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**	**Titolari dell'oggetto di conservazione, Personale Cineca**

STATO/STORIA DELLE REVISIONI

Versione	Data	Paragrafo revisionato	Oggetto dalla revisione	Autore/i principale della revisione	Altri contributi	Validato
2.2	09/01/2023	5	Cambiamento dei ruoli e aggiornamento storico dei ruoli	Massimiliano Valente	N. Carofiglio	M.Valente
2.1	26/10/2022	Intestazione	Modificato ente certificatore e rispettivo logo	M. Mingrone	-	M.Valente
2.00	29/11/2021	2.1 2.2 3.1 3.2 4 5.1 5.2 7.1	Glossario Acronimi Normativa di riferimento Standard di riferimento Ruoli e responsabilità Organigramma Matrice RACI attività del servizio Aggiunto capitolo "Redazione Accordi di versamento"	M. Mingrone N. Carofiglio	A. De Angelis	M.Valente
1.12	12/05/2021	5	Cambiamento dei ruoli e aggiornamento storico dei ruoli	Massimiliano Valente		M.Valente
1.11	11/01/2021	5	Cambiamento di ruoli	Riccardo Righi		R.Righi

1.10	08/04/2020	4 5 6.1	Definito meglio il ruolo del Responsabile del trattamento dei dati personali Recepite modifiche organigramma Definita meglio la proprietà degli oggetti conservati	Riccardo Righi		R.Righi
1.9	03/05/2019	Tutto 3.1 6.1 6.3, 6.4 5.1 8.1 8.2 8.3 9.3	Sistemazione Layout Adeguata Normativa Esplicitati formati conservati Revisione PdA e PdV Revisione organigramma Revisione Componenti Logiche Revisione Componenti Tecnologiche Revisione Componenti Fisiche Revisione politiche di Conservazione dei log	Stefano Capelli Laura Nisi		R. Righi
1.8	08/02/2018	5	Inserimento storico dei ruoli	Stefano Capelli Laura Nisi		R. Righi
1.7	15/12/2017	5	Cambiamento di ruoli	Stefano Capelli		R. Righi
1.6	06/11/2017	5 5.1	Cambiamento di ruoli Aggiornamento dell'organigramma	Laura Nisi	R. Righi	R. Righi
1.5	11/08/2017	8.3	Variazione struttura base dati	Laura Nisi		R. Righi
1.4	22/06/2017		Cambiamento di ruoli	Laura Nisi		R. Righi
1.3	10/10/2016		Revisione a seguito delle osservazioni dell'AGID	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
1.1	22/04/2016		Revisione a seguito delle osservazioni dello Studio Lisi	Laura Nisi	A. De Angelis	P. Vandelli

1.0	01/12/2015		Emissione	Laura Nisi	P. Tentoni F. Merighi A. De Angelis P. Vandelli	P. Vandelli

Sommario

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;
- 8 allegati tecnici:
  - Allegato 1 - Modello accordo di versamento
  - Allegato 2 - Pacchetto di versamento
  - Allegato 3 - Indice UNISinCRO
  - Allegato 4 - Mezzi di trasmissione
  - Allegato 5 - Rapporto di versamento
  - Allegato 6 - Controlli sul pacchetto di versamento
  - Allegato 7 – Organigramma
  - Allegato 8 – Formati accettati

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 di prendere visione dei documenti informatici.	LLGG
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 versamento formalizzano sia i	OAIS

	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.	
Affidabilità	Caratteristica che, con riferimento a un sistema di gestione documentale o conservazione, esprime il livello di fiducia che l'utente ripone nel sistema stesso, mentre con riferimento al documento informatico esprime la credibilità e l'accuratezza della rappresentazione di atti e fatti in esso contenuta.	LLGG
Aggregazione documentale informatica	Insieme di documenti informatici o insieme 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.	LLGG
AgID	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.	CAD
Archival Information Package (AIP)	Denominazione in OAIS del pacchetto di archiviazione. Per l'accezione utilizzata in questo manuale cfr. Pacchetto di archiviazione.	OAIS
Archivio	Complesso dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività.	LLGG

Archivio informatico	Archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche.	LLGG
Area Organizzativa Omogenea	Un insieme di funzioni e di uffici individuati dall'ente al fine di gestire i documenti in modo unitario e coordinato, secondo quanto disposto dall'art. 50 comma 4 del D.P.R. 28 dicembre 2000, n. 445. Essa rappresenta il canale ufficiale per l'invio di istanze e l'avvio di procedimenti amministrativi.	LLGG
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.	LLGG
Autenticità	Caratteristica in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto un oggetto è autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze.	LLGG
Base di dati	Collezione di dati registrati e correlati tra loro.	CINECA
Codice dell'amministrazione digitale (CAD)	Decreto legislativo n° 82 del 2005 smi.	
Certificazione	Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi.	LLGG

Classificazione	Attività di organizzazione di tutti i documenti secondo uno schema costituito da un insieme di voci articolate in modo gerarchico e che individuano, in astratto, le funzioni, competenze, attività e/o materie del soggetto produttore.	LLGG
Cliente	Il soggetto che per legge ha l'obbligo di conservare.	CINECA
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.	OAIS
Controllo forzabile	Sono forzabili i controlli il cui mancato superamento rimette la responsabilità del versamento dell'unità al Responsabile della conservazione.	CINECA
Controllo non forzabile	Sono non forzabili i controlli il cui mancato superamento comporta il rifiuto inderogabile dell'unità di versamento controllata.	CINECA
CONSERVA	Sistema di conservazione Cineca	CINECA
Conservatore	Soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici.	LLGG
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 garantendo nel tempo le caratteristiche di	LLGG

	autenticità, integrità, leggibilità, reperibilità dei documenti.	
Consumer	Denominazione in OAIS di utente. Per l'accezione utilizzata in questo manuale cfr. Utente.	OAIS
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.	OAIS
Convenzioni di denominazione del file	Insieme di regole sintattiche che definisce il nome dei file all'interno di un filesystem o pacchetto. (Anche ***Naming convention)***	LLGG
Coordinatore della Gestione Documentale	Soggetto 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.	LLGG
Copia informatica di documento analogico	Il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto.	CAD
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.	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.	CAD
Destinatario	Il soggetto/sistema al quale il documento informatico è indirizzato.	LLGG
Digest	Vedi impronta crittografica.	LLGG
Dissemination Information Package (DIP)	Denominazione in OAIS del pacchetto di distribuzione. Per l'accezione utilizzata in questo manuale cfr. Pacchetto di distribuzione.	OAIS
Documento amministrativo informatico	Gli atti formati dalle pubbliche amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse.	LLGG
Documento analogico	La rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.	CAD
Documento elettronico	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva.	LLGG
Documento informatico	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.	LLGG
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.	CAD
eIDAS - electronic IDentification Authentication and Signature	Regolamento (UE) № 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel	

	mercato interno e che abroga la direttiva 1999/93/CE.	
Esibizione	Operazione che consente di visualizzare un documento conservato.	LLGG
Evidenza informatica	Una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.	
Fascicolo informatico	Aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento.	LLGG
File	Insieme di informazioni, dati o comandi logicamente correlati, raccolti sotto un unico nome e registrati, per mezzo di un programma di elaborazione o di scrittura, nella memoria di un computer.	LLGG
Filesystem	Sistema di gestione dei file, strutturato mediante una o più gerarchie ad albero, che determina le modalità di assegnazione dei nomi, memorizzazione e organizzazione all'interno di uno storage.	LLGG
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,	CAD

	rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.	
Firma elettronica	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare.	EIDAS
Firma elettronica avanzata	Una firma elettronica che soddisfi i requisiti di cui all'articolo 26 del regolamento Eidas.	EIDAS
Firma elettronica qualificata	Una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche.	EIDAS
Formato contenitore	Formato di file progettato per consentire l'inclusione ("imbustamento" o wrapping), in uno stesso file, di una o più evidenze informatiche soggette a differenti tipi di codifica e al quale possono essere associati specifici metadati.	LLGG
Formato del documento informatico	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.	LLGG
Formato "deprecato"	Formato in passato considerato ufficiale il cui uso è attualmente sconsigliato a favore di una versione più recente.	LLGG
Funzioni aggiuntive del protocollo informatico	Nel sistema di protocollo informatico, componenti supplementari rispetto a quelle	LLGG

	minime, necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni.	
Funzioni minime del protocollo informatico	Componenti del sistema di protocollo informatico che rispettano i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445.	LLGG
Funzione di hash crittografica	Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o digest in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.	LLGG
GDPR - General Data Protection Regulation	Regolamento (UE) № 679/2016 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.	LLGG
Gestione documentale	Processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta, uso, selezione e conservazione dei documenti.	LLGG
Hash	Termine inglese usato, impropriamente, come sinonimo d'uso di "impronta crittografica" o "*digest*" (vedi).	LLGG

Identificativo univoco	Sequenza di numeri o caratteri alfanumerici associata in modo univoco e persistente ad un'entità all'interno di uno specifico ambito di applicazione.	LLGG
Impronta crittografica	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di hash crittografica a un'evidenza informatica.	LLGG
Indice di conservazione	File associato ad ogni volume di conservazione, contenente un insieme di informazioni organizzate conformemente allo Schema XML fornito in questo documento.	UNISINCRO
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. Sono riportate all'interno degli Accordi di Versamento. Compongono il pacchetto insieme alle informazioni sulla conservazione.	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. Sono riportate all'interno degli Accordi di Versamento.	OAIS
Informazioni sull'accesso	Le informazioni che identificano le restrizioni di accesso. Sono riportate all'interno degli Accordi di Versamento.	OAIS

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. Sono riportate all'interno degli Accordi di Versamento.	OAIS
Informazioni sull'impacchettamento	Le informazioni usate per collegare e identificare le componenti di un pacchetto informativo. Sono riportate all'interno degli Accordi di Versamento.	OAIS
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. Sono riportate all'interno degli Accordi di Versamento.	OAIS
Informazioni sulla conservazione	Le informazioni necessarie per un'adeguata conservazione del contenuto informativo. Includono le informazioni sull'identificazione, provenienza, contesto, integrità e accesso.	OAIS
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. Sono	OAIS

	riportate all'interno degli Accordi di Versamento.	
Informazioni sulla rappresentazione	Le informazioni che associano un oggetto dati a concetti più significativi. Sono riportate all'interno degli Accordi di Versamento.	OAIS
Integrità	Caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità.	LLGG
Interoperabilità	Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi.	LLGG
Leggibilità	Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica.	LLGG
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.	CINECA

Manuale di conservazione	Documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture.	LLGG
Manuale di gestione	Documento informatico che descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.	LLGG
Metadati	Dati associati a un o documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017.	LLGG
Oggetto di conservazione	Oggetto digitale versato in un sistema di conservazione.	LLGG
Oggetto digitale	Oggetto informativo digitale, che può assumere varie forme tra le quali quelle di documento informatico, fascicolo informatico, aggregazione documentale informatica o archivio informatico.	LLGG

Oggetto informativo	Un oggetto dati insieme con le sue informazioni sulla rappresentazione.	OAIS
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.	CAD
Pacchetto di archiviazione	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel manuale di conservazione.	LLGG
Pacchetto di distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione.	LLGG
Pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione.	LLGG
Pacchetto informativo	Contenitore logico che racchiude uno o più oggetti di conservazione con i relativi metadati, oppure anche i soli metadati riferiti agli oggetti di conservazione.	LLGG
Path	Informazioni relative alla localizzazione virtuale del file all'interno del filesystem espressa come concatenazione ordinata del nome dei nodi del percorso. (anche *Percorso*)	LLGG
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	LLGG

	conservazione dei documenti informatici da possibili rischi.	
Piano di classificazione (Titolario)	Struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata.	LLGG
Piano di conservazione	Documento, allegato al manuale di gestione e integrato con il sistema di classificazione, in cui sono definiti i 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.	LLGG
Piano di organizzazione delle aggregazioni documentali	Strumento integrato con il sistema di classificazione a partire dai livelli gerarchici inferiori di quest'ultimo e finalizzato a individuare le tipologie di aggregazioni documentali (tipologie di serie e tipologie di fascicoli) che devono essere prodotte e gestite in rapporto ai procedimenti e attività in cui si declinano le funzioni svolte dall'ente	LLGG
Piano generale della sicurezza	Documento che pianifica le 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.	LLGG
Posta elettronica certificata	Sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di	CAD

	posta elettronica e di fornire ricevute opponibili ai terzi.	
Presa in carico	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione e in caso di affidamento del servizio all'esterno, dagli accordi stipulati tra il titolare dell'oggetto di conservazione e il responsabile del servizio di conservazione.	LLGG
Processo di conservazione	Insieme delle attività finalizzate alla conservazione dei documenti informatici.	CINECA
Producer	Denominazione in OAIS di produttore. Per l'accezione utilizzata in questo manuale cfr. produttore.	OAIS
Produttore dei PdV	Persona fisica, 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.	LLGG
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.	LLGG
Registro di protocollo	Registro informatico ove sono memorizzate le informazioni prescritte dalla normativa per tutti	LLGG

	i documenti ricevuti e spediti da un ente e per tutti i documenti informatici dell'ente stesso.	
Registro particolare	Registro informatico individuato da una pubblica amministrazione per la memorizzazione delle informazioni relative a documenti soggetti a registrazione particolare.	LLGG
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.	CINECA
Resoconto di versamento	Documento informatico che comunica al Produttore, immediatamente dopo il versamento, lo stato del pacchetto di versamento (*interamente_versato, parzialmente_versato o rifiutato)* con il dettaglio dell'esito di tutti i controlli sulle singole unità.	CINECA
Responsabile del servizio di conservazione	Soggetto che coordina il processo di conservazione all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID.	LLGG
Responsabile della conservazione	Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.	LLGG

Responsabile della funzione archivistica di conservazione	Soggetto che coordina il processo di conservazione dal punto di vista archivistico all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID	LLGG
Responsabile della gestione documentale	Soggetto responsabile della gestione del sistema documentale o responsabile del 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.	LLGG
Responsabile della protezione dei dati	Persona con conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, in grado di assolvere i compiti di cui all'articolo 39 del Regolamento (UE) 2016/679.	LLGG
Riferimento temporale	Insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC).	LLGG
Riversamento	Procedura mediante la quale uno o più documenti informatici sono convertiti da un formato di file (ovvero di busta, ovvero di pacchetto di file) ad un altro, lasciandone invariato il contenuto per quanto possibilmente permesso dalle caratteristiche tecniche del formato (ovvero dei formati) dei file e delle codifiche di destinazione.	LLGG
Scarto	Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più	LLGG

	rilevanti ai fini giuridico-amministrativo e storico-culturale.	
Serie	Raggruppamento di documenti con caratteristiche omogenee (vedi anche aggregazione documentale informatica).	LLGG
Sigillo elettronico	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi.	LLGG
Sistema di conservazione	Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, comma 1, del CAD.	LLGG
Sistema di gestione informatica dei documenti	Insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle organizzazioni per la gestione dei documenti. Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445.	CAD
Submission Information Package (SIP)	Denominazione in OAIS del pacchetto di versamento. Per l'accezione utilizzata in questo manuale cfr. Pacchetto di versamento.	OAIS
Tag library	Dizionario dei marcatori contenente le definizioni in ordine alfabetico di tutti gli elementi, i tipi e gli attributi individuati da uno Schema XML, mirato a definire la loro semantica.	UNISINCRO

Tipologia documentale	Categoria di documenti omogenei per natura e funzione giuridica, modalità di registrazione o di produzione, che hanno comuni caratteristiche formali e/o intellettuali.	CINECA
Titolare dell'oggetto di conservazione	Soggetto produttore degli oggetti di conservazione. Nel contesto Cineca corrisponde al Cliente. (Nel testo anche Titolare)	LLGG
Trasferimento	Passaggio di custodia dei documenti da una persona o un ente ad un'altra persona o un altro ente.	LLGG
TUDA	Testo Unico della Documentazione Amministrativa, Decreto del Presidente della Repubblica 28 dicembre 2000, n.445, e successive modificazioni.	LLGG
Ufficio	Riferito ad un'area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico.	LLGG
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 di conservazione al fine di consentire agli operatori del settore di raggiungere una soddisfacente interoperabilità.	CINECA
Unità archivistica	Indica un insieme di documenti raggruppati secondo un nesso di collegamento organico,	CINECA

	che costituiscono un'unità non divisibile: repertorio, serie o 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).	CINECA
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.	CINECA
Utente abilitato	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.	LLGG
Versamento	Passaggio di custodia, di proprietà e/o di responsabilità dei documenti. Nel caso di un organo giudiziario e amministrativo dello Stato operazione con la quale il responsabile della conservazione trasferisce 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.	LLGG

Volume di conservazione	Unità logica risultato finale di un processo mirato a conservare un insieme di oggetti digitali.	UNISINCRO
Web Service	Sistema software progettato per supportare l'interoperabilità tra diversi elaboratori su di una medesima rete ovvero in un contesto distribuito.	CINECA

Torna al sommario

2.2 Acronimi

AGID	Agenzia per l'Italia Digitale
AIP	Archival Information Package (OAIS) anche PdA
DIP	Dissemination Information Package (OAIS) anche PdD
ETSI	European Telecommunications Standards Institute
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 (ISO 20652)
PDI	Preservation Descriptive Information
PdA	Pacchetto di Archiviazione
PdD	Pacchetto di Distribuzione
PdV	Pacchetto di Versamento
PEC	Posta Elettronica Certificata

RdC	Responsabile della conservazione
SIP	Submission Information Package (OAIS) anche PdV
UNI	Ente Nazionale Italiano di Unificazione
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 ed internazionale.

Alla data di stesura del presente manuale l'elenco dei principali riferimenti normativi in materia è costituito da:

- **Codice Civile** – R.D del 16 marzo 1942 n. 262;
- **Legge 241/1990** - Nuove norme sul procedimento amministrativo;
- **DPR 445/2000** - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- **DPR 37/2001** - Regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli uffici dello Stato;
- **D.lgs 196/2003** - recante il Codice in materia di protezione dei dati personali;
- **D.lgs 42/2004** - Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n.137;
- **D.lgs 82/2005** e ss.mm.ii. - Codice dell'amministrazione digitale;
- **D.lgs 33/2013** - Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni;
- **DPCM 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;
- **DPCM 21 marzo 2013** - Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro

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

- **Reg. UE 910/2014** - in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE - Regolamento eIDAS;
- **Circolare 40 e 41 del 14 dicembre 2015 della Direzione generale degli archivi -** Autorizzazione alla distruzione di originali analogici riprodotti secondo le regole tecniche di cui al DPCM 13.11.2014 e conservati secondo le regole tecniche di cui al DPCM 13.12.2013;
- **Reg. UE 679/2016 (GDPR)** - relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- **Circolare 18 aprile 2017, n. 2/2017 dell'Agenzia per l'Italia Digitale** - recante le misure minime di sicurezza ICT per le pubbliche amministrazioni;
- **Circolare n. 2 del 9 aprile 2018** - recante i criteri per la qualificazione dei Cloud Service Provider per la PA;
- **Circolare n. 3 del 9 aprile 2018** - recante i criteri per la qualificazione di servizi SaaS per il Cloud dellaPA;
- **Reg. UE 2018/1807** - relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea;
- **Linee guida del 15 aprile 2019 dell'indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi**;
- **Linee guida del 09/01/2020 sull'Accessibilità degli strumenti informatici**;
- **Linee Guida sulla formazione, gestione e conservazione dei documenti informatici** - Maggio 2021 e relativi allegati;
- **Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici** - Giugno 2021 e relativi allegati.

Torna al sommario

3.2 Standard di riferimento

Si riportano di seguito gli standard di riferimento:

- **ISO 14721 OAIS -** (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- **ISO/IEC 27001 -** Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- **UNI 11386 -** Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- **ISO 15836 -** Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.
- **ISO 20652 -** Paimas, Space data and information transfer systems – Methodology abstract standard;
- **ISO 15489 -1 -** Information and documentation – Records Management – part 1: General;
- **ISO 13008** - Information and documentation — Digital records conversion and migration process;
- **ETSI EN 319 401** - Electronic Signatures and Infrastructures (ESI) General Policy Requirements for Trust Service Providers (laddove applicabile);
- **ETSI TS 119 511** - Electronic Signatures and Infrastructures (ESI) Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques;
- **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.

Torna al sommario

4 Ruoli e responsabilità

Il presente capitolo richiama quanto previsto dalla normativa 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***: come definito dall'art. 44, comma 1-quater, del CAD e dalle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici,
  Il responsabile della conservazione, che opera d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei sistemi informativi, può affidare, ai sensi dell'articolo 34, comma 1-bis, lettera b), la conservazione dei documenti informatici ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative, e tecnologiche e di protezione dei dati personali. Il responsabile della conservazione della pubblica amministrazione, che opera d'intesa, oltre che con i responsabili di cui al comma 1-bis, anche con il responsabile della gestione documentale, effettua la conservazione dei documenti informatici secondo quanto previsto all'articolo 34, comma 1-bis.
  Il responsabile della conservazione definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.
  In particolare, il responsabile della conservazione:
  a) definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della

natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;

b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
c) genera e sottoscrive il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
d) genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
f) effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;
g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;
h) provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
i) predispone le misure necessarie per la sicurezza fisica e logica del sistema di conservazione come previsto dal par. 4.11;
j) assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
l) provvede per le amministrazioni statali centrali e periferiche a versare i documenti informatici, le aggregazioni informatiche e gli archivi informatici, nonché gli strumenti che ne garantiscono la consultazione, rispettivamente all'Archivio centrale dello

Stato e agli archivi di Stato territorialmente competenti, secondo le tempistiche fissate dall'art. 41, comma 1, del Codice dei beni culturali 45;

m) predispone il manuale di conservazione di cui al par. 4.7 e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Il servizio di conservazione CINECA prevede che tutte le attività suddette, ad esclusione delle lettere l) e m), sono affidate al responsabile del servizio di conservazione, rimanendo in ogni caso inteso che la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile/affidabile, rimane in capo al responsabile della conservazione.
Per ulteriori dettagli si rimanda ai manuali di conservazioni dei clienti Cineca.

- 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 all'ente produttore;
  - gestione delle convenzioni, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.

- il ***Responsabile della funzione archivistica di conservazione*** si occupa della:
  - Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato;

• definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici;

• monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione;

• collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.

- il ***Responsabile della sicurezza dei sistemi per la conservazione*** si occupa del/della:
  - rispetto dei requisiti e monitoraggio della 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

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo	Eventuali deleghe
Responsabile del servizio di conservazione (RSERV)	Massimiliano Valente	Cfr. Capitolo 2 - Ruoli e Responsabilità	Maggio 2021	Nessuna
Responsabile Sicurezza dei sistemi per la conservazione (RSIC)	Paola Tentoni	Cfr. Capitolo 2 - Ruoli e Responsabilità	Gennaio 2015	Nessuna
Responsabile funzione archivistica di conservazione (RARCH)	Mariagrazia Mingrone	Cfr. Capitolo 2 - Ruoli e Responsabilità	Gennaio 2023	Nessuna
Responsabile sistemi informativi per la conservazione (RSINF)	Angelo Neri	Cfr. Capitolo 2 - Ruoli e Responsabilità	Aprile 2015	Nessuna
Responsabile sviluppo e manutenzione del sistema di conservazione (RSVIL)	Massimiliano Valente	Cfr. Capitolo 2 - Ruoli e Responsabilità	Ottobre 2017	Nessuna

Nella seguente tabella sono indicati le attività svolte e i nominativi delle persone che ricoprono i ruoli specifici del processo di conservazione. 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.

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 e 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 preimpostato per la comunicazione del Responsabile della conservazione 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.

Precedenti Responsabili

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo
Responsabile del servizio di conservazione	Riccardo Righi	Cfr. Capitolo 2 - Ruoli e Responsabilità	Da luglio 2017 ad aprile 2021
	Paolo Vandelli	Cfr. Capitolo 2 - Ruoli e Responsabilità	Da luglio 2015 a luglio 2017
Responsabile trattamento dati personali	Emilio Ferrari	Cfr. Capitolo 2 - Ruoli e Responsabilità	Da gennaio 2014 a febbraio 2018

Responsabile sviluppo e manutenzione del sistema di conservazione	Francesca Merighi	Cfr. Capitolo 2 - Ruoli e Responsabilità	Da aprile 2015 a ottobre 2017
Responsabile funzione archivistica di conservazione	Massimiliano Valente	Cfr. Capitolo 2 - Ruoli e Responsabilità	Da maggio 2021 a dicembre 2022
	Riccardo Righi	Cfr. Capitolo 2 - Ruoli e Responsabilità	Da ottobre 2020 ad aprile 2021
	Laura Federica Nisi	Cfr. Capitolo 2 - Ruoli e Responsabilità	Da luglio 2015 a ottobre 2020

Torna al sommario

5.1 Organigramma

Per i dettagli sull'organigramma si rimanda all'Allegato 7 – Organigramma.

Torna al sommario

5.2 Strutture organizzative

Di seguito vengono descritti analiticamente i processi organizzativi interni del Conservatore che intervengono nelle principali attività che riguardano il Servizio di conservazione per ciascun contratto di conservazione stipulato. Le responsabilità di ciascuna attività sono espresse in matrice RACI.

ATTIVITA' PROPRIE DI CIASCUN CONTRATTO DI SERVIZIO DI CONSERVAZIONE	*RdC*	*RSERV*	*RSIC*	*RARCH*	*RSINF*	*RSVIL*
Attivazione del servizio di conservazione (a seguito della sottoscrizione di un contratto)	*C*	*A*		*R*		*C*
Acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento	*I*	*R/A*				*C*
Preparazione e gestione del pacchetto di archiviazione		*R/A*				*C*
Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta	*A*	*R*		*I*		*C*
Scarto dei pacchetti di archiviazione	*R/A*	*R*		*C*		*C*
Chiusura del servizio di conservazione	*R/A*	*R/A*	*I*	*I*	*I*	*C*
ATTIVITA' PROPRIE DI GESTIONE DEI SISTEMI INFORMATIVI						
Conduzione e manutenzione del sistema di conservazione		*R*	*C*	*C*	*C*	*A*
Monitoraggio del sistema di conservazione		*R*	*C*		*C*	*A*
Change management		*R*	*C*		*C*	
Verifica periodica di conformità a normativa e standard di riferimento		*R*	*C*	*A*	*I*	*C*

[R- Responsible; A- Accountable; C- Consulted; I- Informed]

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 OAIS[1] (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 metadatazione 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 costituito da una o più unità documentali o da un pacchetto di archiviazione, generato dal Sistema su richiesta dell'utente in una forma idonea alle specifiche esigenze di utilizzo.

La descrizione puntuale delle tipologie di oggetti conservati all'interno del sistema viene riportata nei relativi Accordi di versamento stipulati con i Clienti per due motivi:

- la grande rapidità di aggiornamento delle tipologie di oggetti informativi da conservare;
- gli oggetti informativi da conservare variano da un Titolare 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 metadatazione.

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

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

L'allegato 2 - "Formati di file e riversamento" alle Linee Guida sulla formazione, gestione e conservazione dei documenti digitali viene preso come punto di riferimento per i formati da accettare ai fini della conservazione a lungo termine.
I formati attualmente trattati dal sistema di conservazione Cineca sono quelli indicati nell'Allegato 8 al presente manuale.

Nel caso in cui il Titolare dell'oggetto di conservazione necessiti di formati aggiuntivi, essi dovranno essere concordati durante la stesura dell'accordo di versamento, nel quale verranno descritte in dettaglio le azioni da intraprendere per garantire la leggibilità dei file per tutto il periodo di conservazione. Non è possibile inviare in conservazione visualizzatori e formati non preventivamente concordati e configurati nel sistema. Si specifica che attualmente non vengono gestiti dati sanitari o giudiziari.
Gli oggetti conservati all'interno del sistema di conservazione di CINECA sono di proprietà del Titolare e CINECA li custodisce in sua vece.
Ogni azione sugli oggetti conservati che esuli dal controllo, monitoraggio, mantenimento degli stessi e del sistema, verifiche da parte dell'autorità pubblica non può essere compiuta da CINECA senza il nulla osta del Titolare. Ogni deroga alla regola sopra descritta deve essere concordata con il Titolare tramite accordo di versamento o mediante altro accordo formale.

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 documentali e/o archivistiche che formano il pacchetto
- **unità documentali e/o archivistiche** costituite da uno o più file;
- **impronta dell'indice del pacchetto di versamento**.

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 web.

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 dalla normativa;
- i **metadati integrativi** ritenuti utili ai fini di una corretta conservazione delle unità di versamento;
- i **metadati personalizzati**, specifici del Titolare 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.

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 costituito dalle unità correttamente versate nel sistema di conservazione ed è soggetto a possibili aggiornamenti nella metadatazione affinché si possa assicurare intellegibilità e l'accessibilità nel tempo.

A livello generale il pacchetto di archiviazione è costituito da:

- un ***indice del pacchetto di archiviazione*** contenente i metadati relativi alle unità documentali e/o archivistiche che formano il pacchetto
- **unità documentali e/o archivistiche** costituite da uno o più file;
- file contenente la **firma** del responsabile del servizio di conservazione sull' indice del pacchetto di archiviazione.

I pacchetti di archiviazione possono essere costruiti seguendo due criteri:

- serie di unità documentarie omogenee;
- unità archivistiche.

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 3 dedicato all'implementazione di UNISInCRO in Conserva.

Torna al sommario

6.4 Pacchetto di distribuzione

Il pacchetto di distribuzione è formato su specifica richiesta di un utente autorizzato; viene costruito sulla base della ricerca dell'utente e sui suoi diritti di accesso all'oggetto informativo.

A livello generale il pacchetto di distribuzione è costituito da:

- un dall'indice del pacchetto di distribuzione strutturato secondo lo standard UNI SInCRO;
- **unità documentali e/o archivistiche** costituite da uno o più file;
- **dichiarazione di integrità** (rapporto-esito-controlli-distribuzione), la quale esplicita che gli oggetti digitali richiesti non hanno subito alcuna alterazione dal momento in cui sono stati presi in carico dal servizio di conservazione fino alla loro esibizione;
- **schemi xsd** necessari alla validazione dell'xml dell'indice del PdD

La dichiarazione di conformità e l'indice del pacchetto di distribuzione sono firmati digitalmente e marcati temporalmente. L'intero pacchetto viene fornito all'utente in formato compresso, firmato digitalmente e marcato temporalmente.

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 Titolare al Conservatore.
Per strutturare questa fase di acquisizione degli oggetti informativi è stato preso come modello di riferimento lo standard ISO 20652 Paimas[2] (di seguito chiamato Paimas), il cui scopo è quello di definire la metodologia da seguire dal primo contatto tra il Titolare 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 Titolare e il Conservatore in cui si definiscono gli interlocutori e l'obiettivo della conservazione; in questa fase si dà inizio alla redazione della relativa documentazione e si individuano gli oggetti informativi che il Titolare intende inviare al sistema di conservazione;
- **fase di definizione formale**: permette di entrare nel merito dei dettagli dell'intero processo di conservazione per stilare l'accordo di versamento la cui sottoscrizione è a cura del Responsabile della conservazione del Titolare e del Responsabile del servizio di conservazione (*"Allegato 1 Modello di Accordo di versamento"*);

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

- **fase di trasferimento**: concretizza il trasferimento degli oggetti informativi dal sistema produttore al sistema di conservazione, ossia la modalità di presa in carico dei pacchetti;
- **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.

Torna al sommario

7.1 Redazione Accordo di versamento

Secondo la normativa e gli standard vigenti l'attività preliminare per qualsiasi processo di conservazione è la stesura di un accordo di versamento tra l'Ente Titolare dell'oggetto di conservazione e CINECA per ciascuna tipologia documentale.
L'accordo di versamento descrive le condizioni di versamento dal sistema informativo del Titolare al sistema di conservazione.
Le condizioni di versamento formalizzano:

- dettagli tecnici:
  - il protocollo di comunicazione,
  - lo standard di firme,
  - i controlli sul buon esito del versamento
- aspetti archivistici:
  - descrizione della tipologia del documento
  - metadati descrittivi specifici
  - metadati di contesto e strutturali
  - tempistiche di selezione

La necessità di esplicitare ogni singolo aspetto del versamento e di quanto versato deriva dalla complessità dell'azione conservativa nel contesto digitale; di conseguenza più le informazioni raccolte in fase di versamento sono dettagliate e precise, più l'attività conservativa potrà essere efficiente e completa. Successivamente alla sottoscrizione di ogni accordo di versamento, CINECA predispone il servizio perché operi, in fase di versamento, secondo quanto previsto dall'accordo

stesso. L'accordo di versamento è passibile di revisione nel caso in cui degli aspetti del processo di conservazione siano da modificare. Per ulteriori dettagli circa l'accordo di versamento si rimanda all' "Allegato 1 Modello di Accordo di versamento" al presente Manuale.

7.2 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 di versamento.

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

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 dei campi specifici delle differenti 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 all'interno del 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 interfaccia web.

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

7.3 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 Titolare.
Sulla base della tipologia dell'oggetto informativo da conservare e delle esigenze del Titolare, dichiarate nell'accordo di versamento, in controlli si differenziano in:

- *Controlli Forzabili / Controlli Non forzabili:*
  - ***Forzabili***: controlli il cui mancato superamento, rimette al Responsabile della conservazione la responsabilità del versamento dell'unità tramite la procedura di forzatura;
  - ***Non forzabili***: controlli il cui mancato superamento comporta il rifiuto inderogabile dell'unità di versamento controllata.
- *Controlli di sistema / Controlli custom:*
  - ***Di sistema:*** controlli 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
  - ***Custom:*** controlli concordati con il cliente e descritti nell'accordo di versamento.

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 in CONSERVA.

Per ulteriori informazioni circa i controlli di CONSERVA si rimanda all'Allegato 6 "Controlli sul pacchetto di versamento".

Torna al sommario

7.4 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.

In CONSERVA, il rapporto di versamento è rappresentato da un file XML firmato digitalmente e marcato temporalmente, attraverso firma automatica, dal Responsabile del servizio di conservazione.

Il processo di produzione del rapporto di versamento è il seguente:

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

Nella versione precedente di CONSERVA, il sistema accettava anche un'altra modalità di gestione rapporti di versamento, generando un unico rapporto di versamento per tutti i pacchetti di versamento inviati da uno specifico 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 Titolare, 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 Titolare.

Il rapporto di versamento è sempre identificato univocamente all'interno del sistema e gli viene attribuito un riferimento temporale in standard UTC tramite la valorizzazione degli attributi *IdSistema* e *RiferimentoTemporale* all'interno della struttura XML; inoltre riporta per ogni pacchetto di versamento sia l'impronta dell'indice che di ogni singola unità documentale versata.
Per ulteriori dettagli relativi alla struttura del rapporto di versamento si rimanda all'allegato relativo alla descrizione del rapporto di versamento.

Torna al sommario

7.5 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 Titolare, può avvenire in due momenti distinti: nella fase di **trasferimento** o nella fase di **versamento**.
Il rifiuto in fase di trasferimento viene comunicato in maniera sincrona al Titolare 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 Titolare in fase di trasferimento, nell'allegato relativo ai controlli.
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 Titolare 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 Titolare. 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 Titolare in fase di versamento nell'allegato relativo ai controlli.

Torna al sommario

7.6 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.

Lo standard UNI SInCRO è uno schema xml e contiene sia i metadati finalizzati alla conservazione e acquisiti dal Titolare, 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, e vi appone una marca temporale rilasciata da una CA secondo la normativa vigente.

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 Titolare 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

7.7 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 modi:

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

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

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

La produzione di duplicati e copie informatiche, in CONSERVA, avviene tramite richiesta da interfaccia web.

La figura del pubblico ufficiale è necessaria nei seguenti casi:

- 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.

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

Torna al sommario

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

Sulla base delle indicazioni in merito allo scarto 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 gli oggetti informativi 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 della cultura.

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

Torna al sommario

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

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

Il Conservatore è in grado di acquisire pacchetti di distribuzione provenienti da altri conservatori aderenti sia allo 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 distribuzione non dovesse aderire allo standard UNI 11386 SInCRO, dovranno essere stipulati specifici accordi.

Al fine di garantire l'interoperabilità, CINECA espone un servizio di migrazione dei pacchetti di archiviazione prodotti, secondo standard UNI 11386 SInCRO. Se non diversamente concordato, i pacchetti vengono messi a disposizione del Titolare 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 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.

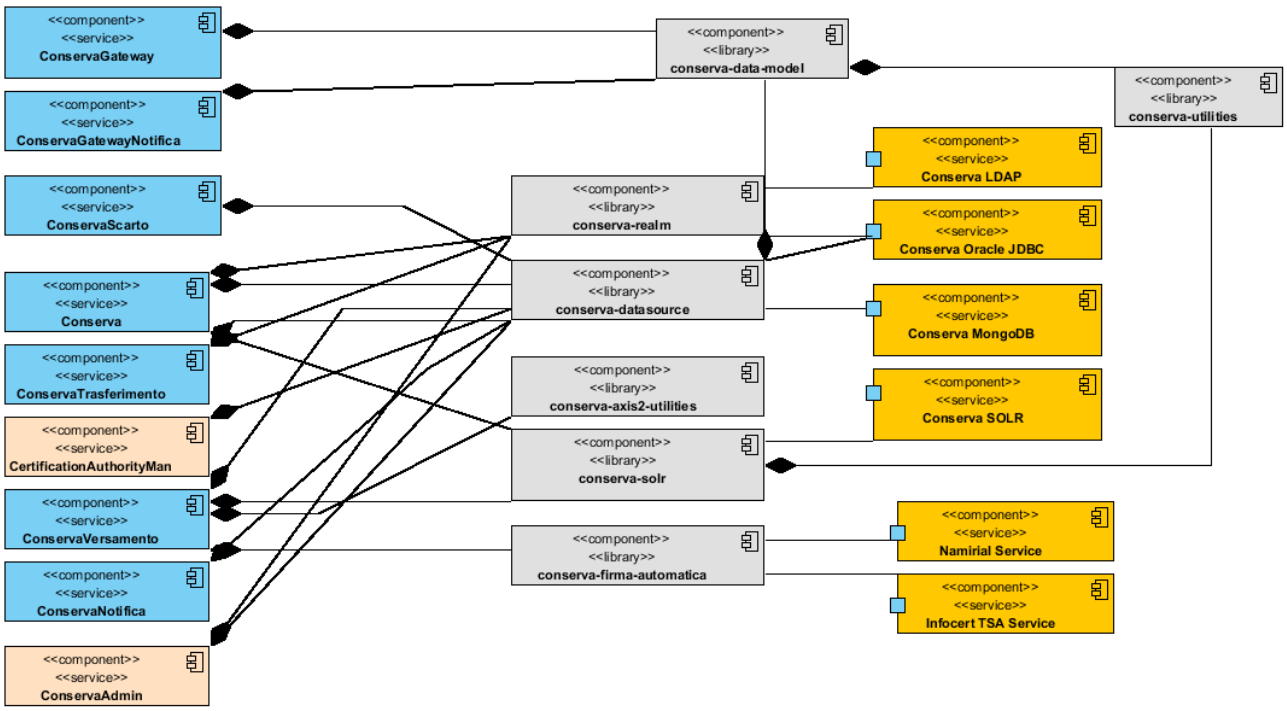

Figura 1- Schema delle componenti logiche che compongono il servizio

- **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.
- **ConservaVersamento servizio** – Componente Web 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, chiude e infine distribuisce i pacchetti di archiviazione in cui gli oggetti informativi vengono conservati.
- **Conserva-datasource libreria** – Libreria che si occupa di tutte le comunicazioni tra i componenti software e le basi di dati.
- **Conserva-data-model libreria** - Componente software dove vengono descritti gli oggetti che vengono elaborati e popolati da tutti gli altri componenti.
- **Conserva-utilities libreria** - Componente che mette a disposizione dell'intero sistema di conservazione metodi di utilità comuni a tutti gli altri componenti.
- **Conserva-axis2-utilities libreria** - Componente che mette a disposizione metodi che riguardano le connessioni tramite *web service*.
- **Conserva-solr libreria** - Componente che mette a disposizione metodi che consentono di indicizzare e ricercare elementi indicizzati.
- **Conserva-realm libreria** - Componente che mette a disposizione metodi che consentono di dialogare con il sistema di autenticazione e il sistema di autorizzazione.
- **Conserva-firma-automatica libreria** - Componente che si occupa dell'interazione con il Gateway di firma per l'apposizione delle firme automatiche necessarie al funzionamento di CONSERVA.
- **ConservaNotifica servizio** – Componente che gestisce le notifiche push dei rapporti e dei resoconti di versamento ai webservice registrati dei produttori.

- **CertificationAuthority servizio** – Componente che gestisce l'aggiornamento del repository locale dei certificati e delle CRL.
- **ConservaAdministration servizio** - Componente che permette l'amministrazione del sistema e della maggior parte dei componenti precedentemente descritti: ad esempio la creazione e la gestione di tutte le utenze che possono accedere a Conserva, la gestione dei servizi temporizzati, la creazione e gestione degli enti produttori e la creazione e gestione di nuovi accordi di versamento.
- **ConservaScarto servizio** – Componente che gestisce l'interazione fra il componente Conserva (interfaccia web di consultazione dell'archivio) e il componente conserva-versamento per la gestione dell'attività di scarto di oggetti informativi con la conseguente revisione dei pacchetti di archiviazione.

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:

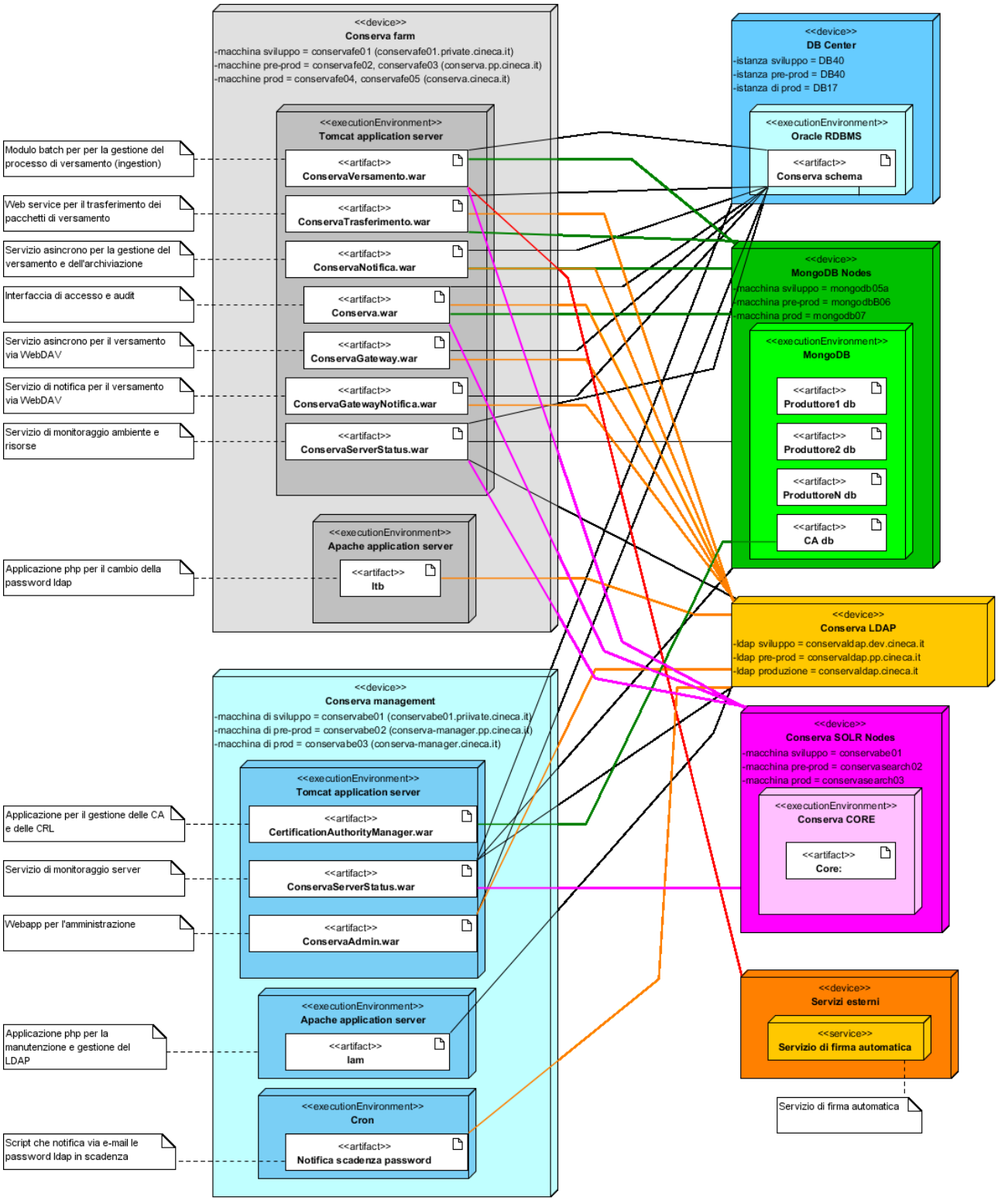

Figura 2 - Diagramma descrittivo dei componenti di Conserva

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
Oracle	DB per gestire le relazioni tra gli oggetti che compongono Conserva
MongoDB	DB per salvataggio oggetti conservati
Apache Solr	Search Engine
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 Titolari, 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 di 24H. La ripartenza del servizio sul sito di Disaster Recovery - RTO (Recovery Time Objective) è di 48H.
- I dati dei Titolari, gestiti nell'ambito del servizio di hosting, risiedono all'interno del territorio italiano, nella fattispecie presso i siti primario e secondario previsti per il servizio. Cineca si

impegna a comunicare al Titolare, con adeguato preavviso, ogni variazione all'ubicazione dei siti, pur garantendo sempre l'ubicazione interna al territorio italiano.

- Cineca garantisce i servizi per la riattivazione e il ripristino del sistema informativo primario, in presenza di un evento catastrofico, di una condizione di emergenza o di un disastro. I criteri per la definizione di tali eventi e la responsabilità per l'attivazione del Piano di Disaster Recovery rimangono in carico a Cineca, che provvederà a darne visibilità ai Titolari. A fronte di eventuali integrazioni fra l'applicazione e sistemi terzi del Titolare, Cineca si impegnerà nel coordinamento con lo stesso per la gestione in fase di emergenza dei rispettivi Piani di Disaster Recovery.
- Cineca si impegna ad eseguire test periodici (almeno una volta l'anno) per simulare il funzionamento del sito di Disaster Recovery in caso di disastro del sito primario, al fine di verificare che sia assicurato il corretto ripristino del funzionamento del sistema informativo di produzione.

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

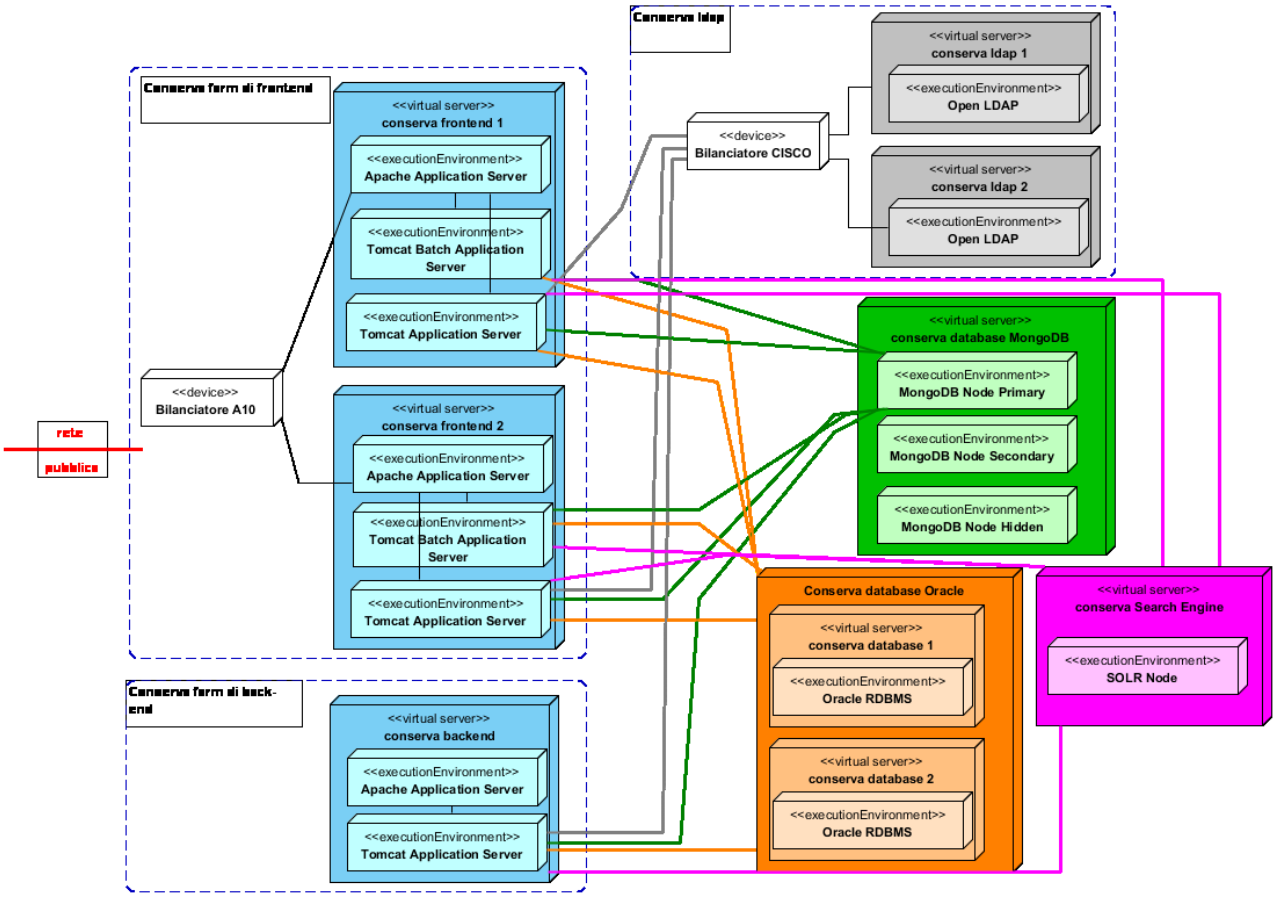

Figura 3 - Distribuzione componenti di Conserva

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 Solr**: un server singolo visibile solo da rete privata, con Apache Solr e Apache ZooKeeper
- **Sistema MongoDB**: un ReplicaSet a tre nodi (primary , secondary , hidden), visibile solo da rete privata, con database MongoDB.
- **Sistema Oracle**: due server active/passive, visibili solo da rete privata, con database Oracle RDBMS.
- **Sistema LDAP**: due server in farm dietro bilanciatore, visibili solo da rete privata, con Open LDAP.
- **Servizio di firma automatica**: servizio offerto da fornitore esterno accreditato AgID.
- **Servizio di marcatura temporale**: servizio offerto da fornitore esterno accreditato AgID.

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.

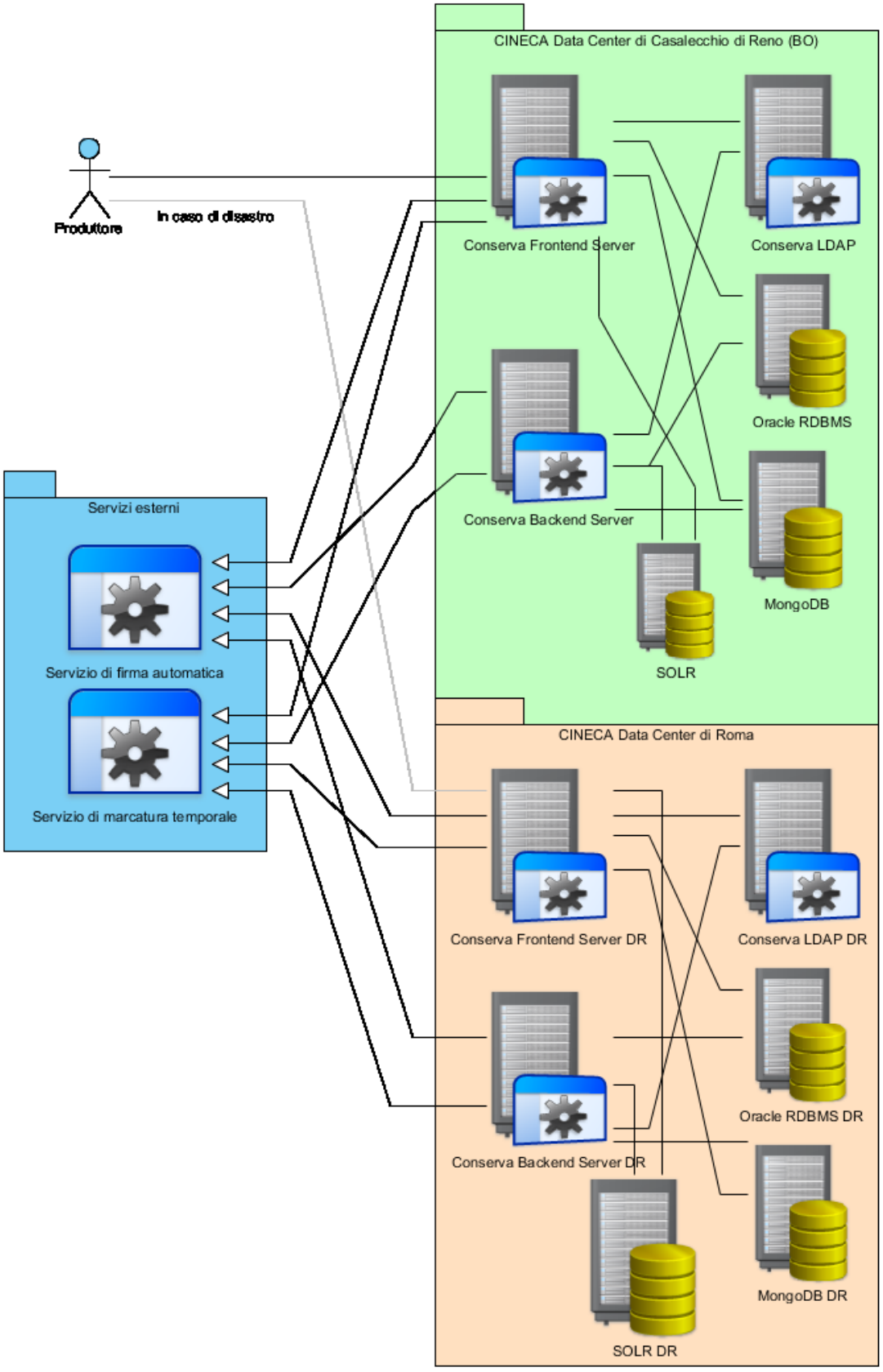
CINECA Data Center di Casalecchio di Reno (BO)
Produttore
In caso di disastro
Conserva Frontend Server
Conserva LDAP
Oracle RDBMS
Conserva Backend Server
MongoDB
SOLR
Servizi esterni
Servizio di firma automatica
Servizio di marcatura temporale
CINECA Data Center di Roma
Conserva Frontend Server DR
Conserva LDAP DR
Oracle RDBMS DR
Conserva Backend Server DR
MongoDB DR
SOLR DR

Figura 4 - 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:

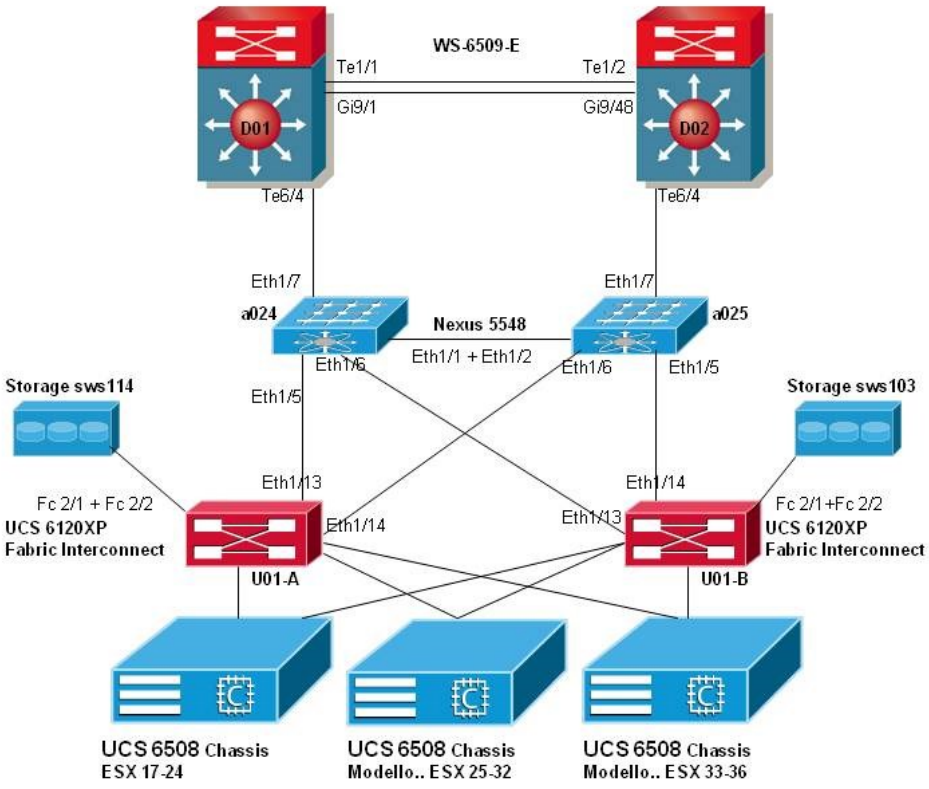

Figura 5 - Schema interconnessioni degli apparati di Conserva

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 alla normativa vigente e 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.

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

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*.

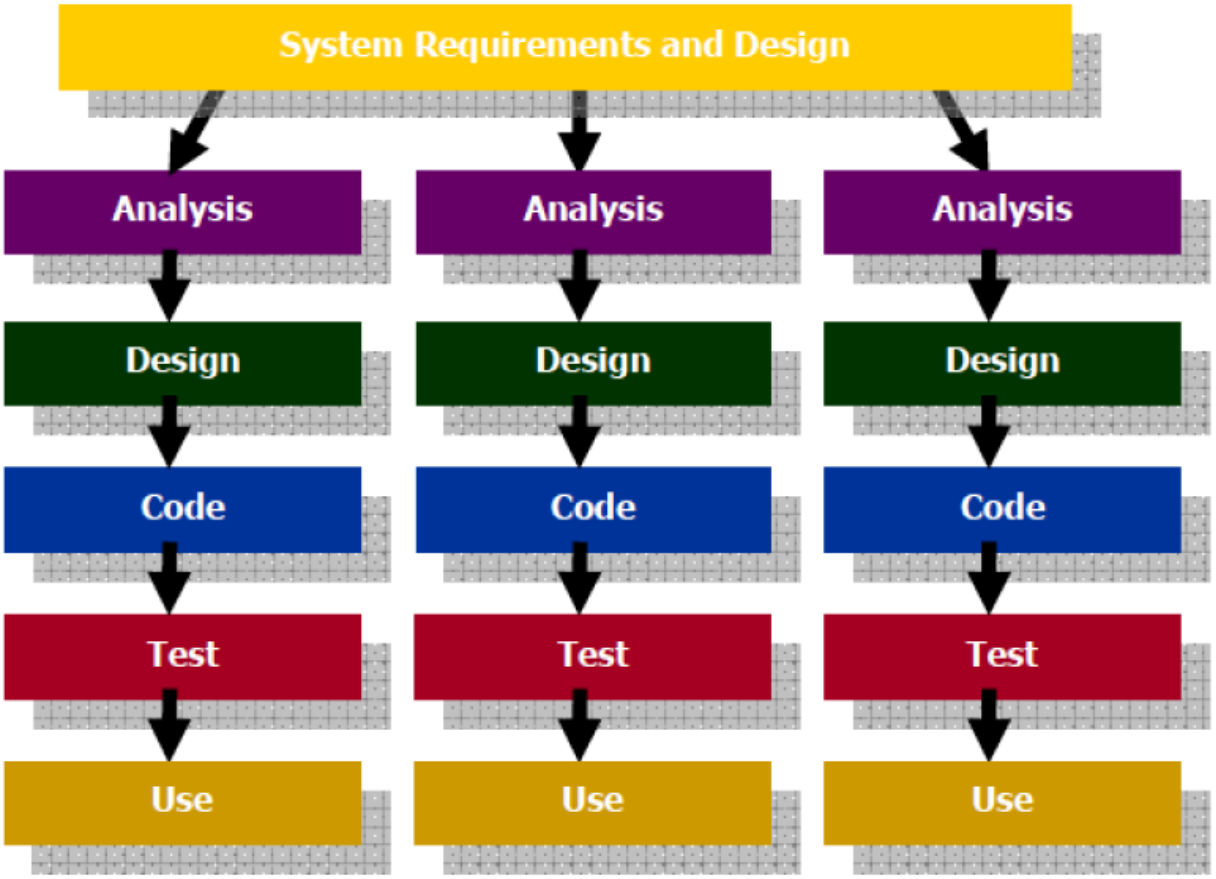

Figura 6 - Ciclo di vita iterativo-incrementale dello sviluppo del software

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)).

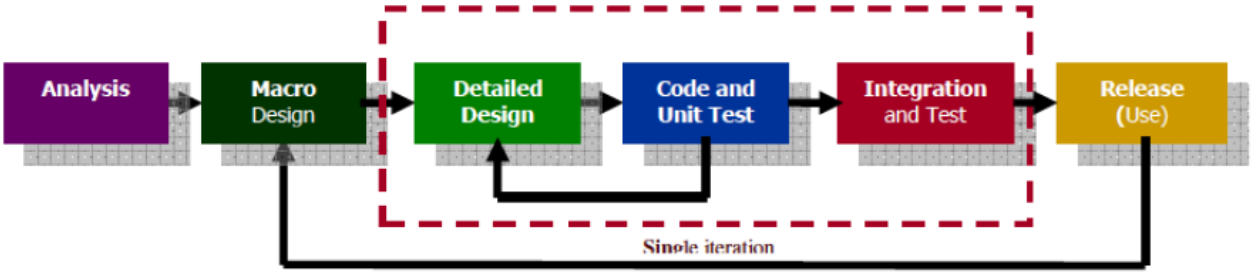

Figura 7 - Dettaglio del ciclo di vita iterativo-incrementale dello sviluppo del software

Torna al sommario

8.4.2 Ciclo di sviluppo e rilascio del software

Le fasi attraverso le quali si è prodotto e rilasciato il software CONSERVA sono riassunte e descritte nel seguente grafico

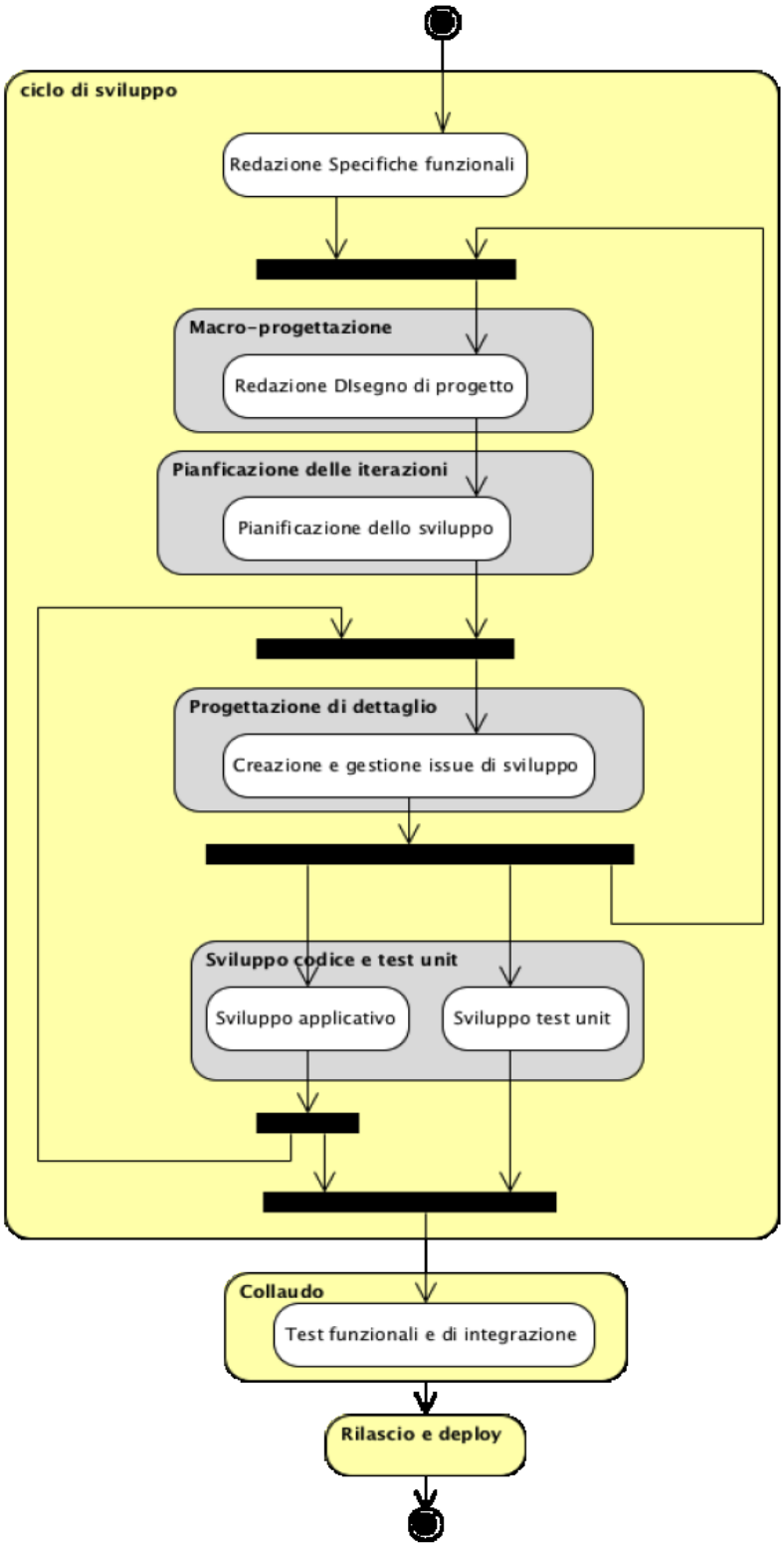

Figura 8 - Fasi di produzione e rilascio del software

Torna al sommario

8.4.3 Metodologia di sviluppo Agile in JIRA

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

Torna al sommario

8.4.3.1 Issue

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

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

- possono essere specificate altre informazioni generali.

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

- **Bug.** Segnalazione di errore sul sistema o su uno specifico componente. Utilizzato soprattutto in fase di codifica, test o esercizio.
- **Requirement.** Specifica di requisiti generica. Utilizzato soprattutto nella fase di macro-analisi o progettazione dettagliata.
- **New feature.** Descrizione di una nuova funzionalità da implementare. Utilizzato soprattutto nella fase di macro-analisi o progettazione dettagliata.
- **Improvement.** Descrizione di miglioria da applicare a una o più funzionalità. Utilizzato soprattutto nella fase di macro-analisi, progettazione dettagliata e dopo l'esecuzione di collaudi.
- **Task.** Compito generico non classificabile come uno dei precedenti.

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

- **Analysis Task:** sub-task che descrive un'attività di analisi.
- **Development task:** sub-task che descrive un'attività di sviluppo.
- **Test task:** sub-task che descrive un'attività di collaudo di una o più funzionalità.

Ogni issue o sub-task può essere collegato ad uno o più issue o sub-task.

Ogni issue ha una priorità (Priority) in ordine di urgenza di risoluzione:

1. **Red Code:** l'attività segnalata è urgente e bloccante;
2. **Very High:** l'attività segnalata può essere urgente e di alta gravità, oppure non urgente ma bloccante;
3. **High:** l'attività segnalata può essere di alta gravità ma non urgente oppure urgente ma di gravità media;
4. **Medium:** l'attività segnalata può essere di gravità media ma non urgente, oppure urgente ma di gravità bassa;
5. **Low:** l'attività segnalata non è urgente ed è di bassa gravità.

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

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

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

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

Di seguito il workflow che seguono gli stati della issue:

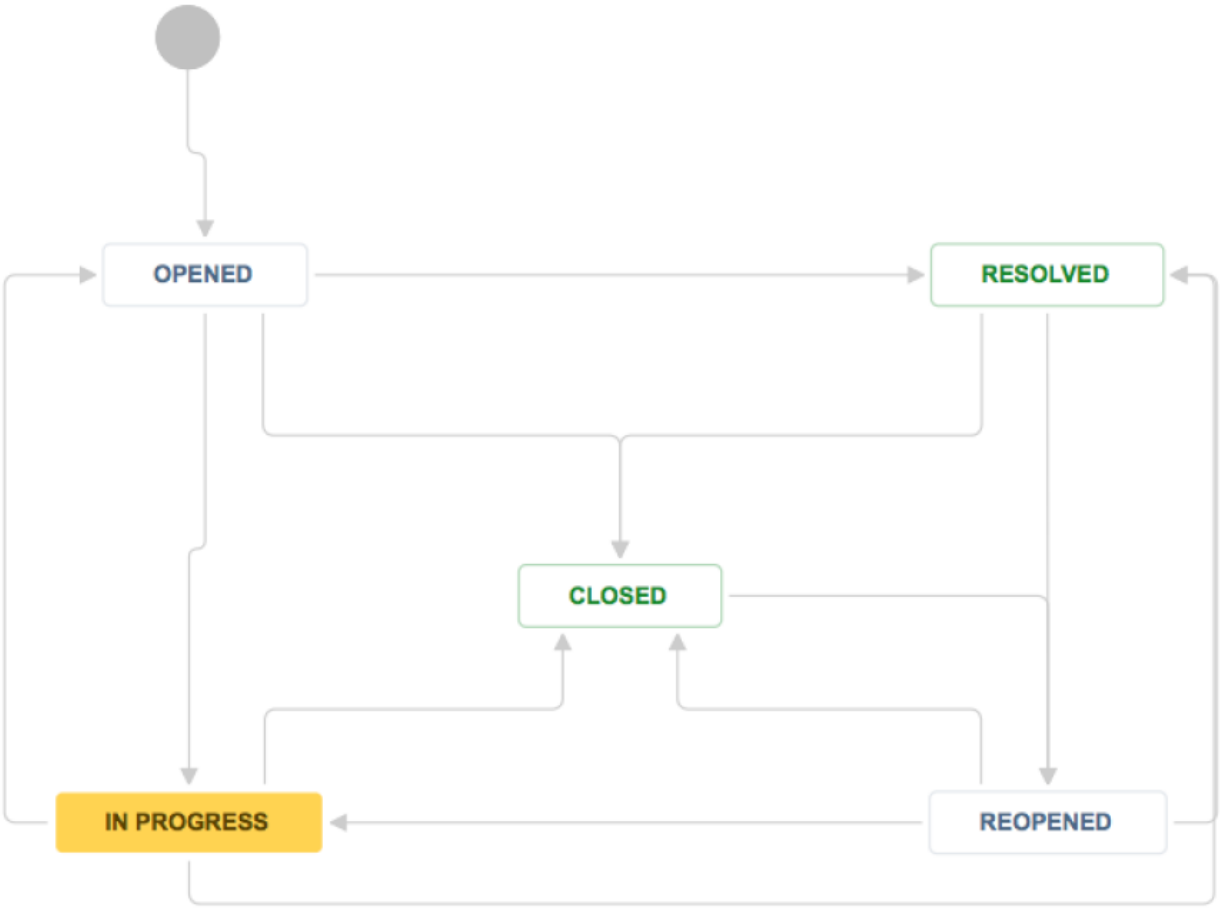

Figura 9 - Workflow degli stati delle singole issue

Torna al sommario

8.4.3.2 Progetti

Le issue in JIRA sono organizzate in progetti.

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

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

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

Sono stati predisposti due progetti speciali Jira:

- *Conserva Avviamenti:* il progetto raccoglie i task di avvio di nuovi Produttori oppure di definizione di nuovi Accordi di Versamento sottoscritti con i Produttori;
- *Conserva Progetti*: trasversale ai macro-componenti, contiene le issue comuni ai 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

8.4.3.3 Backlog

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

Torna al sommario

8.4.3.4 Sprint

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

Ad ogni sprint si aggiungono funzionalità e si verifica il risultato dell'attività svolta. Uno sprint può essere associato a issue contenute nel backlog, appartenenti ad uno o più progetti JIRA.
Il termine dello sprint può o meno coincidere con il rilascio della versione di uno o più progetti, ovvero l'emissione della release di uno o più macro-componenti.
La durata dello sprint, mediamente di una settimana, può variare a seconda del numero di giorni lavorativi oppure da particolari attività che richiedano un arco temporale più breve o più lungo. Lo sprint raramente coincide con le iterazioni del ciclo di sviluppo, sia a causa della durata che dell'eventuale sovrapposizione temporale delle stesse.

Torna al sommario

8.4.4 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

8.4.5 Gli ambienti di esercizio

8.4.5.1 Separazione degli ambienti

Per CONSERVA sono attivi tre ambienti distinti e separati:

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

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

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

Quelli di sviluppo e pre-produzione sono ambienti che non garantiscono né sicurezza né affidabilità. Per questo motivo devono essere utilizzati solo a fini di implementazione e test e possono ospitare dati non anonimi solo per il tempo strettamente necessario ai fini operativi.

Torna al sommario

8.4.5.2 Gestione e validazione degli ambienti

Gli ambienti sono gestiti dalla Divisione sistemi e tecnologie di CINECA.
I requisiti degli ambienti sono stabiliti dal Responsabile dello sviluppo e dal Responsabile del servizio di conservazione in accordo con la Divisione sistemi e tecnologie. Con cadenza almeno annuale il Responsabile dello sviluppo revisiona i requisiti per valutarne la correttezza in funzione dell'utilizzo passato e futuro di oggetti informativi.
Le richieste d'installazione, di aggiornamento e d'intervento straordinario sono gestite da apposite istruzioni operative aziendali.
In seguito ad ogni rilascio, modifica o aggiornamento degli ambienti di esercizio, è prevista un'attività di validazione nel rispetto di istruzioni operative a questo dedicate.

Torna al sommario

8.4.5.3 Sicurezza dei servizi e delle transazioni applicative

Indipendentemente dai requisiti stabiliti, vengono applicati meccanismi di protezione dei dati che transitano in rete, tali da impedirne accessi fraudolenti o non autorizzati. In particolare tutti gli host dei servizi sono accessibili esclusivamente attraverso protocollo HTTPS.
Gli algoritmi crittografici, la lunghezza delle chiavi asimmetriche e in generale gli aspetti di sicurezza inerenti il protocollo devono essere conformi a quanto indicato nella normativa vigente in materia ed agli standard internazionali.

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 ITILv3[4].

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;
- Pacchetti di archiviazione.

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

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 Titolare coinvolto ed agli eventuali suoi delegati, al Responsabile del servizio di Conservazione, al Responsabile della funzione archivistica di conservazione e al Responsabile dello sviluppo. Questi ultimi avvieranno la procedura di gestione

dell'incidente coinvolgendo il Responsabile della sicurezza ed il Responsabile della conservazione del Titolare se necessario.

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.

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

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

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

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

- raccolto centralmente il log per gli accessi ai dispositivi critici: rete, DB, sicurezza, sistemi;
- attuato un sistema per la non modificabilità degli stessi log;
- mantenuto aggiornato l'elenco degli amministratori di sistema e database, nominati con lettera di incarico registrata dall'ufficio personale, depositando l'elenco sull'area documentale dell'intranet aziendale;
- effettuata la verifica periodica sul corretto utilizzo tramite una checklist operativa documentata per definire la procedura di verifica (es.: verifica che non siano presenti login

non autorizzati come amministratori di sistema, che il log esista, che gli hash che ne garantiscono la non alterazione corrispondano);

- mantenuto l'elenco di tali verifiche periodiche con data di effettuazione, issue che traccia l'esecuzione, sistemi testati, esito della verifica;

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

Livello di severità	Periodo di archiviazione
Eventi informativi	1 mese
Eventi anomali	Il tempo necessario all'investigazione e risoluzione dell'anomalia
Dati traffico telematico	12 mesi
Amministratori sistema	6 mesi

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

Di seguito sono elencate le diverse componenti logiche di Conserva.

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 Titolare 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 distribuzione (JOB_DISTRIBUZIONE);
- aggiornamento delle statistiche (JOB_STATISTICHE_GIORNALIERE)
- registrazione delle statistiche di fine anno (JOB_STATISTICHE_ANNUALI)

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 ConservaNotifica

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

- notifica resoconto di versamento (JOB_NOTIFICA_RESOCONTO);
- notifica rapporto di versamento (JOB_NOTIFICA_RAPPORTO);

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

- data dell'evento;
- produttore;
- livello del log (INFO, WARN, ERROR);
- tipo di job che genera il log;
- nome della macchina Conserva che ha gestito l'attività;
- informazioni riguardanti endpoint di notifica.

Torna al sommario

9.3.4 Conserva

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

- registra il login e il logout;
- registra le ricerche effettuate;
- registra la visualizzazione di unità archivistiche/unità documentali;
- registra il download di file;
- registra le richieste di esibizione dei documenti.

Le informazioni registrate sono riguardo le attività sono:

- username dell'utente;
- nome del Titolare 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

9.4 Soluzioni adottate in caso di anomalie

Le anomalie generate durante il normale esercizio del servizio di conservazione possono essere distinte 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 Titolare, detta *Customer Portal*.
La segnalazione di un'anomalia può provenire:

- dal Titolare 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, Titolare (*Customer*) su cui si riflette l'incidente e l'ambiente (*Environment*) coinvolto (componente software e sua versione).
Se la segnalazione dell'anomalia è effettuata da personale CINECA, la procedura di registrazione appena specificata è eseguita contestualmente all'apertura della *issue* di segnalazione su Jira.
Una volta avvenuta la registrazione l'incidente deve essere trattato.

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

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

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

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

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

Torna al sommario