



UNIVERSITÀ DI PARMA

ALLEGATO 8

Manuale di Conservazione

Consorzio interuniversitario CINECA

Allegato in riferimento al MANUALE DELLA CONSERVAZIONE

REVISIONI

Nr	Data	Modifiche
00	20 giugno 2017	Prima stesura

Manuale di Conservazione

Consorzio Interuniversitario CINECA

INFORMAZIONI SULLA CLASSIFICAZIONE DEL DOCUMENTO

LIVELLO DI CLASSIFICAZIONE		DATA DI CLASSIFICAZIONE O DI MODIFICA ALLA CLASSIFICAZIONE INIZIALE	RESPONSABILE DELLA CLASSIFICAZIONE DEL DOCUMENTO	DESTINATARI DEL DOCUMENTO
Riservato				
Ad uso interno				
Di dominio pubblico	X	24/06/2016	P. Vandelli	

STATO/STORIA DELLE REVISIONI

Versione	Data	Paragrafo revisionato	Oggetto dalla revisione	Autore/i principale della revisione	Altri contributi	Validato
1.0	01/12/2015		Emissione	Laura Nisi	P. Tentoni F. Merighi A. De Angelis P. Vandelli	P. Vandelli
1.1	22/04/2016		Revisione a seguito delle osservazioni dello Studio Lisi	Laura Nisi	A. De Angelis	P. Vandelli
1.2	16/06/2016		Revisione a seguito delle osservazioni dello Studio Lisi	Laura Nisi	A. De Angelis	P. Vandelli
1.3	10/10/2016		Revisione a seguito delle osservazioni dell'AGID	Laura Nisi	A. De Angelis	P. Vandelli



Sommario

1. Scopo e ambito del documento	5
2. Terminologia.....	6
2.1 Glossario	6
2.2 Acronimi	24
3. Normativa e standard di riferimento	26
3.1 Normativa.....	26
3.2 Standard di riferimento	28
4. Ruoli e responsabilità	29
5. Struttura organizzativa per il servizio di conservazione	33
5.1 Organigramma.....	35
5.2 Strutture organizzative	37
5.2.1 Attività proprie di ciascun contratto di servizio di conservazione	37
5.2.2 Attività proprie di gestione dei sistemi informativi.....	38
6. Oggetti sottoposti a conservazione.....	38
6.1 Oggetti conservati	39
6.2 Pacchetto di versamento.....	40
6.3 Pacchetto di archiviazione.....	41
6.4 Pacchetto di distribuzione	41
7. Il processo di conservazione.....	43
7.1 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico	44
7.2 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in esso contenuti.....	46
7.3 Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico	47
7.4 Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie	48
7.5 Preparazione e gestione del pacchetto di archiviazione	49



MANUALE DI CONSERVAZIONE

Rev. 1.3 del 10/10/2016



7.6	Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione	51
7.7	Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti	52
7.8	Scarto dei pacchetti di archiviazione	52
7.9	Predisposizione di misure e garanzia dell'interoperabilità e trasferibilità ad altri conservatori	53
8.	Il sistema di conservazione	55
8.1	Componenti logiche	55
8.2	Componenti tecnologiche	57
8.2.1	Software e strumenti software utilizzati	57
8.2.2	Disaster recovery	59
8.3	Componenti fisiche	60
8.4	Procedure di gestione e di evoluzione	65
8.4.1	Strategia di sviluppo e ciclo di vita del sistema Conserva	65
8.4.2	Metodologia di sviluppo Agile in JIRA	67
8.4.2.1	Issue	68
8.4.2.2	Progetti	71
8.4.2.3	Backlog	72
8.4.2.4	Sprint	73
8.4.3	Versionamento semantico dei componenti	73
8.4.4	Gli ambienti di esercizio	74
8.4.4.1	Separazione degli ambienti	74
8.4.4.2	Gestione e validazione degli ambienti	74
8.4.4.3	Sicurezza dei servizi e delle transazioni applicative	75
8.4.5	Ciclo di sviluppo del software	75
9.	Monitoraggio e controlli	77
9.1	Procedure di monitoraggio	77
9.2	Verifica dell'integrità degli archivi	78



MANUALE DI CONSERVAZIONE

Rev. 1.3 del 10/10/2016



9.2.1	Monitoraggio a campione degli archivi	78
9.2.2	Controllo integrità unità a seguito di richiesta di esibizione	79
9.3	Politiche di conservazione dei log	80
9.3.1	ConservaTrasferimento	80
9.3.2	ConservaVersamento	81
9.3.3	Conserva	81
9.3.4	Altri componenti.....	82
9.4	Soluzioni adottate in caso di anomalie.....	84
9.4.1	Gestione segnalazione delle anomalie	84

1. Scopo e ambito del documento

Il presente manuale illustra dettagliatamente l'organizzazione, i soggetti coinvolti, i ruoli, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.

In particolare, il presente manuale descrive le soluzioni organizzative, tecnologiche e archivistiche scelte e sviluppate da CINECA al fine di garantire un sistema di conservazione a lungo termine affidabile.

La struttura del manuale è la seguente:

- il presente elaborato che costituisce la sezione generale del manuale di conservazione;
- l'allegato *Specificità del contratto* contenente sia informazioni da aggiornare periodicamente che specifiche proprie di ciascun produttore;
- gli allegati tecnici.

[Torna al sommario](#)

2. Terminologia

Il seguente glossario riprende le definizioni e i glossari presenti nella normativa di riferimento; nel dettaglio:

- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

In aggiunta alle suddette definizioni sono presenti anche dei termini utilizzati in maniera ricorrente nel testo, specifici di questo servizio e che necessitano di essere definiti.

[Torna al sommario](#)

2.1 Glossario

Accesso

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

Accordo di versamento

Accordo firmato dal cliente e dal conservatore che descrive le condizioni di versamento di oggetti informativi dal sistema informativo del cliente al sistema di conservazione. Le condizioni di

	<p>versamento formalizzano sia i dettagli tecnici della procedura di versamento - quali il protocollo di comunicazione, lo standard di firme, i controlli sul buon esito del versamento - che gli aspetti archivistici come la descrizione della tipologia del documento, del contesto, della provenienza.</p>
Accreditamento	<p>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.</p>
Affidabilità	<p>Caratteristica che esprime il livello di fiducia che l’utente ripone nel documento informatico.</p>
Aggregazione documentale informatica	<p>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.</p>
AgID	<p>Agenzia per l’Italia Digitale. Ha il compito di garantire la realizzazione degli obiettivi dell’Agenda digitale italiana in coerenza con l’Agenda digitale europea.</p>
Archival Information Package (AIP)	<p>Denominazione in OAIS del pacchetto di archiviazione. Per l’accezione utilizzata in questo manuale cfr. Pacchetto di archiviazione.</p>
Archivio	<p>Complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un cliente durante lo svolgimento dell’attività.</p>

Archivio informatico	Archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico.
Area Organizzativa Omogenea	Un insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445.
Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.
Autenticità	Caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico.
Base di dati	Collezione di dati registrati e correlati tra loro.
Certificatore accreditato	Soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza.
Ciclo di gestione	Arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo.

Classificazione	Attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati.
Cliente	Il soggetto che per legge ha l'obbligo di conservare.
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.
Comunità di riferimento	Un gruppo ben individuato di potenziali utenti che dovrebbero essere in grado di comprendere un particolare insieme di informazioni. La comunità di riferimento può essere composta da più comunità di utenti.
Controllo forzabile	Sono forzabili i controlli il cui mancato superamento rimette la responsabilità del versamento dell'unità al Responsabile della conservazione.
Controllo non forzabile	Sono non forzabili i controlli il cui mancato superamento comporta il rifiuto inderogabile dell'unità di versamento controllata.
Conservatore accreditato	Soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agazia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, dall'Agazia 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.
Consumer	Denominazione in OAIS di utente. Per l'accezione utilizzata in questo manuale cfr. Utente.
Contenuto informativo	L'insieme di informazioni che costituisce l'obiettivo originario della conservazione. È un oggetto informativo composto dal suo oggetto-dati e dalle sue informazioni sulla rappresentazione.
Coordinatore della Gestione Documentale	Responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 nei casi di amministrazioni che abbiano istituito più Aree Organizzative Omogenee.
Copia analogica del documento informatico	Documento analogico avente contenuto identico a quello del documento informatico da cui è tratto.
Copia di sicurezza	Copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 delle Regole tecniche sistema di conservazione.
Copia informatica di documento analogico	Il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto.
Copia informatica di documento informatico	Il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari. Modifiche ed integrazioni al CAD.
Copia per immagine su supporto informatico di documento analogico	Il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto.

Documento analogico	La rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.
Documento informatico	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
Destinatario	Il soggetto/sistema al quale il documento informatico è indirizzato.
Dissemination Information Package (DIP)	Denominazione in OAIS del pacchetto di distribuzione. Per l'accezione utilizzata in questo manuale cfr. Pacchetto di distribuzione.
Duplicato informatico	Il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario.
Duplicazione dei documenti informatici	Produzione di duplicati informatici.
Esibizione	Operazione che consente di visualizzare un documento conservato e di ottenerne una copia.
Evidenza informatica	Una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.
Fascicolo informatico	Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del Codice.
Firma digitale	Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite

	la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.
Formato	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
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.

Gestione informatica dei documenti	L'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato, effettuate mediante sistemi informatici.
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 di una opportuna funzione di hash su di un'altra sequenza di bit.
Informazioni descrittive	L'insieme delle informazioni, composto essenzialmente dalla descrizione del pacchetto per coadiuvare l'utente nella ricerca, nella richiesta e nel recupero di informazioni in un OAIS.
Informazioni sul contesto	Le informazioni che documentano le relazioni del contenuto informativo con il suo ambiente, ivi inclusi i motivi della creazione del contenuto informativo e il modo in cui è in relazione con altri

	contenuti informativi.
Informazioni sull'accesso	Le informazioni che identificano le restrizioni di accesso.
Informazioni sull'identificazione	Le informazioni che identificano, e se necessario descrivono, uno o più meccanismi di attribuzione di identificatori al contenuto informativo. Tali informazioni forniscono anche degli identificatori che consentono a sistemi esterni di riferirsi in maniera non ambigua ad un particolare contenuto informativo.
Informazioni sull'impacchettamento	Le informazioni usate per collegare e identificare le componenti di un pacchetto informativo.
Informazioni sull'integrità	Le informazioni che documentano i meccanismi di autenticazione e forniscono le chiavi di autenticazione per garantire che l'oggetto contenuto Informativo non sia stato alterato senza una documentazione dell'evento.
Informazioni sulla conservazione	Le informazioni necessarie per un'adeguata conservazione del contenuto informativo.
Informazioni sulla provenienza	Le informazioni che documentano la storia del contenuto informativo, sui cambiamenti avvenuti dal momento della sua creazione e su chi ne ha curato la custodia sin dall'origine.
Informazioni sulla rappresentazione	Le informazioni che associano un oggetto dati a concetti più significativi.
Insieme minimo di metadati del documento informatico	Complesso dei metadati, la cui struttura è descritta nell'allegato 5 del presente decreto, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta.

Integrità	Insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato.
Interoperabilità	Capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi.
Leggibilità	Insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti.
Log di sistema	Registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati.
Manuale di conservazione	Strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 delle Regole tecniche sistema di conservazione.
Manuale di gestione	Strumento che descrive il sistema di gestione informatica dei documenti di cui all'articolo 5 delle Regole tecniche protocollo informatico.
Memorizzazione	Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici.
Metadati	Insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale

	insieme è descritto nell'allegato 5 delle Regole tecniche sistema di conservazione.
Metadati minimi documento amministrativo informatico	Schema esplicitato nelle ultime Regole tecniche documento Informatico.
Metadati minimi documento informatico	Schema esplicitato nelle ultime Regole tecniche documento Informatico.
Metadati minimi fascicolo informatico	Schema esplicitato nelle ultime Regole tecniche documento Informatico.
Oggetto dati	Un oggetto materiale oppure un oggetto digitale.
Oggetto digitale	Un oggetto composto da un insieme di sequenze di bit.
Oggetto informativo	Un oggetto dati insieme con le sue informazioni sulla rappresentazione.
Oggetto materiale	Un oggetto con proprietà fisiche osservabili che rappresentano informazioni adatte per essere adeguatamente documentate ai fini della conservazione, della distribuzione e dell'utilizzo autonomo.
Originali non unici	I documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi.
Pacchetto di archiviazione	Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 delle Regole tecniche sistema di conservazione e secondo le modalità riportate nel manuale di conservazione.
Pacchetto di distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua

	richiesta.
Pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione.
Pacchetto informativo	Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare.
Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza.
Piano della sicurezza del sistema di gestione informatica dei documenti	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi nell'ambito dell'organizzazione di appartenenza.
Piano di conservazione	Strumento integrato con il sistema di classificazione per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445.
Piano generale della sicurezza	Documento per la pianificazione delle attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza.

Posta elettronica certificata	Sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi.
Presenza in carico	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione.
Processo di conservazione	Insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 10 delle Regole tecniche sistema di conservazione.
Producer	Denominazione in OAIS di produttore. Per l'accezione utilizzata in questo manuale cfr. produttore.
Produttore	Persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con il responsabile della gestione documentale.
Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.
Registrazione informatica	Insieme delle informazioni risultanti da transazioni informatiche o dalla presentazione in via telematica di dati attraverso moduli o formulari resi disponibili in vario modo all'utente.
Registro particolare	Registro informatico di particolari tipologie di atti

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

Registro di protocollo

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

Regole tecniche protocollo informatico

DPCM 3 dicembre 2013 - Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

Regole tecniche in materia di sistema di conservazione

DPCM 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

Regole tecniche documento informatico

DPCM 13 novembre 2014 - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23 -bis, 23 -ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

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.
Resoconto di versamento	Documento informatico che comunica al Produttore, immediatamente dopo il versamento, lo stato del pacchetto di versamento (<i>interamente_versato, parzialmente_versato o rifiutato</i>) con il dettaglio dell'esito di tutti i controlli sulle singole unità.
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 conservazione	Soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 delle Regole tecniche sistema di conservazione.
Responsabile della gestione documentale o Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi	Dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione.
Responsabile della sicurezza	Soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione

	delle disposizioni in materia di sicurezza.
Riferimento temporale	Informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento.
Scarto	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale.
Serie	Unità Archivistiche o Unità Documentarie ordinate secondo un sistema di classificazione o conservati insieme perché sono il risultato di un medesimo processo di sedimentazione o archiviazione o di una medesima attività.
Sistema di classificazione	Strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata.
Sistema di conservazione	Sistema di conservazione dei documenti informatici di cui all'articolo 44 del Codice.
Sistema di gestione informatica dei documenti	Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445; per i privati è il sistema che consente la tenuta di un documento informatico.
Staticità	Caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione.

Submission Information Package (SIP)	Denominazione in OAIS del pacchetto di versamento. Per l'accezione utilizzata in questo manuale cfr. Pacchetto di versamento.
Testo unico	Decreto del Presidente della Repubblica 28 dicembre 2000, n.445, e successive modificazioni.
Tipologia documentaria	Categoria di documenti omogenei per natura e funzione giuridica, modalità di registrazione o di produzione, che hanno comuni caratteristiche formali e/o intellettuali.
Transazione informatica	Particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche della base di dati.
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.
UNI SinCRO	Norma UNI che definisce, tramite uno Schema XML, la struttura dell'insieme dei dati a supporto del processo di conservazione. Essa individua la struttura del cosiddetto indice del pacchetto di archiviazione previsto dal Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 al fine di consentire agli operatori del settore di raggiungere una soddisfacente interoperabilità.
Unità archivistica	Indica un insieme di documenti raggruppati secondo un nesso di collegamento organico, che costituiscono un'unità non divisibile: registro, serie, fascicolo.
Unità di versamento	Elemento ripetibile all'interno del pacchetto di versamento e corrispondente ad una unità archivistica (fascicolo) o ad una unità documentale

	(documento con uno o più file associati).
Unità documentale	La minima unità, concettualmente non divisibile, di cui è composto un archivio, per esempio, una lettera, un memorandum, un rapporto, una fotografia, una registrazione sonora. Può essere composta da più file.
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.
Validazione temporale	Il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili a terzi.
Versamento agli archivi di stato	Operazione con cui il Responsabile della conservazione di un organo giudiziario o amministrativo dello Stato effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali.
Web Service	Sistema software progettato per supportare l'interoperabilità tra diversi elaboratori su di una medesima rete ovvero in un contesto distribuito.

[Torna al sommario](#)

2.2 Acronimi

AGID	Agenzia per l'Italia Digitale
AIP	Archival Information Package
DIP	Dissemination Information Package
EAC	Encoded Archival Context
EAD	Encoded Archival Description
ETSI	European Telecommunications Standards Institute
ISAAR	International Standard Archival Authority Record for Corporate Bodies, Persons and Families
ISAD	General International Standard Archival Description
IPA	Indice Pubblica Amministrazione
ISO	International Standard Organization
OAIS	Open Archival Information System
PAIMAS	Space Data and Information Transfer Systems - Producer-Archive Interface - Methodology Abstract Standard (2006 - ISO 20652)
PDI	Preservation Descriptive Information
PdA	Pacchetto di Archiviazione
PdD	Pacchetto di Distribuzione
PdV	Pacchetto di Versamento
PEC	Posta Elettronica Certificata
PREMIS	PREservation Metadata: Implementation Strategies
RdC	Responsabile della conservazione
SinCRO	Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (Norma UNI 11386)
UNI	Ente Nazionale Italiano di Unificazione
UNI 11386	Norma UNI SinCRO: Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti Digitali

URL	Uniform Resource Locator
WebDAV	Web-based Distributed Authoring and Versioning: protocollo che consente di trasformare il web in mezzo di lettura e scrittura analogo al disco locale. In particolare WebDAV si riferisce a un set di istruzioni del protocollo HTTP, che permettono all'utente di gestire in modo collaborativo dei file in un server remoto.
XML	EXtensible Markup Language

[Torna al sommario](#)

3. Normativa e standard di riferimento

3.1 Normativa

Viene riportata qui di seguito la principale normativa di riferimento per l'attività di conservazione a livello nazionale.

Alla data di stesura del presente manuale l'elenco dei principali riferimenti normativi italiani in materia, ordinati secondo il criterio della gerarchia delle fonti, è costituito da:

- **Codice Civile** – R.D del 16 marzo 1942 n. 262;
- **Legge 7 agosto 1990, n. 241** e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- **Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445** e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- **Decreto Legislativo 30 giugno 2003, n. 196** e s.m.i. – Codice in materia di protezione dei dati personali;
- **Decreto Legislativo 22 gennaio 2004, n. 42** e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- **Decreto Legislativo 7 marzo 2005 n. 82** e s.m.i. – Codice dell'amministrazione digitale (CAD);
- **Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013** – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;
- **Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013** - Regole tecniche per il protocollo informatico ai sensi degli articoli 40, 41, 47, 57 bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- **Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013** - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;

- **Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014** - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- **Decreto del Ministero dell'Economia e delle Finanze del 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;
- **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;
- **Circolare dell'Agenzia per l'Italia Digitale del 23 gennaio 2013, n. 60** – Formato e definizioni dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le pubbliche amministrazioni;
- **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.

[Torna al sommario](#)

3.2 Standard di riferimento

Si riportano di seguito gli standard di riferimento utilizzati al fine di sviluppare il sistema di conservazione; in particolare sono elencati quelli obbligatori dell'allegato 3 delle Regole Tecniche in materia di Sistema di conservazione con indicazione delle versioni aggiornate al 1° ottobre 2014 assieme ad altri ritenuti utili alla corretta costruzione del sistema sia dal punto di vista organizzativo che archivistico:

- **ISO 14721:2012 OAIS** (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- **ISO/IEC 27001:2013**, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- **ETSI TS 101 533-1 V1.3.1 (2012-04)** Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- **ETSI TR 101 533-2 V1.3.1 (2012-04)** Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- **UNI 11386:2010** Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- **ISO 15836:2009** Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.
- **ISO 20652:2006** Paimas, Space data and information transfer systems – Methodology abstract standard.

[Torna al sommario](#)

4. Ruoli e responsabilità

Il presente capitolo richiama quanto previsto dalla normativa e dalla Circolare AgID n. 65/2014 per quanto riguarda le attività di competenza dei soggetti responsabili e presenti nel processo di conservazione.

Di seguito l'elenco dei profili richiesti e/o ritenuti utili al fine di una corretta gestione del processo di conservazione:

- il **Responsabile della conservazione**: ai sensi dell'art. 7 delle *Regole Tecniche*, il Responsabile della conservazione opera d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei sistemi informativi che, nel caso delle pubbliche amministrazioni centrali, coincide con il responsabile dell'ufficio di cui all'art. 17 del Codice, oltre che con il responsabile della gestione documentale ovvero il coordinatore della gestione documentale ove nominato, per quanto attiene alle pubbliche amministrazioni. In particolare il Responsabile della conservazione, che deve appartenere alla stessa organizzazione (Ente, Azienda, Università...) del Cliente; coadiuvato dal Responsabile del servizio di conservazione Conserva di CINECA:
 - accerta, con periodicità almeno annuale, la conformità del processo di conservazione alla normativa vigente;
 - archivia e gestisce i rapporti di versamento prodotti dal Conservatore CINECA secondo le modalità descritte nel manuale di conservazione;
 - genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione o in specifici accordi di versamento;
 - effettua il monitoraggio del corretto funzionamento del sistema di conservazione;
 - assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;

- provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
 - 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;
 - assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
 - provvede, per gli organi giudiziari e amministrativi dello Stato, al versamento dei documenti conservati all'Archivio Centrale dello Stato e agli Archivi di Stato secondo quanto previsto dalle norme vigenti;
 - predispone il manuale di conservazione di cui all'art. 8 e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti. Inoltre affida al Conservatore CINECA il mandato di:
 - definire le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente;
 - gestire il processo di conservazione garantendone nel tempo la conformità alla normativa vigente;
 - generare il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
 - adottare, al fine di garantire la conservazione e l'accesso ai documenti informatici, misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità;
 - adottare analoghe misure con riguardo all'obsolescenza dei formati; adottare le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12.
- il **Responsabile del servizio di conservazione** si occupa della:

- definizione e attuazione delle politiche complessive del sistema di conservazione nonché del governo della gestione del sistema di conservazione;
 - definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente;
 - corretta erogazione del servizio di conservazione al produttore;
 - gestione delle convenzioni, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.
- il **Responsabile della funzione archivistica di conservazione** si occupa della:
- definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte del produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato;
 - definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici;
 - monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità all'interno del sistema di conservazione;
 - collaborazione con il produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.
- il **Responsabile del trattamento dei dati personali** si occupa della:
- garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali;
 - garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.
- il **Responsabile della sicurezza dei sistemi per la conservazione** si occupa del/della:

- rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza;
 - segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.
- il **Responsabile dei sistemi informativi per la conservazione** si occupa del/della:
- gestione dell'esercizio delle componenti hardware e software del sistema di conservazione;
 - monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con il cliente;
 - segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive;
 - pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione;
 - controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.
- il **Responsabile dello sviluppo e della manutenzione del sistema di conservazione** si occupa del/della:
- coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione;
 - pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione;
 - monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione;
 - interfaccia con il produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche;
 - gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.

[Torna al sommario](#)

5. Struttura organizzativa per il servizio di conservazione

Nella seguente tabella sono indicati le attività svolte e i nominativi delle persone che ricoprono i ruoli previsti nel documento “Profili professionali” dell’AGID ai fini dell’accreditamento. Non è esclusa la possibilità che più ruoli siano ricoperti da una stessa persona.

Nel caso di deleghe, per ciascuna delega sono indicate le attività delegate, i dati identificativi del soggetto delegato e il periodo di validità della delega.

La tabella tiene conto della storicizzazione dei ruoli mantenendo i dati delle persone che nel tempo li hanno ricoperti.

[Torna al sommario](#)

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo	Eventuali deleghe
<i>Responsabile del servizio di conservazione</i>	Paolo Vandelli	Cfr. Capitolo 2 - Ruoli e Responsabilità	01/07/2015	Nessuna
<i>Responsabile Sicurezza dei sistemi per la conservazione</i>	Paola Tentoni	Cfr. Capitolo 2 - Ruoli e Responsabilità	15/01/2015	Nessuna
<i>Responsabile funzione archivistica di conservazione</i>	Laura Federica Nisi	Cfr. Capitolo 2 - Ruoli e Responsabilità	01/07/2015	Nessuna
<i>Responsabile trattamento dati personali</i>	Emilio Ferrari	Cfr. Capitolo 2 - Ruoli e Responsabilità	15/01/2014	Nessuna
<i>Responsabile sistemi informativi per la conservazione</i>	Angelo Neri	Cfr. Capitolo 2 - Ruoli e Responsabilità	01/04/2015	Nessuna
<i>Responsabile sviluppo e manutenzione del</i>	Francesca Merighi	Cfr. Capitolo 2 - Ruoli e Responsabilità	01/04/2015	Nessuna

L'organico di CINECA, per quanto riguarda il sistema di conservazione, prevede una figura di riferimento per tutti i ruoli sopra descritti (fatta eccezione per il ruolo di Responsabile della conservazione che, come descritto, è di diretta emanazione della stessa organizzazione alla quale appartiene il cliente).

In particolare Responsabile del servizio di conservazione e Responsabile della funzione archivistica di conservazione, collaborano con il Responsabile della conservazione ed i suoi delegati nel redigere il manuale della conservazione, nel definire i singoli accordi di versamento e nelle azioni di audit (verifica e monitoraggio) del sistema.

È responsabilità delle parti informare tempestivamente la controparte di ogni variazione di uno qualunque dei ruoli sopra descritti. A questo proposito CINECA mette a disposizione del cliente un modello pre-impostato per la comunicazione di RdC e dei suoi eventuali delegati.

L'attivazione del servizio di conservazione è subordinata alla comunicazione formale degli estremi del Responsabile della conservazione ed eventuali suoi delegati.

[Torna al sommario](#)

5.1 Organigramma

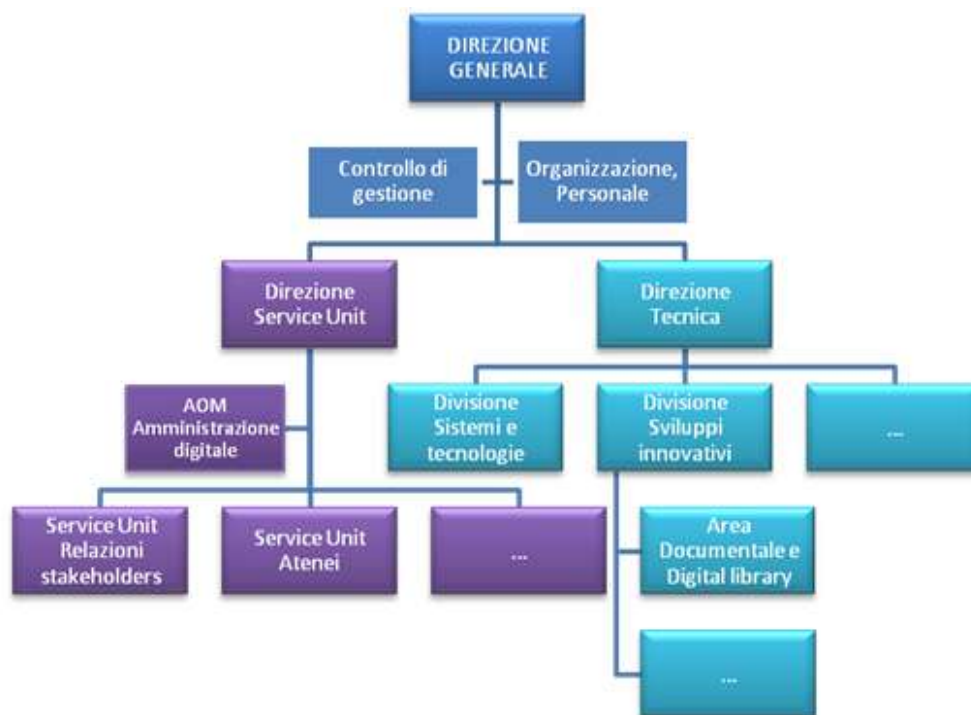


Figura 1 - Organigramma Aziendale

Al fine di un'efficiente attività conservativa di seguito vengono descritte le unità organizzative e le responsabilità delle principali funzioni CINECA:

- **Direzione generale:** garantisce il raggiungimento degli obiettivi e del piano pluriennale definiti dagli Organi di governo.
- **Direzione Service Unit:** ha la responsabilità di sostenere lo sviluppo delle attività commerciali per il raggiungimento degli obiettivi di budget e di piano pluriennale secondo

le indicazioni della Direzione Generale, attraverso una specifica suddivisione delle service unit basata sulla natura degli stakeholders.

- **Direzione Tecnica:** ha la responsabilità di coordinare tutte le azioni infrastrutturali, di sviluppo, manutenzione, evoluzione ed erogazione del sistema di conservazione Conserva di CINECA.
- **Service Unit Relazione Stakeholders:** cura le attività commerciali di pre e post vendita del sistema di conservazione Conserva. È responsabile, tramite la propria rete di account, della gestione commerciale dei consorziati e dei clienti; cura gli aspetti formali legati alla sottoscrizione degli accordi contrattuali.
- **AOM Amministrazione digitale:** in staff alla Direzione Service Unit, ha il compito di curare gli aspetti di formazione, sensibilizzazione ed alfabetizzazione sui temi dell'amministrazione digitale. Supporta le altre SU nelle attività di pre-vendita e contribuisce alla definizione dei requisiti del sistema di conservazione Conserva di CINECA.
- **Divisione Sistemi Tecnologie:** ha il compito di gestire l'infrastruttura ICT per il sistema di conservazione Conserva di CINECA e di garantire qualità ed economicità di servizio:
 - gestendo l'infrastruttura ICT nei suoi componenti (servizi di rete, storage e relativi servizi, server fisici e virtualizzati, data base, middleware, postazioni di lavoro);
 - assicurando l'aggiornamento tecnologico e fornendo servizi ad alto valore (continuità, sicurezza, qualità) e competitivi in termini economici;
 - gestendo gli ambienti di sviluppo applicativi, i sistemi di gestione aziendali, i servizi di rete e fonia;
 - garantendo il rispetto degli SLA in termini di business continuity e disaster recovery;
 - sviluppando consulenze tecnologiche.
- **Divisione sviluppi innovativi:** ha il compito di sostenere la innovazione nell'"offerta" aziendale con attività di ricerca e sviluppi avanzati che recepiscano spunti innovativi nelle tecnologie, nei processi organizzativi, nel rapporto uomo-macchina:
 - analizzando i contesti esterni più evoluti;
 - studiando le prospettive offerte dalla tecnologia;
 - sviluppando studi di fattibilità;
 - realizzando soluzioni prototipali;

- contribuendo al passaggio verso soluzioni di prodotto.
- **Area documentale e digital library:** cura sviluppo, manutenzione ed evoluzione del sistema di conservazione Conserva di CINECA. Individua le tecnologie da utilizzare e valuta eventuali cambiamenti tecnologici da mettere in atto. Verifica la qualità del servizio erogato da terze parti ed evidenzia eventuali criticità al Responsabile del servizio di conservazione. Garantisce il raggiungimento della roadmap evolutiva del servizio sulla base dei requisiti normativi e funzionali provenienti dalla Direzione Service Unit, dal Responsabile del servizio di conservazione e dal Responsabile della funzione archivistica di conservazione. Cura l'attivazione e la configurazione di nuovi enti produttori.

[Torna al sommario](#)

5.2 Strutture organizzative

5.2.1 Attività proprie di ciascun contratto di servizio di conservazione

Attività	Figure Coinvolte
Attivazione del servizio di conservazione (a seguito della sottoscrizione di un contratto)	Responsabile della funzione archivistica Responsabile Servizio di conservazione
Acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento	Responsabile servizio di conservazione Responsabile dello sviluppo
Preparazione e gestione del pacchetto di archiviazione	Responsabile dello sviluppo Responsabile funzione archivistica Responsabile servizio di conservazione
Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta	Responsabile dello sviluppo Responsabile funzione archivistica Responsabile servizio di conservazione Responsabile della conservazione

Scarto dei pacchetti di archiviazione	Responsabile della conservazione Responsabile della funzione archivistica Responsabile servizio di conservazione
Chiusura del servizio di conservazione	Responsabile della conservazione Responsabile servizio di conservazione

[Torna al sommario](#)

5.2.2 Attività proprie di gestione dei sistemi informativi

Attività	Figure Coinvolte
Conduzione e manutenzione del sistema di conservazione	Responsabile servizio di conservazione Responsabile dello sviluppo Responsabile dei sistemi informativi Responsabile della sicurezza
Monitoraggio del sistema di conservazione	Responsabile dello sviluppo Responsabile dei sistemi Informativi Responsabile della sicurezza
Change management	Responsabile dello sviluppo Responsabile dei sistemi informativi Responsabile della sicurezza
Verifica periodica di conformità a normativa e standard di riferimento	Responsabile servizio di conservazione Responsabile dello sviluppo Responsabile dei sistemi informativi Responsabile della sicurezza Responsabile della funzione archivistica

[Torna al sommario](#)

6. Oggetti sottoposti a conservazione

6.1 Oggetti conservati

Il servizio di conservazione Conserva in ottemperanza alla normativa segue il modello informativo dello standard ISO 14721:2012 OAIS¹ (di seguito solo OAIS).

Lo standard OAIS ha la peculiarità di organizzare gli oggetti informativi da conservare in pacchetti informativi tipizzati in base alla fase del processo di conservazione. I tipi di pacchetto sono tre e racchiudono gli oggetti informativi inviati in conservazione assieme alla relativa metadattazione utile ai fini conservativi:

- il **pacchetto di versamento (PdV)**: pacchetto versato dal produttore e utilizzato per l'acquisizione degli oggetti informativi e dei metadati da parte del sistema di conservazione;
- il **pacchetto di archiviazione (PdA)**: pacchetto finalizzato alla memorizzazione a lungo termine degli oggetti informativi digitali nel sistema di conservazione;
- il **pacchetto di distribuzione (PdD)**: pacchetto di oggetti informativi conservati costruito secondo le esigenze e il profilo dell'utenza esterna che ne fa richiesta.

La descrizione puntuale delle tipologie di oggetti conservati all'interno del sistema viene riportata direttamente nell'allegato "Specificità del contratto" e nei relativi accordi di versamento per due motivi:

- la rapidità con cui le tipologie di oggetti informativi da conservare aumentano si riflette sul frequente aggiornamento della relativa documentazione;
- gli oggetti informativi da conservare variano da un produttore a un altro ed è possibile che le stesse tipologie di oggetti informativi da conservare possano variare sia dal punto di vista del contenuto informativo che della metadattazione.

Le tipologie degli oggetti informativi sono individuate e concordate assieme al produttore; tendenzialmente sono oggetti che hanno caratteristiche omogenee dal punto di vista della forma o in relazione all'oggetto, alla materia o alle funzioni del produttore.

¹ ISO 14721:2012, *Space data and information transfer systems - Open archival information system (OAIS) - Reference model*.

[Torna al sommario](#)

6.2 Pacchetto di versamento

Il pacchetto di versamento è preparato dal produttore in collaborazione col Conservatore secondo determinate specifiche descritte nell'allegato relativo alla descrizione del Pacchetto di versamento.

A livello generale il pacchetto di versamento è costituito da un **indice del pacchetto di versamento** contenente i metadati relativi alle unità (di versamento) che formano il pacchetto, e dai relativi **file**.

L'indice del pacchetto di versamento è un oggetto xml rispondente ad uno specifico schema che definisce e descrive i metadati necessari per la conservazione di oggetti digitali.

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 può avvenire tramite due modalità:

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

Lo schema del pacchetto è descritto nell'allegato relativo alla descrizione del pacchetto di versamento.

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

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

I formati dei file trasmessi vengono concordati da Responsabile della conservazione, Responsabile del servizio di conservazione e Responsabile della funzione archivistica della conservazione e devono essere esplicitati all'interno dell'accordo di versamento.

L'allegato 2 "Formati" delle Regole tecniche per il sistema di conservazione viene preso come punto di riferimento per i formati da accettare ai fini della conservazione a lungo termine con preferenza, ove possibile, verso i formati PDF/A e XML. Non si esclude la possibilità di concordare differenti formati nell'ambito di specifici accordi di versamento, all'interno dei quali dovranno tuttavia essere descritte in dettaglio le azioni da intraprendere per garantire la leggibilità dei file per tutto il periodo di conservazione.

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.

[Torna al sommario](#)

6.3 Pacchetto di archiviazione

Il pacchetto di archiviazione è il pacchetto presente all'interno del sistema di conservazione ed è soggetto a numerosi aggiornamenti nella metadatazione affinché permanga intellegibile e accessibile nel tempo attraverso i cambiamenti delle piattaforme hardware-software.

Come il pacchetto di versamento, il pacchetto di archiviazione è 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 è conforme allo standard UNI 11386 SInCRO, al fine di facilitare l'interoperabilità tra i sistemi di conservazione. La descrizione puntuale della valorizzazione dei singoli elementi dello standard SInCRO è riportata nell'allegato dedicato all'implementazione di UNISInCRO in Conserva.

[Torna al sommario](#)

6.4 Pacchetto di distribuzione



MANUALE DI CONSERVAZIONE

Rev. 1.3 del 10/10/2016



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.

[Torna al sommario](#)

7. Il processo di conservazione

Il processo di conservazione è costituito essenzialmente da tre macro-fasi che esplicitano i passaggi dell'oggetto informativo attraverso il suo iter di conservazione e fruizione:

- la fase di versamento;
- la fase di archiviazione;
- la fase di distribuzione.

La fase di versamento è la prima fase del processo di conservazione che disciplina formalmente il passaggio di custodia e gestione degli oggetti informativi dal produttore al Conservatore.

Per strutturare questa fase di acquisizione degli oggetti informativi è stato preso come modello di riferimento lo standard ISO 20652:2006 Paimas² (di seguito chiamato Paimas), il cui scopo è quello di definire la metodologia da seguire dal primo contatto tra il produttore e il Conservatore fino alla ricezione e validazione dell'unità di versamento nel sistema di conservazione.

Il suddetto standard struttura la fase di versamento in:

- **fase preliminare:** include i primi contatti tra il produttore e il Conservatore in cui si definiscono gli interlocutori dei singoli enti e l'obiettivo della conservazione; in questa fase si dà inizio alla redazione della relativa documentazione;
- **fase di definizione formale:** permette di entrare nel merito dei dettagli dell'intero processo di conservazione per stilare e firmare l'accordo di versamento (Cfr. allegato relativo al modello dell'accordo di versamento);
- **fase di trasferimento:** concretizza il trasferimento degli oggetti informativi dal sistema del produttore al sistema di conservazione, ossia la modalità di presa in carico dei pacchetti;

² ISO 20652:2006 Paimas, *Space data and information transfer systems – Methodology abstract standard*.

- **fase di validazione:** effettua i controlli standard sul pacchetto di versamento e quelli concordati con il Responsabile della conservazione al fine di assicurarsi che le risorse versate siano corrette, integre e coerenti con la struttura prevista dal sistema.

La fase preliminare è costituita da contatti telefonici o tramite mail in cui si informa il Responsabile della conservazione dei servizi offerti dal sistema di conservazione e si individuano, inoltre, gli oggetti informativi che il produttore intende inviare al sistema di conservazione.

In seguito alla fase preliminare si analizza nel dettaglio la tipologia dell'oggetto informativo da conservare e il suo percorso dalla prima formazione fino all'invio al sistema di conservazione. Essendo un modello astratto, lo standard OAIS necessita di indicazioni di implementazione che si delineino sulle esigenze rilevate dal Responsabile della conservazione e sulla tipologia degli oggetti informativi da conservare; per questa ragione prima di accettare qualsiasi oggetto informativo il Conservatore richiede la presenza di apposito accordo di versamento. L'accordo di versamento viene sottoscritto dal produttore e dal Responsabile della conservazione e viene successivamente proposto al Responsabile del servizio di conservazione (Conservatore) che lo sottoscriverà per accettazione. Nell'ambito dell'accordo di versamento vengono delineate anche le tempistiche con le quali gli oggetti informativi vengano versati al servizio di conservazione.

[Torna al sommario](#)

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

Una volta firmato l'accordo di versamento e configurato il servizio di conservazione secondo quanto dichiarato nell'accordo, è possibile procedere alla preparazione del pacchetto finalizzato al trasferimento.

L'intera fase di trasferimento è asincrona e inizia con la preparazione del pacchetto di versamento e termina con il suo completo passaggio nel sistema di conservazione attraverso il mezzo di trasmissione scelto.

La preparazione del pacchetto di versamento consiste nella formazione dell'indice del pacchetto di versamento e nel reperimento dei file che compongono gli oggetti informativi da conservare.

L'indice del pacchetto di versamento deve essere conforme allo schema xml riportato nell'allegato relativo alla descrizione del pacchetto di versamento (con eventuali specificità descritte nell'accordo di versamento) e deve essere completo di tutti campi tipici delle tipologie degli oggetti informativi che descrive.

L'indice del pacchetto di versamento contiene anche il riferimento e l'impronta dei file appartenenti agli oggetti informativi che lo compongono, rendendo possibile verificare l'integrità dei file stessi in seguito al trasferimento ed in qualsiasi momento del ciclo di vita nel sistema di conservazione.

Dal punto di vista tecnico il servizio di conservazione dispone di due canali per l'invio del pacchetto di versamento:

- tramite *web service*;
- tramite *WebDAV*.

Per ulteriori dettagli sulle specifiche dei due canali si rimanda all'allegato relativo ai mezzi di trasmissione scelti.

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.

[Torna al sommario](#)

7.2 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; il primo tra questi è l'identificazione del Produttore.

Questi controlli si differenziano tra a) *forzabili* e *non forzabili* e b) controlli *di sistema* e controlli *custom*, sulla base della tipologia dell'oggetto informativo da conservare e delle esigenze del produttore, dichiarate nell'accordo di versamento.

Sono *forzabili* i controlli il cui mancato superamento rimette la responsabilità del versamento dell'unità al Responsabile della conservazione; sono *non forzabili* i controlli il cui mancato superamento comporta il rifiuto inderogabile dell'unità di versamento controllata.

I controlli di sistema che il pacchetto di versamento deve superare al fine di concludere positivamente la fase di validazione sono descritti dettagliatamente nell'allegato relativo ai controlli effettuati da Conserva.

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.

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 di CINECA.

[Torna al sommario](#)

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

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.

Nel sistema di conservazione Conserva, il rapporto di versamento è rappresentato da un file XML firmato e marcato attraverso firma automatica dal Responsabile del servizio di conservazione.

Il processo di produzione del rapporto di versamento può avvenire in due modalità in base alla versione del sistema o a particolari esigenze di conservazione.

Nella prima modalità il sistema di conservazione:

- raccoglie tutti i pacchetti di versamento inviati da uno specifico produttore (sia quelli versati che quelli rifiutati);
- genera il file XML che rappresenta il rapporto di versamento relativo a tutti i pacchetti raccolti;
- firma digitalmente ed appone la marca temporale sul rapporto di versamento XML (firma XAdES);
- rende disponibile il rapporto di versamento al produttore.

Nella seconda modalità il sistema di conservazione:

- genera un rapporto di versamento per ogni pacchetto di versamento ricevuto dal produttore;
- firma digitalmente il rapporto (firma XAdES) e lo rende disponibile al produttore.

Al termine della giornata, genera un pacchetto di versamento con tutti i rapporti di versamento prodotti in giornata e lo versa al sistema di conservazione. In questo caso CINECA si avvale del servizio di conservazione in qualità di produttore, per conservare i rapporti di versamento generati.

Il fine del rapporto di versamento è di dare evidenza dei 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.

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 unita documentale versata.

Per ulteriori dettagli relativi alla struttura del rapporto di versamento si rimanda all'allegato relativo alla descrizione del rapporto di versamento.

[Torna al sommario](#)

7.4 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. È possibile consultare tutti i messaggi di errore che il servizio comunica al produttore in fase di trasferimento nell'allegato relativo ai controlli, in particolare nella sezione *Controlli eseguiti in fase di trasferimento*.

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 (alcuni comuni a tutti i pacchetti di versamento, altri diversi a seconda della tipologia dell'unità di versamento, altri ancora richiesti dal produttore e quindi diversi da ente a ente). 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. 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. 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*.

[Torna al sommario](#)

7.5 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.

In assenza di un pacchetto di archiviazione idoneo ad accogliere l'unità di versamento, il sistema genera un nuovo pacchetto di archiviazione e vi colloca l'unità di versamento.

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, descritto nella sua versione italiana nell'allegato 4 delle *Regole Tecniche*.

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.

La generazione dell'indice del pacchetto di archiviazione avviene al momento della chiusura del pacchetto di archiviazione. Il pacchetto, normalmente, viene chiuso 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.

Al fine di render stabile l'indice, questo viene firmato digitalmente dal Responsabile del servizio di conservazione, su affidamento del Responsabile della conservazione (tramite procedura di firma

automatica rilasciata da un ente di certificazione accreditato presso AGID) e vi appone una marca temporale rilasciata da una CA accreditata.

La chiusura del pacchetto di archiviazione può essere anticipata in caso di richiesta di esibizione.

I criteri di chiusura sono determinati nell'accordo di versamento e ad esempio possono corrispondere alla chiusura del fascicolo, alla chiusura della serie annuale o al raggiungimento della quota massima di documenti previsti per ogni pacchetto di archiviazione di una determinata tipologia.

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.

[Torna al sommario](#)

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

Il pacchetto di distribuzione viene prodotto sulla base delle specifiche richieste da parte dell'utente e dei relativi diritti di visibilità

Il Responsabile della conservazione e i suoi delegati, oltre a svolgere un'attività di monitoraggio del servizio di conservazione, hanno la facoltà di richiedere l'esibizione di un pacchetto di distribuzione opponibile a terzi nei seguenti modo:

- 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.

Su esplicita richiesta da parte degli Utenti autorizzati, il sistema di conservazione può fornire pacchetti di distribuzione in modalità concordate con gli Utenti che garantiscano la sicurezza e l'integrità dei contenuti veicolati; fermo restando che tali pacchetti rimarranno sempre disponibili attraverso l'interfaccia di consultazione messa a disposizione dal sistema di conservazione per tutta la durata del servizio di conservazione reso disponibile dal Conservatore (fatte salve eventuali unità per le quali sia stato autorizzato lo scarto).

Responsabile della conservazione e Conservatore concordano le condizioni di distribuzione, cioè le modalità con le quali sarà messo a disposizione il contenuto dei pacchetti di archiviazione presenti in conservazione.

A maggior garanzia dell'integrità di quanto conservato, nella ricerca di ogni unità informativa è possibile risalire a:

- le eventuali versioni precedenti dell'unità sul sistema di conservazione;
- l'indice del pacchetto di versamento con cui è entrata l'unità nel sistema;
- l'indice del rapporto di versamento che conferma l'avvenuta conservazione dell'unità;
- l'indice del pacchetto o dei pacchetti di archiviazione di cui l'unità fa parte.

[Torna al sommario](#)

7.7 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 tramite richiesta ad apposita interfaccia web.

La figura del pubblico ufficiale è necessaria nei seguenti casi:

- dichiarazione di conformità di una copia analogica di un documento informatico conservato nel sistema di conservazione;
- dichiarazione di conformità di una copia informatica di un documento informatico 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).

Nel caso in cui il produttore sia una pubblica amministrazione, il pubblico ufficiale può essere individuato all'interno al produttore stesso.

[Torna al sommario](#)

7.8 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 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.

L'azione di scarto dovrà essere esplicitamente autorizzata dal Responsabile della conservazione o suo delegato, attraverso la spunta dei componenti da scartare.

Nel caso di archivi pubblici o privati di particolare interesse culturale, le procedure di scarto avvengono previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo.

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

[Torna al sommario](#)

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

Il cliente ha la possibilità di richiedere al Conservatore l'acquisizione di documenti precedentemente conservati presso altri conservatori.

Il Conservatore è in grado di acquisire per la conservazione pacchetti di distribuzione provenienti da altri conservatori aderenti sia allo standard UNI 11386 SInCRO che alla traduzione italiana presente nelle *Regole Tecniche* dello standard UNI 11386 SInCRO.

Il processo di trasferimento prevede la supervisione del Responsabile della conservazione e del Responsabile del servizio di conservazione o loro delegati; la procedura segnalerà eventuali incongruenze o inesattezze contenute nei pacchetti trasferiti. Come ulteriore strumento di

supervisione, gli incaricati al trasferimento hanno la facoltà di compiere controlli a campione sui documenti trasferiti per assicurare la corretta esecuzione della procedura di trasferimento.

Nel caso in cui il Conservatore da cui provengono i pacchetti di versamento non dovesse aderire alla traduzione italiana presente nelle *Regole Tecniche* dello standard UNI 11386 SInCRO, dovranno essere stipulati specifici accordi.

La conservazione di documenti deve 'sopravvivere' al Conservatore. Basandosi su questo presupposto, CINECA espone un servizio di migrazione dei pacchetti di archiviazione prodotti, secondo la traduzione italiana presente nelle *Regole Tecniche* dello standard UNI 11386 SInCRO. Se non diversamente concordato, i pacchetti vengono messi a disposizione del produttore attraverso accesso sicuro a server FTP di CINECA per il solo periodo necessario alla trasmissione.

[Torna al sommario](#)

8. Il sistema di conservazione

Conserva è un servizio erogato in modalità SaaS installato presso il Data Center di CINECA ed è composto dalle componenti descritte di seguito.

[Torna al sommario](#)

8.1 Componenti logiche

Le componenti logiche in cui è strutturato il sistema di conservazione di CINECA Conserva sono state individuate per agevolare e organizzare al meglio le attività di manutenzione ed evoluzione del sistema. Di seguito viene rappresentato lo schema delle componenti logiche che compongono il servizio, con una breve descrizione di ogni componente.

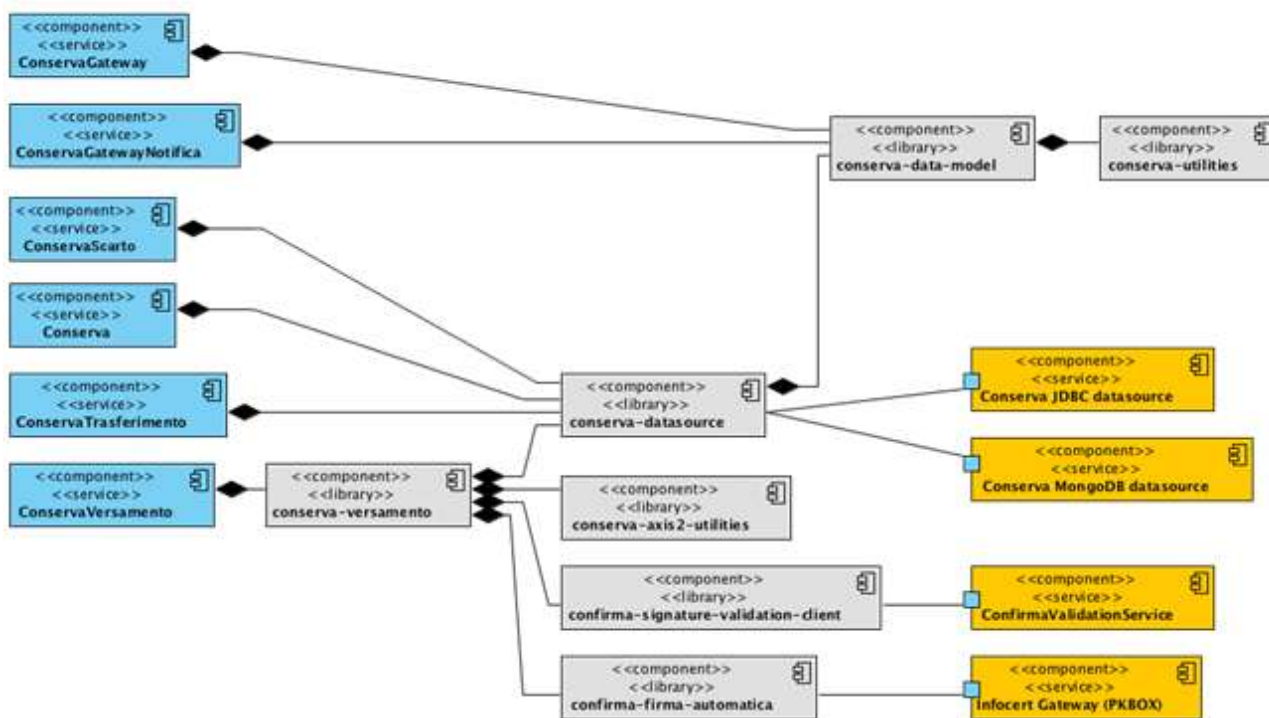


Figura 2 - Schema delle componenti logiche che compongono il servizio

- **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 conserva-versamento e servizi temporizzati.
- **ConservaGateway** e **ConservaGatewayNotifica servizio** - Componenti che, a partire da oggetti informativi caricati su directory WebDAV esposta dal sistema di conservazione, genera e invia pacchetti di versamento al servizio di trasferimento (ConservaTrasferimento). Il servizio di notifica riceve dalla componente ConservaVersamento il resoconto di versamento e il rapporto di versamento usando il primo per controllare gli oggetti informativi rifiutati dal sistema di conservazione e salvando il secondo in modo da renderlo sempre disponibile alla consultazione anche da WebDAV.
- **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*.

- **Confirma-signature-validation-client libreria** - Componente che mette a disposizione metodi per verificare firme digitali e marche temporali apposte sui documenti.
- **Confirma-firma-automatica libreria** - Componente che si occupa dell'interazione con il Gateway di firma per l'apposizione delle firme automatiche necessarie al funzionamento del servizio di conservazione di CINECA Conserva.
- **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.

[Torna al sommario](#)

8.2 Componenti tecnologiche

8.2.1 Software e strumenti software utilizzati

Partendo dal diagramma seguente, si descrivono le tecnologie utilizzate per il corretto funzionamento di Conserva, il servizio di conservazione CINECA:

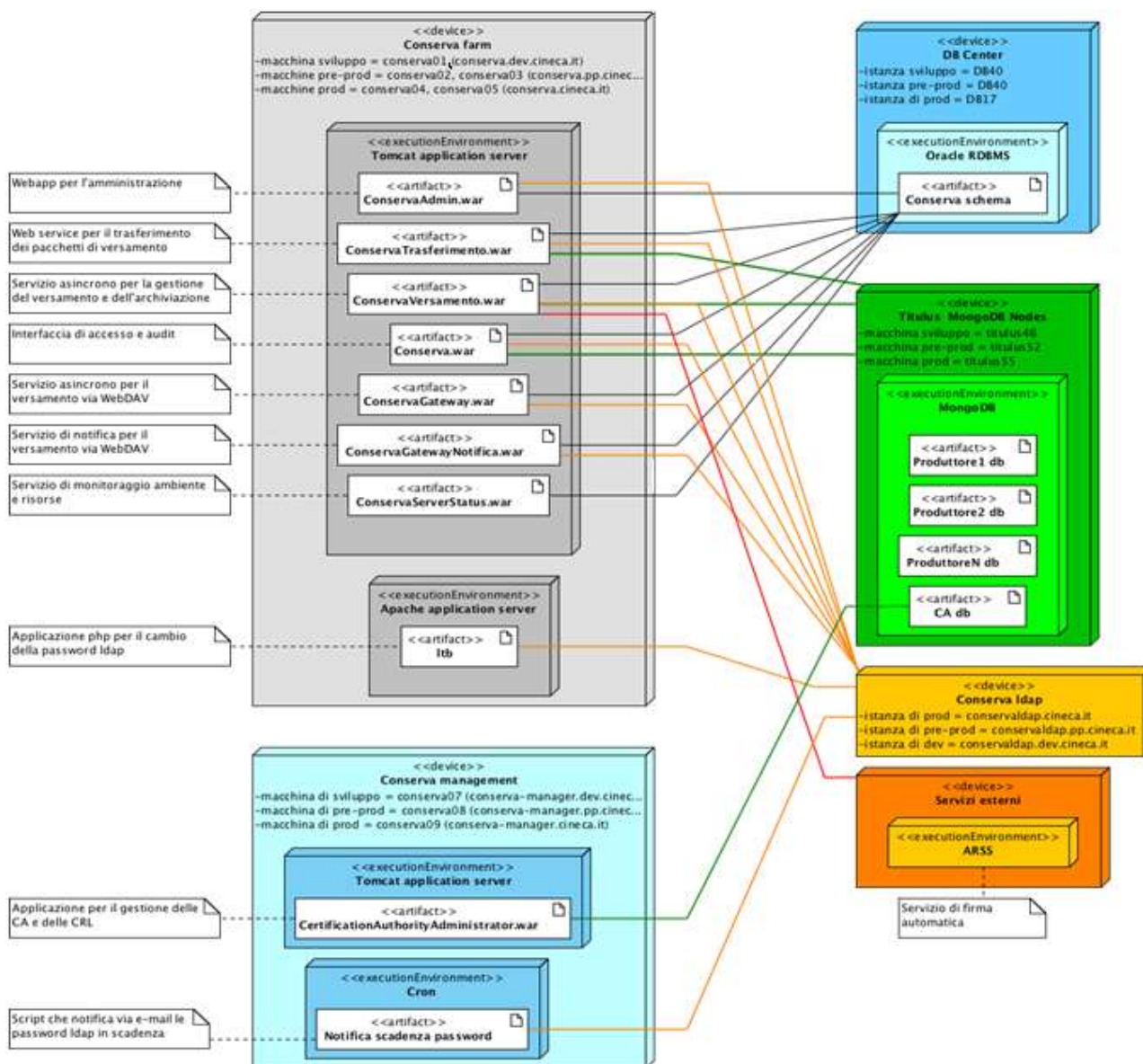


Figura 3 - Diagramma descrittivo dei componenti di Conserva

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

[Torna al sommario](#)

8.2.2 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 produttori 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 produttore, 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 produttori. A fonte di eventuali integrazioni fra l'applicazione e sistemi terzi del

produttore, 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.

[Torna al sommario](#)

8.3 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 che segue rappresenta la distribuzione dei componenti nell'ambiente di produzione

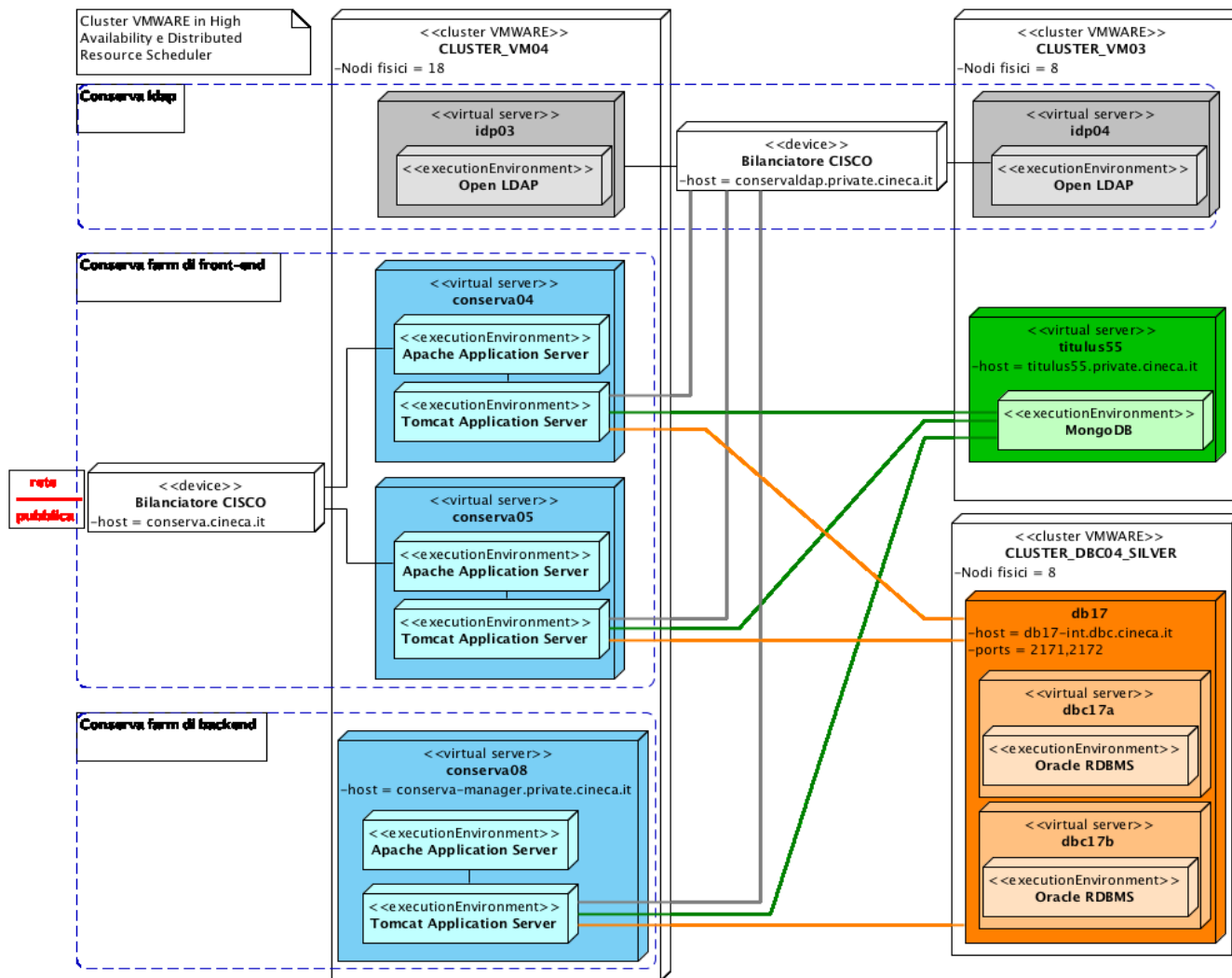


Figura 4 - Distribuzione componenti di Conserva

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 (lame 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 MongoDB:** un server singolo, 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.

Nel seguente grafico 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.

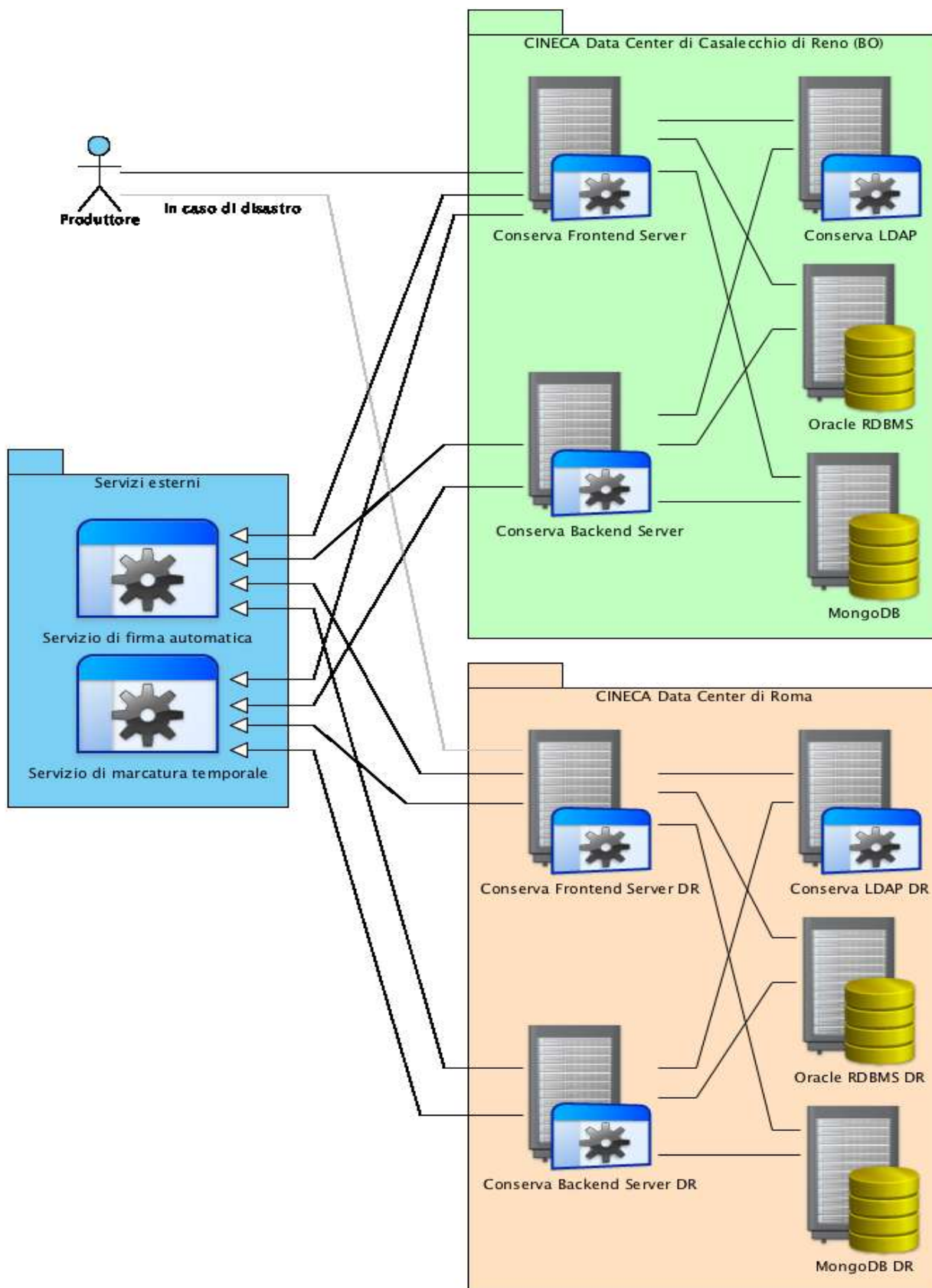


Figura 5 - Distribuzione topologica delle componenti fisiche di Conserva

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:

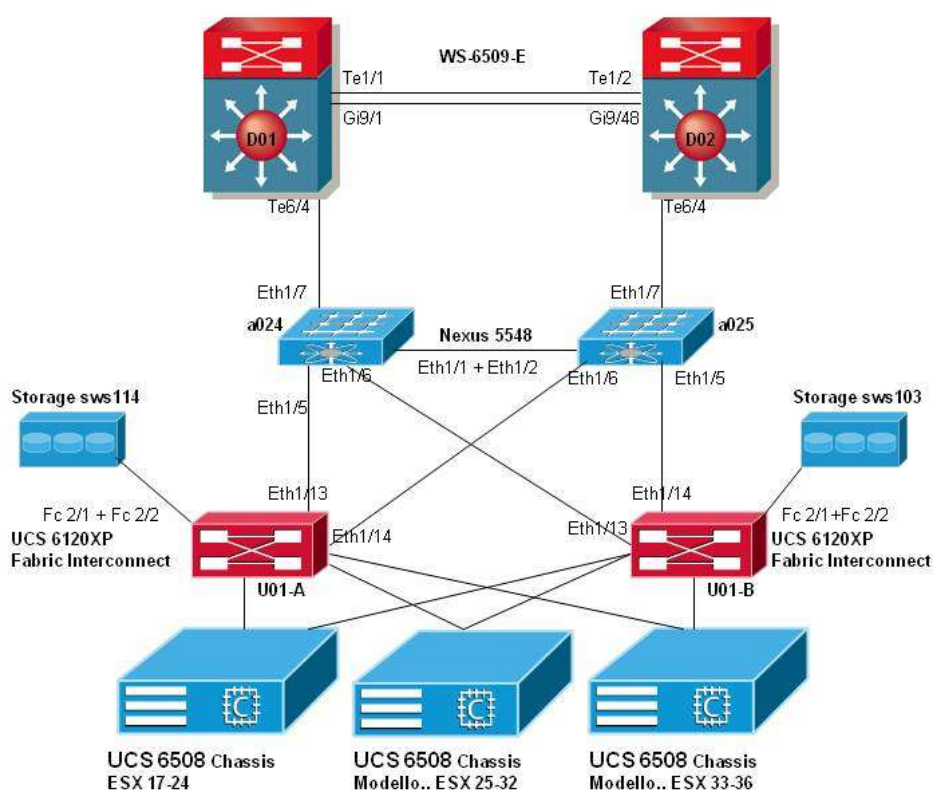


Figura 6 - Schema interconnessioni degli apparati di Conserva

[Torna al sommario](#)

8.4 Procedure di gestione e di evoluzione

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*"³.

[Torna al sommario](#)

8.4.1 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*.

³ Per maggiori informazioni: <http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf>

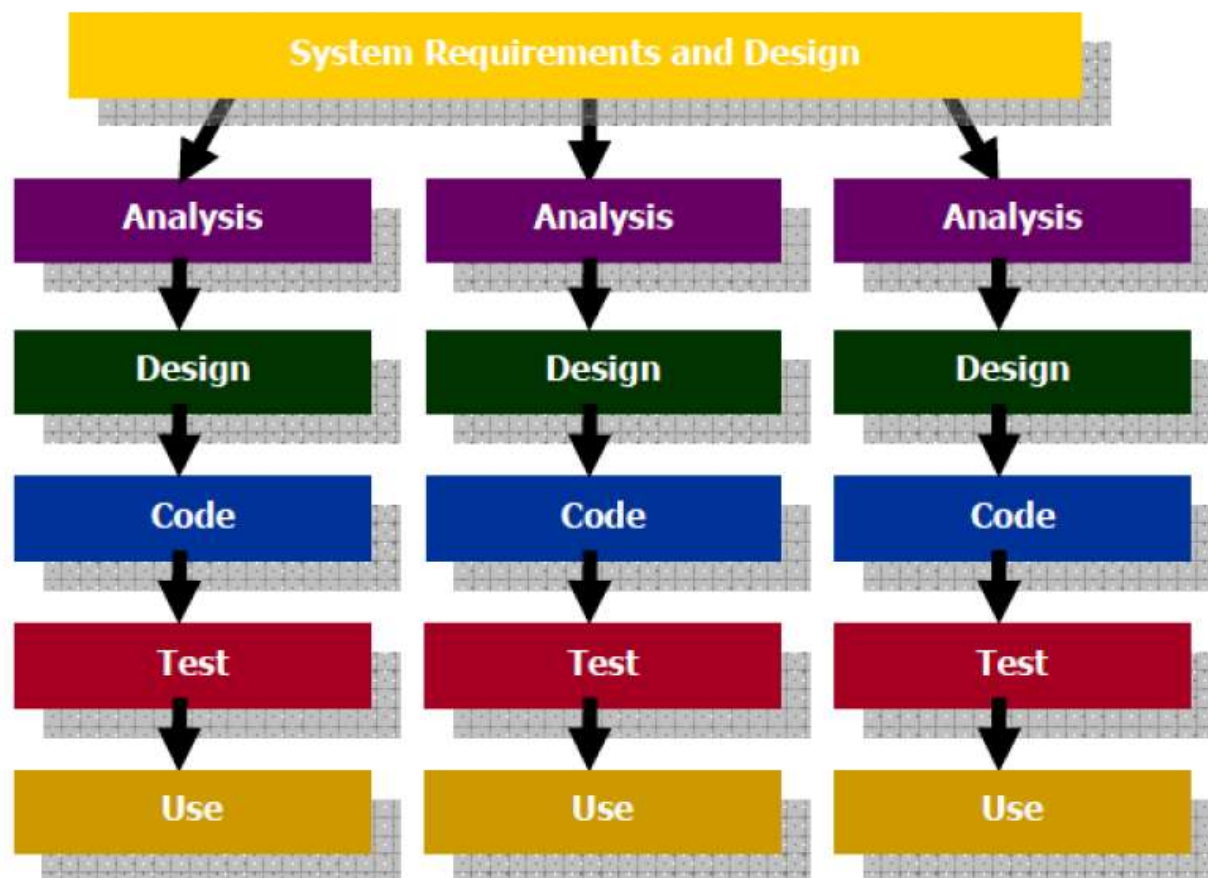


Figura 7 - Ciclo di vita iterativo-incrementale dello sviluppo del software

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 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:

- 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)).

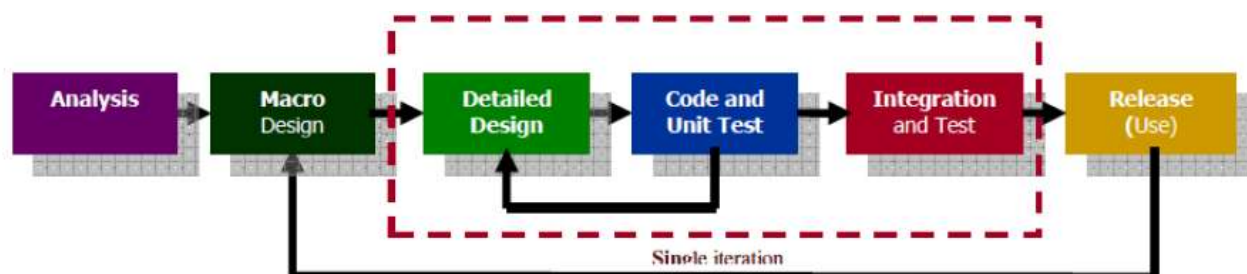


Figura 8 - Dettaglio del ciclo di vita iterativo-incrementale dello sviluppo del software

[Torna al sommario](#)

8.4.2 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 mantenuta dalla Divisione Sistemi e Tecnologie di CINECA, il cui accesso è regolato secondo le regole dettate dall'istruzione operativa pubblicata nell'intranet aziendale.

[Torna al sommario](#)

8.4.2.1 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:

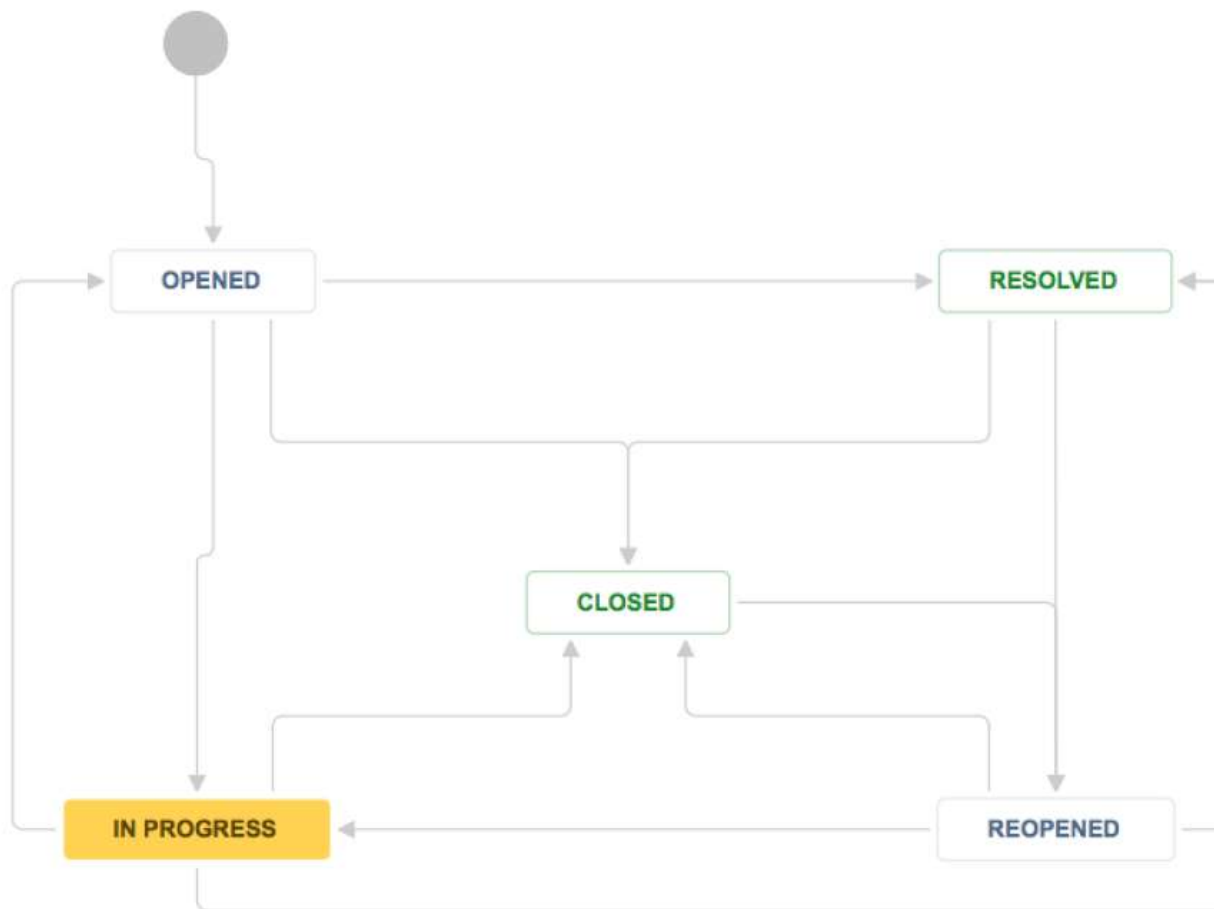


Figura 9 - Workflow degli stati delle singole issue

[Torna al sommario](#)

8.4.2.2 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 macro-componenti 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.

[Torna al sommario](#)

8.4.2.3 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.

[Torna al sommario](#)

8.4.2.4 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.

[Torna al sommario](#)

8.4.3 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.

[Torna al sommario](#)

8.4.4 Gli ambienti di esercizio

8.4.4.1 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.

[Torna al sommario](#)

8.4.4.2 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.

[Torna al sommario](#)

8.4.4.3 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 il protocollo devono essere conformi a quanto indicato nella normativa vigente in materia ed agli standard internazionali.

[Torna al sommario](#)

8.4.5 Ciclo di sviluppo del software

Le fasi attraverso le quali si è prodotto il software del servizio di conservazione Conserva di CINECA e attraverso le quali vengono implementate le modifiche alle varie componenti sono descritte nel seguente grafico

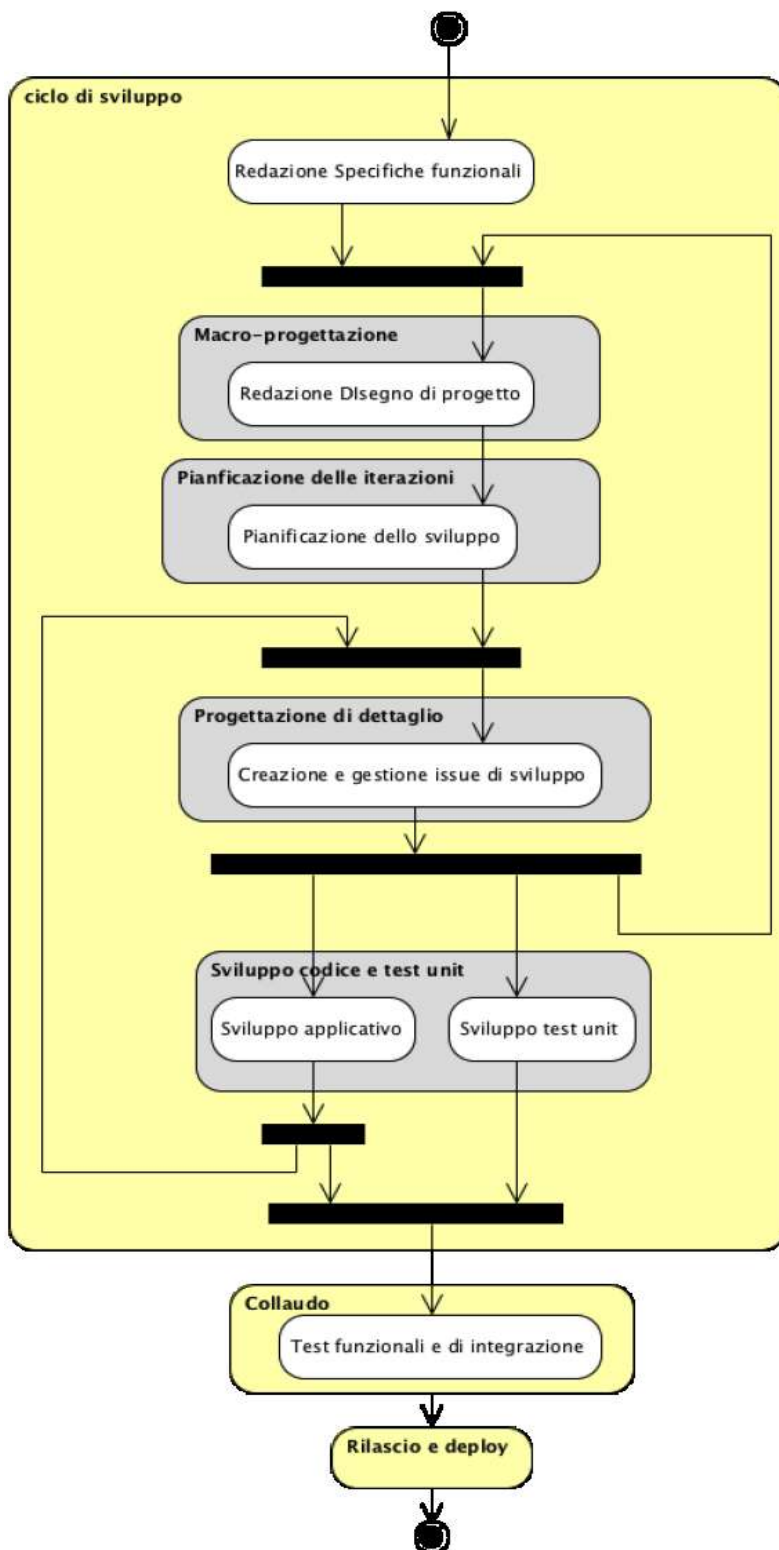


Figura 10 - Fasi di produzione del software

[Torna al sommario](#)

9. 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.

[Torna al sommario](#)

9.1 Procedure di monitoraggio

Tutta l'infrastruttura tecnologica e applicativa 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 quali https, pop3/s, imap/s, smtp, snmp, 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 ITILv3⁴.

[Torna al sommario](#)

9.2 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.

[Torna al sommario](#)

9.2.1 Monitoraggio a campione degli archivi

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

- Oggetti informativi;

⁴ Information Technology Infrastructure Library, per maggiori informazioni: <http://www.itil-italia.com/itilv3.htm>

- 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.

[Torna al sommario](#)

9.2.2 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 produttore 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 produttore se necessario.

[Torna al sommario](#)

9.3 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.

[Torna al sommario](#)

9.3.1 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").

[Torna al sommario](#)

9.3.2 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.

[Torna al sommario](#)

9.3.3 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 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.

[Torna al sommario](#)

9.3.4 Altri componenti

I componenti ConservaGateway e ConservaGatewayNotifica tracciano elaborazione, errori, eccezioni e warning quando si presentano e questi log sono registrati su file presenti sul file system shared tra le macchine di Conserva.

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. Tale infrastruttura raccoglie i log in base ai criteri espressi dal Garante della Privacy (Dlgs 196/2003): **“Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008”** (G.U. n. 300 del 24 dicembre 2008, e modificato con il provvedimento del G.U. n. 149 del 30 giugno 2009). 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.

[Torna al sommario](#)

9.4 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.

[Torna al sommario](#)

9.4.1 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



MANUALE DI CONSERVAZIONE

Rev. 1.3 del 10/10/2016



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*.

[Torna al sommario](#)