazione • Unità Organizzativa • Persona

[17] Chiavi di ricerca tramite le quali è possibile recuperare il documento, il fascicolo o la serie di interesse; Per quanto riguarda la ricerca della tipologia dei lotti è possibile ricercarlo per tutti i campi eccetto quelli relativi ai Dati Fattura elettronica.

REGISTRO INFORMATICO GIORNALIERO DI PROTOCOLLO INFORMAZIONI SULLA CONSERVAZIONE[18]	
Identificativi	• Un proprio identificativo del sistema di provenienza • Il riferimento alla serie documentale dei registri informatici di protocollo giornaliero cui appartiene il documento (numero di repertorio assegnato da Titulus); • Un id univoco assegnato dal sistema di conservazione Conserva.
Informazioni sulla provenienza	• La descrizione del processo di formazione del registro informatico di protocollo (si veda Generazione dell'oggetto informativo); • Gli ulteriori eventi che coinvolgono il documento, dalla generazione in Titulus fino al versamento nel sistema di conservazione Conserva.
Informazioni sul contesto	• La classificazione relativa alla funzione dell'ente a cui il documento attiene • Il riferimento alla serie documentale dei registri informatici di protocollo giornaliero cui appartiene il ocumento (numero di repertorio assegnato da Titulus).
Informazioni sull'integrità	• L'impronta del documento • L'immodificabilità del registro, una volta prodotto • La trasmissione automatica e non presidiata del registro informatico giornaliero di protocollo di ogni AOO al sistema di conservazione Conserva, non appena terminata la produzione dello stesso.
Informazioni sull'accesso	• I permessi di accesso.

[18] Per ogni istanza del documento viene generato un set di metadati che integrano quelli indicati dalla normativa.

REGISTRO INFORMATICO GIORNALIERO DI PROTOCOLLO INFORMAZIONI DESCRITTIVE[19]	
Dati identificativi	• Codice Area Organizzativa Omogenea • Tipo repertorio • Numero repertorio • Data repertorio • Oggetto
Dati gestionali	• Classificazione • Unità Organizzativa • Persona
Dati Registro informatico di protocollo	• Numero registrazioni • Anno • Data registro • Periodo dal … al … (per ricerca per intervalli di date)

Ai documenti soggetti a registrazione particolare, descritti nel §7.11 del *Manuale di gestione dei flussi documentali e del protocollo informatico*, di cui questo documento è parte integrante, vengono associati l'insieme dei metadati previsti per il documento amministrativo informatico e i metadati relativi alla riservatezza del documento.

5.6 I pacchetti informativi

Il servizio di conservazione CONSERVA in ottemperanza alla normativa segue il modello informativo dello standard ISO 14721:2012 OAIS (Open Archival Information System - Sistema informativo aperto per l'archiviazione, di seguito solo OAIS).

Lo standard OAIS[20] ha la peculiarità di organizzare gli oggetti informativi da conservare in pacchetti informativi tipizzati in base alla fase del processo di conservazione; le informazioni contenute nei pacchetti informativi permettono di riprodurre, interpretare e comprendere i dati digitali (formati, software, algoritmi, standard, informazioni semantiche…)

[19] Chiavi di ricerca tramite le quali è possibile recuperare il documento, il fascicolo o la serie di interesse; Per quanto riguarda la ricerca della tipologia dei lotti è possibile ricercarlo per tutti i campi eccetto quelli relativi ai Dati Fattura elettronica.

[20] Da: http://www.conservazionedigitale.org

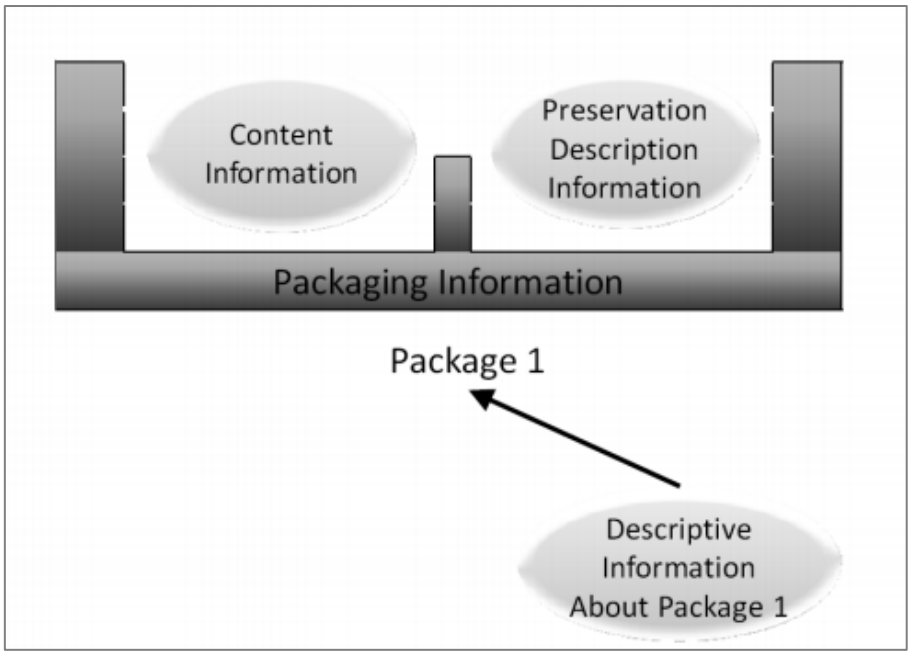

Figura 5 Schema dei pacchetti informativi previsti dal modello OAIS. Da: http://www.conservazionedigitale.org

Questa visione della struttura dei pacchetti informativi, corrisponde al concetto che ogni oggetto digitale, per avere un significato, debba contenere al suo interno due componenti: il Data Object, e cioè la sequenza di bit (bitstream), di per sé poco significativo, e la Representation Information, che specifica le modalità di codifica dell'informazione binaria e ne fornisce quindi l'indispensabile chiave di decodifica e quindi di lettura e di interpretazione, secondo lo schema illustrato in Figura 5.

Un aspetto centrale del modello è costituito dalle cosiddette informazioni sulla conservazione (*Preservation Description Information* – PDI), ovvero sulla quantità e qualità di informazioni che identificano e descrivono gli oggetti informativi da conservare con particolare attenzione per i 'metadati' relativi alla identificazione degli oggetti (*reference*), alla loro origine (*provenance*), al contesto (*context*) e alla loro integrità (*fixity*).

In particolare:

- le informazioni di *refere*nce individuano univocamente e possibilmente in modo persistente gli oggetti digitali (contenuti informativi, RepInfo, ecc.) e, se necessario, descrivono uno o più meccanismi di attribuzione di identificatori; possono consentire a sistemi esterni di riferirsi in maniera non ambigua al contenuto informativo (ad esempio un codice ISBN o un codice DOI);

- le informazioni di *provenance* documentano la storia del contenuto informativo e comprendono origine o fonte, cambiamenti avvenuti, storia e responsabilità della custodia; il deposito è responsabile per la creazione e conservazione delle informazioni sulla provenienza a partire dal versamento, ma tali informazioni devono essere fornite già nella fase di formazione da parte del soggetto produttore dei contenuti (producer);

- le informazioni di *context* documentano le relazioni del contenuto informativo con l'ambiente di riferimento (originario o di ri-uso), ivi incluse le modalità di formazione e le forme in cui si definiscono le relazioni con altri contenuti esistenti anche in sistemi diversi;

- le informazioni di *fixity* documentano i meccanismi di autenticazione e forniscono le chiavi di validazione utilizzate per evitare alterazioni non documentate; gli algoritmi utilizzati (*checksum, hash, object digest*) possono essere di varia natura (SHA, CRC-32, ecc.) e diversamente sicuri, ma in ogni caso vulnerabili, sia pure in diversa misura; si tratta inoltre di informazioni indipendenti dai domini disciplinari cui appartengono i contenuti informativi, a differenza delle altre categorie di PDI;

Le informazioni sui diritti di accesso, ancora, identificano i limiti di accesso al contenuto informativo, inclusi i termini di licenza, le restrizioni legali e i sistemi di controllo; Includono le condizioni di accesso e disseminazione previste nell'accordo di versamento in relazione sia alla conservazione da parte del deposito OAIS sia all'uso da parte degli utenti finali oltre alle specifiche per l'applicazione di misure gestionali in questo ambito.

I tipi di pacchetto sono tre e racchiudono gli oggetti informativi inviati in conservazione assieme alla relativa metadatazione utile ai fini conservativi:

- **SIP** – Submission Information Package, corrispondente al **Pacchetto di versamento (PdV**); è il pacchetto versato dal produttore e utilizzato per l'acquisizione degli oggetti informativi e dei metadati da parte del sistema di conservazione.

- **AIP** – Archival Information Packege, corrispondente al **Pacchetto di archiviazione (PdA)**. E' il pacchetto di informazioni necessarie per gestire il processo di conservazione permanenet o di lungo termine di un oggetto informativo.

- **DIP** – Dissemination information Package, corrispondente al **Pacchetto di distribuzione (PdD)**. E' un pacchetto di oggetti informativi conservati, costruito secondo le esigenze e il profilo dell'utenza esterna che ne fa richiesta.

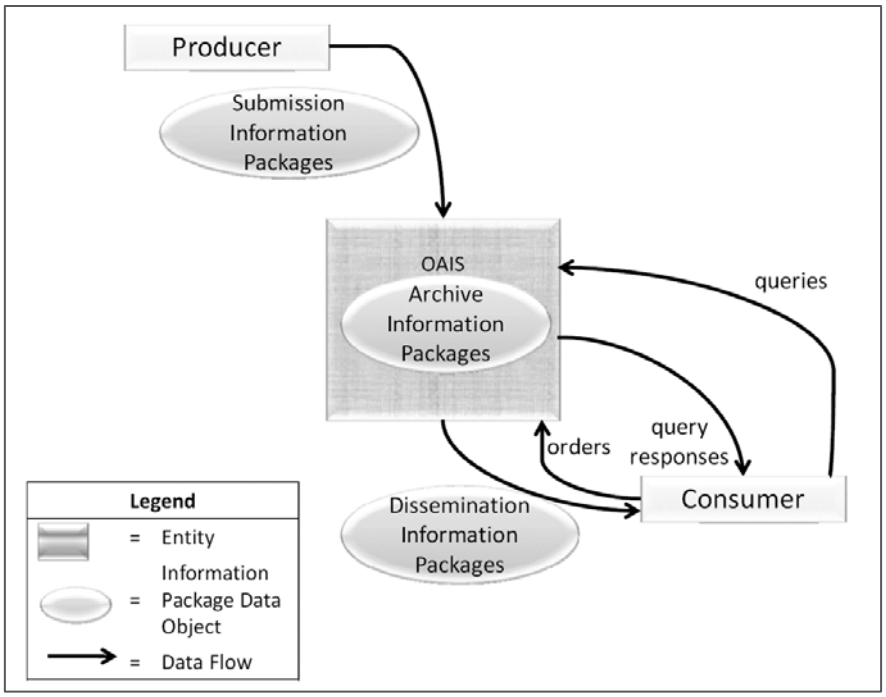

Figura 6. Schema organizzativo dei pacchetti informativi del sistema OAIS. Da: www.conservazionedigitale.org/wp/wp-content/uploads/2014/12/OAIS-3.png

A livello generale, **il pacchetto di versamento**[21] è costituito da:

- un indice del pacchetto di versamento contenente i metadati relativi alle unità (di versamento) che formano il pacchetto, un oggetto XML rispondente ad uno specifico schema che definisce e descrive i metadati necessari per la conservazione di oggetti digitali.
- dai relativi file.

All'interno di un pacchetto di versamento possono essere inviate nuove unità di versamento (prima trasmissione al servizio di conservazione) oppure variazioni (metadati e/o file) ad unità trasmesse in precedenza.

L'invio al sistema di conservazione CONSERVA del Consorzio Interuniversitario Cineca può avvenire tramite due modalità:

- tramite l'uso di web services;
- tramite interfaccia WebDAV.

Per ogni unità che forma il pacchetto, all'interno dell'indice vengono riportati:

[21] Da Manuale di conservazione Cineca
https://www.agid.gov.it/sites/default/files/repository_files/manualediconservazione-cineca_rev1_9pdfsigned.pdf

- i metadati minimi previsti dalle norme tecniche;
- i metadati integrativi ritenuti utili ai fini di una corretta conservazione delle unità di versamento;
- i metadati personalizzati, specifici del produttore del pacchetto.

Il pacchetto di archiviazione[22] è il pacchetto presente all'interno del sistema di conservazione, costituito da un indice del pacchetto di archiviazione e dai file che compongono le unità di versamento.

Al fine di garantirne l'autoconsistenza, i pacchetti di archiviazione contengono anche i riferimenti a tutti i pacchetti di versamento di provenienza di ciascuna unità versata e a tutti i relativi rapporti di versamento.

In linea con la normativa, l'indice del pacchetto di archiviazione impiegato dal sistema CONSERVA, è conforme allo standard UNI 11386 SInCRO, al fine di facilitare l'interoperabilità tra i sistemi di conservazione.

Il Conservatore garantisce l'aggiornamento nella metadatazione affinché permanga intellegibile e accessibile nel tempo attraverso i cambiamenti delle piattaforme hardware-software.

Il pacchetto di distribuzione è il pacchetto che si forma contestualmente su specifica richiesta da parte di un utente autorizzato; viene costruito sulla base della ricerca dell'utente e sui suoi diritti di accesso all'oggetto informativo.

Anche il pacchetto di distribuzione è costituito dall'indice del pacchetto di distribuzione strutturato secondo lo standard UNI SInCRO e dai file contenuti nei relativi documenti.

5.6.1 Informazioni sull'impacchettamento delle tipologie documentali inviate in conservazione

Fatture attive e passive

Le fatture elettroniche vengono gestite in apposite serie documentali ordinate progressivamente e legate al sezionale del registro; possono anche essere parte di procedimenti amministrativi, attività o affari e quindi esser soggette a fascicolazione. Di conseguenza all'interno del sistema di conservazione Conserva, le fatture attive vengono collocate sia nel pacchetto di archiviazione della serie delle fatture attive (una serie per ogni sezionale) che anche all'interno degli eventuali pacchetti di archiviazione relativi al/ai fascicoli in cui le fatture sono state inserite.

Il pacchetto di archiviazione della serie viene chiuso il 31 marzo dell'anno successivo alla serie stessa; il pacchetto di archiviazione relativo al fascicolo verrà chiuso alla chiusura del fascicolo.

Per ogni chiusura il sistema produce un indice del pacchetto di archiviazione firmato digitalmente con firma XADES automatica e marcato temporalmente. Il pacchetto viene chiuso anticipatamente in caso di richiesta di esibizione dello stesso; in tal caso ogni successiva modifica al fascicolo sarà registrata su una nuova versione del pacchetto.

Il sistema di conservazione Conserva mantiene tutte le versioni precedenti di un pacchetto di archiviazione.

Registri IVA

[22] Da Manuale di conservazione Cineca
https://www.agid.gov.it/sites/default/files/repository_files/manualediconservazione-cineca_rev1_9pdfsigned.pdf

I Registri IVA vengono registrati all'interno del sistema di gestione documentale e vengono protocollati nell'ambito del registro di protocollo del Produttore, ottenendo un riferimento temporale valido.
Il pacchetto viene formato raccogliendo tutti i documenti selezionati in maniera interattiva dal Responsabile della gestione documentale oppure in maniera automatica attraverso apposite funzioni presenti sul sistema di gestione documentale Titulus. La periodicità di formazione e trasmissione dei pacchetti è decisa dal Responsabile della gestione documentale assieme al Responsabile della conservazione.

Ogni pacchetto prodotto da Titulus, costituito da una struttura XML e dal file del registro XML allegato, viene compresso prima dell'invio.

Una volta completato l'invio del pacchetto, il sistema di conservazione Conserva avvia procedure di controllo volte a garantire integrità, completezza e congruenza del trasferimento. A fronte di un esito positivo dei controlli, il pacchetto viene collocato in un'area di lavoro del sistema di conservazione Conserva, in attesa del versamento; in caso di un esito negativo, viene restituito un messaggio di errore al sistema mittente.

UBUY GARE E AVVISI

Il pacchetto di versamento è costituito da un indice di versamento (Indice del Pacchetto di Versamento – IPdV) e dai file appartenenti alle unità documentali contenute nel pacchetto.

L'indice del pacchetto di versamento è un file XML che descrive le unità di versamento (documenti o fascicoli) che compongono il pacchetto.

Il Produttore può inviare il pacchetto di versamento in modalità non compressa o compressa, eventualmente diviso in più porzioni, anche non auto consistenti; in questo caso la consistenza viene garantita con il ricongiungimento ordinato di tutti i pacchetti, prima di procedere ai controlli di consistenza.

Registro giornaliero di protocollo

Il pacchetto di versamento è costituito, come per il modulo UBUY GARE ED AVVISI, da un indice del pacchetto di versamento in formato XML che può essere inviato in modalità non compressa o compressa, eventualmente diviso in più porzioni, anche non auto consistenti; in questo caso la consistenza viene garantita con il ricongiungimento ordinato di tutti i pacchetti, prima di procedere ai controlli di consistenza.

Il pacchetto è decompresso da Conserva ed il suo contenuto conservato in formato non compresso.

I registri di protocollo giornalieri vengono registrati, tipicamente entro la giornata lavorativa successiva, all'interno del sistema di gestione documentale Titulus nell'ambito dell'Area Organizzativa Omogenea di riferimento del Produttore.

Lo stesso modulo che produce e repertoria il registro informatico di protocollo giornaliero, si occupa di inviarlo al sistema di conservazione Conserva.

6. IL PROCESSO DI CONSERVAZIONE

Le procedure per l'attivazione del processo di conservazione sono indicate ed attivate sulla base della Convenzione di affidamento stipulato tra l'INRiM e Il Consorzio Interuniversitario Cineca, citato al Capitolo 1.

Il processo di conservazione si basa su di una logica di conservazione caratterizzata dal versamento da parte del Produttore degli oggetti da conservare (documenti informatici e aggregazioni documentali informatiche) secondo la tempistica definita e dettagliata nel Disciplinare tecnico.

I documenti informatici trattati dall'Ente sono memorizzati in un sistema di gestione informatica dei documenti idoneo a garantire le caratteristiche di immodificabilità e integrità degli stessi.

Il sistema di conservazione realizza l'intero ciclo di gestione delle diverse tipologie di oggetti da mandare in conservazione, partendo dalla presa in carico fino all'eventuale scarto, garantendo le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità come previsto dalla normativa vigente in materia di sistemi di conservazione.

6.1.Trasferimento nel sistema di conservazione

Al fine di garantire l'autenticità, l'integrità, l'affidabilità, la leggibilità e la reperibilità dei documenti, i fornitori di servizi di conservazione devono possedere requisiti di elevato livello in termini di qualità e sicurezza in aderenza allo standard ISO/IEC 27001 (Information security management systems requirements) del sistema di gestione della sicurezza delle informazioni nel dominio logico, fisico e organizzativo nel quale viene realizzato il processo di conservazione OAIS, e alle raccomandazioni ETSI TS 101 533-1 v. 1.2.1, *Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.*

Si rimanda al Capitolo 7 di questo documento, dove vengono riportate le specifiche operative e le modalità di descrizione e di versamento nel sistema di conservazione digitale delle diverse tipologie documentali oggetto di conservazione, così come descritto nel manuale di conservazione del Conservatore CINECA.

6.1.1 Acquisizione e presa in carico dei pacchetti di versamento

All'atto del trasferimento il sistema registra le seguenti informazioni:

- data e ora di ricezione dell'operazione registrata;
- il tipo di log;
- il servizio che ha prodotto il log;
- il Produttore che ha inviato il pacchetto;
- l'identificativo del pacchetto;
- dati relativi al web service utilizzato.

6.1.2. Verifiche effettuate sui pacchetti di versamento e sugli oggetti in esso contenuti

Al termine del trasferimento inizia la fase di validazione nel corso della quale, al fine di evitare errori, vengono avviati dei controlli automatici:

- controlli sul pacchetto di versamento e sull'indice del pacchetto di versamento;
- controlli sull'unità di versamento;
- controlli sull'unità documentale;
- controlli sull'unità documentale in serie;
- controlli sull'unità archivistica e l'aggiornamento dell'unità archivistica

Per i documenti contabili il sistema prevede alcuni controlli aggiuntivi, descritti nella seguente tabella:

Tipologia documentale	Controlli aggiuntivi
Registri iva	• la verifica che il file sia sottoscritto in formato PAdES o CAdES; • la validità del certificato di firma alla data di protocollo; • il controllo che la modalità di imbustamento sia enveloping.
Fatture elettroniche passive	• l'accertamento che il file sia sottoscritto in formato XAdES o CAdES; • la validità del certificato di firma alla data di protocollo.
Fatture elettroniche attive	• la verifica che il file sia sottoscritto in formato XAdES o CAdES; • la validità del certificato di firma alla data di protocollo; • l'accertamento che la modalità di imbustamento sia enveloped per il formato XAdES, enveloping per il formato CAdES; • la validazione dello schema XML del contenuto firmato; • la verifica che il numero fattura abbia un formato valido; • la verifica che non sia già presente in conservazione altro documento con medesimo numero di fattura (e ID di provenienza differente). Quest'ultimo controllo evidenzia la presenza di eventuali duplicati sul sistema di gestione documentale, che dovranno essere risolti prima di poter procedere alla conservazione del documento (annullamento di una delle due versioni del documento, correzione di alcuni metadati erroneamente riportati su uno dei due documenti, ecc.).

Tutti i controlli effettuati su ogni unità presente nel pacchetto di versamento sono registrati, insieme al loro esito, in formato XML e vengono utilizzati per stilare il rapporto di versamento. Vengono, inoltre, registrati su database per poter essere sempre accessibili anche dall'applicazione web di CONSERVA di CINECA.

Tutti gli indici dei pacchetti di versamento ricevuti vengono registrati su database per permettere al sistema di ricostruire, in caso di bisogno, il pacchetto di versamento originale con cui un'unità è entrata nel sistema di conservazione CONSERVA.

6.1.3 I versamento di presa in carico

La fase di versamento, qualsiasi sia l'esito, si conclude con la notifica del resoconto di versamento e del rapporto di versamento al Produttore; nel resoconto di versamento viene comunicato lo stato del pacchetto di versamento (interamente versato, parzialmente versato o rifiutato) con il dettaglio dell'esito di tutti i controlli sulle singole unità.

Il rapporto di versamento è un documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal Produttore; il rapporto di versamento evidenza i risultati del processo di versamento, sia che il pacchetto e le relative unità siano state versate o rifiutate, sia che una volta versate risultino esser le stesse concordate con il Produttore.

Nel Rapporto di Versamento sono presenti informazioni simili assieme ad altre più dettagliate relative al pacchetto di versamento per verificarne l'integrità nel tempo; il rapporto di versamento viene firmato digitalmente dal Responsabile del servizio di Conservazione tramite firma automatica.

Tutti i rapporti di versamento vengono sottoposti a procedura di conservazione.

Nel sistema di conservazione CONSERVA, che verrà descritto nel Capitolo 7, il rapporto di versamento è rappresentato da un file XML firmato e marcato attraverso firma automatica dal Responsabile del servizio di conservazione del Conservatore.

Il rapporto di versamento è sempre identificato univocamente all'interno del sistema e collocato temporalmente in standard UTC tramite la valorizzazione degli attributi *IdSistema* e *RiferimentoTemporale* all'interno della struttura XML; inoltre riporta per ogni pacchetto di versamento sia l'impronta dell'indice che di ogni singola unità documentale versata.

6.1.4 Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie

Il rifiuto dei pacchetti di versamento, e di conseguenza la comunicazione del rifiuto al Produttore, può avvenire in due momenti distinti durante il versamento: nella fase di trasferimento e nella fase di versamento.

Il rifiuto in fase di trasferimento viene comunicato in maniera sincrona al Produttore e normalmente avviene nel caso in cui il pacchetto di versamento inviato non corrisponda, in toto o in parte, al pacchetto di versamento ricevuto da Conserva, oppure che il pacchetto stesso non sia stato costruito secondo le regole concordate in fase di accordo di versamento. In fase di versamento, invece, i controlli vengono eseguiti in modalità asincrona. Il sistema, dopo aver ricevuto il pacchetto di versamento, tramite servizio temporizzato elabora il pacchetto stesso effettuando una serie di controlli.

È possibile consultare tutti i messaggi di errore che il servizio comunica al Produttore in fase di versamento nell'allegato relativo ai controlli, in particolare nella sezione controlli eseguiti in fase di versamento.

6.2 Preparazione e gestione del pacchetto di archiviazione

Successivamente alla ricezione del pacchetto di versamento, il sistema individua i pacchetti di archiviazione cui assegnare le unità di versamento in base alla tipologia e ad altri criteri specificati negli accordi di versamento, come ad esempio l'appartenenza ad un repertorio o ad una serie, o l'appartenenza ad un fascicolo.

Per le tipologie documentali versate in conservazione, gli accordi di versamento prevedono:

Tipologie documentali	Gestione del pacchetto di archiviazione
Fatture attive e passive	Le fatture elettroniche vengono gestite in apposite serie documentali ordinate progressivamente e legate al sezionale del registro; possono anche essere parte di procedimenti amministrativi, attività o affari e quindi esser soggette a fascicolazione. Di conseguenza all'interno del sistema di conservazione Conserva, le fatture attive vengono collocate sia nel pacchetto di archiviazione della serie delle fatture attive (una serie per ogni sezionale) che anche all'interno degli eventuali pacchetti di archiviazione relativi al/ai fascicoli in cui le fatture sono state inserite. Il pacchetto di archiviazione della serie viene chiuso il 31 marzo dell'anno successivo alla serie stessa; il pacchetto di archiviazione relativo al fascicolo verrà chiuso alla chiusura del fascicolo. Per ogni chiusura il sistema produce un indice del pacchetto di archiviazione, firmato digitalmente con firma XADES automatica e marcato temporalmente. Il pacchetto viene chiuso anticipatamente in caso di richiesta di esibizione dello stesso ed in tal caso ogni successiva modifica al fascicolo sarà registrata su una nuova versione del pacchetto. Il sistema di conservazione Conserva mantiene tutte le versioni precedenti di un pacchetto di archiviazione.
Registri IVA	I registri IVA versati corrispondono ad una determinata serie documentale annuale; di conseguenza ogni registro IVA andrà a far parte del pacchetto di archiviazione della serie documentale. Criteri e tempistiche di chiusura del Pacchetto di Archiviazione Per le serie documentali, Conserva genera una sequenza di pacchetti di archiviazione collegati fra loro; ogni pacchetto di archiviazione è composto da un massimo di 500 documenti. All'atto dell'archiviazione, Conserva verifica se sia presente un pacchetto di archiviazione aperto per quella serie e gli assegna il documento; nel caso non sia presente un pacchetto di archiviazione aperto per quella serie, ne apre uno nuovo e gli assegna il documento. L'ultimo pacchetto di archiviazione dell'anno viene chiuso il 15 gennaio dell'anno successivo.

Tipologie documentali	Gestione del pacchetto di archiviazione
Registro giornaliero di protocollo	I registri informatici di protocollo versati corrispondono ad una serie documentale annuale; di conseguenza ogni registro informatico di protocollo giornaliero andrà a far parte del pacchetto di archiviazione della serie documentale. Per le serie documentali, Conserva genera una sequenza di Pacchetti di archiviazione collegati fra loro; ogni Pacchetto di archiviazione è composto da un massimo di 500 documenti. All'atto dell'archiviazione, Conserva verifica se sia presente un Pacchetto di archiviazione aperto per quella serie e gli assegna il documento; nel caso non sia presente un Pacchetto di archiviazione aperto per quella serie, ne apre uno nuovo e gli assegna il documento. L'ultimo Pacchetto di archiviazione dell'anno viene chiuso il 15 gennaio dell'anno successivo.
UBUY GARE E AVVISI	Le documentazione del modulo UBUY GARE E AVVISI è organizzata in apposite serie documentali ordinate progressivamente ma possono anche essere parte di procedimenti amministrativi, attività o affari e quindi esser soggette a fascicolazione. Di conseguenza all'interno del sistema di conservazione Conserva, la documentazione in oggetto può esser sia nel pacchetto di archiviazione della serie relativa che anche all'interno degli eventuali pacchetti di archiviazione relativi al/ai fascicoli in cui la documentazione è inserita

La chiusura del pacchetto di archiviazione si verifica, normalmente, al momento di chiusura dell'unità archivistica o della serie a cui corrisponde.

Il tempo che intercorre tra il popolamento del pacchetto e il momento della chiusura non aumenta il rischio di corruzione della documentazione conservata: grazie al monitoraggio periodico e all'infrastruttura di sicurezza è possibile garantirne l'autenticità, ossia la sua identità ed integrità, documentabile tramite una chiara catena di evidenze.

Alla chiusura di un Pacchetto di archiviazione, il sistema produce un indice del pacchetto di archiviazione; ai fini dell'interoperabilità tra i sistemi di conservazione e come previsto dalla norma, l'indice del pacchetto di archiviazione deve corrispondere allo standard UNI 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.

Lo standard UNI SInCRO è uno schema XML e contiene sia i metadati finalizzati alla conservazione e acquisiti dal Produttore, che i riferimenti e le impronte dei file che compongono il pacchetto.

Al fine di render stabile l'indice, questo viene firmato digitalmente dal Responsabile del servizio di conservazione con firma XAdES-T automatica generata in modalità detached, e vi appone una marca temporale rilasciata da una Certificatore accreditato.

La chiusura del pacchetto di archiviazione può essere anticipata in caso di richiesta di esibizione; in tal caso, ogni successiva modifica alla serie sarà registrata su una nuova versione del Pacchetto di archiviazione. Conserva mantiene tutte le versioni di un pacchetto di archiviazione.

6.2.1. Aggiornamento dei pacchetti di archiviazione

Tutte le unità presenti in un pacchetto di archiviazione, sia chiuso che aperto, possono essere aggiornate; tutti gli aggiornamenti sono tracciati e le singole unità versionate.

In caso di aggiornamento di un'unità presente in un pacchetto di archiviazione chiuso, quest'ultimo viene migrato e la migrazione viene tracciata nell'indice del pacchetto di archiviazione.

Se a causa di eventi non previsti o per segnalazione esterna, tramite procedure di controllo a campione, venissero riscontrate perdite di dati o compromissione degli stessi si avvierebbe la procedura di ripristino applicabile in tre modalità:

1. se la perdita o la corruzione di dati è dovuta ad un incidente si attiva la procedura di Disaster Recovery;

2. in altri casi si ricreano, grazie alle informazioni presenti sul sistema, i pacchetti di versamento originali con cui gli oggetti digitali corrotti sono entrati in Conserva al fine di riversarli nuovamente nel sistema;

3. se l'attività descritta al punto 2 non fosse possibile, a causa della perdita definitiva di informazioni, si concorderebbe una procedura con il Produttore al fine di controllare sui sistemi produttori la possibilità di risalire agli oggetti digitali originali; la perdita definitiva dei dati è, ad ogni modo, improbabile, in quanto l'accesso al database è limitato al solo team di Conserva.

6.2.2. Selezione e scarto dei pacchetti di archiviazione

All'interno dell'accordo di versamento vengono riportati anche i tempi di conservazione dell'oggetto informativo stabiliti negli appositi massimari di scarto.

L'accordo, ove possibile, farà anche riferimento alla normativa che disciplina lo scarto di specifiche tipologie di oggetti informativi (ad esempio norme fiscali).

Nell'ambito dell'accordo di versamento vengono quindi specificate regole di scarto di:

- interi pacchetti di archiviazione;
- singoli documenti;
- singoli file all'interno dei documenti (ad esempio versioni differenti dello stesso documento, ricevute PEC, ecc.).

Sulla base delle indicazioni presenti nell'accordo di versamento, il sistema di conservazione mette a disposizione del Responsabile della conservazione del Produttore e dei suoi delegati la possibilità di avviare la procedura di selezione per individuare i pacchetti e/o oggetti informativi contenenti oggetti idonei allo scarto.

Lo scarto di singoli documenti o file comporterà la produzione di una nuova versione del pacchetto di archiviazione.

Lo scarto avviene mediante cancellazione dei documenti conservati; l'azione di scarto deve essere esplicitamente autorizzata dal Responsabile della conservazione o suo delegato, attraverso la spunta dei componenti da scartare della pagina del software di gestione, ad esso dedicata; si formerà una lista che sarà essa stessa oggetto di conservazione.

Per determinare i tempi si rimanda al Massimario di selezione e scarto, collegato con il piano di classificazione e alle informazioni contenute nel *Manuale di gestione dei flussi documentali e del protocollo informatico*; lo scarto viene normato ai sensi del DPR 37/2001, Regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli uffici dello Stato, nonché dalle Linee Guida AGiD.

L' INRiM avvia l'iter di scarto dopo aver ottenuto l'autorizzazione presso la Sovraintendenza Archivistica o la Commissione di sorveglianza di riferimento, come sancito dall' articolo 21 del d.lgs. 22 gennaio 2004, n. 42, Codice dei Beni Culturali e del Paesaggio e dal succitato DPR 37/2001.

Il Conservatore, nella figura del proprio responsabile della Conservazione, mantiene traccia delle richieste di scarto ricevute e correttamente eseguite, con l'indicazione a margine di eventuali errori occorsi durante lo svolgimento del processo, dei rimedi attuati e delle altre informazioni che ritiene meritevoli di annotazione.

6.3 Gestione del pacchetto di distribuzione ai fini dell'esibizione

Il Responsabile della conservazione e i suoi delegati hanno la facoltà di richiedere l'esibizione di un pacchetto di distribuzione opponibile a terzi nei seguenti modi:

- tramite la ricerca degli oggetti informativi dall'apposita interfaccia web di ricerca di Conserva;
- selezionando, sempre da interfaccia web di Conserva, gli oggetti informativi da esibire;
- richiedendo direttamente a CINECA l'esibizione degli oggetti informativi e dei relativi metadati che ne garantiscano autenticità e leggibilità;
- richiedendo la produzione di copia conforme di un documento secondo le modalità descritte nel paragrafo seguente.

Il Responsabile della conservazione e Conservatore hanno concordano le condizioni di distribuzione, cioè le modalità con le quali sarà messo a disposizione il contenuto dei pacchetti di archiviazione presenti in conservazione; allo scopo, l'interfaccia di consultazione del sistema di conservazione produce una lista sintetica delle unità ricercate.

All'interno della lista sintetica vengono riportati:

- Id documento;
- Versione documento;
- Codice Area Organizzativa Omogenea;

- Numero protocollo;
- Data protocollo;
- Oggetto.

Selezionando un'unità dalla lista, saranno mostrati tutti i metadati descrittivi dell'unità e sarà possibile scaricare il/i file contenuti nell'unità.

6.3.1 Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti

La produzione di duplicati e copie informatiche o analogiche, tramite il sistema di conservazione, avviene per mezzo di una richiesta dell'interfaccia web del Sistema di conservazione.

La distribuzione dei pacchetti a fine di esibizione avviene direttamente utilizzando apposite funzionalità dell'interfaccia web del Sistema di conservazione.

L'accesso web consente al Produttore di ricercare i documenti e le aggregazioni versate, di effettuarne il download e di acquisire le prove delle attività di conservazione.

Il Produttore autorizza gli utenti configurati nei ruoli di Responsabile della conservazione e delegato del Responsabile della conservazione, alla consultazione di quanto versato, tramite interfaccia web.

Inoltre, tramite l'interfaccia web, è possibile accedere a un servizio di monitoraggio in tempo reale dei versamenti effettuati, sia andati a buon fine che falliti.

Il Produttore può richiedere i documenti e le aggregazioni versate utilizzando appositi servizi, descritti nel manuale del sistema di conservazione del Conservatore.

La figura del pubblico ufficiale, individuato all'interno dell'Ente stesso, è necessaria nei seguenti casi:

- dichiarazione di conformità di una copia analogica di un documento informatico non protocollato, conservato nel sistema di conservazione;
- dichiarazione di conformità di una copia informatica di un documento informatico non protocollato, conservato nel sistema di conservazione;
- dichiarazione di conformità di copia informatica di documento informatico conservato nel sistema di conservazione nei casi di obsolescenza di formato. In questo caso specifico una volta riscontrato il rischio di obsolescenza, Produttore e Conservatore concordano un piano di migrazione ad altro formato (copia informatica di documento informatico).

6.3.2 Predisposizione di misure e garanzia dell'interoperabilità e trasferibilità ad altri conservatori

La Convenzione con il Conservatore, Consorzio Interuniversitario Cineca, prevede che, in caso di recesso o a scadenza di contratto, il Conservatore è tenuto a riversare i documenti informatici e le aggregazioni documentali informatiche conservate, i metadati a essi associati e le evidenze informatiche generate nel

corso del processo di conservazione nel sistema indicato dal Produttore, secondo modalità e tempi indicati nel Disciplinare tecnico allegato al manuale di conservazione del Conservatore.

Il Conservatore provvederà solo al termine del riversamento e solo dopo le opportune verifiche - effettuate da entrambe le parti e svolte di concerto tra le stesse - di corretto svolgimento del riversamento stesso, all'eliminazione dal proprio sistema di conservazione di tutti gli oggetti riversati e di tutti gli elementi riferiti al Produttore, garantendo la completa cancellazione e non leggibilità dei dati.

L'Ente ha inoltre la possibilità di richiedere al Conservatore l'acquisizione di documenti informatici e aggregazioni documentali informatiche precedentemente conservate presso altri conservatori.

Le operazioni di trasferimento dovranno avvenire con l'autorizzazione e la vigilanza delle competenti autorità, in particolare delle strutture del MiC.

6.3.3. Gestione delle anomalie

La segnalazione di un'anomalia o di un incidente può provenire sia dal Produttore sia dal gestore del Sistema di conservazione.

Tali segnalazioni avvengono mediante il sistema di tracciamento attraverso cui sono veicolate le comunicazioni fra i due attori così come la notifica di risoluzione degli stessi in funzione della tipologia di servizio coinvolto.

Il processo di monitoraggio e gestione delle anomalie si applica a tutti gli incidenti e problemi attinenti alle aree:

- Tecnologica (hardware, sistemi operativi e middleware);
- Applicativa;
- Sicurezza delle informazioni;
- Servizi tecnici impianti.

La gestione degli incidenti è composta dalle fasi:

- presa in carico e gestione della segnalazione;
- presa in carico e gestione incidente di 1° livello;
- presa in carico e gestione incidente di 2° livello;
- chiusura incidente;
- monitoraggio incidente;

La gestione delle anomalie è composta dalle fasi:

- individuazione del problema;

- risoluzione del problema;
- riesame dei problemi.

Si rimanda al Capitolo 7 in cui sono definite le specifiche operative e le modalità di interazione per la gestione delle anomalie e per il monitoraggio.

7. DESCRIZIONE DEL SISTEMA DI CONSERVAZIONE

In questa sezione è descritta l'architettura generale del sistema di conservazione, con particolare riferimento alle componenti logico-funzionali ed alle corrispondenti componenti tecnologiche.

Il sistema di conservazione CONSERVA, adottato dall'INRiM, è un servizio erogato in modalità SaaS installato presso il Data Center di CINECA ed è composto dalle componenti descritte di seguito, così come riportate nel Manuale di Conservazione CINECA aggiornato al 2021.

7.1. Componenti logiche

Le componenti logiche in cui è strutturato il sistema di conservazione CONSERVA del Consorzio Interuniversitario CINECA sono state individuate per agevolare e organizzare al meglio le attività di manutenzione ed evoluzione del sistema.

Di seguito viene rappresentato lo schema (Figura 7) delle componenti logiche che compongono il servizio, con una breve descrizione di ogni componente.

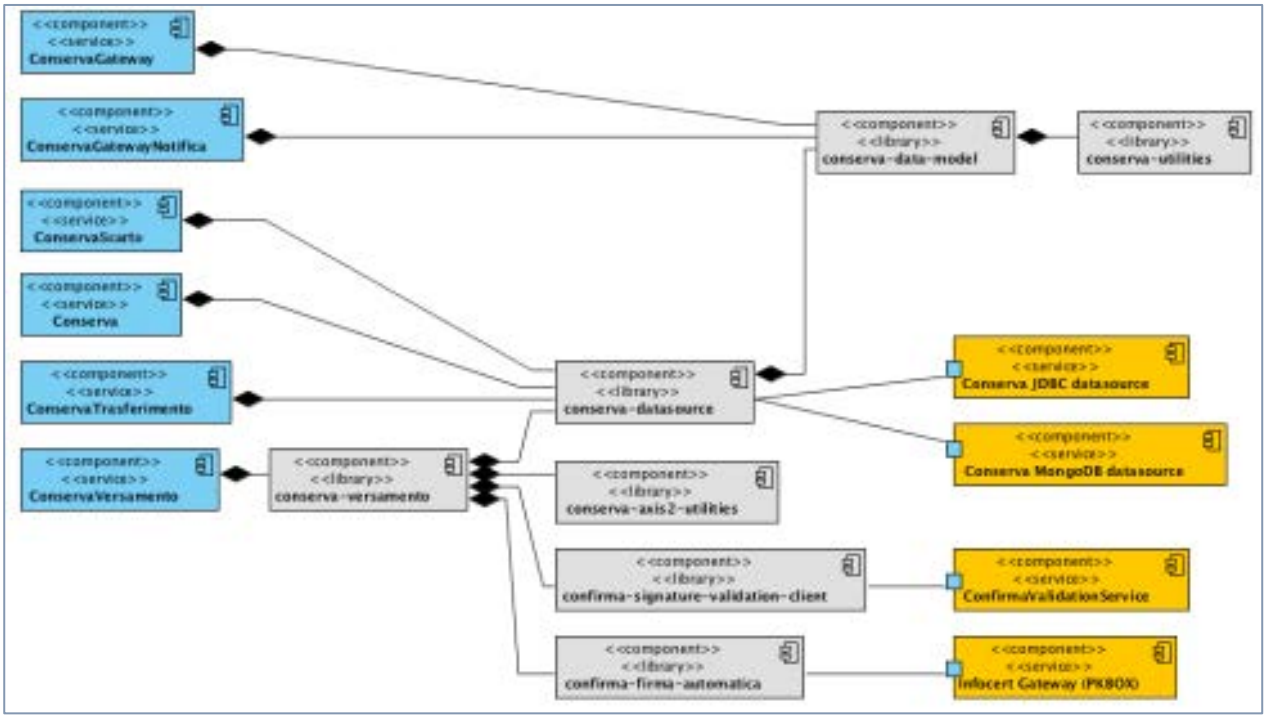

Figura 7. Schema delle componenti logiche che compongono il servizio. Da: Manuale di Conservazione Cineca

- **Conserva Servizio** - Componente che si occupa dell'accesso degli utenti al sistema. È un'applicazione web basata su un'architettura MVC (Model View Controller). Rende disponibili funzioni di ricerca ed esibizione (pacchetti di distribuzione), di consultazione di audit, di amministrazione e di recupero dati di versamento.

- **ConservaTrasferimento servizio** - Componente che riceve tramite web service i pacchetti di versamento inviati dai sistemi produttori. Comprende anche una serie di controlli che riguardano l'integrità e la correttezza formale del pacchetto di versamento.

- **Conserva-versamento libreria** - Componente che elabora i pacchetti di versamento ricevuti, li verifica ed effettua le operazioni necessarie affinché gli oggetti informativi in esso contenuti vengano presi in carico dal sistema di conservazione. Crea, popola e infine chiude i pacchetti di archiviazione in cui gli oggetti informativi vengono conservati.

- **ConservaVersamento servizio** – Web service di interfaccia con la libreria *ConservaVersamento* e servizi temporizzati.

- **Conserva-datasource libreria** – Libreria che si occupa di tutte le comunicazioni tra i componenti software e le basi di dati.

- **Conserva-data-model libreria** - Componente software dove vengono descritti gli oggetti che vengono elaborati e popolati da tutti gli altri componenti.

- **Conserva-utilities libreria** - Componente che mette a disposizione dell'intero sistema di conservazione metodi di utilità comuni a tutti gli altri componenti.

- **Conserva-axis2-utilities libreria** - Componente che mette a disposizione metodi che riguardano le connessioni tramite web service.

- **Conserva-solr libreria** - Componente che mette a disposizione metodi che consentono di indicizzare e ricercare elementi indicizzati.

- **Conserva-realm libreria** - Componente che mette a disposizione metodi che consentono di dialogare con il sistema di autenticazione e il sistema di autorizzazione.

- **Conserva-firma-automatica libreria** - Componente che si occupa dell'interazione con il Gateway di firma per l'apposizione delle firme automatiche necessarie al funzionamento di CONSERVA.

- **ConservaNotifica servizio** – Componente che gestisce le notifiche push dei rapporti e dei resoconti di versamento ai webservice registrati dei produttori.

- **CertificationAuthority servizio** – Componente che gestisce l'aggiornamento del repository locale dei certificati e delle CRL.

- **ConservaAdministration servizio** - Componente che permette l'amministrazione del sistema e della maggior parte dei componenti precedentemente descritti: ad esempio la creazione e la gestione di tutte le utenze che possono accedere a Conserva, la gestione dei servizi temporizzati, la creazione e gestione degli enti produttori e la creazione e gestione di nuovi accordi di versamento.

- **ConservaScarto servizio** – Componente che gestisce l'interazione fra il componente Conserva (interfaccia web di consultazione dell'archivio) e il componente conserva-versamento per la gestione dell'attività di scarto di oggetti informativi con la conseguente revisione dei pacchetti di archiviazione.

7.2. Componenti fisiche

L' architettura di CONSERVA presenta 3 ambienti separati fisicamente e logicamente:

- ambiente di produzione
- ambiente di pre-produzione
- ambiente di sviluppo

Lo schema riportato in Figura 8, rappresenta la distribuzione dei componenti nell'ambiente di produzione

Le componenti di produzione sono tutte virtualizzate. Relativamente ai sistemi di virtualizzazione sono presenti tre CISCO UCS, due a Bologna e uno a Roma.

Tutti i cluster che ospitano le macchine virtuali sono vmware, composti da almeno 8 nodi fisici (la-me UCS), in configurazione di HA (High Availability) e DRS (Distributed Resource Scheduler).

La ridondanza dei server in farm è gestita attraverso bilanciatori CISCO.

Nello specifico i servizi di produzione di CONSERVA sono attualmente così configurati:

- **Sistema di front end (business logic)**: due server in farm dietro bilanciatore, visibili da rete pubblica, con Apache e Tomcat Application Server.
- **Sistema di back end (business logic)**: un server singolo, visibile solo da rete privata, con Apache e Tomcat Application Server.
- **Sistema Solr:** un server singolo visibile solo da rete privata, con Apache Solr e Apache ZooKeeperIn Figura 9 sono descritte più chiaramente la distribuzione topologica delle componenti fisiche di CONSERVA.
- **Sistema MongoDB**: un ReplicaSet a tre nodi (primary , secondary , hidden), visibile solo da rete privata, con database MongoDB.
- **Sistema Oracle**: due server active/passive, visibili solo da rete privata, con database Oracle RDBMS.
- **Sistema LDAP**: due server in farm dietro bilanciatore, visibili solo da rete privata, con Open LDAP.
- **Servizio di firma automatica**: servizio offerto da fornitore esterno accreditato AgID.
- **Servizio di marcatura temporale**: servizio offerto da fornitore esterno accreditato AgID.

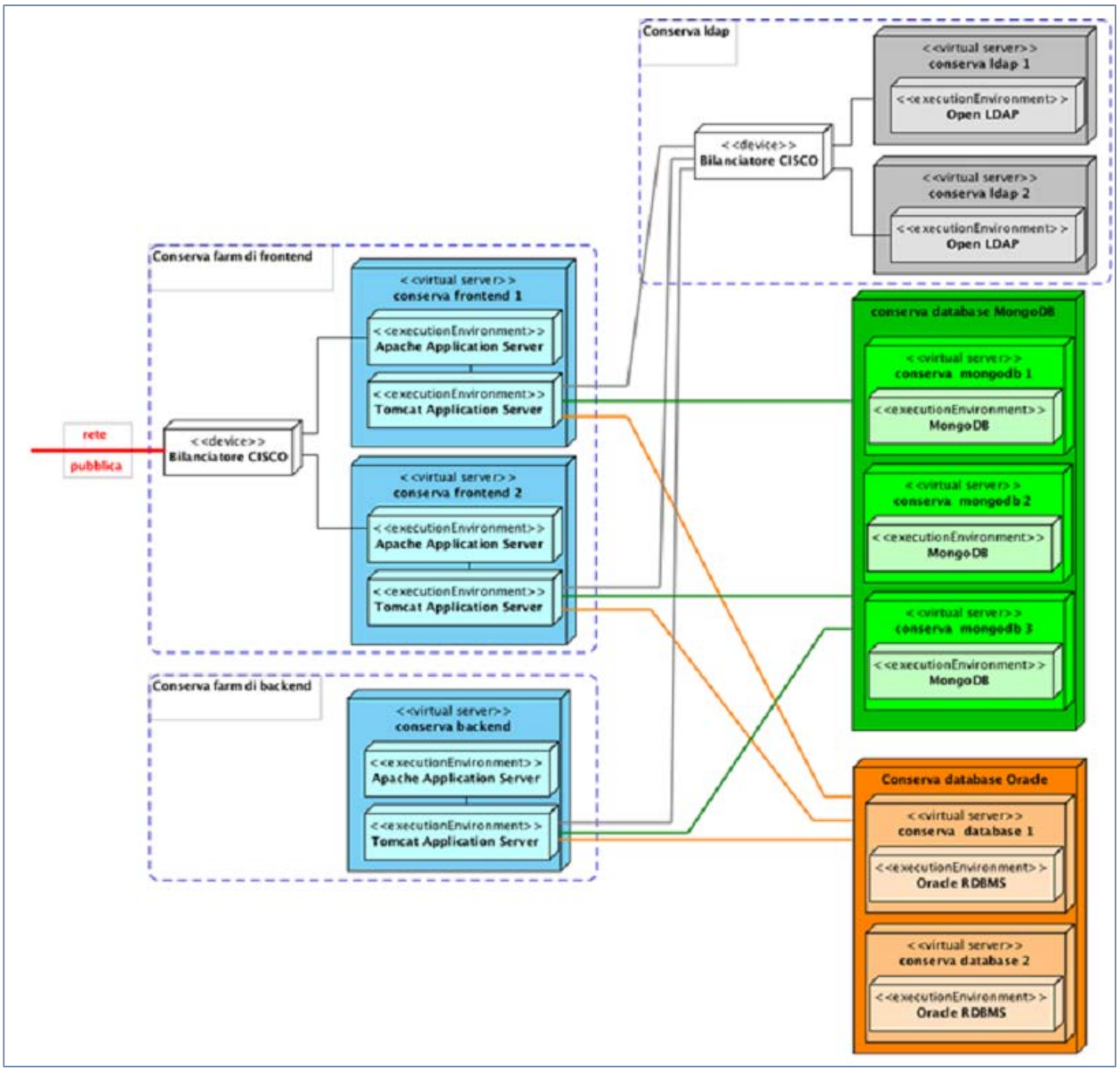

Figura 8. Distribuzione dei componenti CONSERVA. Da: Manuale di Conservazione Cineca

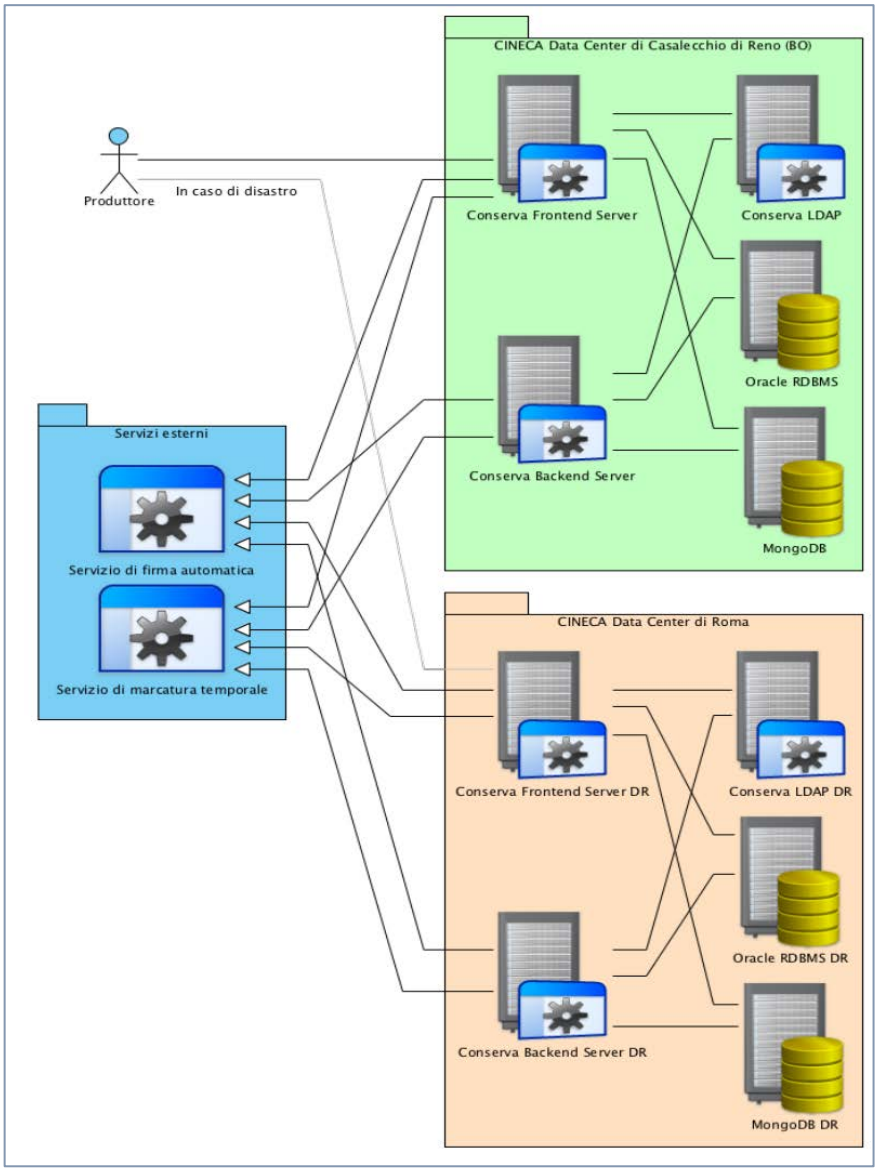

Figura 9. Distribuzione topologica delle componenti fisiche di Conserva. Da: manuale di Conservazione Cineca

Nel grafico di Figura 9 si descrive più chiaramente la distribuzione topologica delle componenti fisiche di Conserva.

Le sedi CINECA coinvolte sono:

- Casalecchio Di Reno, via Magnanelli 6/3 che ospita l'architettura di esercizio;
- Roma, via dei Tizi 6/b che ospita il Disaster Recovery.

Per i servizi di pre-produzione (collaudo) esiste una infrastruttura simile, distinta dalla precedente, ma con la stessa architettura a layer applicativi.

Per lo sviluppo esistono server distinti per layer, ma senza ridondanza.

Dal punto di vista di rete le interconnessioni tra i vari apparati sono schematizzabili come segue, con la dovuta ridondanza che garantisce l'alta affidabilità sia verso la LAN sia verso la SAN

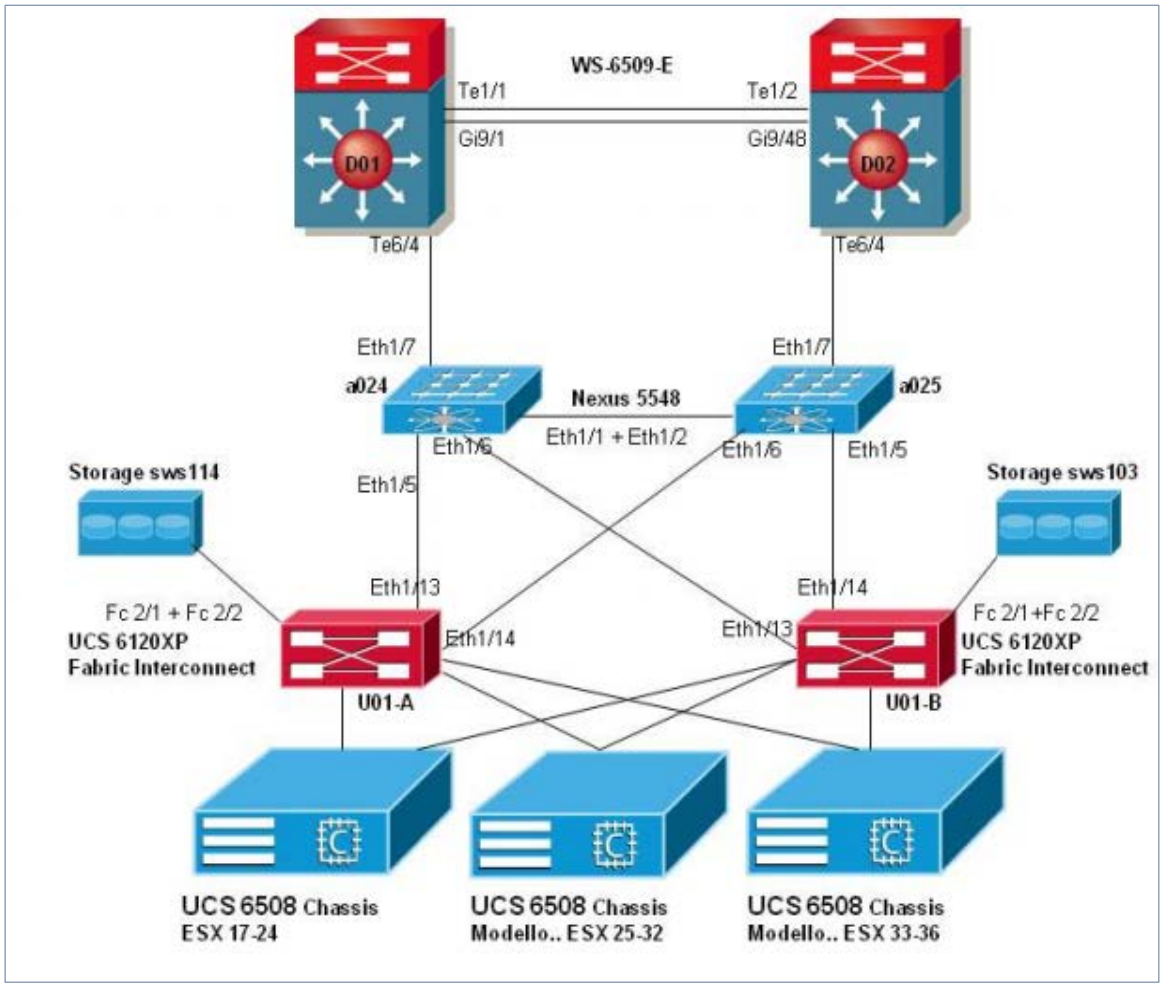

Figura 10. Schema interconnessioni degli apparati di Conserva. Da: manuale di Conservazione Cineca

7.3. Componenti tecnologiche

7.3.1 Software e strumenti software utilizzati

Partendo dal diagramma seguente (Figura 11), si descrivono le tecnologie utilizzate per il corretto funzionamento di CONSERVA, il servizio di conservazione CINECA:

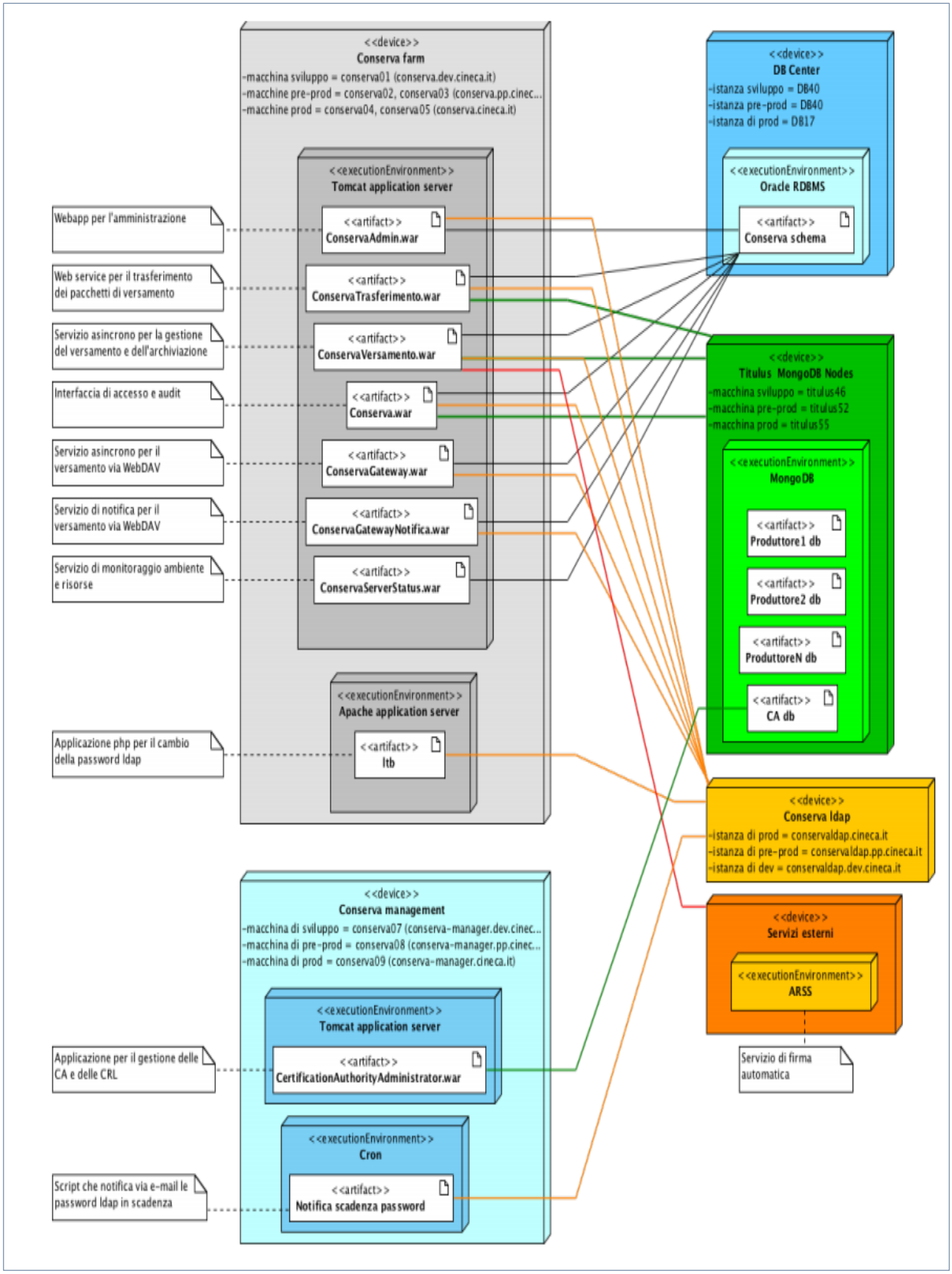

Figura 11. Diagramma descrittivo dei componenti Conserva. Da: Manuale di Conservazione Cineca

La seguente tabella descrive le tecnologie utilizzate per il corretto funzionamento di CONSERVA.

Tecnologia	Uso
JAVA	Sviluppo componenti distribuite sulla farm CONSERVA (*.war)
PHP	Manager per la gestione delle utenze registrate su LDAP
OpenLDAP	Implementazione LDAP per la gestione delle utenze
Apache Struts	Sviluppo componenti di presentation (CONSERVA, ConservaAdmin)
Apache Tiles	Sviluppo componenti di presentation (CONSERVA, ConservaAdmin)
Apache Axis2	Sviluppo Web Services
Apache Tika	Gestione formati file, riconoscimento pdf/a e sue versioni
Apache Tomcat	Servlet container
Apache HTTP Server	Web Server
WebDAV	Gestione condivisa di cartelle e file tra Produttore e Conservatore
Oracle	DB per gestire le relazioni tra gli oggetti che compongono Conserva
MongoDB	DB per salvataggio oggetti conservati
Quartz	Gestione dei servizi temporizzati di CONSERVA

7.3.2 Disaster Recovery

Il servizio di Disaster Recovery (DR) presenta le seguenti caratteristiche:

- Il sito primario del servizio di hosting è ubicato presso la sede Cineca di Casalecchio di Reno, mentre il sito secondario è ubicato presso la sede Cineca di Roma. Cineca si impegna a comunicare ai produttori, con adeguato preavviso, ogni variazione all'ubicazione dei siti.

- La frequenza di copia dei dati – ovvero la freschezza del dato sul sito DR – è detta RPO (Recovery Point Objective) ed è stabilita di 24H. La ripartenza del servizio sul sito di Disaster Recovery - RTO (Recovery Time Objective) è di 48H.

- I dati dei Titolari, gestiti nell'ambito del servizio di hosting, risiedono all'interno del territorio italiano, nella fattispecie presso i siti primario e secondario previsti per il servizio. Cineca si impegna a comunicare al Titolare, con adeguato preavviso, ogni variazione all'ubicazione dei siti, pur garantendo sempre l'ubicazione interna al territorio italiano.

- Cineca garantisce i servizi per la riattivazione e il ripristino del sistema informativo primario, in presenza di un evento catastrofico, di una condizione di emergenza o di un disastro.
  I criteri per la definizione di tali eventi e la responsabilità per l'attivazione del Piano di Disaster Recovery rimangono in carico a Cineca, che provvederà a darne visibilità ai Titolari. A fonte di eventuali integrazioni fra l'applicazione e sistemi terzi del Titolare, Cineca si impegnerà nel coordinamento con lo stesso per la gestione in fase di emergenza dei rispettivi Piani di Disaster Recovery.

- Cineca si impegna ad eseguire test periodici (almeno una volta l'anno) per simulare il funzionamento del sito di Disaster Recovery in caso di disastro del sito primario, al fine di verificare che sia assicurato il corretto ripristino del funzionamento del sistema informativo di produzione.

7.4. Procedure di gestione e di evoluzione del sistema

CONSERVA è concepito secondo il concetto *Secure by design*, ovvero la sicurezza è obiettivo di tutte le fasi del ciclo di vita del servizio.

In particolare ogni fase tiene conto dei principi di sicurezza descritti nella pubblicazione del NIST (National Institute of Standards and Technology) "*Engineering Principles for Information Technology Security*"[23]

7.4.1. Strategia di sviluppo e ciclo di vita del sistema CONSERVA

La scelta della strategia di sviluppo del software è stata decisa per i seguenti elementi:

- **Caratteristiche del prodotto:** un sistema di conservazione deve essere conforme alle Regole Tecniche in materia ed agli standard di riferimento (in particolare OAIS).

- **Modalità di rilascio del prodotto**: il sistema di conservazione può essere reso disponibile in più rilasci, tutti auto-consistenti e testati, che consistono in un arricchimento e miglioramento delle funzionalità precedenti.

- **Coinvolgimento del cliente del progetto:** a causa delle norme cogenti di conservazione, il cliente del servizio partecipa solo parzialmente alle scelte progettuali. In particolare rende chiari e manifesti i propri requisiti attraverso documentazione appositamente redatta e sottoscritta (accordo di versamento) che costituisce la base per la configurazione e personalizzazione del sistema, piuttosto che per lo sviluppo.

In seguito alle considerazioni sopra riportate, per lo sviluppo del sistema di conservazione si adotta una strategia incrementale e un modello di ciclo di vita *iterativo-incrementale*, come illustrato in Figura 12.

La strategia di sviluppo incrementale scompone il prodotto in più parti auto-consistenti, che possono comportare rilasci indipendenti in cui siano realizzate funzionalità specifiche immediatamente utilizzabili

[23] Per maggiori informazioni: http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf

dagli utenti. L'ordine di implementazione dei rilasci è determinato dall'inizio del progetto e concordato con le parti in causa.
Il ciclo di vita è concepito come lo sviluppo di una serie di singoli cicli completi di sviluppo, detti *iterazioni*, ognuno dei quali ha come risultato il rilascio in esercizio di macro-componenti del sistema, ovvero parti auto-consistenti con funzionalità complete utilizzabili dall'utente.

Il ciclo di vita si compone delle seguenti fasi (Figura 13):

- analisi completa (Analysis);
- macro-progettazione (Macro Design) dell'intero applicativo;
- pianificazione delle iterazioni, con definizione dei contenuti e priorità;
- iterazione:
  - progettazione di dettaglio (Detailed Design) delle funzionalità da implementare nell'iterazione;
  - sviluppo di codice e test unit (Code and Unit test) per le funzionalità da implementare nell'iterazione;
- integrazione con le parti precedenti e collaudo funzionale completo (Integration e Test);
- rilascio in esercizio (Release (Use)).

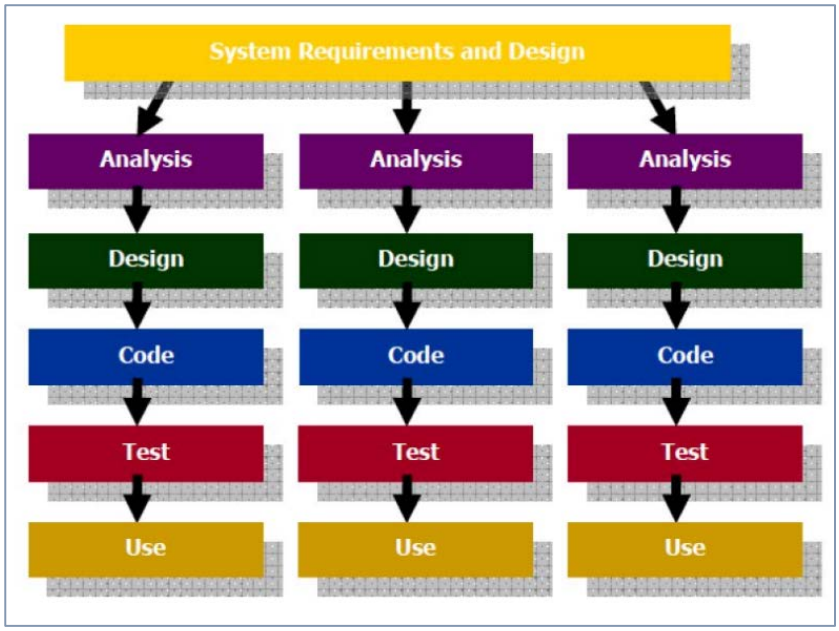

Figura 12. Ciclo di vita iterativo-incrementale dello sviluppo del software

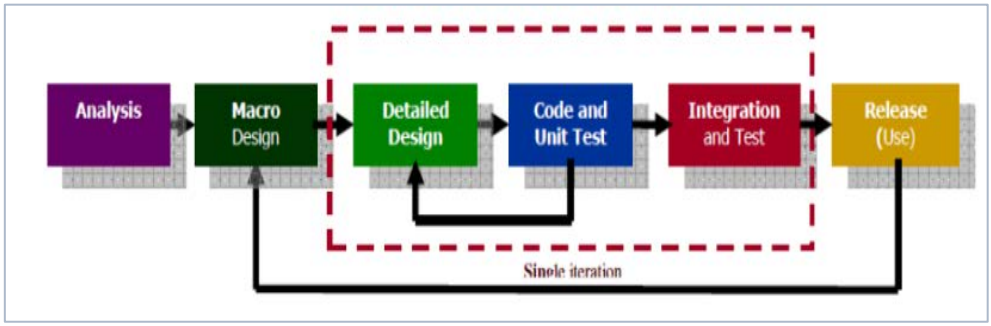

Figura 13. Dettaglio del ciclo di vita iterativo-incrementale dello sviluppo del software

7.4.2. Ciclo di sviluppo e rilascio del software

Le fasi attraverso le quali si è prodotto e rilasciato il software del servizio di conservazione Conserva di CINECA sono riassunte e descritte nel seguente garfico (Figura 14):

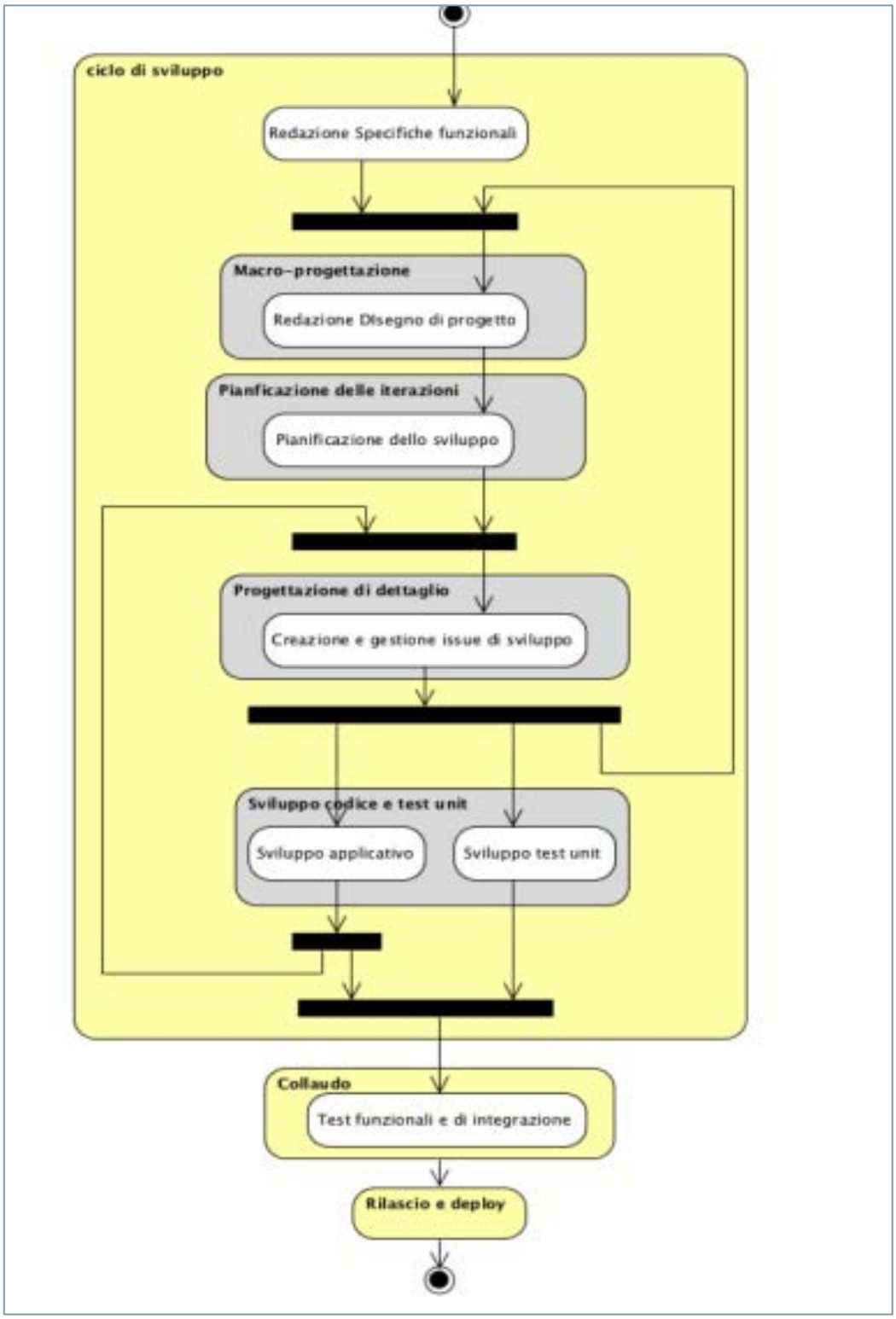

Figura 14. Fasi di produzione e rilascio del software

7.4.3 Metodologia di sviluppo Agile in JIRA

Alla strategia di sviluppo e al ciclo di vita del software scelti si affianca una metodologia di sviluppo agile che prende spunto dal framework di project management Scrum. Lo strumento utilizzato per issue e project tracking è JIRA, una web application installata e manutenuta dalla Divisione Sistemi e Tecnologie di CINECA, il cui accesso è regolato secondo le regole dettate dall'istruzione operativa pubblicata nell'intranet aziendale.

7.4.3.1 Issue

Le attività relative al processo di sviluppo e manutenzione del sistema sono organizzate in issue, per le quali:

- è sempre specificato un progetto di appartenenza (Project);
- è sempre specificato un tipo (Type);
- è sempre specificato un segnalante (Reporter);
- è sempre specificata una priorità di svolgimento (Priority);
- può essere specificato la data di consegna (Due date);
- è sempre specificata una descrizione breve (Summary);
- può essere specificata una descrizione dettagliata (Description);
- può essere specificato un assegnatario;
- possono essere specificate una o più versioni del progetto su cui la issue deve intervenire (Affects Version/s);
- possono essere specificate una o più versioni del progetto in cui verrà incluso il risultato della risoluzione della issue (Fix Version/s);
- possono essere specificati uno o più componenti del progetto a cui la issue fa riferimento (Components);
- può essere specificata una stima dei tempi di risoluzione (Original Estimate);
- possono essere specificate altre informazioni generali.

Il Type delle issue può esser valorizzato con i seguenti valori:

- **Bug**. Segnalazione di errore sul sistema o su uno specifico componente. Utilizzato soprattutto in fase di codifica, test o esercizio.
- **Requirement.** Specifica di requisiti generica. Utilizzato soprattutto nella fase di macro-analisi o progettazione dettagliata.

- **New feature**. Descrizione di una nuova funzionalità da implementare. Utilizzato soprattutto nella fase di macro-analisi o progettazione dettagliata.

- **Improvement.** Descrizione di miglioria da applicare a una o più funzionalità. Utilizzato soprattutto nella fase di macro-analisi, progettazione dettagliata e dopo l'esecuzione di collaudi.

- **Task.** Compito generico non classificabile come uno dei precedenti.

Ogni issue può avere uno o più sub-task, che possono essere di tipo:

- **Analysis Task:** sub-task che descrive un'attività di analisi.

- **Development task:** sub-task che descrive un'attività di sviluppo.

- **Test task_sub-task** che descrive un'attività di collaudo di una o più funzionalità.

Ogni issue o sub-task può essere collegato ad uno o più issue o sub-task. Ogni issue ha una priorità (Priority) in ordine di urgenza di risoluzione:

1. Red Code: l'attività segnalata è urgente e bloccante;

2. Very High: l'attività segnalata può essere urgente e di alta gravità, oppure non urgente ma bloccante;

3. High: l'attività segnalata può essere di alta gravità ma non urgente oppure urgente ma di gravità media;

4. Medium: l'attività segnalata può essere di gravità media ma non urgente, oppure urgente ma di gravità bassa;

5. Low: l'attività segnalata non è urgente ed è di bassa gravità.

Di seguito una tabella esplicativa delle relazioni tra gravità, urgenza e priorità di una issue:

Gravità	Urgenza	Priorità
Bloccante	Urgente	Red Code
Bloccante	Non Urgente	Very High
Alta	Urgente	Very High
Alta	Non Urgente	High
Media	Urgente	High
Media	Non Urgente	Medium
Bassa	Urgente	Medium
Bassa	Non Urgente	Low

Ogni issue e sub-task ha uno stato (Status):

- Opened: la issue è stata creata e deve essere ancora avviata l'attività in essa descritta;
- In progress: l'attività descritta nella issue è in corso;
- Resolved: la problematica descritta nella issue è risolta, e può essere verificata dal segnalante;
- Closed: l'attività descritta nella issue è definitivamente conclusa.

Di seguito il workflow che seguono gli stati della issue:

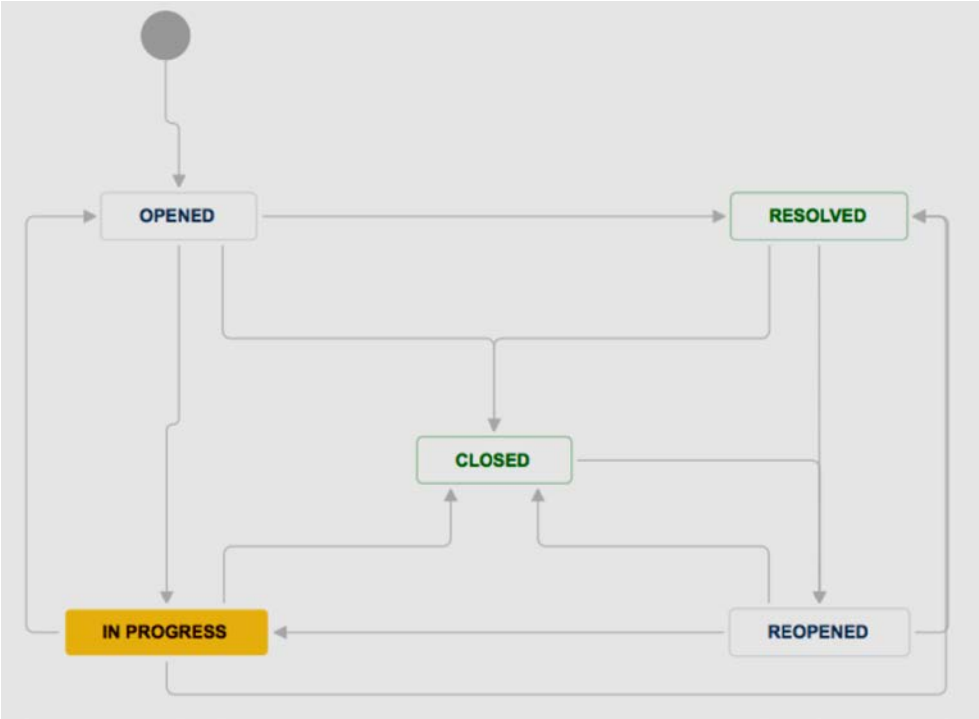

Figura 15. Workflow degli stati delle singole issue

7.4.3.2 Progetti

Le issue in JIRA sono organizzate in progetti.

Per ogni progetto JIRA è possibile specificare più versioni di riferimento, comprensive di data e stato di rilascio, e dei sotto-componenti (Components) che ne fanno parte.

Per ogni macro-componente del sistema di conservazione CONSERVA è stato predisposto un progetto JIRA. La versione del macro-componente del sistema di conservazione corrisponde alla versione del progetto JIRA.

Per ogni progetto JIRA possono essere eventualmente specificati dei componenti, che corrispondono ai sotto-componenti del macro-componente del sistema di conservazione.

Sono stati predisposti due progetti speciali Jira:

- *Conserva Avviamenti*: il progetto raccoglie i task di avvio di nuovi Produttori oppure di definizione di nuovi Accordi di Versamento sottoscritti con i Produttori;

- *Conserva Progetti*: trasversale ai macro-componenti, contiene le issue comuni ai macrocomponenti o che non riguardano macro-componenti.

I progetti JIRA sopra elencati sono accessibili dal Responsabile del servizio di conservazione, dal Responsabile dello sviluppo, dal Responsabile della funzione archivistica e dal team di sviluppo, i quali assumono ruoli specifici nello schema degli accessi.

7.4.3.3 Backlog

Il backlog è un contenitore di tutte le issue di uno o più progetti JIRA. Il backlog del sistema di conservazione è relativo a tutti i progetti JIRA sopra menzionati. La funzione principale del backlog è quella di permettere di visualizzare e organizzare tra i vari sprint le issue aperte su tutti i progetti di CONSERVA.

7.4.3.4 Sprint

La metodologia di sviluppo si basa sulla possibilità di realizzare un progetto per passi successivi, detti sprint.

Ad ogni sprint si aggiungono funzionalità e si verifica il risultato dell'attività svolta.

Uno sprint può essere associato a issue contenute nel backlog, appartenenti ad uno o più progetti JIRA.

Il termine dello sprint può o meno coincidere con il rilascio della versione di uno o più progetti, ovvero l'emissione della release di uno o più macro-componenti.

La durata dello sprint, mediamente di una settimana, può variare a seconda del numero di giorni lavorativi oppure da particolari attività che richiedano un arco temporale più breve o più lungo.

Lo sprint raramente coincide con le iterazioni del ciclo di sviluppo, sia a causa della durata che dell'eventuale sovrapposizione temporale delle stesse.

7.4.3.5 Versionamento semantico dei componenti

Il numero di ogni versione dei componenti di CONSERVA è costituito da 3 cifre:

MAJOR.MINOR.PATCH.

- L'incremento della prima cifra (MAJOR) è a fronte di modifiche sostanziali all'applicazione, che rendono il componente non retro-compatibile con le versioni precedenti.

- L'incremento della seconda cifra (MINOR) è a fronte di modifiche sostanziali all'applicazione, che mantengono il componente retro-compatibile con le versioni precedenti.

- L'incremento della terza cifra (PATCH) indica una release contenente correzioni di bug e interventi minori con un basso impatto sulla stabilità dell'applicazione e sulla sua usabilità.

7.4.5 Gli ambienti di esercizio

7.4.5.1 Separazione degli ambienti

Per CONSERVA sono attivi tre ambienti distinti e separati:

- un ambiente di sviluppo, adatto ad ospitare componenti e dati ai fini di implementazione e test;
- un ambiente di pre-produzione, con le stesse identiche caratteristiche di quello di produzione, adatto ad ospitare componenti e dati ai fini di collaudi e prove di integrazione;
- un ambiente di produzione, adatto ad ospitare i componenti e i dati al fine dell'esercizio.

Ogni ambiente è composto da un'infrastruttura middleware costituita da uno o più application server (tipicamente Apache e Tomcat) e da una banca dati, costituita da database relazionali e non, ed è dedicato unicamente ad applicazioni appartenenti al campo di applicazione del SGSI (Sistema Gestione Sicurezza Informazioni).

L'accesso agli ambienti è regolato da specifiche istruzioni operative.

Quelli di sviluppo e pre-produzione sono ambienti che non garantiscono né sicurezza né affidabilità.

Per questo motivo devono essere utilizzati solo a fini di implementazione e test e possono ospitare dati non anonimi solo per il tempo strettamente necessario ai fini operativi.

7.4.5.2 Gestione e validazione degli ambienti

Gli ambienti sono gestiti dalla Divisione sistemi e tecnologie di CINECA.

I requisiti degli ambienti sono stabiliti dal Responsabile dello sviluppo e dal Responsabile del servizio di conservazione in accordo con la Divisione sistemi e tecnologie.

Con cadenza almeno annuale il Responsabile dello sviluppo revisiona i requisiti per valutarne la correttezza in funzione dell'utilizzo passato e futuro di oggetti informativi.

Le richieste d'installazione, di aggiornamento e d'intervento straordinario sono gestite da apposite istruzioni operative aziendali.

In seguito ad ogni rilascio, modifica o aggiornamento degli ambienti di esercizio, è prevista un’attività di validazione nel rispetto di istruzioni operative a questo dedicate.

7.4.5.3 Sicurezza dei servizi e delle transazioni applicative

Indipendentemente dai requisiti stabiliti, vengono applicati meccanismi di protezione dei dati che transitano in rete, tali da impedirne accessi fraudolenti o non autorizzati. In particolare tutti gli host dei servizi sono accessibili esclusivamente attraverso protocollo HTTPS.

Gli algoritmi crittografici, la lunghezza delle chiavi asimmetriche e in generale gli aspetti di sicurezza inerenti al protocollo devono essere conformi a quanto indicato nella normativa vigente in materia ed agli standard internazionali.

7.5. Monitoraggio e controlli

Possiamo suddividere le attività di monitoraggio e controllo in due macro aree:

- integrità e congruenza strutturale;
- integrità e congruenza logica.

Sul primo lotto di controlli sono attivi appositi strumenti di monitoraggio sotto il diretto controllo della Divisione sistemi e tecnologie di CINECA e del Responsabile della sicurezza. I secondi sono soggetti a controlli automatici e manuali (a cura del Responsabile del servizio e del Responsabile della funzione archivistica di conservazione) tramite appositi strumenti messi a disposizione dal servizio.

7.5.1. Procedure di monitoraggio

Tutta l'infrastruttura tecnologica e applicativa del sistema di conservazione CONSERVA è mantenuta sotto controllo da un sistema di monitoraggio continuo (365/24/7) che consente di misurare lo stato della stessa e dei servizi in ogni momento.

In caso di anomalie rilevate, il sistema allerta i gruppi di gestione infrastrutturale ed applicativa per la gestione degli incidenti o per intervenire in modo proattivo per evitare l'occorrenza di situazioni che possano creare discontinuità del servizio.

Il monitoraggio consente di misurare lo stato e le metriche di funzionamento della maggior parte dei sistemi applicativi, ed è in grado di dialogare secondo i protocolli più diffusi delle applicazioni, ed è in grado di intercettare le metriche di funzionamento (quali CPU, uso della memoria, della rete, I/O, disco, stato complessivo del sistema operativo, raggiungibilità IP, icmp, ecc.) di ogni sistema e/o servizio applicativo; in particolare consente:

- la rilevazione degli incidenti;
- il monitoraggio del funzionamento dei servizi e degli oggetti informativi relative ai "livelli funzionali";
- di avere un servizio di allerta basato su una vasta gamma di parametri e di soglie di allerta configurabili;
- di avere uno strumento per misurare il rispetto dei livelli di servizio;
- di codificare le procedure di reazione agli *alert* che rappresentano criticità sui "livelli funzionali" o sui servizi;
- evitare falsi allarmi su oggetti che non sono realmente down ma sembrano tali a causa del malfunzionamento di un altro oggetto;
- l'analisi proattiva degli indicatori di performance.

Ogni anomalia rilevata viene gestita secondo i processi di *event, incident, problem management* e secondo le procedure che si ispirano alle Linee Guida ITILv3 _Information Technology Infrastructure Library[24].

7.6. Verifica dell'integrità degli archivi

Le procedure utilizzate nello sviluppo, nella manutenzione e nella distribuzione di CONSERVA garantiscono l'integrità dell'archivio, tuttavia si è ritenuto indispensabile prevedere ulteriori strumenti di monitoraggio, attivati a campione o in corrispondenza di specifici eventi.

7.6.1. Monitoraggio a campione degli archivi

Sono disponibili procedure di controllo che, a campione, verificano l'integrità di:

- Oggetti informativi;
- Pacchetti di archiviazione.

Queste procedure, eseguite a campione in maniera non presidiata, secondo una temporizzazione stabilita dal Responsabile del servizio di conservazione, possono essere eseguite su esplicita richiesta del Responsabile della conservazione del cliente, del Responsabile del servizio di conservazione o del Responsabile della funzione archivistica di conservazione.

L'integrità viene accertata attraverso controlli incrociati volti a garantire che file e metadati non abbiano subito variazioni in seguito alla loro acquisizione, fatte salve le produzioni di eventuali copie informatiche a seguito di obsolescenza di formati, per le quali CINECA si riserva di descrivere più in dettaglio il processo.

La medesima procedura verifica anche la presenza di file in formati prossimi all'obsolescenza. Nel caso venissero riscontrate anomalie o formati a rischio di obsolescenza, il sistema notificherà al Responsabile del servizio e al Responsabile dello sviluppo l'incidente. Questi valuteranno le caratteristiche dell'incidente, coinvolgendo ove necessario il Responsabile della sicurezza, il Responsabile della funzione archivistica di conservazione ed il Responsabile della conservazione del cliente per stabilire le modalità di intervento. In particolare la produzione di copie informatiche di documenti informatici, dovuta ad obsolescenza dei formati, dovrà essere preventivamente concordata con il Responsabile della conservazione di ogni cliente coinvolto.

7.6.2. Controllo integrità unità a seguito di richiesta di esibizione

A seguito di una richiesta di esibizione, CONSERVA allega al pacchetto di distribuzione un rapporto in cui viene riportato l'esito delle procedure di verifica effettuate sull'integrità del pacchetto generato.

Nel caso in cui la verifica di integrità del contenuto del pacchetto di distribuzione desse esito negativo, oltre a produrre il rapporto il sistema notifica l'errore a chi ha richiesto l'esibizione, al Responsabile della conservazione del Titolare coinvolto ed agli eventuali suoi delegati, al Responsabile del servizio di Conservazione, al Responsabile della funzione archivistica di conservazione e al Responsabile dello sviluppo. Questi ultimi avvieranno la procedura di gestione dell'incidente coinvolgendo il Responsabile della sicurezza ed il Responsabile della conservazione del Titolare se necessario.

[24] per maggiori informazioni: http://www.itilitalia.com/itilv3.htm

7.7 Politiche di conservazione dei log

I log applicativi di CONSERVA sono divisi in 3 distinti livelli (INFO, WARN, ERROR) e includono diverse informazioni a seconda della componente logica che li produce.

Tutti i componenti elencati, in caso di errori ed eccezioni, oltre a registrare i log, inviano mail al Team di Conserva in modo da sollecitare una risposta al problema generato.

Le categorie di log di sistema gestite per il servizio di conservazione Conserva di CINECA sono le seguenti:

- dati traffico telematico;
- eventi informativi;
- eventi anomali (allarmi, eccezioni);
- access log (login e logout amministratori di sistema).

L'accesso ai sistemi viene tracciato da un sistema di logging centralizzato di tutto il traffico di log.

In particolare viene:

- raccolto centralmente il log per gli accessi ai dispositivi critici: rete, DB, sicurezza, sistemi;
- attuato un sistema per la non modificabilità degli stessi log;
- mantenuto aggiornato l'elenco degli amministratori di sistema e database, nominati con lettera di incarico registrata dall'ufficio personale, depositando l'elenco sull'area documentale dell'intranet aziendale;
- effettuata la verifica periodica sul corretto utilizzo tramite una checklist operativa documentata per definire la procedura di verifica (es.: verifica che non siano presenti login non autorizzati come amministratori di sistema, che il log esista, che gli hash che ne garantiscono la non alterazione corrispondano);
- mantenuto l'elenco di tali verifiche periodiche con data di effettuazione, issue che traccia l'esecuzione, sistemi testati, esito della verifica;

Per ogni tipologia di log di sistema sono definiti specifici attributi come in tabella:

Livello di severità	**Periodo di archiviazione**
Eventi informativi	1 mese
Eventi anomali	Il tempo necessario all'investigazione e risoluzione dell'anomalia

Dati traffico telematico	12 mesi
Amministratori sistema	6 mesi

A questi si aggiungono i log applicativi, per i quali si considera un periodo di conservazione di almeno 6 mesi, indipendentemente dal loro livello di gravità.

Di seguito sono elencate le diverse componenti logiche di Conserva.

7.7.1 ConservaTrasferimento

Il componente *ConservaTrasferimento* registra i log su MongoDB e, come tutti gli altri, traccia errori, eccezioni e warning quando accadono. Questi log sono consultabili dal Responsabile della conservazione tramite interfaccia CONSERVA; inoltre, alla ricezione di un pacchetto di versamento, il componente registra le seguenti informazioni:

• data del trasferimento;

• classe che sta effettuando il log;

• ente produttore che ha inviato il pacchetto di versamento;

• id del pacchetto di versamento per riconoscerlo all'interno di CONSERVA;

• nome macchina CONSERVA che ha elaborato il pacchetto di versamento;

• indirizzo IP della macchina da cui è partito il versamento;

• tipo di azione richiesta;

• tempo impiegato ad effettuare l'azione richiesta;

• livello del log (INFO, WARN, ERROR);

• risultato del trasferimento (es.: "Pacchetto di versamento trasferito con successo").

7.7.2 ConservaVersamento

Il componente CONSERVAVersamento registra i log su MongoDB e, come tutti gli altri, traccia errori, eccezioni e warning quando si accadono. Questi log sono consultabili dal Responsabile della Conservazione tramite interfaccia CONSERVA; inoltre, il componente registra le varie attività del versamento:

• elaborazione controlli versamento (JOB_VERSAMENTO, JOB_RECUPERO_VERSAMENTO);

• elaborazione delle attività riguardanti l'archiviazione (JOB_ARCHIVIAZIONE);

• elaborazione delle attività riguardanti la notifica (JOB_NOTIFICA).

Le informazioni registrate sono diverse a seconda dei job, quelle comuni a tutte le attività sono:

• data dell'evento;

• livello del log (INFO, WARN, ERROR);

• tipo di job che genera il log;

• nome della macchina Conserva che ha gestito l'attività;

• informazioni riguardanti unità di versamento, unità documentale e/o unità archivistica,

pacchetto di versamento e/o pacchetto di archiviazione interessati dall'attività.

7.7.3 ConservaNotifica

Il componente ConservaNotifica registra i log su MongoDB e, come tutti gli altri, traccia errori, eccezioni e warning quando si accadono. Questi log sono consultabili dal Responsabile della Conservazione tramite interfaccia Conserva; inoltre, il componente registra le varie attività del processo di notifica push:

• notifica resoconto di versamento (JOB_NOTIFICA_RESOCONTO);

• notifica rapporto di versamento (JOB_NOTIFICA_RAPPORTO);

Le informazioni registrate sono diverse a seconda dei job, quelle comuni a tutte le attività sono:

• data dell'evento;

• Produttore;

• livello del log (INFO, WARN, ERROR);

• tipo di job che genera il log;

• nome della macchina Conserva che ha gestito l'attività;

• informazioni riguardanti endpoint di notifica.

7.7.4. CONSERVA

Il componente CONSERVA registra i log su MongoDB e, come tutti gli altri, traccia errori, eccezioni e warning quando accadono. Questi log sono consultabili dal Responsabile della Conservazione tramite interfaccia dello stesso componente CONSERVA; inoltre, il componente registra le attività degli utenti che si collegano all'interfaccia:

- registra il login e il logout;
- registra le ricerche effettuate;
- registra la visualizzazione di unità archivistiche/unità documentali;

- registra il download di file;
- registra le richieste di esibizione dei documenti.

Le informazioni registrate sono riguardo le attività sono:

- username dell'utente;
- nome del Produttore a cui l'utente appartiene;
- nome macchina CONSERVA che ha gestito l'attività;
- indirizzo IP del computer dell'utente;
- testo per descrivere l'attività.

7.8. Soluzioni adottate in caso di anomalie

Le anomalie generate durante il normale esercizio del servizio di conservazione possono essere distinti in diverse categorie:

- **anomalie di sistema:** sono anomalie legate all'infrastruttura hardware e middleware che ospita CONSERVA;
- **anomalie applicative:** sono anomalie legate ai componenti applicativi, in particolare:

  • accesso degli utenti alle interfacce web;

  • richieste dell'utente pervenute attraverso interfacce web o chiamate a web service, quali ad esempio: trasferimento dei pacchetti di versamento e richiesta di pacchetti di distribuzione, ecc.;

  • modifiche dello stato degli oggetti durante le fasi di versamento e archiviazione operate automaticamente dal sistema di conservazione (versamento o rifiuto unità, generazione e notifica rapporti di versamento, ecc.);

  • eccezioni causate da malfunzionamenti del software o dell'infrastruttura sottostante rilevabili dagli applicativi (indisponibilità dei database o di servizi esterni, esaurimento della memoria, errori di lettura/scrittura su filesystem, ecc.);

  • verifiche del controllo di consistenza degli oggetti conservati: sia su richiesta, sia come risultato dell'operazione automatica a campione, sia come verifica in fase di esibizione.

- **Anomalie rilevate dai tool di monitoraggio**. L'infrastruttura middleware che ospita CONSERVA è dotata di tool di monitoraggio completamente configurabile che segnala le anomalie al normale funzionamento del servizio.

7.8.1. Gestione segnalazione delle anomalie

Lo strumento per il tracciamento e la gestione degli incidenti è il sistema di issue tracking Jira, a sua volta collegato ad un'interfaccia web semplificata per le utenze del Produttore, detta Customer Portal.

La segnalazione di un'anomalia può provenire:

- dal Produttore attraverso il Customer Portal
- da personale CINECA, attraverso il sistema di issue tracking Jira

Una volta notificata l'anomalia tramite il sistema di Customer Portal, questa deve essere formalmente registrata da parte del team di CONSERVA con l'apertura di una issue su Jira, collegata a quella di notifica, in cui deve essere specificato il tipo Bug, devono essere aggiunti i componenti Sistema, Incidente e, eventualmente, Lesione SLA (solo se l'anomalia riscontrata può comportare una potenziale lesione dei livelli del servizio stabiliti). Se possibile vanno specificati anche il/i, Produttore (Customer) su cui si riflette l'incidente e l'ambiente (Environment) coinvolto (componente software e sua versione).

Se la segnalazione dell'anomalia è effettuata da personale CINECA, la procedura di registrazione appena specificata è eseguita contestualmente all'apertura della issue di segnalazione su Jira.

Una volta avvenuta la registrazione l'incidente deve essere trattato.

Innanzitutto si procede all'analisi dell'anomalia aprendo un sub-task dell'issue Jira di registrazione dell'anomalia di tipo "Analysis Task", in cui verranno indicate le cause dell'incidente (se note), il componente software o infrastrutturale che ha causato il problema ed infine l'indirizzamento della risoluzione dell'anomalia. Si procede, quindi, secondo le seguenti opzioni:

- se la causa è un componente software verrà aperta una nuova issue su Jira di tipo Bug che costituisce l'azione di avvio di un ciclo di sviluppo per la risoluzione dell'anomalia rispettando le regole del "Ciclo di sviluppo del software";
- se la causa è un errore di configurazione verrà aperta una issue su Jira specificando il componente Configurazione e sarà cura del team di CONSERVA risolvere l'anomalia riscontrata riportando lo stato di avanzamento dell'attività nella issue di registrazione formale;
- se la causa è infrastrutturale verrà aperta una segnalazione alla Divisione sistemi e tecnologie di CINECA, nel rispetto di istruzioni operative a questo dedicate, inserendo i riferimenti all'issue di registrazione formale.

Una volta effettuata l'azione correttiva, ove possibile, è necessario effettuare un test della risoluzione del problema: in questo caso deve essere aperto un sub-task di tipo Test Task nella issue di registrazione dell'incidente oppure nella issue di risoluzione dell'incidente collegata alla registrazione.

Ad azione correttiva ultimata, e dopo aver ricevuto dall'autore della segnalazione conferma di avvenuta risoluzione del problema, si potrà chiudere l'incidente modificando lo stato dell'issue di registrazione formale dell'anomalia in closed.

In questo caso specifico una volta riscontrato il rischio di obsolescenza, Titolare e Conservatore concordano un piano di migrazione ad altro formato (copia informatica di documento informatico).

8. TRATTAMENTO DEI DATI PERSONALI

Il Responsabile del trattamento dei dati ha il compito di tutela delle informazioni contenute nei documenti da conservare; tale ruolo viene svolto sia dal Produttore che dal Conservatore nelle forme previste dal Codice in materia di protezione dei dati personali.

L'Ente ha affidato al Consorzio Interuniversitario Cineca, dotato di specifica competenza ed esperienza, lo svolgimento del processo di conservazione secondo quanto stabilito nell' Atto di Nomina del 25 luglio 2016, Prot. n. 0003327 del 05/08/, in conformità all'art. 28 del Regolamento UE 679/2016 e delle Linee Guida AgID 2020, assume il ruolo di Responsabile del trattamento dei dati.

Agli effetti del contratto le parti si sono impegnate a conformarsi alle disposizioni del Codice in materia di protezione dei dati personali e successive modifiche ed integrazioni.

8.1 Istruzioni e individuazione dei compiti ai quali deve attenersi il responsabile esterno al trattamento dei dati personali.

In base all'Atto di nomina a Responsabile del Trattamento del 05/08/2016, Prot. n. 0003327, il Consorzio Interuniversitario CINECA dovrà in particolare curare i seguenti adempimenti:

- nominare gli incaricati del trattamento e gli eventuali amministratori di sistema, di database e di software complesso e fornire loro dettagliate istruzioni operative;
- verificare, almeno annualmente, la sussistenza delle condizioni per la conservazione dei profili di autorizzazione assegnati agli incaricati del trattamento;
- conservare e mantenere aggiornato, in base a quanto prescritto nel provvedimento del 27/11/2008 del Garante (Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni della funzioni di amministratore di sistema) e successive modifiche, gli estremi identificativi (nome, cognome, area organizzativa di appartenenza) delle persone fisiche preposte quali amministratori di sistema/database /software complesso;
- verificare l'operato degli amministratori di sistema/database/software complessi nominati con una cadenza almeno annuale, al fine di controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali;
- comunicare al Titolare i nominativi degli incaricati e degli amministratori di sistema/database/software complesso;
- assicurare la predisposizione e aggiornamento di un sistema di sicurezza dei dati, in conformità con le misure minime prescritte nel D.lgs. 196/2003 e successivi

I dati personali del cui trattamento CINECA è nominato Responsabile sono relativi a:

- personale e soggetti esterni che intrattengono con l'ENTE a qualunque titolo rapporti di natura economica, finanziaria, commerciale, istituzionale o di collaborazione scientifica;

- documenti e fascicoli e contenuti digitali archiviati in Conserva da personale dell'ENTE o da applicativi gestionali in uso presso l'ENTE.

L'ambito di designazione di CINECA a Responsabile del trattamento è individuato come segue:

Manutenzione del sistema informativo che compone il servizio:

- gestione e manutenzioni delle componenti software di infrastruttura (ivi inclusi i database), compresi aggiornamenti del sistema informativo e, ove necessario,
- migrazione e adeguamento delle basi dati;
- tuning dei sistemi (ivi inclusi i database) e dell'infrastruttura;
- monitoraggio dei servizi e dei sistemi (ivi inclusi i database);
- supporto, troubleshooting, problem determination e problem solving sul malfunzionamento del servizio dovuto a cause infrastrutturali del Data Center del CINECA;
- attività di Disaster Recovery;
- attività di database administration (salvataggio e ripristino dei dati, import ed export dei dati, escluse estrazioni selettive dei dati).

- Creazione in CINECA di ambienti di test mediante copia (parziale o totale) delle basi dati utilizzate dal sistema Conserva, da utilizzarsi esclusivamente per la diagnostica degli errori, per l'esecuzione dei piani di test funzionali per la validazione di nuove versioni del software, per le verifiche di carico e performance dell'intero sistema.
- Accesso alle informazioni gestite in Conserva per conto dell'ENTE, in modo procedurale e non procedurale per la verifica delle segnalazioni di anomalie inviate dall'ENTE al personale CINECA incaricato.

Quanto sopra fermo restando l'obbligo di CINECA di operare secondo le istruzioni generali impartite dal titolare e di fornire al medesimo tutte le informazioni necessarie per consentire l'attuazione di adeguate verifiche periodiche.