



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

Uffici di Staff e della Direzione Generale

Settore protocollo ed archivio

Piazza Santa Margherita 2 – 67100 L'AQUILA

E-mail: uosf@strutture.univaq.it

L'Aquila, 13/02/2023

Rep. n. 115/2023 Prot. n. 18486 del Allegati 1
Anno titolo I classe 7

IL DIRETTORE GENERALE

Visto il DPR 28 dicembre 2000 n. 445, Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;

Visto il D.Lgs 22 gennaio 2004, n. 42, Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137;

Visto il D.Lgs 7 marzo 2005, Codice dell'Amministrazione digitale;

Visto il Regolamento per la gestione, tenuta e tutela dei documenti amministrativi dal protocollo all'archivio storico per l'Amministrazione centrale, adottato con Decreto repertorio n. 2757 protocollo n. 43882 del 6 dicembre 2012;

Considerato quanto stabilito dall'Agenzia per l'Italia digitale – AGID nelle “Linee guida sulla formazione, gestione e conservazione dei documenti informatici”;

Ritenuto di adottare un nuovo Manuale di Conservazione, in sostituzione di quello adottato con proprio Dispositivo n. 715/2021 del 13 settembre 2021, in adesione a quanto stabilito da AGID;

DISPONE

di adottare il Manuale di conservazione allegato al presente provvedimento, che sostituisce il precedente adottato con proprio Dispositivo n. 715/2021 del 13 settembre 2021

Il Direttore Generale
(Dott. Pietro Di Benedetto)



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

MANUALE DI CONSERVAZIONE
QUESTO MANUALE È STATO REDATTO SUL MODELLO
DEL PROGETTO PROCEDAMUS

VERSIONE 2.0



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
<i>Redazione</i>	Settembre 2021	Fiorindo Carducci	Responsabile della Conservazione
<i>Verifica</i>			
<i>Approvazione</i>		Pietro Di Benedetto	Direttore Generale

Registro delle versioni

N. Ver. /Rev. /Bozza	Data	Modifiche apportate	Osservazioni
1.0 Versione	13/09/2021	Prima stesura	Stesura a partire dal modello Procedamus
2.0 Versione	30/08/2022	Revisione	Revisione della versione 1.0 per adeguamento alle Linee Guida Agid emanate a settembre 2020 e modificate a maggio 2021



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

SOMMARIO

1.	SCOPO E AMBITO DEL DOCUMENTO	4
2.	MODELLO ORGANIZZATIVO DELLA CONSERVAZIONE: RUOLI E RESPONSABILITÀ ..	5
2.1	Modello organizzativo adottato	5
2.2	Soggetto titolare.....	6
2.3	Organigramma	7
2.4	Struttura organizzativa.....	7
2.5	Utente abilitato.....	7
2.6	Responsabile della conservazione	8
2.7	Responsabile del Sistema di Conservazione.....	10
2.8	Organismi di tutela e di vigilanza	10
3.	ORGANIZZAZIONE DEL SERVIZIO DI CONSERVAZIONE	11
3.1	Responsabilità del sistema di conservazione	11
3.2	Gestione del sistema di conservazione	11
3.2.1	Organigramma	11
3.2.2	Struttura organizzativa.....	11
3.2.3	Pubblico ufficiale.....	12
4.	OGGETTI SOTTOPOSTI A CONSERVAZIONE.....	12
4.1	Documenti informatici e aggregazioni documentali informatiche (serie e relativi repertori)	12
4.2	Unità archivistiche e unità documentarie.....	14
4.3	Formati.....	15
4.4	Metadati	15
4.5	Pacchetto informativo	16
4.5.1	Pacchetto di versamento (SIP).....	16
4.5.2	Pacchetto di archiviazione (AIP)	16
4.5.3	Pacchetto di distribuzione (DIP).....	16
5.	PROCESSO DI CONSERVAZIONE	17
5.1	Fasi del versamento e logiche di conservazione	17
5.2	Acquisizione e presa in carico dei pacchetti di versamento (sip)	17
5.2.1	Pre-acquisizione.....	17
5.2.2	Acquisizione	17
5.2.3	Verifica	17
5.2.4	Rifiuto o accettazione	17



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

5.2.5 Presa in carico e generazione del Rapporto di versamento.....	18
5.2.6 Generazione del Pacchetto di archiviazione (AIP)	18
5.3 Gestione del pacchetto di archiviazione (aip).....	18
5.3.1 Aggiornamento dei pacchetti di archiviazione (AIP)	18
5.3.2 Selezione e scarto dei pacchetti di archiviazione (AIP).....	18
5.4 Gestione del pacchetto di distribuzione (dip)	18
5.4.1 Modalità di esibizione/estensione	18
5.4.2 Produzione di copie, di riproduzioni e di duplicati.....	19
5.4.3 Interoperabilità.....	19
5.5 Monitoraggio e risoluzione delle anomalie.....	20
5.5.1 Gestione delle anomalie.....	20
6. DESCRIZIONE DEL SISTEMA DI CONSERVAZIONE.....	20
6.1 Componenti logiche.....	20
6.2 Componenti fisiche.....	21
6.2.1 Schema generale	21
6.2.2 Caratteristiche tecniche del Sito primario.....	21
6.3 Componenti tecnologiche	21
6.4 Procedure di gestione del sistema.....	21
6.5 Evoluzione del sistema	21
6.6 Monitoraggio e controlli	21
6.6.1 Procedure di monitoraggio	21
6.6.2 Funzionalità per la verifica e il mantenimento dell'integrità degli archivi.....	21
6.6.3 Casistica e soluzioni adottate in caso di anomalie	22
7. STRATEGIE ADOTTATE A GARANZIA DELLA CONSERVAZIONE	22
7.1 Misure a garanzia della intellegibilità, della leggibilità e della reperibilità nel tempo	22
7.2 Misure a garanzia dell'interoperabilità e della trasferibilità ad altri conservatori.....	22
8. CONSERVAZIONE DEI CERTIFICATI STUDENTI FIRMATI DIGITALMENTE	22
9. TRATTAMENTO DEI DATI PERSONALI	23
10. ELENCO ALLEGATI.....	23



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

1. SCOPO E AMBITO DEL DOCUMENTO

Il presente documento è il manuale di conservazione (d'ora in poi Manuale) dei documenti digitali prodotti dall'Università degli Studi dell'Aquila.

Il Manuale, come previsto nelle “Linee guida sulla formazione, gestione e conservazione dei documenti informatici” AGID, (d'ora in poi Linee Guida)¹, è uno strumento operativo che descrive e disciplina il modello organizzativo della conservazione adottato. Esso illustra nel dettaglio l'organizzazione del processo di conservazione, definendo i soggetti coinvolti e i ruoli svolti dagli stessi nel modello organizzativo di funzionamento dell'attività di conservazione dell'Università degli Studi dell'Aquila (d'ora in poi Titolare).

L'Università degli Studi dell'Aquila, come soggetto titolare, sottopone a conservazione digitale fascicoli, serie e aggregazioni documentali, affidando il processo di conservazione, *in outsourcing*, al Consorzio Interuniversitario per la gestione del centro di calcolo elettronico dell'Italia nordorientale - *Cineca* (d'ora in poi Conservatore), salvo quanto stabilito nel capitolo 8.

Il presente Manuale sostituisce il precedente, adottato con dispositivo del Direttore Generale registrato nel repertorio Dispositivi Direttore Generale del Titolare con numero n.715/2021 del 13 settembre 2021, e tiene conto di quanto previsto nelle Linee Guida AgID².

La redazione del Manuale di conservazione contempera l'assolvimento dell'obbligo normativo con le esigenze concrete del Titolare.

Il Manuale costituisce una guida per gli attori coinvolti nel processo di gestione e di conservazione, per il cittadino e per le imprese. Ai primi, per attuare le corrette operazioni di gestione e conservazione documentale, agli ultimi due per comprendere le caratteristiche del Sistema di conservazione documentale e dei processi erogati.

Il presente Manuale integra il manuale di conservazione del *Cineca*, per le parti specifiche di competenza del Titolare e per quanto riguarda i rapporti tra questi e il Conservatore.

Il Manuale descrive, inoltre, il processo, le architetture e le infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del Sistema di conservazione.

Per le tipologie degli oggetti sottoposti a conservazione e i rapporti con il Conservatore, il presente Manuale è integrato dagli Accordi di versamento stipulati con il Conservatore, che definiscono le specifiche operative e

¹ Nel Paragrafo 4.6. rubricato “Manuale di conservazione” delle “Linee guida per la formazione, gestione e conservazione dei documenti informatici”, adottate con determinazione n. 407/2020 e successivamente modificate con determinazione n. 371/2021, l'Agenzia per l'Italia digitale - AGID ha stabilito che il manuale di conservazione è un documento informatico che deve illustrare 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 utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.

² Le Linee Guida hanno abrogato le precedenti regole tecniche, ovvero il DPCM 3 dicembre 2013 “Regole tecniche in materia di conservazione”. L'obiettivo generale delle medesime è aggregare in un corpo unico le regole tecniche di gestione del documento informatico che in precedenza erano disciplinate separatamente, in specifici DPCM. Viene così delineata una disciplina esaustiva e completa, contenente regole e procedure, nell'ambito di un corpo unico, che norma l'intera vita del documento informatico dalla sua formazione, alla trasmissione, all'archiviazione, alla conservazione ed alla disponibilità nel tempo.



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

le modalità di descrizione e di versamento nel Sistema di conservazione digitale dei documenti informatici e delle aggregazioni documentali informatiche oggetto di conservazione.

L'Accordo di versamento è formato da specifiche parti relative alle diverse tipologie documentarie oggetto di conservazione ed è compilato tenendo conto delle indicazioni contenute nella documentazione redatta da *Cineca*.

2. MODELLO ORGANIZZATIVO DELLA CONSERVAZIONE: RUOLI E RESPONSABILITÀ

2.1 Modello organizzativo adottato

Il Titolare ha stabilito di realizzare i processi di conservazione secondo il modello “*in outsourcing*”, il quale prevede che il servizio di conservazione venga affidato parzialmente o totalmente a soggetti pubblici o privati.

L'Università degli Studi dell'Aquila è titolare delle unità documentarie informatiche poste in conservazione e, attraverso il proprio Responsabile della conservazione, definisce e attua le politiche complessive del Sistema di conservazione governandone la gestione con piena responsabilità e autonomia, in relazione al modello organizzativo adottato, affida al Conservatore la gestione del servizio di conservazione secondo quanto previsto dalla normativa in materia.

Nella fattispecie, l'Università degli Studi dell'Aquila, quale Titolare, ha scelto di avvalersi del servizio di conservazione di *Cineca*, salvo quanto stabilito nel capitolo 8. L'atto di affidamento del servizio di conservazione è stato formalizzato con Dispositivo del Direttore Generale registrato nel repertorio Dispositivi Direttore Generale con numero 11 del 22 dicembre 2016.

Di seguito è riportato graficamente il diagramma del modello organizzativo adottato dall'Università degli Studi dell'Aquila. Il modello riporta le principali caratteristiche, in conformità allo Standard funzionale OAI (Open Archival Information System), definendo i ruoli dei singoli attori che intervengono nel processo di archiviazione per i rispettivi ambiti di competenza. Nel diagramma è previsto che il soggetto Titolare si faccia carico della distribuzione dell'informazione al fruitore.



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

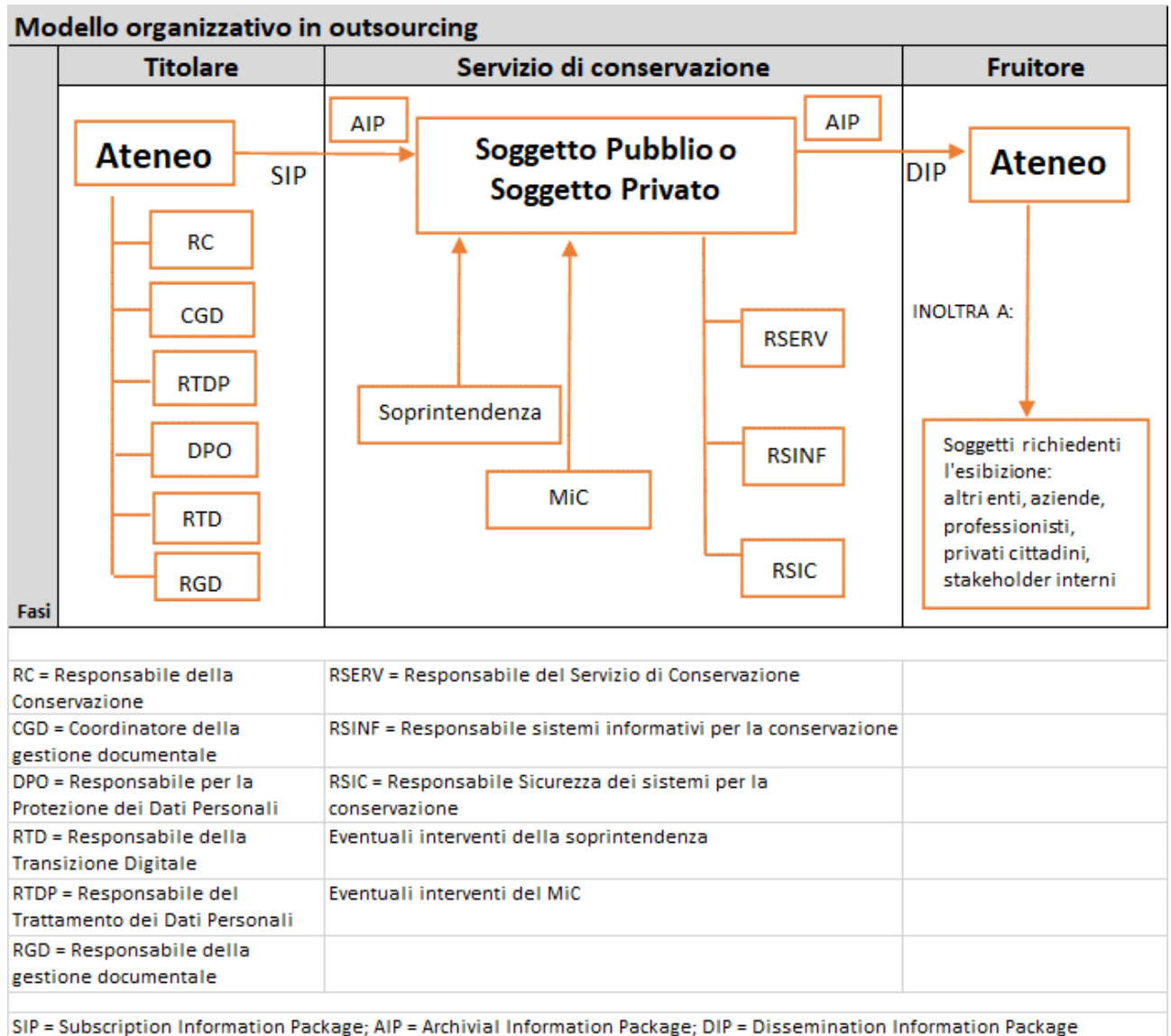


Figura 1

2.2 Soggetto titolare

L'Università degli Studi dell'Aquila è il soggetto titolare che versa le unità documentarie informatiche da conservare con gli opportuni metadati, in continuità con il processo di gestione documentale, iniziato nella fase corrente all'interno dell'Ateneo.

I rapporti tra Titolare e Conservatore sono formalizzati e regolati per mezzo di alcuni documenti fondamentali:

- Atto di affidamento per l'utilizzo del sistema Conserva;
- Atto di nomina del Responsabile esterno del trattamento dei dati personali con il sistema Conserva;
- Accordi di versamento



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

Alla data di adozione del presente manuale sono stati stipulati gli accordi di versamento per le tipologie documentali riportati nell'Allegato 2 – Accordi di versamento.

2.3 Organigramma

L'Università degli Studi dell'Aquila è organizzata in *AOO* (Area Organizzativa Omogenea) e *UOR* (Unità Organizzativa Responsabile).

L'area organizzativa omogenea (*AOO*) è l'insieme di funzioni e di strutture individuate dall'amministrazione cui sono assegnate funzioni omogenee. Essa, pertanto, presenta esigenze di gestione documentale in modo unitario e coordinato, ai sensi della normativa vigente.

L'unità organizzativa responsabile (*UOR*) è, all'interno della *AOO*, un complesso organizzato di risorse umane e strumentali cui è stata affidata una competenza omogenea nell'ambito della quale i dipendenti assumono la responsabilità nella trattazione di affari, attività e procedimenti amministrativi.

Il versamento in conservazione dei documenti informatici gestiti nella fase corrente dalle articolazioni amministrative (*AOO* e *UOR*) del Titolare è effettuato unicamente dal Responsabile della conservazione, laddove non avvenga con processi automatici stabiliti nei singoli accordi di versamento.

L'articolazione organizzativa dell'Università degli Studi dell'Aquila è riportata sul [Portale di Ateneo](#).

2.4 Struttura organizzativa

Il Sistema di conservazione delle unità documentarie informatiche e delle unità archivistiche informatiche di Ateneo prevede la collaborazione tra unità organizzative e soggetti interni ed esterni cui il Titolare ha affidato il coordinamento del processo di conservazione in base all'atto di affidamento e relativi accordi di versamento nel quale sono inoltre definite le tipologie documentali, i tempi di versamento e conservazione, i formati e i metadati descrittivi utili a garantire una corretta interazione tra Titolare e Conservatore.

In virtù degli affidamenti del servizio di conservazione il Conservatore si impegna alla conservazione dei documenti trasferiti garantendo il rispetto dei requisiti previsti dalle norme in vigore nel tempo per i Sistemi di conservazione.

In particolare, l'esecuzione del processo di conservazione avviene sotto la vigilanza del Responsabile della conservazione, il quale interagisce con il Conservatore così come dettagliato al § 2.6.

2.5 Utente abilitato

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

In termini di sistema OAIS la comunità degli utenti può essere definita come Comunità di riferimento.



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

L'utente finale del servizio di conservazione è lo stesso Ateneo che interagisce tramite i propri funzionari autorizzati con il servizio di conservazione per accedere ai documenti per finalità gestionali, amministrative, storiche, scientifiche o per soddisfare le richieste di eventuali soggetti esterni legittimati all'esibizione/accesso alla documentazione (es: amministrazioni/enti pubblici, soggetti privati, aziende, professionisti, cittadini, stakeholder interni).

Il Sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, ai documenti informatici conservati e consente la produzione di un Pacchetto di distribuzione direttamente acquisibile dai soggetti autorizzati.

Nel ruolo dell'utente sono definiti gli specifici soggetti abilitati dell'Ateneo, in particolare gli operatori indicati dal Titolare e riportati negli accordi di versamento, che possono accedere esclusivamente ai documenti versati dal Titolare stesso o solo ad alcuni di essi secondo le regole di visibilità e di accesso concordate tra Titolare e Conservatore.

Si identificano gli utenti del Sistema di conservazione nelle seguenti persone:

- Responsabile della conservazione;
- Delegato del responsabile della conservazione.

L'abilitazione e l'autenticazione di tali operatori avviene in base alle procedure di gestione utenze indicate nel Piano della sicurezza del sistema di conservazione.

2.6 Responsabile della conservazione

Il Responsabile della conservazione, previsto dall'art. 44, comma 1-quater del CAD³, è la figura cardine che governa il processo della conservazione digitale: è la persona fisica inserita stabilmente nell'organico del soggetto titolare dei documenti, che definisce e attua le politiche complessive del Sistema di conservazione e ne governa la gestione con piena responsabilità e autonomia, in relazione al modello organizzativo adottato.

Nelle pubbliche amministrazioni il ruolo di Responsabile della conservazione può essere svolto dal Responsabile della gestione documentale, ovvero dal Coordinatore della gestione documentale, ove nominato.

Il Responsabile della conservazione, coadiuvato dal Responsabile del sistema di conservazione Conserva di *Cineca*, ha i seguenti compiti:

- 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;

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



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

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

Il Responsabile della conservazione può nominare i propri delegati all'interno della struttura organizzativa.

Il Responsabile della conservazione opera d'intesa con il Responsabile del servizio di conservazione, con il Responsabile del trattamento dei dati personali e con il Responsabile della gestione documentale ovvero con il Coordinatore della gestione documentale, ove nominato, le cui attività sono definite in riferimento al Sistema di gestione documentale.

In particolare, il Coordinatore della gestione documentale ha il compito di:

- produrre il pacchetto di versamento secondo le regole pattuite tra Responsabile della conservazione e Conservatore;
- assicurare la trasmissione del contenuto del pacchetto di versamento nel rispetto di quanto definito, tra Responsabile della conservazione e Responsabile del servizio di conservazione, nel manuale di conservazione;
- d'intesa con il Responsabile della conservazione e con il Responsabile del trattamento dati personali effettuare l'analisi dei procedimenti amministrativi e una ricognizione delle tipologie documentali.



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

2.7 Responsabile del Sistema di Conservazione

Al Responsabile del sistema di conservazione Conserva sono affidati i compiti di cui al paragrafo 2.6 ad esclusione di quelli previsti nelle lettere l) e m) come stabilito nel manuale di conservazione del Cineca allegato al presente documento (Allegato n.4).

2.8 Organismi di tutela e di vigilanza

Gli archivi e i singoli documenti prodotti dagli enti universitari sono beni culturali e sono sottoposti, pertanto, alle disposizioni di tutela previste dal Codice dei beni culturali. Garantire la tutela di archivi e singoli documenti si concreta negli obblighi conservativi, previsti nel comma 4 dell'art. 30 del DLgs. n. 42 del 2004, il quale dispone "l'obbligo di conservare i propri archivi nella loro organicità e di ordinarli. I soggetti medesimi hanno altresì l'obbligo di inventariare i propri archivi storici costituiti dai documenti relativi agli affari esauriti da oltre 40 anni...".

Il rispetto delle disposizioni in ordine alla corretta conservazione è in capo al Ministero della cultura, attraverso la Direzione generale archivi e, in particolare, la Soprintendenza archivistica e bibliografica dell'Abruzzo e del Molise. Tale ente, infatti, è investito del potere di vigilanza e ispezione ai sensi degli artt. 18 e 19 del predetto DLgs. Per quanto riguarda il Sistema di conservazione dell'Università degli Studi dell'Aquila, la Soprintendenza archivistica e bibliografica dell'Abruzzo e del Molise verifica, in particolare, che il processo di conservazione avvenga in modo conforme alla normativa e ai principi di corretta e ininterrotta custodia.

L'importanza della corretta conservazione degli archivi si evince anche dall'esplicito divieto del legislatore di smembrarli (cioè distruggere l'ordine di aggregazione dei documenti, facendo perdere all'archivio la propria organizzazione e il proprio carattere di complesso unitario) e dall'elencazione degli interventi soggetti ad autorizzazione poiché potenzialmente lesivi per l'archivio e i documenti di cui è costituito.

Ai fini della conservazione digitale, è necessario soffermarsi sulla richiesta di autorizzazione che deve essere chiesta per "lo spostamento, anche temporaneo, dei beni culturali mobili" e per il "trasferimento ad altre persone giuridiche di complessi organici di documentazione di archivi pubblici". Il secondo caso, in particolare, contempla proprio il trasferimento di archivi informatici ad altri soggetti giuridici, nell'ottica della conservazione permanente sia del documento sia del contesto archivistico. L'Ente interessato ad attivare il servizio di conservazione digitale del proprio archivio di deposito o storico deve, quindi, preventivamente chiedere l'autorizzazione alla Soprintendenza archivistica e bibliografica competente per territorio.

Il legislatore ha previsto un secondo ente, l'Agenzia per l'Italia digitale – AGID, che, in materia di conservazione digitale, lavora a fianco delle Soprintendenze avendo però un ruolo diverso.



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

3. ORGANIZZAZIONE DEL SERVIZIO DI CONSERVAZIONE

3.1 Responsabilità del sistema di conservazione

Il Sistema di conservazione garantisce l'autenticità, l'integrità, l'affidabilità, la leggibilità e la reperibilità degli oggetti conservati dal momento della loro presa in carico dal Titolare, fino all'eventuale scarto, indipendentemente dall'evolversi del contesto tecnologico e organizzativo.

La responsabilità del Sistema di conservazione come soggetto che svolge attività di conservazione è in capo al Consorzio interuniversitario *Cineca*.

Cineca è un consorzio interuniversitario senza scopo di lucro formato da 70 Università italiane, 6 enti di ricerca, il Ministero dell'Istruzione, dell'Università e della Ricerca - MIUR. Costituito nel 1969 come Consorzio Interuniversitario per il calcolo automatico dell'Italia Nord Orientale, oggi *Cineca* è il maggiore centro di calcolo in Italia. La sua missione istituzionale comprende la realizzazione di sistemi gestionali e servizi a sostegno delle università e del Ministero dell'Università e della Ricerca - MUR. In questo ruolo, il Consorzio si è impegnato nella costante ricerca di soluzioni in grado di accompagnare gli atenei nel loro cammino di ammodernamento dei metodi di governo di realtà così complesse e articolate. *Cineca* ha assunto il ruolo di "braccio tecnico operativo" che, attraverso la realizzazione di sofisticati sistemi telematici, consente l'interazione di tutte le componenti del mondo accademico con l'Amministrazione centrale, garantendo al Ministero il costante monitoraggio dei processi ed il coordinamento di tutte le attività.

Il ruolo del Responsabile del sistema di conservazione è ribadito anche nel testo degli accordi di versamento sottoscritti fra Ateneo e *Cineca*.

In quanto soggetto responsabile, in coerenza con il sistema OAIS, *Cineca* si occupa delle politiche complessive del Sistema di conservazione e ne determina l'ambito di sviluppo e le competenze. A tal fine provvede alla pianificazione strategica, alla ricerca dei finanziamenti, alla revisione periodica dei risultati conseguiti e ad ogni altra attività gestionale mirata a coordinare lo sviluppo del Sistema.

3.2 Gestione del sistema di conservazione

Si rimanda al manuale di conservazione del Conservatore allegato al presente documento (Allegato n.4).

3.2.1 Organigramma

Si rimanda al manuale di conservazione del Conservatore allegato al presente documento (Allegato n.4).

3.2.2 Struttura organizzativa

Si rimanda al manuale di conservazione del Conservatore allegato al presente documento (Allegato n.4).



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

3.2.3 Pubblico ufficiale

Nei casi previsti dalla normativa, il ruolo di pubblico ufficiale viene individuato dal Responsabile della conservazione nei dipendenti formalmente designati, per l'attestazione di conformità all'originale di copie di documenti informatici conservati.

4. OGGETTI SOTTOPOSTI A CONSERVAZIONE

4.1 Documenti informatici e aggregazioni documentali informatiche (serie e relativi repertori)

Il Sistema di conservazione acquisisce, gestisce, organizza e conserva documenti informatici, in particolare documenti amministrativi informatici, e le loro aggregazioni documentali informatiche sotto forma di fascicoli e serie. Ai fini della corretta conservazione nel medio e lungo periodo è indispensabile conoscere la natura di oggetti informativi complessi sia dei documenti che delle loro aggregazioni.

Il documento amministrativo informatico è prodotto e memorizzato su di un supporto elettronico durante lo svolgimento di un'attività di carattere amministrativo e, grazie al Sistema di gestione in cui è stato inserito al momento dell'acquisizione, possiede le opportune caratteristiche di immutabilità, integrità e staticità, come previsto dalla normativa vigente.

Durante la vita nel Sistema di gestione corrente Titulus, il documento è sottoposto a una serie di azioni (es. protocollazione o registrazione a sistema, classificazione, attribuzione al Responsabile del procedimento, attribuzione al fascicolo etc.) che ne determinano la posizione logica all'interno dell'archivio così come l'identità: la particolarità e unicità del documento è caratterizzata proprio dalla specifica funzione che esso riveste nello svolgimento dell'attività del Titol. Le caratteristiche proprie del documento vengono tradotte in ambito elettronico in metadati: informazioni connesse al documento che consentono all'interno del Sistema l'identificazione, la descrizione, la gestione e la conservazione. La normativa prescrive un pacchetto minimo di metadati da associare al documento informatico immutabile.

In tal senso risulta fondamentale l'appartenenza del documento al fascicolo. La fascicolazione, oltre a essere un obbligo previsto dalla normativa, è il requisito indispensabile per la corretta gestione del documento all'interno del contesto relazionale che ne determina il significato e l'identità. Fascicolare significa esplicitare la posizione logica e fisica del singolo documento all'interno dell'archivio; quindi, stabilire esattamente la funzione che il documento svolge. Ad esempio, tutti i documenti che fanno parte del medesimo procedimento appartengono allo stesso fascicolo e vanno tenuti insieme nell'ordine cronologico, cosiddetto ordine di sedimentazione, in base al quale si sono formati, e in tal modo si ottiene un fascicolo che contiene la storia del procedimento. Le azioni a cui il documento è soggetto nel corso della propria esistenza sono strettamente determinate dall'appartenenza al fascicolo.



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

Il passaggio del documento dal Sistema di gestione Titulus al Sistema di conservazione Conserva deve consentire il mantenimento delle caratteristiche del documento di immodificabilità, integrità e staticità, così come deve essere mantenuto il legame significativo del documento con il fascicolo al fine di preservare e tramandare per il periodo necessario il valore giuridico probatorio, amministrativo e storico.

Il Codice dell'amministrazione digitale definisce all'art. 1, lettera p) cosa debba intendersi per documento informatico⁴ e al successivo art. 23-ter specifica la particolare categoria di documento informatico rappresentata dal documento amministrativo informatico ribadendone la natura di informazione primaria e originale. Lo stesso art. 23-ter riassume le azioni che è possibile effettuare sul documento amministrativo informatico⁵.

Le aggregazioni di documenti informatici o di fascicoli informatici sono l'insieme definito e qualificato di documenti riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente.

Il fascicolo rappresenta, quindi, la prima forma di aggregazione determinata e può essere organizzato raccogliendo documenti diversi per formato, natura, contenuto giuridico, ma prodotti nel corso di una specifica attività; oppure raccogliendo documenti della stessa tipologia o qualità o forma, raggruppati quindi in base a criteri estrinseci, e riguardanti contenuti disomogenei.

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

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

I fascicoli, così come particolari tipologie di documenti, creano ulteriori aggregazioni documentali definite serie. Si tratta di articolazioni interne all'archivio createsi sulla base del processo di sedimentazione reso esplicito dall'applicazione del titolario di classificazione. Le serie sono funzionali all'individuazione di caratteristiche comuni per documenti o fascicoli, e consentono di conseguenza un'efficiente gestione dei dati oltre a rappresentare un elemento indispensabile della struttura dell'archivio. Dal punto di vista dei fascicoli, le serie si creano rispettando l'articolazione del titolario di classificazione sulla base del quale i singoli fascicoli vengono classificati e inseriti nel repertorio dei fascicoli.

La serie può corrispondere anche al raggruppamento di specifiche tipologie documentali, le quali, quindi, condividono un insieme di caratteristiche omogenee, tradotte in ambito informatico in un set di metadati. Da un punto di vista normativo, il fascicolo informatico viene introdotto dal Codice dell'amministrazione digitale

⁴ Per documento informatico si intende documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti

⁵ Gli atti formati dalle pubbliche amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi o identici tipi di supporto, duplicazioni e copie per gli usi consentiti dalla legge.



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

all'art. 41 in relazione al procedimento amministrativo: “La pubblica amministrazione titolare del procedimento raccoglie in un fascicolo informatico gli atti, i documenti e i dati del procedimento medesimo da chiunque formati”; nel comma 2-ter del predetto articolo, vengono elencate le indicazioni di cui il fascicolo deve essere provvisto per la corretta identificazione e gestione: “Il fascicolo informatico reca l’indicazione: a) dell’amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo; b) delle altre amministrazioni partecipanti; c) del Responsabile del procedimento; d) dell’oggetto del procedimento; e) dell’elenco dei documenti contenuti, salvo quanto disposto dal comma 2-quater; e-bis) dell’identificativo del fascicolo medesimo”. Il successivo art. 44, esplicitando i Requisiti per la gestione e conservazione dei documenti informatici, dichiara che annualmente devono essere trasferiti al Sistema di conservazione “i fascicoli e le serie documentarie anche relative a procedimenti conclusi”. La gestione del fascicolo e delle aggregazioni documentali viene affrontata anche dalle *Linee guida AGID sulla formazione, gestione e conservazione dei documenti informatici*.

4.2 Unità archivistiche e unità documentarie

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

L’unità archivistica in ambito analogico è l’unità base costituita dall’insieme di documenti che condividono determinate caratteristiche identificative, risultato di un processo di produzione, che fanno dell’unità un’aggregazione qualificata e non casuale. In tal senso, l’unità archivistica è il livello di definizione e descrizione dell’aggregazione documentale oltre il quale non è possibile procedere, ossia i documenti che la costituiscono sono elementi che non possiedono un’identità propria se tolti, ad esempio, dal fascicolo, cioè se decontestualizzati.

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

In ambito informatico tale rapporto, benché mantenga il rispetto dei principi archivistici, risulta più complesso, poiché l’unità documentaria diventa a sua volta un contenitore la cui natura è pre-strutturata sulla base della tipologia di informazioni che deve contenere: si articola in documenti principali, allegati, componenti. Le unità informative principali costituiscono il nucleo dell’unità documentaria e determinano la struttura e i metadati di riferimento.

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



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

4.3 Formati

Il formato è l'insieme di informazioni che determinano la modalità con cui un oggetto digitale viene creato, memorizzato e riprodotto. Un oggetto digitale è una sequenza di bit fissati con una certa organizzazione fisica su di una memoria. Tale contenuto digitale viene memorizzato e definito file. La possibilità di fruire e utilizzare un file è determinata dalla capacità di rappresentare la sequenza di bit per mezzo di un apposito software che riproduca, sulla base dei codici e delle regole che costituiscono il file stesso, il contenuto e la forma che gli era stata conferita dall'autore.

La corretta conservazione dei documenti nel tempo è determinata anche dalla scelta dei formati idonei a tale scopo, infatti, un problema di cui è necessario tener presente, è costituito dall'obsolescenza dei formati. Attualmente la soluzione più sicura è adottare, fin dal momento della formazione dei contenuti digitali, formati che abbiano le caratteristiche per fornire le maggiori garanzie in termini di conservazione a lungo termine.

Si rimanda al manuale di conservazione del Conservatore e agli accordi di versamento allegati al presente documento in cui sono definite le specifiche operative e le modalità di descrizione e di versamento nel Sistema di conservazione digitale delle diverse tipologie documentali oggetto di conservazione inclusi struttura e formati utilizzati.

4.4 Metadati

Insieme alla scelta dei formati, la definizione dei metadati è un'operazione fondamentale per l'attività conservativa delle memorie digitali a medio e lungo termine. I metadati vengono esplicitamente citati come oggetti da sottoporre a conservazione associati ai documenti informatici, ai documenti amministrativi informatici e ai fascicoli informatici o aggregazioni documentali.

I metadati sono informazioni associate ai dati primari creati e trattati: sono a loro volta dati che descrivono, spiegano, localizzano una risorsa informativa rendendo più semplice il suo recupero, utilizzo e gestione. Ad esempio, il riferimento all'autore o alla tipologia di dato, il riferimento temporale alla creazione o registrazione del dato, la classificazione, etc. Come si può intuire i metadati associati a una risorsa sono potenzialmente infiniti; quindi, si è deciso di distinguerli in tre principali categorie:

- Metadati descrittivi, descrivono una risorsa con lo scopo di scoprirla ed identificarla;
- Metadati strutturali, indicano la struttura di oggetti composti, ad esempio i capitoli che assemblano le pagine;
- Metadati amministrativi, descrivono le informazioni volte a favorire la gestione del file (tipo di file, nome del produttore, riferimento temporale etc.).

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



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

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

Si rimanda al manuale di conservazione del Conservatore e agli accordi di versamento in cui sono definite le specifiche operative e le modalità di descrizione e di versamento nel Sistema di conservazione digitale delle diverse tipologie documentali oggetto di conservazione inclusi individuazione e gestione dei metadati relativi ai documenti versati nel Sistema di conservazione.

4.5 Pacchetto informativo

Gli oggetti sottoposti a conservazione, siano essi aggregazioni documentali informatiche, documenti informatici, o metadati, sono trasmessi dal Titolare, memorizzati e conservati nel Sistema e distribuiti agli Utenti sotto forma di pacchetti informativi. Il pacchetto informativo, a seconda sia utilizzato per versare, conservare o distribuire gli oggetti sottoposti a conservazione, assume la forma, rispettivamente, di Pacchetto di versamento (SIP), Pacchetto di archiviazione (AIP) e Pacchetto di distribuzione (DIP).

4.5.1 Pacchetto di versamento (SIP)

I SIP sono concordati per struttura e contenuto con il Titolare e contengono l'oggetto o gli oggetti da conservare. In base alle specifiche esigenze possono contenere una o più unità archivistiche, una o più unità documentarie, eventuali aggiornamenti all'unità documentaria già versata o solo informazioni da associare a un'unità documentaria già conservata. Ogni SIP può generare uno o più Pacchetti di archiviazione così come più SIP possono costituire un unico Pacchetto di archiviazione.

4.5.2 Pacchetto di archiviazione (AIP)

Il Pacchetto di archiviazione viene generato dal Sistema a conclusione del processo di acquisizione e presa in carico dei SIP. È composto dagli oggetti-dati (file) e dall'indice dell'AIP, un file XML che contiene tutti gli elementi del pacchetto informativo, derivati sia dalle informazioni contenute nel SIP (o nei SIP) trasmessi dal Titolare, sia da quelle generate dal Sistema nel corso del processo di conservazione.

4.5.3 Pacchetto di distribuzione (DIP)

Il Pacchetto di distribuzione viene generato dal Sistema a partire dai Pacchetti di archiviazione conservati ed è finalizzato a mettere a disposizione degli utenti, in una forma idonea alle specifiche esigenze di utilizzo, gli oggetti sottoposti a conservazione.



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

5. PROCESSO DI CONSERVAZIONE

5.1 Fasi del versamento e logiche di conservazione

Il processo di conservazione è attivato sulla base degli accordi di versamento stipulati tra l'Ateneo e il Conservatore, in qualità di soggetto che svolge attività di conservazione.

Le procedure per l'attivazione del processo di conservazione sono indicate nell'atto di affidamento dei servizi per l'utilizzo delle soluzioni *Cineca* e dei servizi di assistenza connessi, e sono dettagliati negli accordi di versamento.

Il processo di conservazione si basa su di una logica di conservazione caratterizzata dal versamento da parte del Titolare degli oggetti da conservare, cioè documenti informatici e aggregazioni documentali informatiche, secondo la tempistica definita e dettagliata negli accordi di versamento.

5.2 Acquisizione e presa in carico dei pacchetti di versamento (sip)

Si rimanda al manuale di conservazione del Conservatore allegato al presente documento (Allegato n.4) e agli accordi di versamento.

5.2.1 Pre-acquisizione

Si rimanda al manuale di conservazione del Conservatore allegato al presente documento (Allegato n.4) e agli accordi di versamento

5.2.2 Acquisizione

Si rimanda al manuale di conservazione del Conservatore allegato al presente documento (Allegato n.4) e agli accordi di versamento.

5.2.3 Verifica

Si rimanda al manuale di conservazione del Conservatore allegato al presente documento (Allegato n.4) e agli accordi di versamento.

5.2.4 Rifiuto o accettazione

Si rimanda al manuale di conservazione del Conservatore allegato al presente documento (Allegato n.4) e agli accordi di versamento.



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

5.2.5 Presa in carico e generazione del Rapporto di versamento

Si rimanda al manuale di conservazione del Conservatore allegato al presente documento (Allegato n.4) e agli accordi di versamento.

5.2.6 Generazione del Pacchetto di archiviazione (AIP)

Si rimanda al manuale di conservazione del Conservatore allegato al presente documento (Allegato n.4) e agli accordi di versamento.

5.3 Gestione del pacchetto di archiviazione (aip)

Si rimanda al manuale di conservazione del Conservatore allegato al presente documento (Allegato n.4) e agli accordi di versamento.

5.3.1 Aggiornamento dei pacchetti di archiviazione (AIP)

Si rimanda al manuale di conservazione del Conservatore allegato al presente documento (Allegato n.4) e agli accordi di versamento.

5.3.2 Selezione e scarto dei pacchetti di archiviazione (AIP)

Si rimanda al manuale di conservazione del Conservatore allegato al presente documento (Allegato n.4) e agli accordi di versamento.

5.4 Gestione del pacchetto di distribuzione (dip)

Si rimanda al manuale di conservazione del Conservatore allegato al presente documento (Allegato n.4) e agli accordi di versamento.

5.4.1 Modalità di esibizione/estensione

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

Il Titolare autorizza gli utenti configurati nei ruoli di Responsabile della conservazione e suoi delegati, ove nominati, alla consultazione di quanto versato in Conserva, tramite interfaccia web. Gli utenti si collegano all'indirizzo comunicato dal Conservatore secondo le modalità e regole fornite da quest'ultimo. Le unità organizzative (AOO e UOR) del Titolare che hanno la necessità di consultare i documenti presenti nel



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

Sistema di conservazione devono pertanto inoltrare apposita richiesta formale al Responsabile della conservazione.

Gli operatori da abilitare per l'accesso tramite interfaccia web al Sistema di conservazione sono comunicati dal Titolare al Conservatore, che provvede a inviare le credenziali di accesso via e-mail ai diretti interessati.

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

5.4.2 Produzione di copie, di riproduzioni e di duplicati

La produzione di duplicati e copie informatiche o analogiche tramite il Sistema di conservazione, avviene in seguito a richiesta ad apposita interfaccia web.

La figura del pubblico ufficiale è necessaria nei seguenti casi:

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

Si rimanda al manuale di conservazione del Conservatore allegato al presente documento (Allegato n.4) e agli accordi di versamento.

5.4.3 Interoperabilità

L'atto di affidamento prevede che, in caso di recesso o a scadenza di contratto, *Cineca* è tenuto a riversare i documenti informatici e le aggregazioni documentali informatiche conservate, i metadati a essi associati e le evidenze informatiche generate nel corso del processo di conservazione nel sistema indicato dal Titolare, secondo le modalità e i tempi indicati negli accordi di versamento.

L'Ateneo ha inoltre la possibilità di richiedere al Conservatore *Cineca* l'acquisizione di documenti informatici e aggregazioni documentali informatiche precedentemente conservate presso altri conservatori. *Cineca* provvederà solo al termine del riversamento e solo dopo le opportune verifiche - effettuate da entrambe le parti e svolte di concerto tra le stesse - di corretto svolgimento del riversamento stesso, all'eliminazione dal proprio Sistema di conservazione di tutti gli oggetti riversati e di tutti gli elementi riferiti al Titolare, garantendo la completa cancellazione e non leggibilità dei dati.



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

L'intera operazione dovrà avvenire con l'autorizzazione e la vigilanza delle competenti autorità, in particolare delle strutture del MiC.

Si rimanda al manuale di conservazione del Conservatore allegato al presente documento (Allegato n.4) e agli accordi di versamento.

5.5 Monitoraggio e risoluzione delle anomalie

5.5.1 Gestione delle anomalie

La segnalazione di un'anomalia o di un incidente può provenire sia dal Titolare sia dal gestore del Sistema di conservazione. Tali segnalazioni avvengono mediante il sistema di tracciamento attraverso cui sono veicolate le comunicazioni fra i due attori così come la notifica di risoluzione degli stessi in funzione della tipologia di servizio coinvolto.

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

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

La gestione degli incidenti e anomalie è composta dalle fasi:

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

Si rimanda al manuale di conservazione del Conservatore, in cui sono definite le specifiche operative e le modalità di interazione per la gestione delle anomalie e per il monitoraggio.

6. DESCRIZIONE DEL SISTEMA DI CONSERVAZIONE

6.1 Componenti logiche

Si rimanda al manuale di conservazione del Conservatore allegato al presente documento (Allegato n.4).



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

6.2 Componenti fisiche

Si rimanda al manuale di conservazione del Conservatore allegato al presente documento (Allegato n.4).

6.2.1 Schema generale

Si rimanda al manuale di conservazione del Conservatore allegato al presente documento (Allegato n.4).

6.2.2 Caratteristiche tecniche del Sito primario

Si rimanda al manuale di conservazione del Conservatore allegato al presente documento (Allegato n.4).

6.3 Componenti tecnologiche

Si rimanda al manuale di conservazione del Conservatore allegato al presente documento (Allegato n.4).

6.4 Procedure di gestione del sistema

Si rimanda al manuale di conservazione del Conservatore allegato al presente documento (Allegato n.4).

6.5 Evoluzione del sistema

Si rimanda al manuale di conservazione del Conservatore allegato al presente documento (Allegato n.4).

6.6 Monitoraggio e controlli

Si rimanda al manuale di conservazione del Conservatore allegato al presente documento (Allegato n.4).

6.6.1 Procedure di monitoraggio

Si rimanda al manuale di conservazione del Conservatore allegato al presente documento (Allegato n.4).

6.6.2 Funzionalità per la verifica e il mantenimento dell'integrità degli archivi

Si rimanda al manuale di conservazione del Conservatore allegato al presente documento (Allegato n.4).



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

6.6.3 Casistica e soluzioni adottate in caso di anomalie

Si rimanda al manuale di conservazione del Conservatore allegato al presente documento (Allegato n.4).

7. STRATEGIE ADOTTATE A GARANZIA DELLA CONSERVAZIONE

7.1 Misure a garanzia della intellegibilità, della leggibilità e della reperibilità nel tempo

Si rimanda al manuale di conservazione del Conservatore allegato al presente documento (Allegato n.4).

7.2 Misure a garanzia dell'interoperabilità e della trasferibilità ad altri conservatori

Si rimanda al manuale di conservazione del Conservatore allegato al presente documento (Allegato n.4).

8. CONSERVAZIONE DEI CERTIFICATI STUDENTI FIRMATI DIGITALMENTE

L'Università degli Studi dell'Aquila ha affidato alla società *Unimatica-RGI S.p.A.* il servizio per la gestione del sistema di firma digitale automatica remota da apporre ai certificati studenti generati dal gestionale delle segreterie studenti, il servizio di archiviazione digitale e conservazione a norma dei certificati studenti firmati digitalmente sul sistema *Unistorage*.

La sola conservazione dei certificati studenti firmati digitalmente è stata affidata alla società *Unimatica-RGI S.p.A.* con atto affidamento prot. n. 71617/2019 del 06/12/2019.

Con provvedimenti prot. n. 47337/2020 del 11/06/2020 e prot. n. 48426/2020 del 15/06/2020 il Legale rappresentante di *Unimatica-RGI S.p.A.* è stato delegato al ruolo di *Responsabile del servizio di conservazione*. I compiti previsti nel paragrafo 4.5 delle Linee guida dell'Agenzia per l'Italia digitale (AgID) sono stati delegati alla società *Unimatica* fatta eccezione quelli di cui alle lettere l) e m).

Con provvedimenti prot. n. 47336/2020 del 11/06/2020 e prot. n. 48426/2020 del 15/06/2020 il Legale rappresentante di *Unimatica-RGI S.p.A.* è stato nominato *Responsabile esterno del trattamento dei dati*.

Con prot. n. 24844/2022 del 24/02/2022 la società *Unimatica-RGI S.p.A.* ha comunicato al Titolare la modifica della delega a *Responsabile del servizio di conservazione* a norma dei documenti digitali, in conformità alle Linee guida dell'Agenzia per l'Italia digitale (AgID) sulla formazione, gestione e conservazione dei documenti informatici.

Nel Manuale del sistema di conservazione *Unimatica-RGI S.p.A.* vengono illustrati:

- la struttura del sistema di conservazione;
- gli oggetti sottoposti a conservazione;
- il processo di conservazione e le componenti logiche, tecnologiche e fisiche relative al suo funzionamento;



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

- i soggetti coinvolti nelle attività e nei processi di conservazione con le relative responsabilità del sistema.

9. TRATTAMENTO DEI DATI PERSONALI

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

L'Ateneo ha affidato lo svolgimento del processo di conservazione secondo quanto stabilito nell'atto di affidamento a *Cineca* che assume il ruolo di Responsabile del trattamento dei dati.

L'Ateneo, titolare dei dati, ha altresì affidato alla società *Unimatica-RGI S.p.A.*, lo svolgimento del processo di conservazione dei certificati studenti firmati digitalmente, secondo quanto stabilito nell'atto di affidamento su citato. Il Titolare ha nominato con apposito atto la società *Unimatica-RGI S.p.A.* Responsabile esterno del trattamento dei dati individuando i compiti ai quali deve attenersi.

I dati trattati sono sia i «dati personali contenuti nei documenti oggetto di conservazione» che i «dati personali degli utenti del servizio di conservazione» per consentire l'accesso al Sistema di conservazione.

Le attività di trattamento dei dati personali sono svolte nei limiti strettamente necessari alla realizzazione delle prestazioni richieste, unicamente tramite soggetti debitamente autorizzati, secondo i principi di liceità, proporzionalità e correttezza, nel rispetto delle misure minime di sicurezza.

10. ELENCO ALLEGATI

- Allegato 1 - Glossario
- Allegato 2 - Accordi di versamento
- Allegato 3 - Ruoli e responsabilità
- Allegato 4 - Manuale di Conservazione del Consorzio Interuniversitario *Cineca*
- Allegato 5 - Manuale di Conservazione di *Unimatica-RGI S.p.A.*



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

ALLEGATO 1 – GLOSSARIO

GLOSSARIO DEI TERMINI	5
TERMINE	5
Accesso	5
Accreditamento	5
Affidabilità.....	5
Aggregazione documentale informatica	5
Archivio	5
Archivio informatico.....	5
Area Organizzativa Omogenea	5
Autenticità.....	5
Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	5
Certificazione.....	5
Classificazione	5
Codec	5
Conservatore	5
Conservatore accreditato.....	6
Conservazione.....	6
Convenzioni di denominazione del file	6
Coordinatore della Gestione Documentale	6
Destinatario	6
Digest.....	6
Documento elettronico.....	6
Documento informatico	6
Duplicato informatico	6
eSeal.....	6
Esibizione.....	6
eSignature	6
Estratto di documento	6



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

informatico.....	6
Estratto per riassunto di documento informatico	6
Evidenza informatica	6
Fascicolo informatico.....	6
File	6
File container	6
File wrapper	6
File-manifesto	7
Filesystem	7
Firma elettronica	7
Firma elettronica avanzata	7
Firma elettronica qualificata	7
Flusso (binario).....	7
Formato contenitore	7
Formato del documento	7
informatico.....	7
Funzioni aggiuntive del protocollo informatico.....	7
Funzioni minime del protocollo informatico	7
Funzione di <i>hash</i> crittografica.....	7
Gestione Documentale	7
Hash	7
Identificativo univoco	7
Impronta crittografica	7
Integrità	7
Interoperabilità.....	8
Leggibilità.....	8
Manuale di conservazione.....	8
Manuale di gestione	8
Metadati	8
Naming convention.....	8
Oggetto di conservazione.....	8
Oggetto digitale.....	8



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

Pacchetto di archiviazione	8
Pacchetto di distribuzione	8
Pacchetto di file (<i>file package</i>).....	8
Pacchetto di versamento	8
Pacchetto informativo	8
Path	8
Pathname.....	8
Percorso	8
Piano della sicurezza del sistema di conservazione	9
Piano della sicurezza del sistema di gestione Informatica dei documenti	9
Piano di conservazione	9
Piano generale della sicurezza	9
Presenza in carico	9
Processo	9
Produttore dei PdV.....	9
qSeal.....	9
qSignature	9
Rapporto di versamento	9
Registro di protocollo	9
Registro particolare.....	9
Regolamento eIDAS	9
Responsabile dei sistemi informativi per la conservazione	10
Responsabile del servizio conservazione.....	10
Responsabile della conservazione.....	10
Responsabile della funzione archivistica di conservazione	10
Responsabile della gestione documentale.....	10
Responsabile della sicurezza dei sistemi di conservazione.....	10
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	10
Riferimento temporale	10
Riversamento	10
Scarto	10
Serie	10



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

Sidecar (file).....	10
Sigillo elettronico.....	10
Sistema di classificazione	11
Sistema di conservazione	11
Sistema di gestione informatica dei documenti	11
Timeline	11
Titolare dell'oggetto di conservazione.....	11
Trasferimento.....	11
TUDA	11
Ufficio.....	11
Utente abilitato.....	11
Versamento	11
GLOSSARIO DEGLI ACRONIMI	12
AGID	12
AOO.....	12
CAD.....	12
FEA.....	12
FEQ.....	12
GDPR.....	12
PdA (AiP)	12
PdD (DiP)	12
PdV (SiP)	12
eIDAS	12



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

GLOSSARIO DEI TERMINI

TERMINE	DEFINIZIONE
Accesso	Operazione che consente di prendere visione dei documenti informatici
Accreditamento	Riconoscimento, da parte dell'Agenzia per l'Italia digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione.
Affidabilità	Caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico o nel sistema di gestione o conservazione.
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.
Archivio	Complesso dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività.
Archivio informatico	Archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche.
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.
Autenticità	Il grado con cui una persona o un sistema considera un oggetto per quanto riguarda ciò che dichiara di essere. L'autenticità è valutata sulla base della capacità di essere provata.
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.
Certificazione	Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi.
Classificazione	Attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati
Codec	Algoritmo di codifica e decodifica che consente di generare flussi binari, eventualmente imbustarli in un file o in un <i>wrapper</i> (codifica), così come di estrarli da esso (decodifica).
Conservatore	Soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici.



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

Conservatore accreditato	Conservatore a cui AGID ha riconosciuto il possesso dei requisiti a livello più elevato, in termini di qualità e di sicurezza, tramite procedura di accreditamento.
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 autenticità, integrità, leggibilità, reperibilità dei documenti
Convenzioni di denominazione del file	Insieme di regole sintattiche che definisce il nome dei file all'interno di un filesystem o pacchetto.
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 AOO.
Destinatario	Soggetto o sistema al quale il documento informatico è indirizzato.
Digest	Vedi Impronta crittografica.
Documento elettronico	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva
Documento informatico	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Duplicato informatico	Vedi art. 1, comma 1, lett) i quinquies del CAD.
eSeal	Vedi sigillo elettronico.
Esibizione	Operazione che consente di visualizzare un documento conservato
eSignature	Vedi firma elettronica.
Estratto di documento informatico	Parte del documento tratto dal documento originale
Estratto per riassunto di documento informatico	Documento nel quale si attestano in maniera sintetica fatti, stati o qualità desunti da documenti informatici.
Evidenza informatica	Sequenza finita di <i>bit</i> 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.
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.
File container	Vedi Formato contenitore.
File wrapper	Vedi Formato contenitore.



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

File-manifesto	File che contiene metadati riferiti ad un file o ad un pacchetto di file.
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.
Firma elettronica	Vedi articolo 3 del Regolamento eIDAS.
Firma elettronica avanzata	Vedi articoli 3 e 26 del Regolamento eIDAS.
Firma elettronica qualificata	Vedi articolo 3 del Regolamento eIDAS.
Flusso (binario)	Sequenza di bit prodotta in un intervallo temporale finito e continuativo che ha un'origine precisa ma di cui potrebbe non essere predeterminato il suo istante di interruzione.
Formato contenitore	Formato di file progettato per consentire l'inclusione ("imbustamento" o <i>wrapping</i>), in uno stesso file, di una o più evidenze informatiche soggette a differenti tipi di codifica e al quale possono essere associati specifici metadati.
Formato del documento informatico	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
Funzioni aggiuntive del protocollo informatico	Nel sistema di protocollo informatico, componenti supplementari rispetto a quelle 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.
Funzione di <i>hash</i> crittografica	Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o <i>digest</i> (vedi) 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.
Gestione Documentale	Processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta uso, selezione e conservazione dei documenti.
Hash	Termine inglese usato, impropriamente, come sinonimo d'uso di "impronta crittografica" o " <i>digest</i> " (vedi).
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.
Impronta crittografica	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di <i>hash</i> crittografica a un'evidenza informatica.
Integrità	Caratteristica di un documento informatico, di un'aggregazione o di un sistema di gestione o conservazione che garantisca la sua inalterabilità nel tempo.



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

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.
Leggibilità	Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica.
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.
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.
Metadati	Dati associati ad un oggetto digitale per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo, in conformità a quanto definito nella norma ISO 15489-1:2016.
Naming convention	Vedi Convenzioni di denominazione
Oggetto di conservazione	Oggetto digitale versato in un sistema di conservazione.
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.
Pacchetto di archiviazione	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel manuale di conservazione.
Pacchetto di distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione.
Pacchetto di file (<i>file package</i>)	Insieme finito di più file (possibilmente organizzati in una struttura di sottoalbero all'interno di un filesystem) che costituiscono, collettivamente oltre che individualmente, un contenuto informativo unitario e auto-consistente.
Pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione.
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.
Path	Percorso (<i>vedi</i>).
Pathname	Concatenazione ordinata del percorso di un file e del suo nome.
Percorso	Informazioni relative alla localizzazione virtuale del file all'interno del filesystem espressa come concatenazione ordinata del nome dei nodi del percorso.



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza.
Piano della sicurezza del sistema di gestione Informatica dei documenti	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi nell'ambito dell'organizzazione di appartenenza.
Piano di conservazione	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.
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.
Presenza in carico	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione 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.
Processo	Insieme di attività correlate o interagenti che trasformano elementi in ingresso in elementi in uscita.
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.
qSeal	Sigillo elettronico qualificato, come da art. 35 del Regolamento eIDAS.
qSignature	Firma elettronica qualificata, come da art. 25 del Regolamento eIDAS.
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.
Registro di protocollo	Registro informatico ove sono memorizzate le informazioni prescritte dalla normativa per tutti 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-
Regolamento 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.



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

Responsabile dei sistemi informativi per la conservazione	Soggetto che coordina i sistemi informativi all'interno del conservatore accreditato, in possesso dei requisiti professionali individuati da AGID.
Responsabile del servizio conservazione	Soggetto che coordina il processo di conservazione all'interno del conservatore accreditato, in possesso dei requisiti professionali individuati da AGID
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.
Responsabile della funzione archivistica di conservazione	Soggetto che coordina il processo di conservazione dal punto di vista archivistico all'interno del conservatore accreditato, in possesso dei requisiti professionali individuati da AGID
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.
Responsabile della sicurezza dei sistemi di conservazione	Soggetto che assicura il rispetto dei requisiti di sicurezza all'interno del conservatore accreditato, in possesso dei requisiti professionali individuati da AGID
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Soggetto che assicura lo sviluppo e la manutenzione del sistema all'interno del conservatore accreditato, in possesso dei requisiti professionali individuati da AGID
Riferimento temporale	Insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC).
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.
Scarto	Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storicoculturale.
Serie	Raggruppamento di documenti con caratteristiche omogenee (vedi anche aggregazione documentale informatica).
Sidecar (file)	File-manifesto (<i>vedi</i>).
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.



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

Sistema di classificazione	Struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata.
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.
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
Timeline	Linea temporale virtuale su cui sono disposti degli eventi relativi ad un sistema informativo o a un documento informatico. Costituiscono esempi molto diversi di <i>timeline</i> un file di log di sistema, un flusso multimediale contenente essenze audio\video sincronizzate.
Titolare dell'oggetto di conservazione	Soggetto produttore degli oggetti di conservazione.
Trasferimento	Passaggio di custodia dei documenti da una persona o un ente ad un'altra persona o un altro ente.
TUDA	Testo Unico della Documentazione Amministrativa, Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni e integrazioni.
Ufficio	Riferito ad un'area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico.
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.
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.



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

GLOSSARIO DEGLI ACRONIMI

ACRONIMO	DEFINIZIONE
AGID	Agenzia per l'Italia digitale
AOO	Area Organizzativa Omogenea
CAD	Codice dell'Amministrazione Digitale - Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni.
FEA	Vedi firma elettronica avanzata.
FEQ	Vedi firma elettronica qualifica.
GDPR	Regolamento (UE) № 679/2016 del Parlamento Europeo e del Consiglio, del 27 aprile 2016 (" <i>General Data Protection Regulation</i> "), 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.
PdA (AiP)	Pacchetto di Archiviazione.
PdD (DiP)	Pacchetto di Distribuzione.
PdV (SiP)	Pacchetto di Versamento.
eIDAS	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.



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

ALLEGATO 2 – ACCORDI DI VERSAMENTO

Sommario

Registro informatico di protocollo giornaliero.....	2
Registri IVA inviati da Titulus	2
Fatture elettroniche attive verso PA trasmesse da Titulus tramite SDI (Sistema Di Interscambio).....	2
Fatture elettroniche passive e dei lotti ricevuti tramite SDI (Sistema Di Interscambio).....	2
Verbali di esame elettronici inviati da Esse3	2
Verbali di esame elettronici fascicolati ed inviati da Titulus	2
Fatture elettroniche attive verso privati trasmesse da Titulus	2
Libri contabili inviati da titulus tramite integrazione con U-gov	2
Ordinativi informatici inviati da titulus tramite integrazione con U-gov e Siope+	2
Documentazione prodotta dai moduli U-buy gare e avvisi trasmessi da Titulus	3
Tesi di laurea magistrali e di dottorato inviati da Titulus.....	3



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

Registro informatico di protocollo giornaliero

Versione approvata dalle parti 01.04.01 del 09.01.2018 - associato alla registrazione di protocollo 1094/2018.

Registri IVA inviati da Titulus

Versione approvata dalle parti 01.03.01 del 09.01.2018 - associato alla registrazione di protocollo 1094/2018.

Fatture elettroniche attive verso PA trasmesse da Titulus tramite SDI (Sistema Di Interscambio)

Versione approvata dalle parti 01.06.01 del 09.01.2018 - associato alla registrazione di protocollo 1094/2018.

Fatture elettroniche passive e dei lotti ricevuti tramite SDI (Sistema Di Interscambio)

Versione approvata dalle parti 01.03.01 del 09.01.2018 - protocollo n. 1094/2018.

Verbali di esame elettronici inviati da Esse3

Versione approvata dalle parti 01.05.01 del 05.07.2017 – protocollo n. 26463/2017

Allegato 1: dizionario dei tag del verbale d'esame elettronico.

Verbali di esame elettronici fascicolati ed inviati da Titulus

Versione approvata dalle parti 01.05.01 del 16.06.2020 – repertorio contratti e convenzioni n. 172/2020 protocollo n. 50002/2020.

Allegato 1: dizionario dei tag del verbale d'esame elettronico - versione approvata dalle parti 01.01.01 del 16.06.2020.

Fatture elettroniche attive verso privati trasmesse da Titulus

Versione approvata dalle parti 01.01.01 del 27.05.2020 - repertorio contratti e convenzioni n. 165/2020 protocollo n. 44799/2020.

Libri contabili inviati da Titulus tramite integrazione con U-gov

Versione approvata dalle parti 01.01.01 del 27.05.2020 - repertorio contratti e convenzioni n. 164/2020 protocollo n. 44796/2020.

Ordinativi informatici inviati da Titulus tramite integrazione con U-gov e Siope+

Versione approvata dalle parti 01.01.01 del 27.05.2020 - repertorio contratti e convenzioni n. 163/2020 protocollo 44784/2020.



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

Documentazione prodotta dai moduli U-buy gare e avvisi trasmessi da Titulus

Versione approvata dalle parti 01.01.01 del 14.11.2019 – repertorio contratti e convenzioni n. 1275/2019 protocollo n. 66440/2019.

Tesi di laurea magistrali e di dottorato inviati da Titulus

Versione approvata dalle parti 01.01.01 del 10.03.2020 - repertorio contratti e convenzioni 116/2020 protocollo n. 30857/2020.



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

ALLEGATO 3 – RUOLI E RESPONSABILITA'

SOMMARIO

1. Figure interne facenti capo al Titolare	2
1.1 RC - Responsabile della conservazione	2
1.2 CGD - Coordinatore della gestione documentale	2
1.3 RGd - Responsabile della gestione documentale	2
1.4 DPO - Responsabile per la Protezione dei Dati Personali (Data protection officer)	3
1.5 TT - Titolare trattamento dati personali	3
1.6 RTD Responsabile della Transizione Digitale	3
1.7 RTDP - Responsabile trattamento dati personali	4
2. Figure esterne facenti capo al servizio di conservazione in outsourcing	4



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

1. Figure interne facenti capo al Titolare

1.1 RC - Responsabile della conservazione

Definisce le politiche del Sistema di conservazione e predispone il manuale di conservazione, è il soggetto cui fa capo la responsabilità di verifica del corretto svolgimento del processo di conservazione.

Nominativo	Periodo nel ruolo	Eventuali deleghe
Francesco Mazzotta	Dal 29/05/2017 al 15/12/2018 DDG prot. n. 19074	Fiorindo Carducci delegato con provvedimento prot. n. 19074 del 29/05/2017
Fiorindo Carducci	Dal 29/01/2019 DDG prot. n. 3728	Giovanni Franceschini delegato con provvedimento prot. n. 6716 del 19/02/2019 Berardinella Castellani delegato con provvedimento prot. n. 89500 del 27/07/2021

1.2 CGD - Coordinatore della gestione documentale

Responsabile della definizione di criteri uniformi di trattamento dei documenti e di classificazione e archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'art. 50 comma 4 del DPR 28 dicembre 2000 n. 445 nei casi di amministrazioni che abbiano istituito più Aree Organizzative. Produce il pacchetto di versamento e assicura il trasferimento del suo contenuto al Sistema di conservazione.

Nominativo	Periodo nel ruolo	Eventuali deleghe
Fiorindo Carducci	Dal 29/05/2017 prot. n. 19074/2017	

1.3 RGD - Responsabile della gestione documentale

Soggetto responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi (art. 61 DPR 28 dicembre 2000 n. 445); è anche responsabile della produzione del pacchetto di versamento (art. 6 comma 3 – DPCM 3 dicembre 2013 sulla conservazione).

Nominativo	AOO	Periodo nel ruolo	Eventuali deleghe
Pierpaolo Baldini	Dipartimento Mesva	Dal 29/05/2017 prot. n. 19074/2017	
Mara Grisenti	Dipartimento Disim	Dal 29/05/2017 prot. n. 19074/2017	
Rossella Rotesi	Dipartimento Dfsc	Dal 29/05/2017 prot. n. 19074/2017	
Gianluigi Giordani	Dipartimento Discab	Dal 29/05/2017 al 24/01/2019 prot. n. 19074/2017	
Ciccione Alessio	Dipartimento Discab	Dal 25/01/2019 prot. n. 3464/2019	
Domenico Schettini	Dipartimento Diie	Dal 29/05/2017 prot. n. 19074/2017	



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

Flavio Grimaldi	Dipartimento Dicaa	Dal 29/05/2017 prot. n. 19074/2017	
Morena Del Vecchio	Dipartimento Dsu	Dal 29/05/2017 prot. n. 19074/2017	

1.4 DPO - Responsabile per la Protezione dei Dati Personali (Data protection officer)

Il Responsabile della protezione dei dati deve: a) informare e consigliare il Titolare o il Responsabile del trattamento, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento europeo e da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati; b) verificare l'attuazione e l'applicazione del Regolamento, delle altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare o del Responsabile del trattamento in materia di protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, e gli audit relativi; c) fornire, se richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare i relativi adempimenti; d) fungere da punto di contatto per gli interessati in merito a qualunque problematica connessa al trattamento dei loro dati o all'esercizio dei loro diritti; e) fungere da punto di contatto per il Garante per la protezione dei dati personali oppure, eventualmente, consultare il Garante di propria iniziativa.

Nominativo	Periodo nel ruolo	Eventuali deleghe
Francesco Mazzotta	Dal 17/05/2018 al 15/12/2018 D.R. prot. n. 22081	
Gianfranco Cardinale	Dal 21/12/2018 al 28/02/2022 D.R. prot. n. 56570	
Claudio Rossi	Dal 01/03/2022 D.R. prot. n. 28508	

1.5 TT - Titolare trattamento dati personali

Ex art. 4 comma 1, lettera F) Codice Privacy. (...) la pubblica amministrazione (...) cui competono, (...) le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Nominativo	Periodo nel ruolo	Eventuali deleghe
Edoardo Alesse	Dall'a.a. 2019/2020 all'a.a. 2024/2025	

1.6 RTD Responsabile della Transizione Digitale

Ex art. 17 comma 1 CAD, come modificato dal DLgs 179/2016. È il soggetto che deve garantire la transizione dell'ente alla modalità operativa digitale.

Nominativo	Periodo nel ruolo	Eventuali deleghe
Rocco Matriccioni	Dal 19/12/2017 D.R. 48882	



UNIVERSITÀ DEGLI STUDI DELL'AQUILA

1.7 RTDP - Responsabile trattamento dati personali

Responsabile dell'unità organizzativa che tratta i documenti poi inviati al Sistema di conservazione nominato dal Titolare ai sensi del Codice Privacy.

<i>Nominativo</i>	<i>Periodo nel ruolo</i>	<i>Eventuali deleghe</i>
Responsabili delle unità organizzative	Periodi diversi	

2. Figure esterne facenti capo al servizio di conservazione in outsourcing

Si rinvia al manuale di conservazione dei Conservatori allegati al presente documento (Allegato n. 4 e Allegato n. 5)

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
2.00	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 Recepte 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	6
2	Terminologia.....	7
2.1	Glossario	7
2.2	Acronimi	27
3	Normativa e standard di riferimento	28
3.1	Normativa.....	28
3.2	Standard di riferimento	30
4	Ruoli e responsabilità	31
5	Struttura organizzativa per il servizio di conservazione	35
5.1	Organigramma.....	37
5.2	Strutture organizzative	37
6	Oggetti sottoposti a conservazione.....	39
6.1	Oggetti conservati	39
6.2	Pacchetto di versamento.....	40
6.3	Pacchetto di archiviazione.....	42
6.4	Pacchetto di distribuzione	42
7	Il processo di conservazione.....	44
7.1	Redazione Accordo di versamento.....	45
7.2	Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico	46
7.3	Verifiche effettuate sui pacchetti di versamento e sugli oggetti in esso contenuti.....	47
7.4	Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico	48
7.5	Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie	49
7.6	Preparazione e gestione del pacchetto di archiviazione	50
7.7	Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione	51

7.8	Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti	52
7.9	Scarto dei pacchetti di archiviazione.....	53
7.10	Predisposizione di misure e garanzia dell'interoperabilità e trasferibilità ad altri conservatori	53
8	Il sistema di conservazione.....	55
8.1	Componenti logiche.....	55
8.2	Componenti tecnologiche	57
8.2.1	Software e strumenti software utilizzati	57
8.2.2	Disaster recovery	59
8.3	Componenti fisiche.....	60
8.4	Procedure di gestione e di evoluzione	65
8.4.1	Strategia di sviluppo e ciclo di vita del sistema Conserva	65
8.4.2	Ciclo di sviluppo e rilascio del software.....	67
8.4.3	Metodologia di sviluppo Agile in JIRA.....	69
8.4.4	Versionamento semantico dei componenti	74
8.4.5	Gli ambienti di esercizio	75
9	Monitoraggio e controlli.....	77
9.1	Procedure di monitoraggio.....	77
9.2	Verifica dell'integrità degli archivi.....	78
9.2.1	Monitoraggio a campione degli archivi	78
9.2.2	Controllo integrità unità a seguito di richiesta di esibizione	79
9.3	Politiche di conservazione dei log	80
9.3.1	ConservaTrasferimento	81
9.3.2	ConservaVersamento	82
9.3.3	ConservaNotifica	82
9.3.4	Conserva	83
9.4	Soluzioni adottate in caso di anomalie.....	84

9.4.1 Gestione segnalazione delle anomalie 85

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 dettagli tecnici della procedura di versamento -	OAIS

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,	LLGG

	competenze, attività e/o materie del soggetto produttore.	
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 autenticità, integrità, leggibilità, reperibilità dei documenti.	LLGG
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 <i>Naming convention</i>)	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 OAIS distribuzione. Per l'accezione utilizzata in questo manuale cfr. Pacchetto di distribuzione.	
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	LLGG

contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento.

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, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici. CAD

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 minime, necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni.	LLGG
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	LLGG

computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.

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	OAIS

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.

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	OAIS

contenuto Informativo non sia stato alterato senza una documentazione dell'evento. Sono riportate all'interno degli Accordi di Versamento.

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 riportate all'interno degli Accordi di Versamento.	OAIS
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 LLGG conservazione.	
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	LLGG

	concatenazione ordinata del nome dei nodi del percorso. (anche <i>Percorso</i>)	
Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi.	LLGG
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 posta elettronica e di fornire ricevute opponibili ai terzi.	CAD
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 (<i>interamente_versato, parzialmente_versato o rifiutato</i>) 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	LLGG

all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID

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 rilevanti ai fini giuridico-amministrativo e storico-culturale.	LLGG
---------------	--	------

Serie	Raggruppamento di documenti con LLGG caratteristiche omogenee (vedi anche aggregazione documentale informatica).	
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 LLGG conservazione. Nel contesto Cineca corrisponde al Cliente. (Nel testo anche Titolare)	
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, che costituiscono un'unità non divisibile: repertorio, serie o fascicolo.	CINECA
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 CINECA divisibile, di cui è composto un archivio, per esempio, una lettera, un memorandum, un rapporto, una fotografia, una registrazione sonora. Può essere composta da più file.
Utente abilitato	Persona, ente o sistema che interagisce con i LLGG servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.
Versamento	Passaggio di custodia, di proprietà e/o di LLGG 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.
Volume di conservazione	Unità logica risultato finale di un processo UNISINCRO mirato a conservare un insieme di oggetti digitali.
Web Service	Sistema software progettato per supportare CINECA l'interoperabilità tra diversi elaboratori su di una medesima rete ovvero in un contesto distribuito.

[Torna al sommario](#)

2.2 Acronimi

AGID	Agenzia per l'Italia Digitale
AIP	Archival Information Package (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'Agazia 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
<i>Responsabile del servizio di conservazione (RSERV)</i>	Massimiliano Valente	Cfr. Capitolo 2 - Ruoli e Responsabilità	Maggio 2021	Nessuna
<i>Responsabile Sicurezza dei sistemi per la conservazione (RSIC)</i>	Paola Tentoni	Cfr. Capitolo 2 - Ruoli e Responsabilità	Gennaio 2015	Nessuna
<i>Responsabile funzione archivistica di conservazione (RARCH)</i>	Massimiliano Valente	Cfr. Capitolo 2 - Ruoli e Responsabilità	Maggio 2021	Nessuna
<i>Responsabile sistemi informativi per la conservazione (RSINF)</i>	Angelo Neri	Cfr. Capitolo 2 - Ruoli e Responsabilità	Aprile 2015	Nessuna
<i>Responsabile sviluppo e manutenzione del sistema di conservazione (RSVIL)</i>	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	Francesca Merighi	Cfr. Capitolo 2 - Ruoli e Responsabilità	Da aprile 2015 a ottobre 2017

<i>sistema di conservazione</i>			
<i>Responsabile funzione archivistica di conservazione</i>	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.

<i>ATTIVITA' PROPRIE DI CIASCUN CONTRATTO DI SERVIZIO DI CONSERVAZIONE</i>	<i>RdC</i>	<i>RSERV</i>	<i>RSIC</i>	<i>RARCH</i>	<i>RSINF</i>	<i>RSVIL</i>
<i>Attivazione del servizio di conservazione (a seguito della sottoscrizione di un contratto)</i>	<i>C</i>	<i>A</i>		<i>R</i>		<i>C</i>
<i>Acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento</i>	<i>I</i>	<i>R/A</i>				<i>C</i>
<i>Preparazione e gestione del pacchetto di archiviazione</i>		<i>R/A</i>				<i>C</i>

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 OAIS¹ (di seguito solo OAIS).

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

- il **pacchetto di versamento (PdV)**: pacchetto versato dal produttore e utilizzato per l'acquisizione degli oggetti informativi e dei metadati da parte del sistema di conservazione;
- il **pacchetto di archiviazione (PdA)**: pacchetto finalizzato alla memorizzazione a lungo termine degli oggetti informativi digitali nel sistema di conservazione;
- il **pacchetto di distribuzione (PdD)**: pacchetto 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 metadattazione.

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.

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

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 metadattazione 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 Paimas² (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"*);
- **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;

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

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

[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 essere 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.

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.

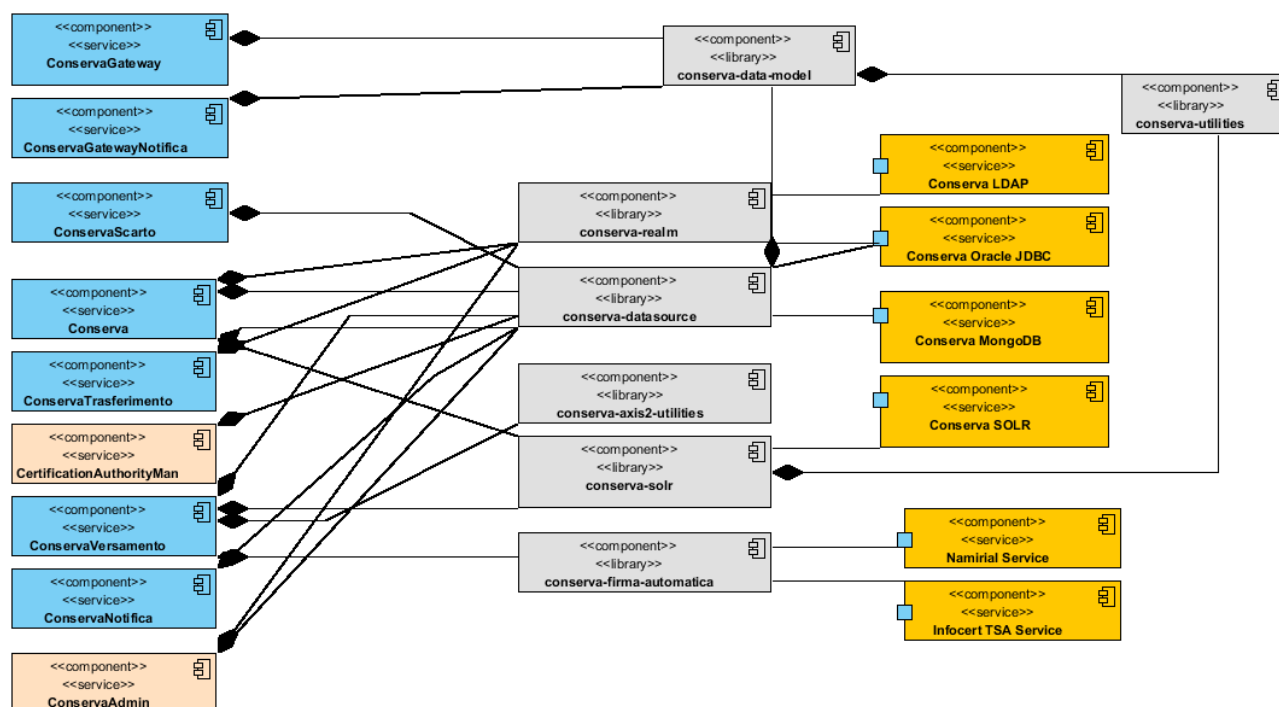


Figura 1- Schema delle componenti logiche che compongono il servizio

- **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 conservaversamento 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:

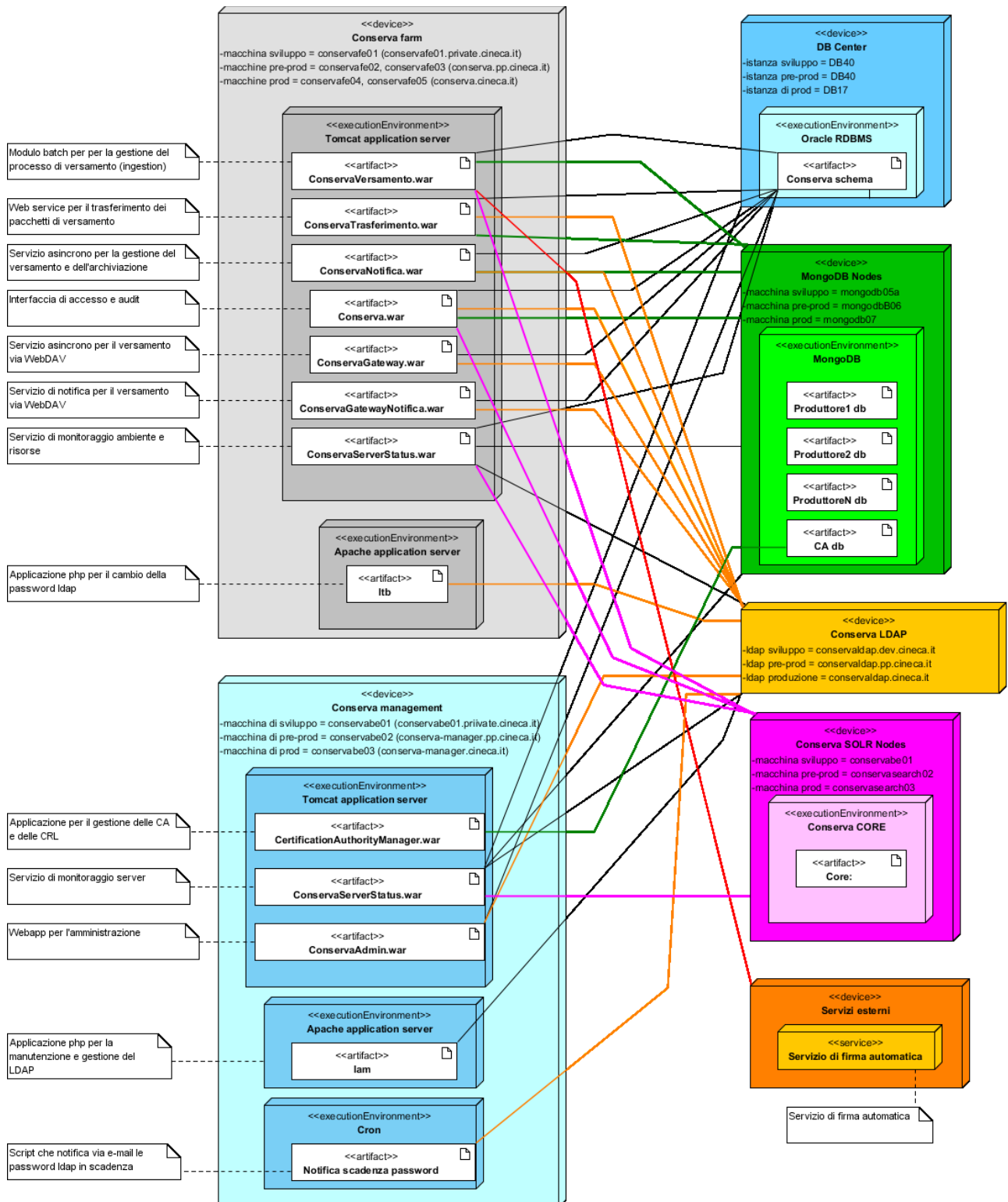


Figura 2 - Diagramma descrittivo dei componenti di Conserve

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

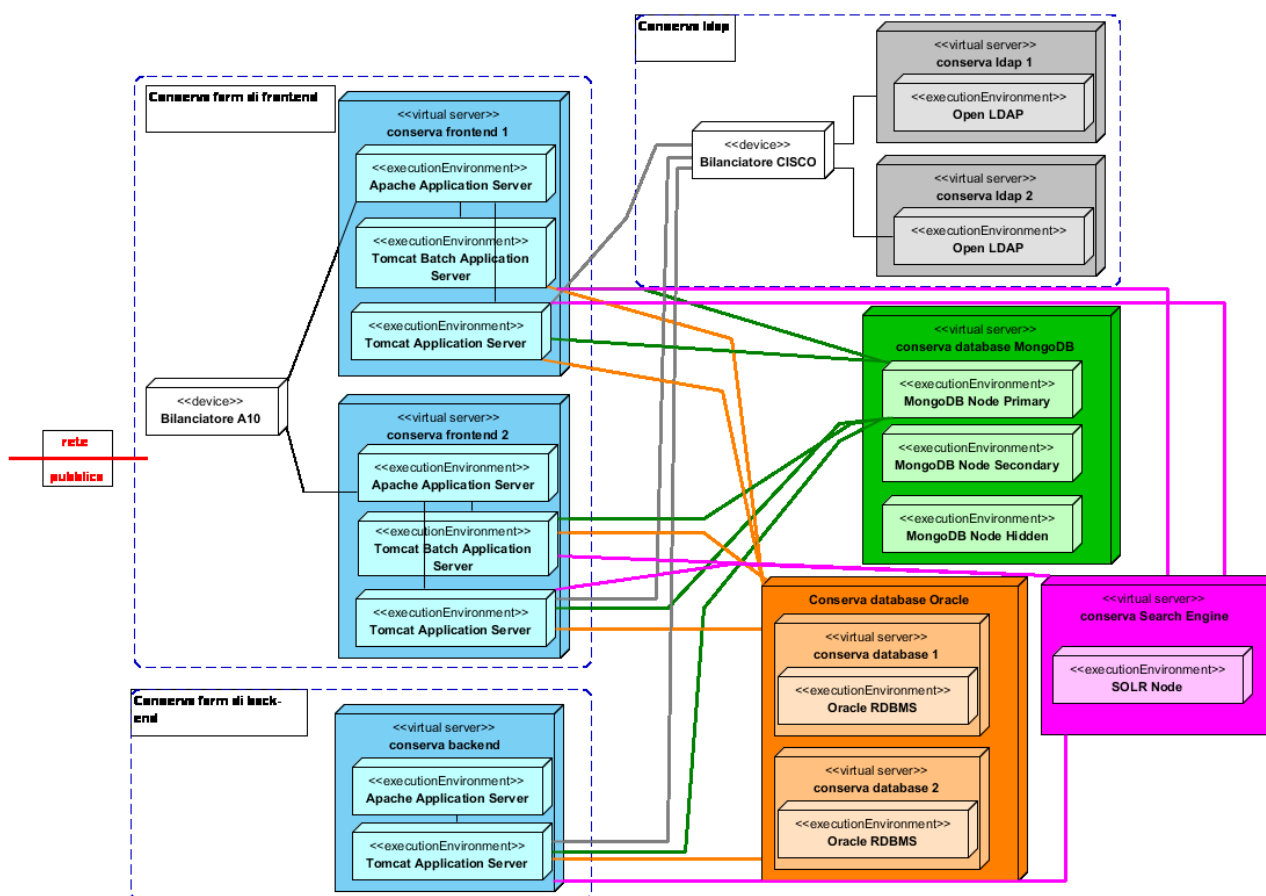


Figura 3 - Distribuzione componenti di Conserva

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.

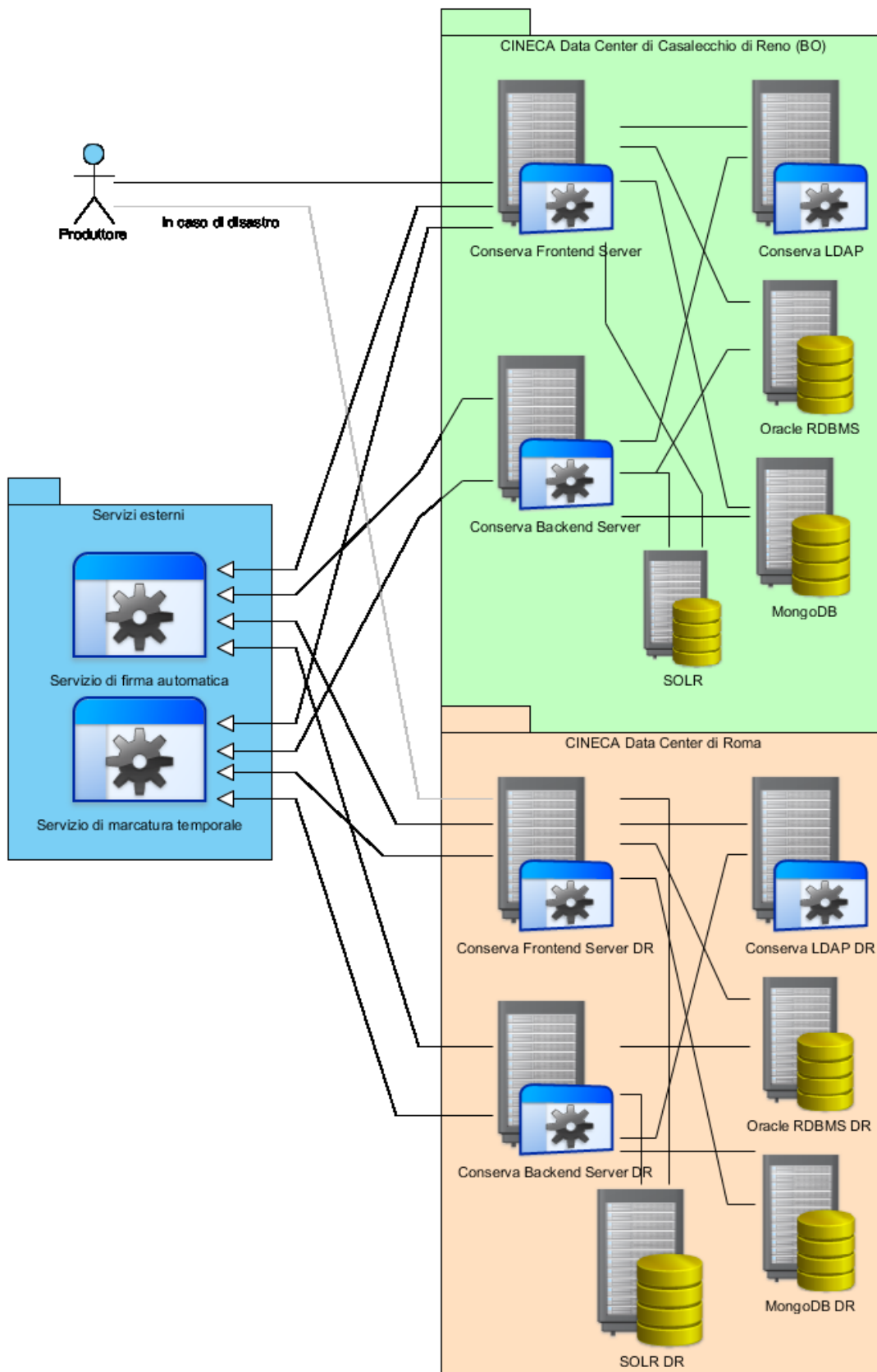


Figura 4 - Distribuzione topologica delle componenti fisiche di Conserva

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:

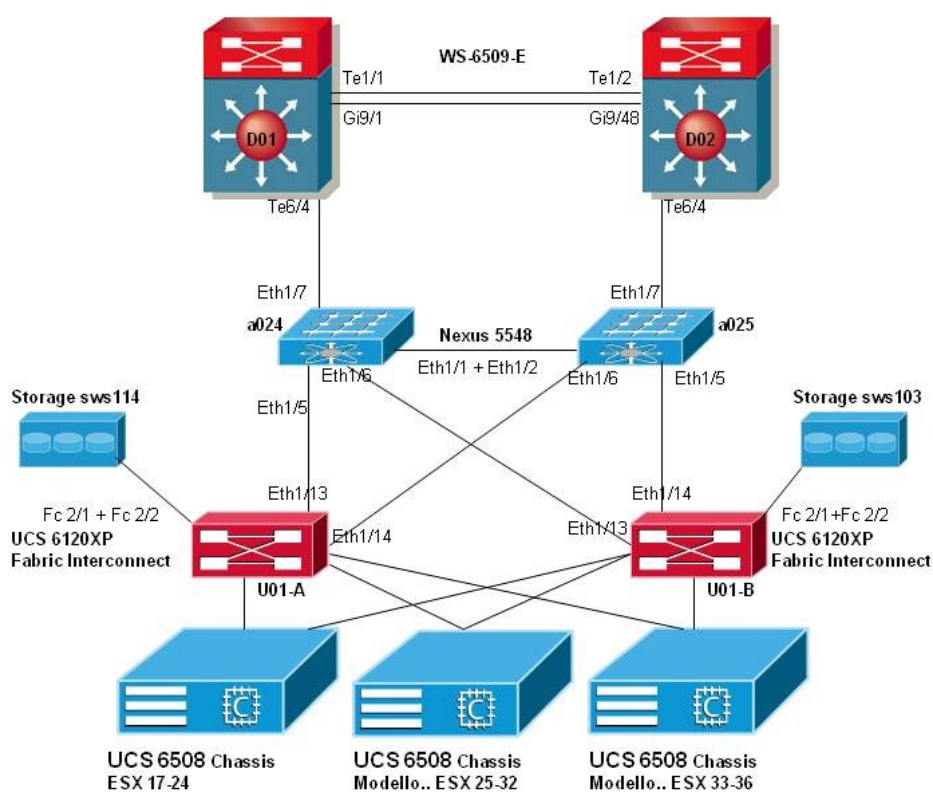


Figura 5 - Schema interconnessioni degli apparati di Conserva

[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.

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

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

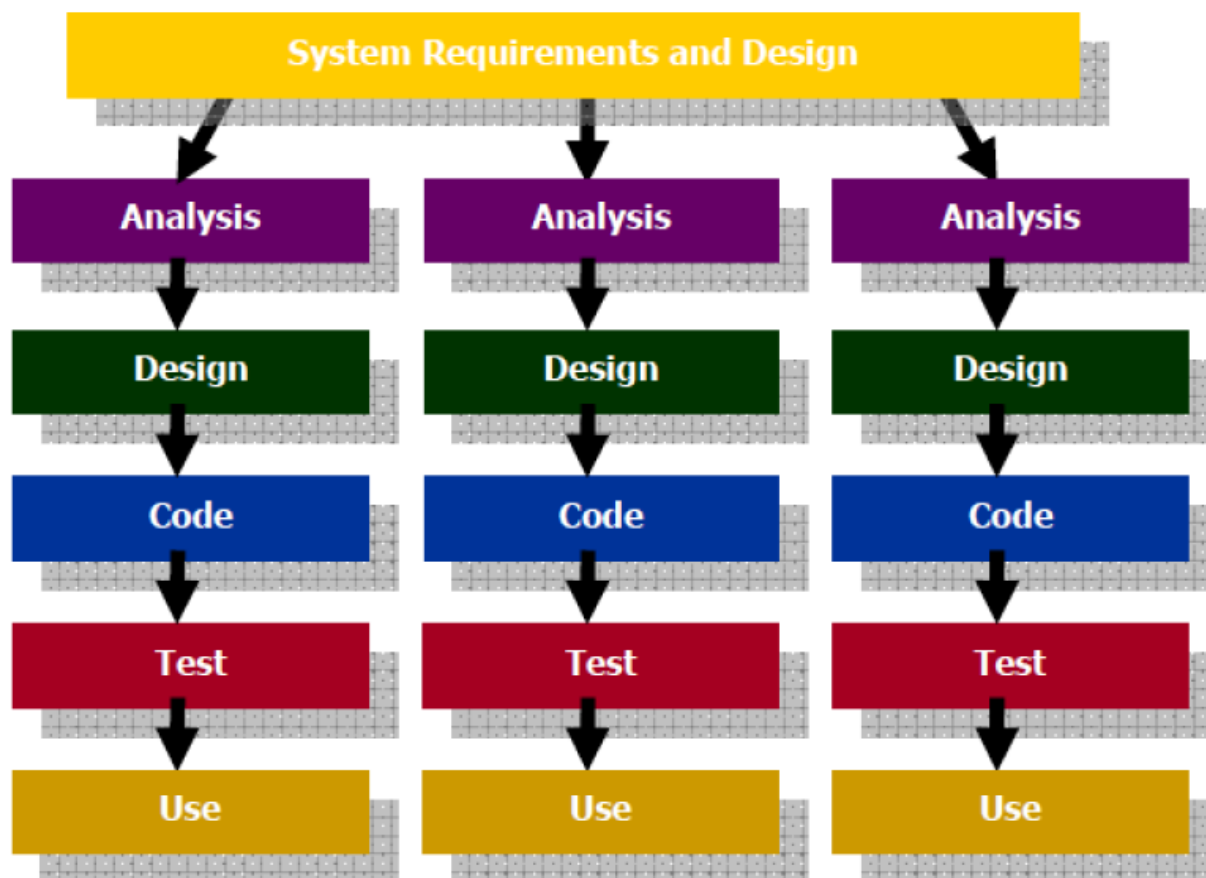


Figura 6 - Ciclo di vita iterativo-incrementale dello sviluppo del software

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)).

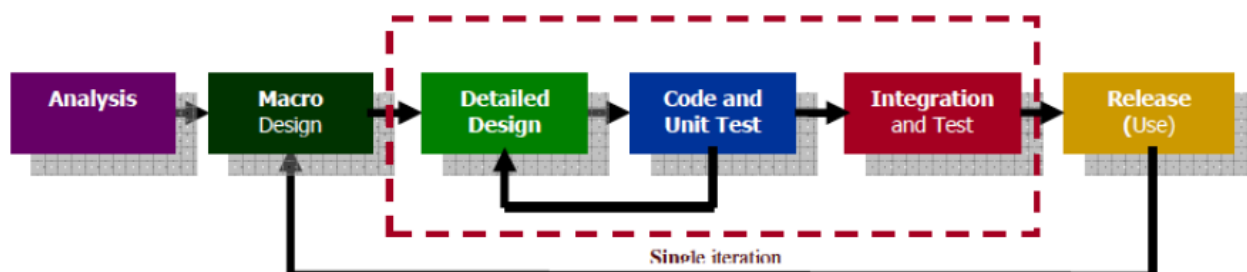


Figura 7 - Dettaglio del ciclo di vita iterativo-incrementale dello sviluppo del software

[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

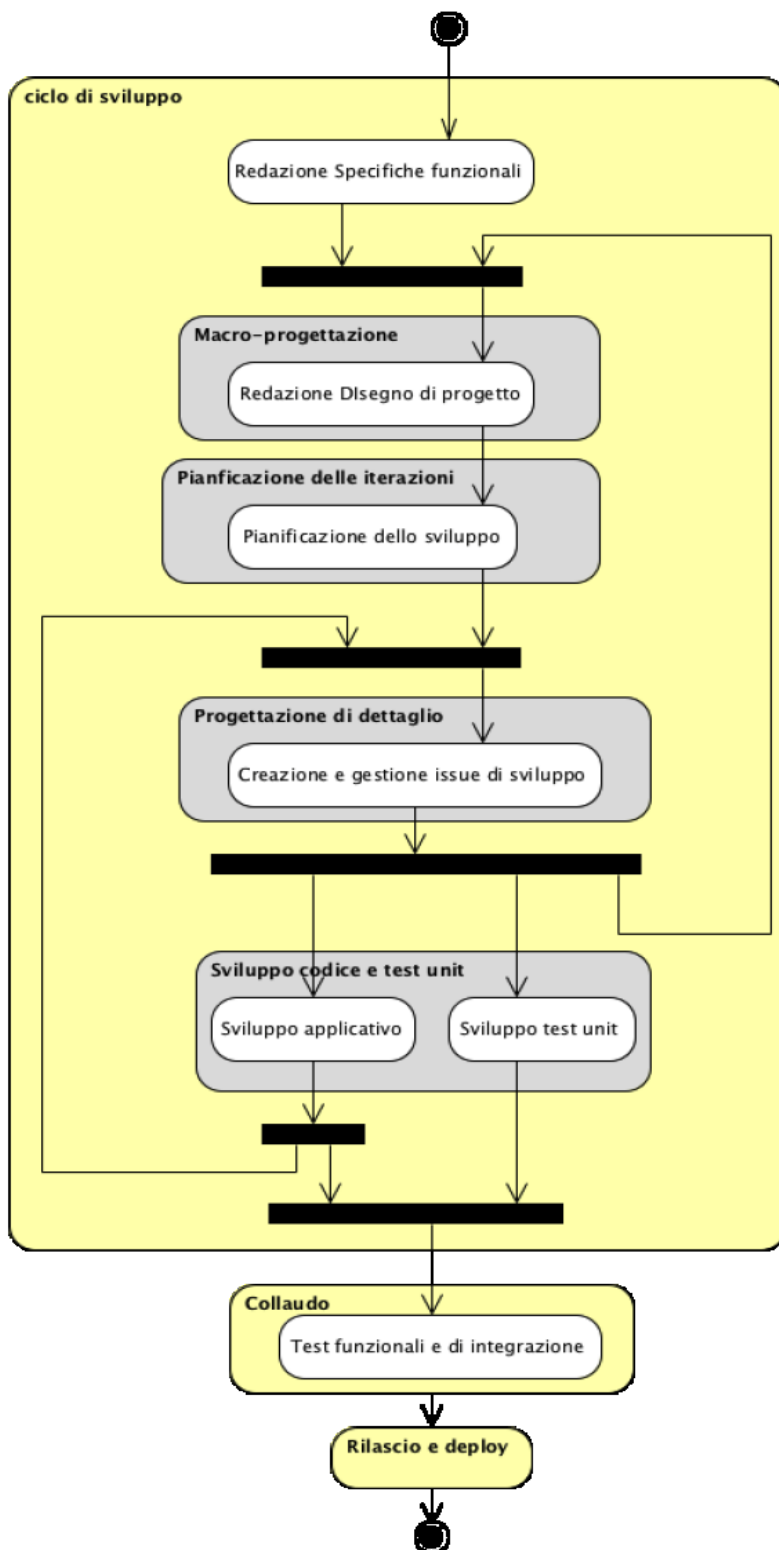


Figura 8 - Fasi di produzione e rilascio del software

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

[Torna al sommario](#)

8.4.3.1 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:

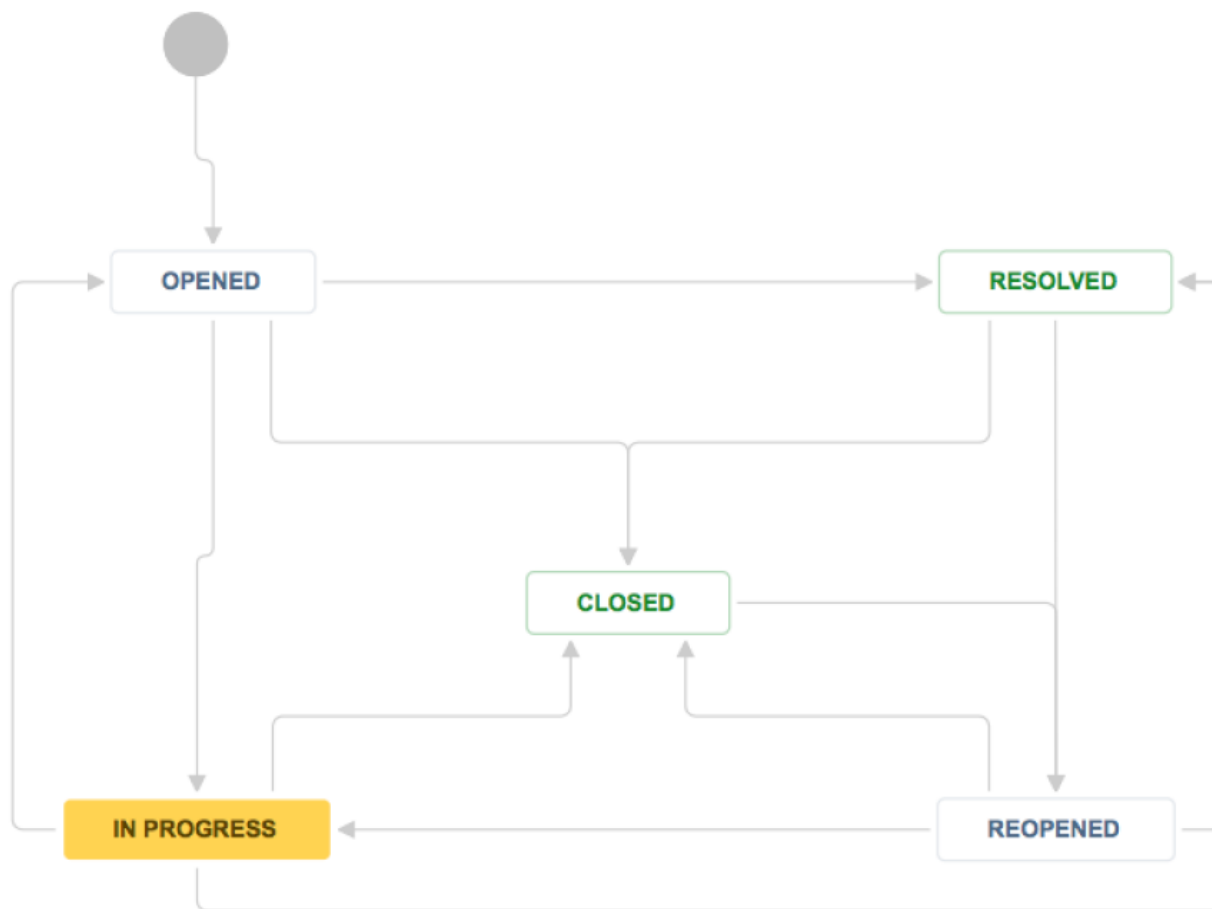


Figura 9 - Workflow degli stati delle singole issue

[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 ITILv3⁴.

[Torna al sommario](#)

9.2 Verifica dell’integrità degli archivi

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

[Torna al sommario](#)

9.2.1 Monitoraggio a campione degli archivi

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

- Oggetti informativi;
- Pacchetti di archiviazione.

Queste procedure, eseguite a campione in maniera non presidiata, secondo una temporizzazione stabilita dal Responsabile del servizio di conservazione, possono essere eseguite su esplicita

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

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](#)

UNIMATICARGI

MANUALE DEL SISTEMA DI CONSERVAZIONE



Sommario

Registro delle versioni	4
1. Scopo e ambito del documento.....	6
1.1. Trattamento dei dati personali.....	6
1.2. Trasparenza	8
2. Terminologia	10
3. Normativa e standard di riferimento	11
3.1. Normativa di Riferimento.....	11
3.2. Standard di Riferimento.....	12
4. Ruoli e responsabilità	14
4.1. Ruoli di ausilio al processo di conservazione	17
4.2. Precedenti responsabili.....	17
5. Struttura organizzativa per il servizio di conservazione.....	18
5.1. Organigramma.....	18
5.2. Strutture organizzative	19
6. Oggetti sottoposti a conservazione	21
6.1. Metadati	21
6.1.1 Metadati del documento informatico	22
6.1.2 Metadati del documento amministrativo informatico.....	24
6.1.3 Metadati delle aggregazioni documentali informatiche	26
6.1.4 Metadati del documento informatico di natura fiscale e contabile	29
6.2 Formati	29
6.2.1 Riversamento.....	29
6.3 Struttura dati del Pacchetto di versamento.....	30
6.4 Struttura dati del Pacchetto di archiviazione	30
6.5 Struttura dati del Pacchetto di distribuzione.....	31
7. Il processo di erogazione del servizio di conservazione.....	32
7.1 Il processo di conservazione	33
7.2 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico	33
7.3 Verifiche effettuate sui Pacchetti di versamento e sugli oggetti in esso contenuti.....	34
7.4 Accettazione dei Pacchetti di versamento e generazione del Rapporto di versamento di presa in carico	35
7.5 Rifiuto dei Pacchetti di versamento e modalità di comunicazione delle anomalie	36
7.6 Preparazione e gestione dei Pacchetti di archiviazione	36
7.7 Preparazione e gestione dei Pacchetti di distribuzione ai fini dell'esibizione.....	37
7.8 Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento di un pubblico ufficiale	38
7.9 Scarto dei Pacchetti di archiviazione.....	38
7.10 Predisposizione di misure per l'interoperabilità e la trasferibilità ad altri conservatori	39
7.11 Chiusura del contratto	40
8. Procedure di gestione e di evoluzione.....	41
8.1. Misure di sicurezza logica	41
8.1.1 Gestione utenze.....	41
8.1.2 Gestione sistemi di protezione	42
8.1.3 Gestione degli incidenti di sicurezza	42
8.1.4 Gestione dei backup e Disaster Recovery.....	43
8.1.4.1 Siti Settimo e Firenze	43
8.1.4.2 Siti di Bologna e Acilia (Roma)	44
8.1.4.3 Disaster Recovery	45
8.1.5 Gestione dei supporti di memorizzazione	45
8.2. Procedure di evoluzione e Change management	46
8.3. Cessazione del Servizio di conservazione	46
9. Monitoraggio e controlli	48
9.1 Audit interni e Verifica dell'integrità degli archivi	48

9.2 Reportistica di servizio	49
10. La server farm di Unimatica-RGI	51
10.1 UniStorage - Il sistema per la conservazione.....	54
Appendice A.....	56

Indice delle figure

Figura 1 - Struttura volumi	31
Figura 2 - Modello OAIS	32
Figura 3 - Architettura di conservazione	53

Registro delle versioni

Revisione	Data	Motivo Revisione	Redatto da	Approvato da
1.0	03/10/2009	Emissione	Andrea Anghinolfi	Silvano Ghedini
2.0	12/02/2010	Aggiornamento funzionalità	Andrea Anghinolfi	Silvano Ghedini
3.0	20/06/2010	Aggiornamento funzionalità	Andrea Anghinolfi	Silvano Ghedini
4.0	28/09/2010	Aggiornamento funzionalità	Andrea Anghinolfi	Silvano Ghedini
5.0	15/10/2010	Aggiornamento funzionalità	Andrea Anghinolfi	Silvano Ghedini
6.0	10/02/2011	Modifica gestione anomalie – Ampliamento funzionalità Unistorage	Andrea Anghinolfi	Silvano Ghedini
7.0	20/05/2011	Aggiornamento composizione societaria Unimatica-RGI	Andrea Anghinolfi	Silvano Ghedini
8.0	30/11/2012	Aggiornamento Data Center	Andrea Anghinolfi	Silvano Ghedini
8.1	11/12/2012	Personalizzazioni	Andrea Anghinolfi	Silvano Ghedini
8.2	20/06/2013	Aggiornamento compiti e responsabilità della conservazione	Sabina Falcinelli	Andrea Anghinolfi
8.3	04/07/2013	Aggiornamento normative	Sabina Falcinelli	Andrea Anghinolfi
8.4	05/02/2014	Aggiornamento normative	Sabina Falcinelli	Andrea Anghinolfi
8.5	11/02/2014	Aggiornamento Data Center	Sabina Falcinelli	Andrea Anghinolfi
8.6	05/03/2014	Adeguamento normative	Sabina Falcinelli	Andrea Anghinolfi
8.7	17/02/2015	Adeguamento DPCM 03/12/2013	Roberta Rosatone	Silvano Ghedini
8.8	15/10/2015	Passaggio alla ISO 27001:2013	Roberta Rosatone	Silvano Ghedini
8.9	20/01/2016	Adeguamento Schema Manuale della conservazione AgID	Roberta Rosatone	Silvano Ghedini
9.0	11/04/2017	Modifica ruolo Responsabile della Funzione Archivistica	Roberta Rosatone	Silvano Ghedini
9.1	14/06/2017	Aggiornamento definizioni per termine "Produttore"	Roberta Rosatone	Silvano Ghedini
9.2	05/10/2017	<ul style="list-style-type: none"> • Aggiornamento Server farm • Visualizzazione di 200 risultati da portale 	Roberta Rosatone	Silvano Ghedini
9.3	20/10/2017	<ul style="list-style-type: none"> • Capitolo Trasparenza • Aggiornamento elenco formati • Aggiunto testo alternativo mancante su alcune immagini • Sostituita immagine 7 precedentemente con parti nascoste 	Roberta Rosatone	Silvano Ghedini
9.4	25/10/2018	<ul style="list-style-type: none"> • Aggiornamento par. 1.1 adeguamento GDPR • Modifica ruolo Privacy Manager cap. 4 • Aggiornamento tabella normativa par. 3.1 • Aggiunto ruolo DPO al par.4.1 	Roberta Rosatone	Silvano Ghedini
9.5	29/01/2019	<ul style="list-style-type: none"> • Recepimento N.C. AgID • Recepimento Oss. Audit interno • Aggiornamento Nomina ad Interim Responsabile della funzione archivistica • Aggiornamento proc. Gestione Incident par. 8.1.3 	Roberta Rosatone	Silvano Ghedini

9.6	19/04/2019	<ul style="list-style-type: none"> Revoca nomina ad Interim per la Responsabilità della funzione archivistica Aggiornamento nomina ad interim DPO 	Roberta Rosatone	Silvano Ghedini
9.7	27/09/2019	<ul style="list-style-type: none"> Aggiornamento Ruoli (Delegato Responsabile del servizio di conservazione – Responsabile dello sviluppo e della manutenzione – Responsabile dei sistemi informative – DPO) Aggiornamento proc. Gestione Incident par. 8.1.3 Aggiornamento estensioni ISO 27017 – 27018 Aggiornamento descrizione par. 7.5 Rifiuto PDV 	Roberta Rosatone Paolo Vandelli	Silvano Ghedini
9.8	20/12/2019	<ul style="list-style-type: none"> Aggiornamento capp. 4 e 5 a seguito della sostituzione del Delegato alla Responsabilità del servizio di conservazione, della Responsabile della funzione archivistica e della Responsabile dello sviluppo e manutenzione A seguito delle NC ricevute in fase di audit è stato eliminato il par. 9.2 ed aggiornato il par. 8.1.3 sulla Gestione degli incident di sicurezza. 	Roberta Rosatone Paolo Vandelli	Silvano Ghedini
9.9	13/01/2021	<ul style="list-style-type: none"> Aggiornamento cap. 4 a seguito di Oss da Audit interno. Aggiunto nominativo Resp. dello sviluppo in carica. Aggiornamento tabella formati par. 6.2 	Roberta Rosatone	Silvano Ghedini
10	13/09/2021	<ul style="list-style-type: none"> Aggiornamenti a seguito del cambio ragione sociale Aggiornamento par. 1.1 sulla privacy Aggiornamento par. 1.2 per certificazione ISO 14001 Aggiornamento modifica sito d/r secondario Acilia (RM) 	Roberta Rosatone	Silvano Ghedini
11	30/12/2021	<ul style="list-style-type: none"> Aggiornamento a seguito dell'adeguamento alle Linee guida per la formazione, gestione e conservazione del documento informatico (revisionati cap. 1-2-3-4-6-7) 	Eleonora Luzi	Paolo Vandelli
12	21/06/2022	<ul style="list-style-type: none"> Capitolo 4.1.: riportato nuovo responsabile del servizio; rimossa evidenza della delega assegnata a Paolo Vandelli dal precedente responsabile del servizio; Aggiunto capitolo '4.2. Precedenti responsabili' Rivisto capitolo '5.1. Organigramma' in funzione della nuova nomina 	Eleonora Luzi	Paolo Vandelli

1. Scopo e ambito del documento

Il presente documento costituisce il Manuale del servizio di conservazione erogato da Unimatica-RGI ed ha lo scopo di illustrare la struttura del sistema di conservazione descrivendone analiticamente gli oggetti sottoposti a conservazione, il processo di conservazione e le componenti logiche, tecnologiche e fisiche relative al suo funzionamento. Delinea, inoltre, i soggetti che sono coinvolti nelle attività e nei processi di conservazione i quali hanno la responsabilità del sistema.

Il Manuale del servizio unitamente alla Scheda cliente predisposta da Unimatica-RGI, al fine di personalizzare il rapporto contrattuale con il Cliente Soggetto produttore (da ora in poi Soggetto produttore), costituiscono parte integrante del contratto di fornitura del servizio e mira a garantire e illustrare formalmente ai propri clienti il sistema di conservazione e le sue caratteristiche di disponibilità nel tempo di documenti integri, autentici, legalmente validi e facilmente consultabili.

Questo documento è reso disponibile a tutte le parti interessate a seguito di apposita richiesta.

[Torna al sommario](#)

1.1. Trattamento dei dati personali

Ai sensi e per gli effetti dell'articolo 28 del Regolamento (UE) n. 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (d'ora innanzi anche "GDPR" o "Regolamento") e del D.lgs. 30 giugno 2003 n. 196, relativamente e limitatamente ai trattamenti riguardanti la conservazione degli oggetti digitali affidati a Unimatica-RGI, a partire dalla data di sottoscrizione del contratto, il Soggetto produttore, nella sua qualità di Titolare del trattamento, affida a Unimatica-RGI, che diventa Responsabile del trattamento dei dati personali trattati in esecuzione del contratto, i seguenti compiti e impartisce le seguenti istruzioni per il trattamento dei dati cui Unimatica-RGI deve attenersi:

1. Unimatica-RGI per espletare le attività pattuite per conto del Soggetto produttore potrebbe trattare direttamente o anche solo indirettamente una o più delle seguenti categorie di dati:

- dati personali,
- dati rientranti nelle categorie "particolari" di dati personali,
- dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, di cui è Titolare il Soggetto produttore. Per i dettagli, occorre fare riferimento a quanto pattuito nel contratto/ordine/accordo.

2. I dati trattati da Unimatica-RGI si riferiscono potenzialmente, a titolo esemplificativo, ma non esaustivo, alle seguenti categorie di interessati: clienti, dipendenti, utenti, fornitori, richiedenti impiego, soci, etc.

3. Il trattamento dei dati in questione è effettuato da Unimatica-RGI esclusivamente per lo svolgimento del servizio di Conservazione a norma, in modo lecito e secondo correttezza, attenendosi alle prescrizioni della normativa sulla protezione dei dati personali nonché alle previsioni della specifica delega a Responsabile del Servizio di Conservazione o successivamente concordate tra le parti; è fatto esplicito divieto di diffondere o comunicare i dati in questione a soggetti che siano estranei all'esecuzione del trattamento.

4. Unimatica-RGI, nella sua qualità di Responsabile del trattamento, in particolare è tenuta a:

a) effettuare tutte le operazioni in termini di mansioni, definendo regole e modelli di comportamento che assicurino la riservatezza e il rispetto del divieto di comunicazione e diffusione dei dati ai quali si ha accesso;

b) trattare direttamente, o per il tramite dei propri dipendenti, collaboratori esterni, consulenti, etc. - designati autorizzati al trattamento - i dati personali del Soggetto produttore, Titolare del trattamento, per le sole finalità connesse allo svolgimento delle attività previste dal

contratto/ordine/accordo, in modo lecito e secondo correttezza, nonché nel pieno rispetto delle disposizioni impartite dal GDPR, nonché, infine, dalle presenti istruzioni;

- c) non divulgare o rendere noti a terzi - per alcuna ragione ed in alcun momento, presente o futuro ed anche una volta cessati i trattamenti oggetto del contratto/ordine/accordo - i dati personali ricevuti dal Titolare o pervenuti a sua conoscenza in relazione all'esecuzione del servizio prestato, se non previamente autorizzato per iscritto dal Titolare, fatti salvi eventuali obblighi di legge o ordini dell'Autorità Giudiziaria e/o di competenti Autorità amministrative;
- d) collaborare con il Titolare per garantire la puntuale osservanza e conformità alla normativa in materia di protezione dei dati personali;
- e) incaricare per iscritto i soggetti che abbiano le caratteristiche di Responsabili di Sistema e di Amministratori di Sistema, tenerne l'elenco aggiornato a disposizione del Soggetto produttore e fornirne eventualmente copia a semplice richiesta dello stesso;
- f) adottare, se del caso, adeguate misure di sicurezza, in modo da ridurre al minimo i rischi di distruzione e perdita, anche accidentale dei dati/documenti stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- g) informare immediatamente il Soggetto produttore di qualsiasi richiesta o comunicazione da parte dell'Autorità Garante e/o Giudiziaria, per concordare congiuntamente l'evasione delle stesse;
- h) collaborare con il Soggetto produttore per l'attuazione delle prescrizioni eventualmente impartite dall'Autorità Garante;
- i) comunicare al Soggetto produttore qualsiasi accadimento che possa compromettere il corretto trattamento dei dati personali;
- j) segnalare eventuali criticità al Soggetto produttore che possono mettere a repentaglio la sicurezza dei dati, al fine di consentire idonei interventi da parte dello stesso;
- k) prestare particolare attenzione all'eventuale trattamento di dati personali rientranti nelle categorie particolari e/o relative a condanne penali o reati degli interessati conosciuti, anche incidentalmente, in esecuzione dell'incarico affidato, procedendo alla loro raccolta e archiviazione solo ove ciò si renda necessario per lo svolgimento delle attività di competenza e istruendo in tal senso le persone autorizzate che operano all'interno della propria struttura.

5. Il trattamento dei dati deve intendersi effettuato sotto la vigilanza del Soggetto produttore il quale, in ogni momento e con congruo preavviso, potrà operare controlli e impartire eventuali ulteriori specifiche istruzioni per il suo svolgimento, nonché chiederne la cessazione se imposta dalla necessità di adempiere a divieti od obblighi di legge, ovvero a provvedimenti dell'Autorità Garante e/o Giudiziaria.

6. Unimatica-RGI, nella sua qualità di Responsabile esterno del trattamento, si impegna a notificare al Soggetto produttore, Titolare del trattamento, senza ingiustificato ritardo dall'avvenuta conoscenza, e comunque entro 24 ore dalla scoperta con comunicazione da inviarsi all'indirizzo PEC del Soggetto produttore, (salvo diversa email indicata) ogni violazione dei dati personali (*data breach*). Unimatica-RGI si impegna a prestare ogni più ampia assistenza al Soggetto produttore al fine di consentirgli di assolvere agli obblighi di cui agli artt. 32 - 34 del GDPR.

Una volta definite le ragioni della violazione, Unimatica-RGI di concerto con il Soggetto produttore e/o altro soggetto da quest'ultimo indicato, si attiverà per implementare nel minor tempo possibile tutte le misure di sicurezza fisiche e/o logiche e/o organizzative atte ad arginare il verificarsi di una nuova violazione della stessa specie di quella verificatasi.

7. In esecuzione degli accordi in essere con il Soggetto produttore, Unimatica-RGI potrà affidare l'esecuzione - parziale o totale - delle relative attività a soggetti terzi, dei quali garantisce il possesso dei requisiti di esperienza, capacità ed affidabilità, ivi compreso il profilo relativo alla sicurezza. Ove ricorra tale ipotesi, Unimatica-RGI, nella sua qualità di Responsabile esterno del trattamento, provvede personalmente a designare Responsabile del trattamento ai sensi dell'art. 28 del GDPR i suddetti soggetti terzi (nel seguito anche "Sub-Responsabile del trattamento") con idoneo atto giuridico e ne dà notizia al Soggetto produttore tramite il seguente link: <https://www.unimaticaspa.it/it/gdpr-elenco-sub-responsabili>.

8. Unimatica-RGI assicura che nessun dato personale potrà essere trasferito all'esterno dell'Area Economica Europea (EEA).

9. Premesso che l'accesso ai dati personali da parte degli interessati esercitato ai sensi degli artt. 15 e seguenti del GDPR sarà gestito direttamente dal Soggetto produttore, Unimatica-RGI si rende disponibile a collaborare con il Soggetto produttore stesso fornendogli tutte le informazioni necessarie a soddisfare le eventuali richieste ricevute in tal senso.

10. Unimatica-RGI – ove tale obbligo si applichi anche alla stessa, nella sua qualità di Responsabile del trattamento e in base alle disposizioni del comma 5 dell'art. 30 del GDPR - mantiene un registro di tutte le categorie di attività relative al trattamento svolte per conto del Soggetto produttore.

11. Unimatica-RGI si impegna a mettere a disposizione del Soggetto produttore tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di sicurezza descritti nel presente documento e, in generale, il rispetto delle obbligazioni assunte in forza del GDPR, consentendo e, su richiesta, contribuendo alle attività di audit, comprese le ispezioni, realizzate dal Soggetto produttore o da altro soggetto da esso incaricato.

12. L'autorizzazione al trattamento dei dati personali avrà la medesima validità ed efficacia della durata della conservazione legale dei documenti, stabilita dalla normativa.

[Torna al sommario](#)

1.2. Trasparenza

La conservazione a norma di Unimatica-RGI è rivolta a Pubbliche amministrazioni, banche, assicurazioni, strutture sanitarie ed ai privati in genere.

Al fine di rendere tali servizi agevoli ed accessibili ad un pubblico variegato e disomogeneo, Unimatica-RGI rende disponibili una serie di strumenti ed informazioni utili a garantire una totale trasparenza delle proprie attività mediante canali diretti ed indiretti.

In generale, nel sito internet aziendale www.unimaticaspa.it sono disponibili:

- i contatti principali quali telefono, fax, email ed indirizzo.
- La certificazione per la Qualità ISO 9001:2015 (Unimatica-RGI è certificata dal 2006)
- La certificazione per il Sistema di Gestione Ambientale ISO 14001:2015
- La certificazione per la Sicurezza delle Informazioni ISO 27001:2013 (Unimatica-RGI è certificata dal 2014) con estensioni alle Linee guida ISO 27017:2015, ISO 27018:2019 ed ISO 27701:2019
- Il Codice Etico aziendale
- Il Modello di Organizzazione, Gestione e Controllo (MOG), ai sensi della L. 231/01 (consultabile a richiesta)
- La Politica Aziendale (consultabile a richiesta)
- L'elenco delle Associazioni di cui l'azienda fa parte e delle Partnership tecnico/commerciali
- La descrizione dei servizi e prodotti offerti dall'azienda e le modalità attraverso cui ottenere informazioni dettagliate su di essi e su come richiederli
- Le informazioni sulle principali attività svolte o in corso

Oltre alle certificazioni sopra elencate, Unimatica-RGI sta implementando un sistema di gestione anticorruzione ISO 37001:2016.

Tale certificazione, obbligatoria ai fini dell'adeguamento alle Linee guida per la formazione, gestione e conservazione dei documenti informatici in vigore dal 1° gennaio 2022, verrà aggiunta alle altre presenti nella sezione Trasparenza.

Negli anni, il settore Conservazione di Unimatica-RGI ha ottemperato a tutti gli obblighi normativi applicabili. Nello specifico, infatti, da marzo del 2015 ha mantenuto l'accreditamento presso l'Agenzia per l'Italia Digitale (AgID) con la pubblicazione del Manuale della conservazione nell'apposita area a ciò dedicata sul sito web di AgID.

Dall'ottobre del 2017 fino ad abrogazione, in continuità con le disposizioni normative, ha ottenuto e mantenuto la certificazione in conformità all'art. 24 del Regolamento Eidas e alla check list "*Lista di riscontro per la visita ispettiva AgID e la certificazione di conformità*".

Tali strumenti, oltre ad essere sinonimo di eccellenza, sono risultati negli anni passi indispensabili per la crescita dell'azienda, del team e per migliorare continuamente il prodotto Unistorage e il servizio offerto ai clienti.

Unimatica-RGI considera altrettanto importante il concetto di trasparenza rivolto ai propri dipendenti. Sull'intranet aziendale, infatti, ogni dipendente ha a disposizione strumenti e materiali informativi relativi al sistema di gestione integrato della Qualità, della Sicurezza, dell'Ambiente, e della Privacy (ISO 27001, ISO 9001, ISO 14001) e a tutte le Procedure di conservazione. L'impegno, l'attenzione, la formazione e le competenze di tutta l'azienda sulla tematica specifica ed i risultati raggiunti nel corso degli anni di attività hanno permesso ad Unimatica-RGI di ottenere l'iscrizione quale socio sostenitore presso l'associazione ANORC (Associazione Nazionale per Operatori e Responsabili della Conservazione Digitale).

Per dimostrare trasparenza ed affidabilità, inoltre, Unimatica-RGI garantisce da sempre la propria disponibilità ad ospitare audit finanziari e/o di seconda parte, rispettando così le disposizioni delle autorità di controllo e, previo accordo, anche gli accordi stabiliti con clienti per i quali presta servizi.

[Torna al sommario](#)

2. Terminologia

La terminologia e gli acronimi utilizzati in questo manuale richiamano quelli elencati *nell'Allegato 1 Glossario dei termini e degli acronimi* alle Linee guida per la formazione, gestione e conservazione dei documenti informatici al quale si rimanda.

[Torna al sommario](#)

3. Normativa e standard di riferimento

Il sistema di conservazione sviluppato da Unimatica-RGI è conforme alla normativa e agli standard elencati nei successivi paragrafi.

Periodicamente vengono effettuate verifiche per l'aggiornamento dei requisiti normativi al fine di assicurare una puntuale conformità alle disposizioni legislative. Eventuali ulteriori riferimenti normativi non direttamente riconducibili alla conservazione, ma comunque applicabili per via di servizi correlati ad essa, sono elencati in uno specifico documento facente parte del sistema di gestione integrato, denominato SIC040 – Monitoraggio.

[Torna al sommario](#)

3.1. Normativa di Riferimento

Notazione abbreviata	Riferimento
Codice Civile	[Libro Quinto del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle Scritture contabili], art. 2215 bis – Documentazione informatica.
RD 1163/1911	Regolamento per gli archivi di Stato
DPR 1409/1963	Norme relative all'ordinamento ed al personale degli archivi di Stato
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
Legge 9 gennaio 2004, n. 4 aggiornata dal decreto legislativo 10 agosto 2018, n. 106	Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici
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 della PA;
Reg. UE 2018/1807	Relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea;
DPCM 19 giugno 2019 n. 76	Regolamento di organizzazione del Ministero per i beni e le attività culturali, degli uffici di diretta collaborazione del Ministro e dell'Organismo indipendente di valutazione della performance.
Linee guida AgID ed Allegati	Linee guida sulla Formazione, Gestione, Conservazione dei documenti informatici Allegato 1 Glossario dei termini e degli acronimi Allegato 2 Formati di File e Riversamento Allegato 3 Certificazione di processo Allegato 4 Standard e specifiche tecniche Allegato 5 Metadati
Regolamento AgID ed Allegati	Regolamento sui criteri di conservazione Allegato A Requisiti per l'erogazione del servizio di conservazione per conto delle pubbliche amministrazioni Allegato B Piano di cessazione del servizio di conservazione dei documenti informatici

[Torna al sommario](#)

3.2. Standard di Riferimento

Sigla	Titolo standard
UNI 11386	Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.
ISO 14721	OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione.
ISO 15836	Information and documentation - The Dublin Core metadata element set, Sistema di metadati del Dublin Core
ISO/TR 18492	Long-term preservation of electronic document-based information.
ISO 20652	Space data and information transfer systems - Producer-Archive interface - Methodology abstract standard.
ISO 20104	Space data and information transfer systems — Producer-Archive Interface Specification (PAIS).
ISO/CD TR 26102	Requirements for long-term preservation of electronic records.
SIARD	Software Independent Archiving of Relational Databases 2.0 Ministère de la culture et de la communication, Service interministériel des Archives de France,

	Standard d'échange de données pour l'archivage. Transfert – Communication – Élimination – Restitution - Modification, ver. 2.1, 2018
METS	Metadata Encoding and Transmission Standard
PREMIS	PREservation Metadata: Implementation Strategies.
EAD (3)/ISAD (G)	
EAC (CPF)/ISAAR (CPF)/NIERA (CPF)	
SCONS2/EAG/ISDIAH	

[Torna al sommario](#)

4. Ruoli e responsabilità

Conformemente al par. 4.4 delle Linee guida sulla Formazione, gestione e conservazione dei documenti informatici, si individuano i seguenti ruoli coinvolti nel processo di conservazione:

- **Titolare dell'oggetto della conservazione** (citato nel manuale come soggetto produttore), identificato come il soggetto produttore degli oggetti di conservazione.
- **Produttore dei PdV**, ovvero la 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, identificato con il responsabile della gestione documentale nelle pubbliche amministrazioni
- **Utente abilitato**, ossia la persona, l'ente o il sistema che interagisce con i servizi di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse
- **Responsabile della conservazione**, ovvero il soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.
- **Conservatore**, identificato come l'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 autenticità, integrità, leggibilità, reperibilità dei documenti.

Il processo di conservazione vede direttamente coinvolti tutti i soggetti sopra elencati.

Unimatica-RGI ha individuato le seguenti figure di responsabilità per l'erogazione del servizio di conservazione, a garanzia di elevati standard di qualità e sicurezza:

Il Responsabile del servizio di conservazione espleta, a seguito di delega formale e in ogni caso rimanendo inteso che la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile, rimane in capo al responsabile della conservazione, le seguenti attività:

1. 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
2. gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
3. genera e sottoscrive il Rapporto di Versamento, secondo le modalità previste dal manuale di conservazione;
4. genera il pacchetto di archiviazione conforme allo Standard SInCRO UNI 11386 - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali e lo sottoscrive con firma digitale;
5. genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione, ai fini dell'esibizione richiesta dall'utente;
6. effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
7. 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;

8. 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;
9. provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
10. adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione;
11. 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;
12. assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
13. 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

garantendo un particolare riguardo alla:

- 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 del servizio di conservazione nominato da Unimatica-RGI è **Paolo Vandelli**.

In assenza del Responsabile del servizio di conservazione, le sue funzioni operative vengono delegate a **Cecilia Canova**.

Il Responsabile della funzione archivistica di conservazione, in accordo con il Responsabile del servizio di conservazione, si occupa di

- definire e gestire il processo di conservazione, incluse le modalità di trasferimento da parte del produttore dei PDV, 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
- monitorare set di metadati di conservazione dei documenti, dei fascicoli informatici e delle aggregazioni documentali informatiche
- monitorare il processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema
- collaborare con il Produttore dei PDV 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.

La **Responsabile della funzione archivistica di conservazione** nominata da Unimatica-RGI è **Eleonora Luzi**.

Responsabile sicurezza dei sistemi per la conservazione il quale si occupa di:

- monitorare e rispettare i requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza. In caso di eventuali difformità si occupa di segnalarle al Responsabile del servizio di conservazione e, quindi, individua e pianifica le necessarie azioni correttive.

Il **Responsabile sicurezza dei sistemi per la conservazione** nominato da Unimatica-RGI è **Massimo Ortensi**.

Responsabile dei sistemi informativi per la conservazione il quale si occupa di:

- gestire l'esercizio delle componenti hardware e software del sistema di conservazione e monitorare il mantenimento dei livelli di servizio (SLA) concordati con il Titolare e il Produttore
- segnalare le eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuare e pianificare le necessarie azioni correttive
- pianificare lo sviluppo delle infrastrutture tecnologiche del sistema di conservazione e verifica i livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.

Il **Responsabile dei sistemi informativi per la conservazione** nominato da Unimatica-RGI è **Massimo Ortensi**.

Responsabile sviluppo e manutenzione del sistema di conservazione il quale si occupa di:

- coordinare lo sviluppo e la manutenzione delle componenti hardware e software del sistema di conservazione
- pianificare e monitorare i progetti di sviluppo del sistema di conservazione
- monitora gli SLA relativi alla manutenzione del sistema di conservazione
- interfacciarsi con il Produttore dei PDV relativamente alle modalità di trasferimento dei documenti, fascicoli informatici e aggregazioni documentali informatiche in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche
- gestire lo sviluppo di siti web e portali connessi al servizio di conservazione.

La **Responsabile dello sviluppo e manutenzione del sistema di conservazione** nominata da Unimatica-RGI è **Annachiara Coviello**.

Nell'attribuire ruoli e responsabilità Unimatica-RGI presta importante attenzione alle competenze delle risorse valutate, vanta infatti personale altamente specializzato e formato sulle tematiche legate alla conservazione e all'archiviazione digitale.

Tale personale è costantemente aggiornato sull'evoluzione della normativa e sugli aspetti tecnologici, grazie alla documentazione interna messa a disposizione dall'azienda e garantisce, inoltre, l'opportunità ai dipendenti di partecipare ad appositi corsi qualificanti di approfondimento, interni ed esterni.

[Torna al sommario](#)

4.1. Ruoli di ausilio al processo di conservazione

In ottemperanza a quanto previsto dal Regolamento (UE) 2016/679 Unimatica-RGI, al fine di garantire una maggior tutela dei dati propri e di quelli dei clienti, ha nominato un **Data Protection Officer** il quale si occupa di

- offrire idonea consulenza per progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali, interagendo coi sistemi di gestione aziendali, compreso il sistema di conservazione, per curare l'adozione di misure di sicurezza finalizzate alla tutela dei dati trattati dall'azienda, che soddisfino i requisiti di legge e per evitare i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

La **DPO** nominato da Unimatica-RGI è **Anna Veltri**.

[Torna al sommario](#)

4.2. Precedenti responsabili

Nominativo	Ruolo	Periodo
Silvano Ghedini	Responsabile servizio di conservazione	01-2004 – 06-2022

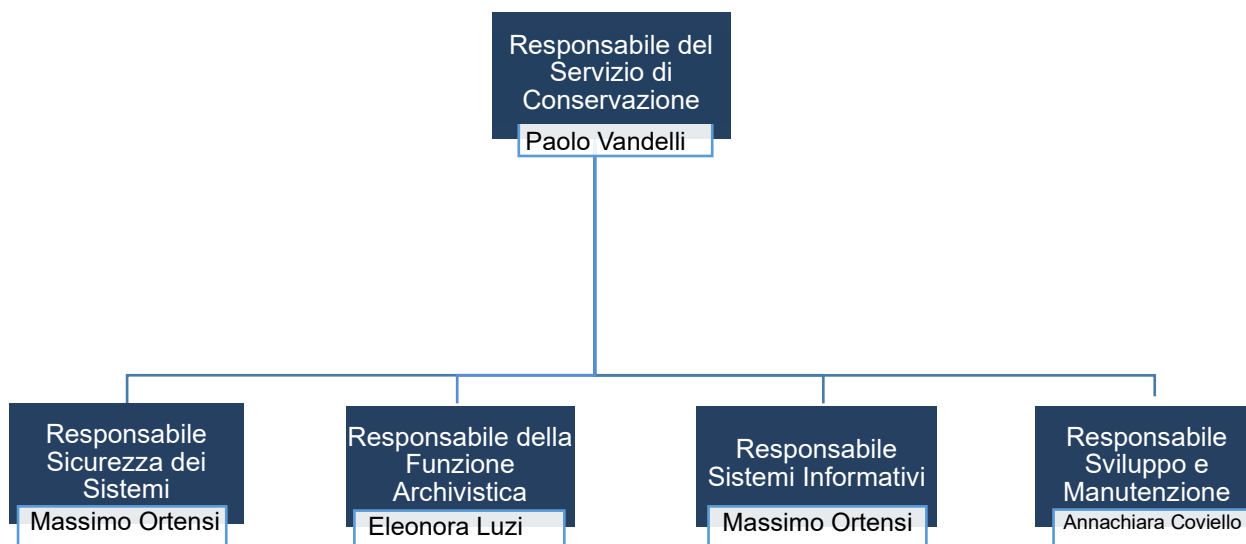
[Torna al sommario](#)

5. Struttura organizzativa per il servizio di conservazione

Il presente capitolo ha lo scopo di illustrare la struttura organizzativa del settore conservazione di Unimatica-RGI. L'espletamento di un processo di conservazione prevede una serie di complesse attività, pertanto la società si avvale di personale altamente qualificato e con esperienza decennale. Si riporta di seguito l'organigramma della struttura organizzativa e una sintetica descrizione¹ delle funzioni e delle responsabilità che intervengono nel processo di conservazione.

[Torna al sommario](#)

5.1. Organigramma



[Torna al sommario](#)

¹ La descrizione dettagliata del processo di conservazione è riportata nel capitolo 7 "[Il processo di erogazione del servizio di conservazione](#)".

5.2. Strutture organizzative

Nel presente paragrafo vengono descritte sinteticamente le fasi principali del processo di conservazione e le attività di gestione dei sistemi informativi, individuando per ciascuna di queste le figure che ne assumono le responsabilità.

Attività proprie di ciascun contratto di servizio			
Fase	Attività	Descrizione	Responsabilità
1	Attivazione del servizio di conservazione (a seguito della sottoscrizione del contratto).	Il Soggetto produttore invia una richiesta di attivazione del servizio che avviene in seguito alla compilazione del modulo "Scheda cliente" dove vengono dichiarati dettagli degli oggetti da conservare, come: dimensioni, frequenza invio, ecc.	RSC PM RFA RSM
2	Acquisizione, verifica e gestione dei Pacchetti di versamento e generazione del Rapporto di versamento.	Sui PdV vengono effettuate verifiche circa l'identificazione certa del Soggetto produttore, la firma digitale, formati e metadati sulla base di quanto concordato nella Fase 1. In caso di verifiche andate a buon fine viene generato il RdV, altrimenti viene generata la Comunicazione delle anomalie.	RSC RFA
3	Preparazione e gestione dei Pacchetti di archiviazione ² .	Gli oggetti versati vengono trasformati in PdA contenenti, oltre agli oggetti da conservare, l'IdPA ³ formato secondo le regole dello standard SInCRO. L'IdPA viene sottoscritto con firma digitale dal RSC e viene marcato temporalmente.	RSC RFA
4	Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta.	I PdD, vengono creati in base alle richieste dell'Utente. Possono essere visualizzati mediante interfaccia web, WS o, se richiesto, tramite memorizzazione su supporto.	RSC RFA PM
5	Scarto dei pacchetti di archiviazione	Prima della scadenza del periodo di conservazione, Unimatica-RGI contatta il Soggetto produttore il quale in caso di rescissione del contratto comunicherà in forma scritta la decisione. Unimatica-RGI eliminerà fisicamente i PdA. Per i PdA provenienti da enti pubblici o da archivi privati per i quali è stato dichiarato l'interesse culturale si terrà	RSC RFA PM

² Traduzione di Archival Information Package dal Modello OAIS Open Archival Information Standard che individua nel sistema di archiviazione tre diversi tipi di Pacchetti: Submission Information Package (SIP), Archival Information Package (AIP) e Dissemination Information Package (DIP).

³ Indice del pacchetto di archiviazione.

		conto dei massimari di scarto di questi e della decisione ultima della Soprintendenza archivistica.	
6	Chiusura del servizio di conservazione (al termine di un contratto)	Il Soggetto produttore comunicherà ad Unimatica-RGI la rescissione del contratto.	RSC PM

Attività proprie di gestione dei sistemi informativi

Fase	Attività	Descrizione	Responsabilità
1	Conduzione e manutenzione del sistema di conservazione	Le attività di manutenzione vengono svolte sia sui processi che sulle strutture hardware e software e viene condotta una quotidiana verifica delle attività sulle infrastrutture parallelamente ad una pianificazione delle eventuali procedure straordinarie da condurre in caso di anomalie.	RSM RSSI
2	Monitoraggio del sistema di conservazione	Viene effettuato il monitoraggio del sistema di Log che consente la registrazione degli accessi e degli eventi (operazioni). Tra le attività di monitoraggio rientrano anche la verifica dell'integrità degli archivi e la gestione delle anomalie.	RSC RFA RSSI
3	Change management	Vengono definite politiche, priorità e tempistiche dell'adeguamento all'evoluzione tecnologica affinché il sistema di conservazione possa garantire nel tempo integrità, disponibilità e sicurezza.	RFA RSI
4	Verifica periodica di conformità a normativa e standard di riferimento	La conformità a normativa e standard è costantemente monitorata ed eventualmente aggiornata.	RSC RSSI

Legenda

RSC	Responsabile del Servizio di Conservazione
RSSI	Responsabile Sicurezza dei Sistemi Informativi per la Conservazione
PM	Privacy Manager
RFA	Responsabile Funzione Archivistica per la Conservazione
RSI	Responsabile Sistemi Informativi per la Conservazione
RSM	Responsabile Sviluppo e Manutenzione del Sistema di Conservazione

[Torna al sommario](#)

6. Oggetti sottoposti a conservazione

Unimatica-RGI mediante il proprio sistema di conservazione Unistorage, sviluppato integralmente dalla società, è in grado di accettare e gestire, come richiesto ai sensi dell'art. 44, comma 1-bis, del CAD⁴,

- a) I fascicoli informatici chiusi e le serie informatiche chiuse,
- b) i fascicoli informatici e le serie non ancora chiusi accettando i documenti in essi contenuti sulla base di specifiche esigenze del soggetto produttore. In particolare, in questo caso, il Titolare e il Conservatore garantiscono specifico monitoraggio al fine di evitare rischi di obsolescenza tecnologica che possono sopravvenire prima della chiusura.

Unistorage è predisposto per accettare aggregazioni documentali e tutte le tipologie di documenti informatici relativi a diversi ambiti applicativi.

In accordo con il soggetto produttore, Unimatica-RGI si riserva infatti la facoltà di accettare qualsiasi tipologia documentale. L'indicazione delle tipologie documentali, compresa la gestione di queste, verrà indicata nella scheda cliente allegata al contratto stipulato con il soggetto produttore.

Unimatica-RGI accetta e conserva solo documenti informatici. Il sistema di conservazione permette l'acquisizione sia di documenti firmati digitalmente, sia di documenti non firmati. Entrambe le tipologie entrano nel medesimo processo di Ingestion. Con l'ausilio del Responsabile del servizio di conservazione, è il Soggetto produttore a definire nella scheda cliente le modalità di trattamento dei documenti firmati o non firmati.

[Torna al sommario](#)

6.1. Metadati

Come previsto dal par. 4.1 delle Linee guida, il sistema di conservazione assicura dalla presa in carico fino all'eventuale scarto, la conservazione di oggetti digitali tramite l'adozione di regole, procedure e tecnologie, necessarie al mantenimento delle caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità.

Al fine di rendere agevole ed efficiente la ricerca di un documento, di un fascicolo, o di un'aggregazione documentale informatica conservati, è necessario corredare tali oggetti da un set di metadati che ne descrivono il contenuto e lo identificano all'interno del sistema. Unimatica-RGI, in piena conformità alle Linee guida e all'Allegato 5, garantisce l'acquisizione, la gestione e la conservazione di:

- Metadati del documento informatico
- Metadati del documento amministrativo informatico
- Metadati delle aggregazioni documentali informatiche
- Metadati del documento informatico di natura fiscale e contabile

Nei paragrafi successivi si elencano per ogni tipologia, a titolo esemplificativo e non esaustivo, i metadati obbligatori individuati dalle Linee guida. Per tutti i dettagli specifici sul lessico, campi e schemi si rimanda alle schede di dettaglio presenti all'interno dell'*Allegato 5* alle Linee guida e

⁴ L'art. 44, comma 1-bis, del CAD prevede che: "[...] Almeno una volta all'anno il responsabile della gestione dei documenti informatici provvede a trasmettere al sistema di conservazione i fascicoli e le serie documentarie anche relative a procedimenti non conclusi"

all'Elenco AgID "L'utilizzo dei metadati del documento informatico - I metadati del documento informatico di natura fiscale e contabile"

[Torna al sommario](#)

6.1.1 Metadati del documento informatico

Di seguito vengono elencati i metadati, ed i principali campi e sottocampi *obbligatori* del documento informatico:

IdDoc: Identificativo univoco e persistente associato in modo univoco e permanente al documento informatico in modo da consentirne l'identificazione

Il metadato è costituito dai seguenti:

- Impronta: sottocampo in cui viene memorizzato l'hash del documento
- Algoritmo: sottocampo nel quale deve essere indicata la tipologia dell'algoritmo applicato riportati nell'Allegato 6 delle Linee Guida nella tabella 1 del paragrafo 2.2 "Regole di processamento"
- Identificativo: come da sistema di identificazione formalmente definito

Modalità di formazione: modalità di generazione del documento informatico

Sono previste le seguenti modalità:

- creazione tramite l'utilizzo di strumenti software che assicurino la produzione di documenti nei formati previsti nell'Allegato 2 delle Linee Guida;
- acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;
- memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;
- generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica

Tipologia documentale: metadato funzionale che indica la tipologia del documento tra quelle trattate per lo svolgimento delle attività

Metadato testuale libero per indicare le tipologie documentali trattate (ad esempio, fatture, delibere, determine, etc)

Dati di registrazione: Metadato che comprende i dati di registrazione del documento sia nel caso di documento protocollato che non protocollato. Si intende per registrazione l'operazione che, in senso lato, associa ad un documento una data e un numero. In tale ottica, quindi potrebbe non essere identificabile uno specifico registro, ma sono sempre identificabili una data di registrazione e un numero di registrazione del documento.

Sono previsti i seguenti campi:

- Tipologia di flusso: indica se si tratta di un documento in uscita, in entrata o interno.
- Tipo registro: indica il sistema di registrazione adottato: protocollo ordinario/protocollo emergenza, o Repertorio/Registro.
- Data: è la data associata al documento all'atto della registrazione
- Numero documento: Numero identificativo del documento nel caso di documento non protocollato (ad esempio, numero fattura), numero di protocollo nel caso di documento protocollato.
- Codice Registro: Identificativo del registro nel caso in cui il tipo registro sia protocollo ordinario/protocollo emergenza, o Repertorio/Registro.

Soggetti: indica il metadato che consente di individuare le informazioni relative a tutti i soggetti coinvolti e competenti sul documento a vario titolo e definiti dal campo Ruolo.

Sono definiti i seguenti attributi:

- Ruolo: consente di indicare, a seconda delle necessità, l'autore del documento, il mittente, il destinatario, l'assegnatario. Al fine di rendere i dati di registrazione univoci deve essere sempre indicato il Soggetto che effettua la registrazione del documento (tipicamente l'Organizzazione che protocolla). Obbligatorio inoltre indicare almeno l'autore o il mittente. Nel caso di documento protocollato deve essere obbligatoriamente indicato il mittente.
- Tipo soggetto: consente di tipizzare i soggetti come persone fisiche, giuridiche, amministrazioni pubbliche (italiane ed estere). Il Tipo Soggetto = SW è indicabile solo se si è indicato il ruolo = "Produttore". Per ogni Tipo Soggetto sono indicati i metadati di riferimento

Chiave descrittiva: metadato funzionale volto a riassumere il contenuto del documento o comunque a chiarirne la natura.

È costituito da seguenti campi:

- Oggetto: testo libero

Allegati: Indica il numero di allegati al documento e, nell'eventualità che il numero di allegati indicati sia maggiore di zero, devono essere compilati, in modalità ricorsiva, i dati:

- IdDoc: Identificativo del documento relativo all'allegato
- Descrizione: Titolo dell'Allegato

Classificazione: classificazione del documento secondo il Piano di classificazione utilizzato da indicare sia nel caso di documento protocollato che nel caso di documento non protocollato (*facoltativo*, per le specifiche si rimanda all'Allegato 5)

Riservato: rappresenta il livello di sicurezza di accesso al documento:

- vero: se il documento è considerato riservato
- falso: se il documento non è considerato riservato

Consente di gestire gli accessi al documento al solo personale autorizzato.

Identificativo del formato: indica il formato del documento e la versione del software utilizzato per la creazione del documento stesso.

È costituito da:

- formato: secondo quanto previsto dall'Allegato 2 delle Linee Guida.
- prodotto software: prodotto software utilizzato per la creazione del documento e relativa versione, suddiviso a sua volta in tre sottocampi:
 - nome prodotto
 - versione prodotto
 - produttore

Verifica: heck di controllo presenza Firma elettronica, Sigillo, Marcatura temporale e Conformità copie immagine nelle modalità di formazione del documento informatico previste nelle Linee Guida.

Identificativo dell'Aggregazione documentale: identificativo univoco dell'Aggregazione come definito nel paragrafo dei Metadati delle aggregazioni documentali informatiche. Metadato ricorsivo (*facoltativo*, per le specifiche si rimanda all'Allegato 5).

Identificativo del Documento Primario: identificativo univoco e persistente del Documento primario (*obbligatorio nel caso in cui sia presente un documento primario*).

Nome del documento\file: nome del documento\file così come riconosciuto all'esterno.

Versione del documento: versione del documento.

Tracciatore modifiche documento: metadato volto a tracciare la presenza di operazioni di modifica effettuate sul documento e la data in cui esse sono state effettuate. L'autore delle modifiche è tracciato nel metadato "Soggetti" con il ruolo "Operatore" (*obbligatorio nel caso di versione > 1 o in caso di annullamento*).

Tempo di conservazione: tempo di conservazione del documento desunto dal Piano di conservazione integrato con il Piano di classificazione (ove presenti) o prescritto dalla normativa salvo contenzioso. In generale il tempo di conservazione a livello di singolo documento deve essere indicato solo qualora esso presenti un tempo di conservazione distinto da quello assegnato all'aggregazione documentale informatica a cui il documento stesso appartiene. Espresso in numero di anni, il valore 9999 indica un tempo di conservazione "Permanente" (*facoltativo*).

Note: eventuali indicazioni aggiuntive utili ad indicare situazioni particolari (*facoltativo*).

Nella scheda cliente è possibile personalizzare ed indicare i set di metadati in base alle esigenze del soggetto produttore e alle diverse tipologie documentali conservate. In un'apposita tabella il cliente specificherà i metadati di proprio interesse.

[Torna al sommario](#)

6.1.2 Metadati del documento amministrativo informatico

Di seguito vengono elencati i metadati, ed i principali campi e sottocampi obbligatori del documento informatico:

IdDoc: Identificativo univoco e persistente associato in modo univoco e permanente al documento informatico in modo da consentirne l'identificazione

Il metadato è costituito dai seguenti:

- Impronta crittografica del documento: a sua volta suddiviso in:
 - Impronta: sottocampo in cui viene memorizzato l'hash del documento
 - Algoritmo: sottocampo nel quale deve essere indicata la tipologia dell'algoritmo applicato riportati nell'Allegato 6 delle Linee Guida nella tabella 1 del paragrafo 2.2 "Regole di processamento"
- Identificativo: come da sistema di identificazione formalmente definito
- Segnatura: segnatura di protocollo, da indicare obbligatoriamente nel caso di documento amministrativo protocollato, a sua volta strutturato come da Allegato 6 delle Linee Guida.

Modalità di formazione: modalità di generazione del documento informatico

Sono previste le seguenti modalità:

- creazione tramite l'utilizzo di strumenti software che assicurino la produzione di documenti nei formati previsti nell'Allegato 2 delle Linee Guida;
- acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;
- memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;
- generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica

Soggetti: indica il metadato che consente di individuare le informazioni relative a tutti i soggetti coinvolti e competenti sul documento a vario titolo e definiti dal campo Ruolo.

Sono definiti i seguenti attributi:

- Ruolo: consente di indicare, a seconda delle necessità, l'autore del documento, il mittente, il destinatario, l'assegnatario. Al fine di rendere i dati di registrazione univoci deve essere sempre indicato il Soggetto che effettua la registrazione del documento (tipicamente l'Organizzazione che protocolla). Obbligatorio inoltre indicare almeno l'autore o il mittente. Nel caso di documento protocollato deve essere obbligatoriamente indicato il mittente.
- Tipo soggetto: consente di tipizzare i soggetti come persone fisiche, giuridiche, amministrazioni pubbliche (italiane ed estere). Il Tipo Soggetto = SW è indicabile solo se si è indicato il ruolo = "Produttore". Per ogni Tipo Soggetto sono indicati i metadati di riferimento

Chiave descrittiva: metadato funzionale volto a riassumere il contenuto del documento o comunque a chiarirne la natura.

È costituito da seguenti campi:

- Oggetto: testo libero

Allegati: Indica il numero di allegati al documento e, nell'eventualità che il numero di allegati indicati sia maggiore di zero, devono essere compilati, in modalità ricorsiva, i dati:

- IdDoc: Identificativo del documento relativo all'allegato
- Descrizione: Titolo dell'Allegato

Classificazione: classificazione del documento secondo il Piano di classificazione utilizzato da indicare sia nel caso di documento protocollato che nel caso di documento non protocollato

- Indice di classificazione: codifica del documento secondo il Piano di classificazione utilizzato
- Descrizione: descrizione per esteso dell'Indice di classificazione indicato.

Riservato: rappresenta il livello di sicurezza di accesso al documento:

- vero: se il documento è considerato riservato
- falso: se il documento non è considerato riservato

Consente di gestire gli accessi al documento al solo personale autorizzato.

Identificativo del formato: indica il formato del documento e la versione del software utilizzato per la creazione del documento stesso.

È costituito da:

- formato: secondo quanto previsto dall'Allegato 2 delle Linee Guida.
- prodotto software: prodotto software utilizzato per la creazione del documento e relativa versione, suddiviso a sua volta in tre sottocampi:
 - nome prodotto
 - versione prodotto
 - produttore

Verifica: check di controllo presenza Firma elettronica, Sigillo, Marcatura temporale e Conformità copie immagine nelle modalità di formazione del documento informatico previste nelle Linee Guida.

Identificativo dell'Aggregazione documentale: identificativo univoco dell'Aggregazione come definito nel paragrafo dei Metadati delle aggregazioni documentali informatiche. Metadato ricorsivo.

Identificativo del Documento Primario: identificativo univoco e persistente del Documento primario (*obbligatorio nel caso in cui sia presente un documento primario*).

Nome del documento\file: nome del documento\file così come riconosciuto all'esterno.

Versione del documento: versione del documento.

Tracciatore modifiche documento: metadato volto a tracciare la presenza di operazioni di modifica effettuate sul documento e la data in cui esse sono state effettuate. L'autore delle modifiche è tracciato nel metadato "Soggetti" con il ruolo "Operatore" (*obbligatorio nel caso di versione > 1 o in caso di annullamento*).

Tempo di conservazione: tempo di conservazione del documento desunto dal Piano di conservazione integrato con il Piano di classificazione (ove presenti) o prescritto dalla normativa salvo contenzioso. In generale il tempo di conservazione a livello di singolo documento deve essere indicato solo qualora esso presenti un tempo di conservazione distinto da quello assegnato all'aggregazione documentale informatica a cui il documento stesso appartiene. Espresso in numero di anni, il valore 9999 indica un tempo di conservazione "Permanente" (*facoltativo*).

Note: eventuali indicazioni aggiuntive utili ad indicare situazioni particolari (*facoltativo*).

Nella Scheda Cliente predisposta da Unimatica-RGI, è possibile personalizzare ed indicare i set di metadati in base alle esigenze del soggetto produttore e alle diverse tipologie documentali conservate. In un'apposita tabella il cliente specificherà i metadati di proprio interesse.

6.1.3 Metadati delle aggregazioni documentali informatiche

Di seguito vengono elencati i metadati, ed i principali campi e sottocampi obbligatori delle aggregazioni documentali informatiche:

Identificativo dell'Aggregazione documentale: si tratta di una sequenza di caratteri alfanumerici associata in modo univoco all'aggregazione documentale informatica in modo da consentirne l'identificazione, indica se si tratta di un Fascicolo o di una Serie Documentale o di una Serie di Fascicoli.

Il fascicolo è una 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.

Le serie documentarie sono costituite da documenti singoli accorpatis per ragioni funzionali in base alla tipologia di riferimento.

Le serie di fascicoli sono costituite da fascicoli accorpatis per ragioni funzionali in base alla classe di riferimento o alla tipologia di fascicoli.

Sono definiti i seguenti attributi:

- TipoAggregazione
 - Fascicolo
 - Serie Documentale
 - Serie Di Fascicoli
- IdAggregazione: come da sistema di identificazione formalmente definito

Tipologia fascicolo: I fascicoli sono organizzati per:

- **affare:** conserva i documenti relativi a una competenza non proceduralizzata, ma che nella consuetudine amministrativa la PA deve concretamente portare a buon fine. Il fascicolo per affare ha una data di apertura e una durata circoscritta.
- **attività:** comprende i documenti prodotti nello svolgimento di un'attività amministrativa semplice che implica risposte obbligate o meri adempimenti, per la quale quindi non è prevista l'adozione di un provvedimento finale. Ha in genere durata annuale.
- **persona fisica:** comprende tutti i documenti, anche con classifiche diverse, che si riferiscono a una persona fisica. Quasi sempre i fascicoli intestati alle persone restano correnti per molti anni, costituendo serie aperte.
- **persona giuridica:** comprende tutti i documenti, anche con classifiche diverse, che si riferiscono a una persona giuridica. Quasi sempre i fascicoli intestati alle persone restano correnti per molti anni, costituendo serie aperte
- **procedimento amministrativo:** conserva una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un provvedimento amministrativo.

Soggetti: indica il metadato che consente di individuare le informazioni relative a tutti i Soggetti che, a vario titolo, sono coinvolti nella costituzione dell'aggregazione.

Sono definiti quindi i seguenti attributi:

- Ruolo:
 - Amministrazione titolare
 - Amministrazioni partecipanti
 - Assegnatario
 - Soggetto intestatario persona fisica
 - Soggetto intestatario persona giuridica
 - RUP: da indicare solo in caso di TipoAggregazione = 'Fascicolo'
- Tipo soggetto: consente di tipizzare i soggetti come persone fisiche, giuridiche, amministrazioni pubbliche (italiane ed estere) in funzione del Ruolo. Per ogni tipo soggetto sono indicati i metadati di riferimento. Nel caso in cui sia stato definito un Ruolo=RUP è obbligatorio indicare anche l'UOR corrispondente.

Assegnazione: indica il metadato che consente di individuare le informazioni relative all'assegnazione per conoscenza o per competenza. I Soggetti indicati in questo metadato devono essere stati dichiarati nel metadato Soggetti. Sono definiti quindi i seguenti attributi:

- Tipo assegnazione (obbligatorio in caso di fascicolo)
- Soggetto assegnatario (obbligatorio in caso di fascicolo)
- Data inizio assegnazione (obbligatorio in caso di fascicolo)
- Data fine assegnazione (facoltativo)

Il metadato ha una struttura ricorsiva.

Data Apertura: data di apertura dell'aggregazione documentale.

Classificazione: classificazione dell'aggregazione:

- Indice di classificazione: Codifica del documento secondo il Piano di classificazione utilizzato
- Descrizione: Descrizione per esteso dell'Indice di classificazione indicato.
- Piano di classificazione: se presente, riportare eventualmente l'URI di pubblicazione del Piano di classificazione (facoltativo)

Progressivo: progressivo numerico calcolato nell'ambito della chiave della classificazione o in ordine cronologico nell'ambito dell'anno.

Chiave descrittiva: metadato funzionale volto a chiarire la natura del fascicolo o della serie.

È costituito da seguenti campi:

- Oggetto: testo libero

Data Chiusura: data di chiusura dell'aggregazione documentale.

Procedimento Amministrativo: metadato funzionale volto ad indicare il procedimento a cui il fascicolo afferisce, nonché lo stato di avanzamento e le relative fasi.

È costituito da seguenti campi:

- Materia\ Argomento\ Struttura: indicare la materia o l'argomento o la struttura per la quale sono stati catalogati i procedimenti amministrativi
- Procedimento: denominazione del Procedimento
- Catalogo procedimenti: URI di pubblicazione del catalogo
- Fasi: a sua volta suddiviso, in una struttura ricorsiva:
 - Tipo Fase
 - Preparatoria
 - Istruttoria
 - Consultiva
 - decisoria o deliberativa
 - integrazione dell'efficacia
 - Data inizio fase
 - Data fine fase (facoltativo)

da "Data inizio fase" e "Data fine fase" deve considerarsi dinamico, destinato ad essere aggiornato con lo stato di avanzamento dell'iter del procedimento/processo.

Indice documenti: elenco degli identificativi dei documenti contenuti nell'aggregazione, definiti secondo le regole indicate per i documenti informatici o i documenti amministrativi informatici. Metadato ricorsivo.

È costituito da seguenti campi:

- Tipo documento
 - documento amministrativo informatico
 - documento informatico
- IdDoc
 - se documento amministrativo informatico
IdDoc come definito nel precedente paragrafo dei Metadati del documento amministrativo informatico
 - se documento informatico
IdDoc come definito nel precedente paragrafo dei Metadati del documento informatico

Posizione fisica Aggregazione Documentale: posizione fisica dell'aggregazione. Nel caso di fascicoli ibridi indica la posizione della componente cartacea del fascicolo.

6.1.4 Metadati del documento informatico di natura fiscale e contabile

In relazione alla valorizzazione dei metadati specifici del documento informatico di natura fiscale e contabile si rimanda alle specifiche descritte nelle istruzioni dal titolo *1 metadati del documento informatico di natura fiscale e contabile* pubblicato nella sezione Linee guida del sito di AgID.

[Torna al sommario](#)

6.2 Formati

Unistorage, in conformità all'*Allegato 2 "Formati di file e riversamento"* alle Linee guida AgID, accetta e gestisce formati aperti, non proprietari, standard de iure, estendibili, parlanti, completamente robusti, indipendenti dal dispositivo e che garantiscano i principi dell'interoperabilità.

Tuttavia, in accordo con il soggetto produttore, Unimatica-RGI permette anche l'accettazione di formati non esplicitati nell'*Allegato 2*. Infatti qualora l'ordinamento giuridico preveda degli obblighi relativamente all'uso di formati specifici per alcuni Titolari, questi assolvendo tali obblighi, sono chiamati ad effettuare una valutazione di interoperabilità utile anche per garantire la conservazione e la fruibilità degli stessi nel tempo. L'indicazione di tali formati, compresa la gestione di questi, verrà indicata nella scheda cliente.

[Torna al sommario](#)

6.2.1 Riversamento

Unistorage, in relazione all'obsolescenza dei formati, tiene un censimento dei formati di file ricevuti in conservazione a seguito di un'attività di ingestione (compreso il recupero da precedente conservatore). Il responsabile del servizio di conservazione, assieme al responsabile della funzione archivistica, al responsabile sviluppo e manutenzione del sistema di conservazione e al responsabile sicurezza dei sistemi per la conservazione, con cadenza non superiore ai 5 anni, fatta una fotografia dei formati di file censiti al momento sul sistema, ne valuta il grado di obsolescenza.

In fase di analisi dei formati, come da procedura stabilita, per ogni formato si attribuisce un grado di obsolescenza, basandosi sulle caratteristiche di apertura, sicurezza, portabilità, funzionalità,

supporto allo sviluppo e diffusione. Al termine della verbalizzazione di questo processo di verifica, a fronte di evidenze di formati di file per cui è impossibile individuare soluzioni in grado di rappresentare fedelmente il contenuto di questi file, il responsabile del servizio di conservazione attiva il processo di riversamento dei file appartenenti ai formati risultati a rischio di obsolescenza, previa certificazione di processo.

Per tutti i dettagli inerenti l'intero processo di gestione del riversamento si rimanda al documento di sistema "PRO_CONS01 - Procedure di Conservazione".

[Torna al sommario](#)

6.3 Struttura dati del Pacchetto di versamento

Unimatica-RGI mediante il prodotto applicativo UniStorage, con la supervisione del Responsabile del servizio di conservazione permette un duplice iter per la ricezione dei Pacchetti di Versamento: ricezione dei file tramite canale SSH File Transfert Protocol e ricezione tramite sistema Web service.

- La ricezione mediante SSH File Transfert Protocol prevede l'upload del Pacchetto di versamento composto da un file indice e da un insieme di file, in formato .zip. Per maggiori dettagli circa la struttura dei Pacchetti di versamento, fare riferimento al documento Flusso per la conservazione dei Documenti in Unistorage.
- La ricezione tramite Sistema Web Service è possibile da qualsiasi piattaforma che permetta di eseguire e ricevere chiamate Web Service conformi allo standard WS-I Basic Profile 1.0. Con questo servizio il sistema di conservazione riceve singoli documenti ed eventuali allegati, ne verifica la firma digitale se presente e ne gestisce la conservazione autentica. Per maggiori dettagli circa la ricezione degli oggetti digitali tramite Sistema Web Service si rimanda al documento "Specifiche del servizio web per la consegna anticipata di documenti nel Sistema di conservazione".

[Torna al sommario](#)

6.4 Struttura dati del Pacchetto di archiviazione

Terminato il processo di acquisizione dei Pacchetti di versamento, il prodotto applicativo UniStorage sotto la supervisione del Responsabile del servizio di conservazione e del Responsabile della funzione archivistica provvede alla creazione dei Pacchetti di archiviazione e dell'Indice del pacchetto di archiviazione previsto dallo standard UNI 11386 SInCRO – Supporto all'interoperabilità nella conservazione e nel recupero degli oggetti digitali.

I Pacchetti di archiviazione contengono⁵:

- l'oggetto o gli oggetti da conservare;
- l'Indice del Pacchetto di archiviazione, formato secondo le regole dettate dallo Standard UNI 11386 SInCRO – Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.

Tutti i pacchetti di archiviazione prodotti fino al 31 dicembre 2021 implementano lo standard UNI 11386:2010 SInCRO. A partire dal 1° gennaio 2022 viene applicata la versione 2020 dello standard.

⁵ Sono elencate le caratteristiche indicate nell'allegato 4 al DPCM 3 dicembre 2013 Regole tecniche in materia di sistema di conservazione.

[Torna al sommario](#)

6.5 Struttura dati del Pacchetto di distribuzione

La produzione di Pacchetti di distribuzione avviene in seguito alla richiesta da parte dell'Utente.

L'esibizione del materiale di interesse avviene via interfaccia web o mediante memorizzazione su supporto ottico. La descrizione dettagliata delle procedure è indicata nel capitolo 7 "Il processo di erogazione del servizio di conservazione", Fase 6.

Per quanto riguarda i Pacchetti di distribuzione memorizzati su supporto ottico, questi coincidono con i Pacchetti di archiviazione, come previsto delle Regole tecniche in materia di sistemi di conservazione, ma saranno corredati di informazioni aggiuntive necessarie per la creazione dei DVD, CD, ecc. nel caso di richiesta di esibizione da parte dell'Utente.

UniStorage consente la produzione di supporti rimovibili che possono essere forniti all'Utente.

In ogni supporto vengono trasferiti Pacchetti di distribuzione chiamati "Registrazioni", contenenti sia gli oggetti che l'insieme delle evidenze di conservazione.

La registrazione generata è auto-esplicativa, intendendo con questo che i dati sono affiancati da indici e informazioni di riferimento tali da poter permettere la comprensione del contenuto anche da programmi esterni al sistema di conservazione.

La registrazione è contenuta in una directory, il cui nome contiene un'indicazione del blocco dei documenti e data/ora dell'inizio della creazione della registrazione stessa.

Contenuto della directory della registrazione:

- file README.txt
- file autorun
- icona
- directory chrome
- directory chrome_profile
- directory viewer

I vari Pacchetti di distribuzione a seconda delle dimensioni possono venire raggruppati in volumi auto consultanti, la struttura dei volumi è la seguente:

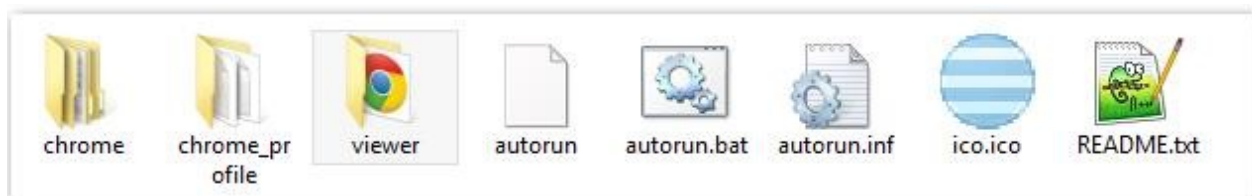


Figura 1 - Struttura volumi

All'interno della directory viewer avremo una directory contenente i documenti suddivisi per Pacchetti. Questi volumi sono auto consultanti e permettono la ricerca e visualizzazione dei documenti conservati, i metadati associati e le marche di conservazione.

[Torna al sommario](#)

7. Il processo di erogazione del servizio di conservazione

Il processo di conservazione eseguito da Unimatica-RGI adotta il modello standard OAIS - Open Archival Information System⁶ che definisce concetti e funzionalità degli archivi digitali. Lo schema seguente illustra brevemente gli aspetti principali di un generico processo di conservazione: il Soggetto produttore invia il Pacchetto di versamento, di cui ha piena responsabilità, al Soggetto conservatore il quale provvede a trasformarlo in Pacchetto di archiviazione. Ai fini dell'esibizione e della distribuzione richiesti dalla comunità di riferimento⁷, il Soggetto conservatore provvederà a creare i Pacchetti di distribuzione in una forma tale che venga garantita la corretta visualizzazione di questi.

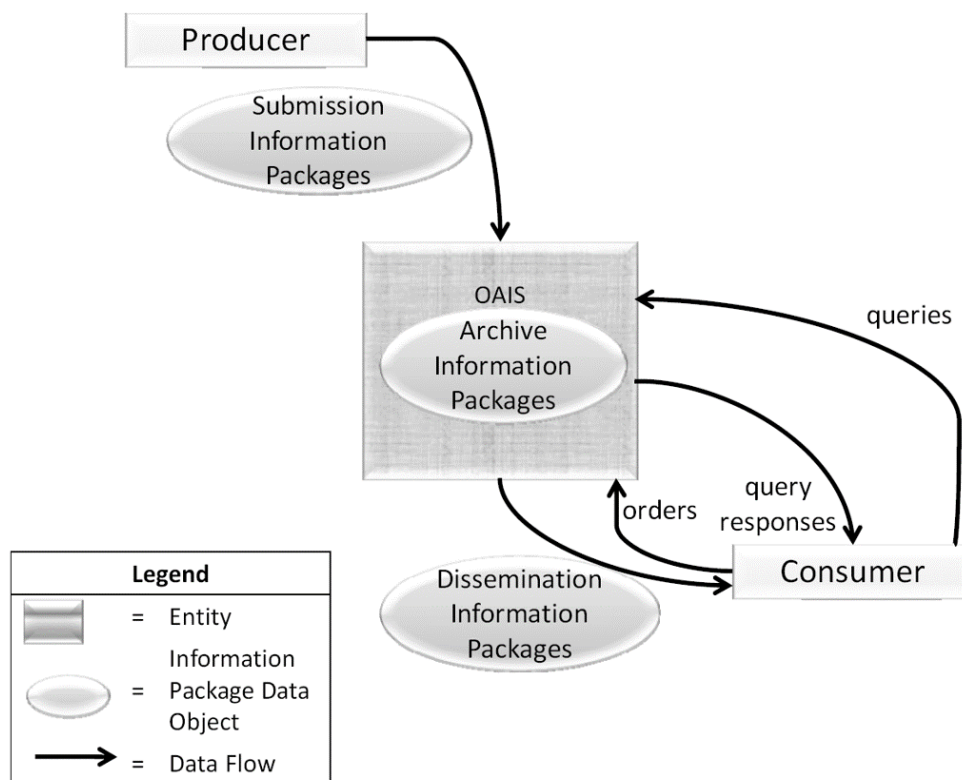


Figura 2 - Modello OAIS

[Torna al sommario](#)

⁶ L'Open Archival Information System è lo standard ISO per la conservazione a lungo termine di archivi digitali.

⁷ Comunità di riferimento: il sottoinsieme degli utenti in grado di comprendere autonomamente l'informazione archiviata nella forma in cui è conservata e resa disponibile dall'OAIS

7.1 Il processo di conservazione

Il servizio offerto da Unimatica-RGI ad ogni Soggetto produttore viene avviato al termine di un processo di attivazione che segue queste fasi fondamentali:

- condivisione di informazioni tecniche di richiesta configurazione e invio dei Pacchetti di versamento;
- verifiche sui Pacchetti di versamento e sugli oggetti in esso contenuti;
- accettazione dei Pacchetti di versamento e generazione del Rapporto di versamento di presa in carico;
- rifiuto dei Pacchetti di versamento e modalità di comunicazione delle anomalie;
- preparazione e gestione del Pacchetto di archiviazione;
- preparazione e gestione del Pacchetto di distribuzione ai fini dell'esibizione;

Ognuno degli step sopra indicati viene eseguito per ogni tipologia di configurazione richiesta.

Di seguito vengono dettagliate le fasi del processo.

[Torna al sommario](#)

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

In questa fase il Soggetto produttore veicola al Responsabile del servizio di conservazione, al Privacy Manager e al Responsabile della funzione archivistica la richiesta di attivazione del servizio per l'invio di Pacchetti di versamento. Le tre figure responsabili sopracitate, con l'ausilio del Responsabile dello sviluppo e della manutenzione, incaricato di curare l'interfaccia con il Soggetto produttore relativamente alle modalità di trasferimento dei documenti, valuteranno la domanda di acquisizione del servizio affinché venga accertato che i requisiti del Soggetto produttore siano compatibili con le policy di Unimatica-RGI

L'attivazione del servizio avviene attraverso la compilazione del Modulo 'Scheda cliente'. In particolare, tale modulo deve essere compilato con le seguenti informazioni:

- ragione sociale;
- indirizzo;
- partita iva;
- e-mail
- oggetti documentali gestiti
- tipo di protocollo da utilizzare per lo scambio dei Pacchetti.
- metadati specifici di tipologia
- utenze da abilitare per l'accesso al portale di distribuzione.

Per ogni Pacchetto di versamento dichiarato dal Soggetto produttore, è possibile definire:

- i volumi in termini di numero documenti annui previsti da gestire e spazio di occupazione previsto per i dati da Conservare (GB);

- la dimensione massima del Pacchetto di versamento;
- la frequenza di invio dei Pacchetti;

Il Responsabile del servizio di conservazione, valuterà in accordo con il Privacy manager, con il Responsabile della funzione archivistica e con il Responsabile dello sviluppo e della manutenzione la domanda di acquisizione del servizio collaborando con il Soggetto produttore guidandolo nella compilazione della domanda per l'attivazione del servizio.

Il Responsabile del servizio di conservazione e il Responsabile della funzione archivistica una volta ricevuta la richiesta, si impegnano a valutarne l'impatto stimando la data di evasione e fornendo al Soggetto produttore una pianificazione delle fasi successive. Se la richiesta di configurazione implica un aggravio di costi, verrà fornita parallelamente al Soggetto produttore la quotazione economica dell'attività redatta dal Referente Commerciale di Unimatica-RGI

L'acquisizione dei Pacchetti di versamento avviene mediante due canali: tramite SSH File Transfert Protocol e tramite canale Web service descritti dettagliatamente nel capitolo "Oggetti sottoposti in conservazione", paragrafo 6.3.

Ad ogni attivazione verranno consegnate le credenziali per accedere all'applicativo web reso disponibile da Unimatica-RGI, in base ai dati presenti nella Scheda cliente. Tale accesso garantirà la piena esibizione dei Pacchetti di distribuzione.

[Torna al sommario](#)

7.3 Verifiche effettuate sui Pacchetti di versamento e sugli oggetti in esso contenuti

I parametri gestionali del Pacchetto di versamento vengono verificati e messi a punto dal Responsabile del servizio di conservazione e dal Responsabile della funzione archivistica in accordo con il Soggetto produttore. Le verifiche effettuate sui Pacchetti di versamento sono le seguenti:

- **identificazione certa del Soggetto produttore;**
- verifica delle **firme digitali** se presenti mediante un controllo crittografico dell'integrità del documento e della validità formale delle firme stesse. In un secondo momento viene verificata l'identità del sottoscrittore. Se una chiave privata sia stata usata in una firma è verificabile, mediante processo crittografico, con la corrispondente chiave "pubblica". Le chiavi pubbliche sono riportate nei "certificati di firma digitale", documenti informatici anch'essi, che definiscono anche i dati d'identità del sottoscrittore. I certificati sono a loro volta firmati da una autorità di certificazione emittente (C.A. - Certification Authority). In generale si risalirà la catena di certificazione fino a raggiungere un "certificato fidato", ovvero pubblicamente noto. Tra le evidenze informatiche che Unimatica-RGI conserva ci sono, per ogni Pacchetto, tutti i certificati a vario modo coinvolti nelle catene di certificazione necessarie alle verifiche di firma digitale. Questo consente di costituire un insieme "auto-contenuto" di evidenze che possono essere verificate anche a posteriori. Si può anche verificare il caso che l'autorità emittente non sia direttamente un'autorità pubblicamente nota, ma che esista una "catena di certificazione" (trust chain) per cui l'autorità di un certificato vada a sua volta identificata risalendo ad un'autorità terza.

- verifica che i **formati** degli oggetti da conservare siano conformi con quanto dichiarato nella scheda cliente e nell'Allegato 2 alle Linee guida per la Formazione, gestione e conservazione dei documenti informatici. Alla ricezione del documento il sistema, attraverso l'uso di una libreria WAZFORMAT, la cui procedura utilizzerà un metodo di indagine diretta con tecniche euristiche, riconosce il formato controllando il valore descritto nel magic number. Questo passaggio permette di associare il formato al documento per garantirne la corretta visualizzazione e quindi leggibilità utilizzando gli opportuni i visualizzatori.
- relativamente alle verifiche dei **metadati** sono previste tre livelli di controllo:
 - o *strict*: l'assenza di anche solo un metadato obbligatorio (Allegato 5 alle Linee guida) comporta la restituzione di un errore alla richiesta di versamento ed il documento non viene conservato
 - o *permissive*: l'assenza di metadati obbligatori (Allegato 5 alle Linee guida) viene segnalata con un warning, ma il processo di conservazione prosegue generando i metadati assenti con un valore nullo.
 - o *skip*: applicato a tutti i soggetti produttori non vincolati alla normativa italiana (Allegato 5 alle Linee guida). In questo caso i metadati obbligatori sono concordati con il soggetto produttore in base alle buone prassi o ai vincoli normativi del paese di origine.

[Torna al sommario](#)

7.4 Accettazione dei Pacchetti di versamento e generazione del Rapporto di versamento di presa in carico

L'esito positivo delle verifiche effettuate sui Pacchetti di versamento viene registrato in un Rapporto di versamento di presa in carico. Il Rapporto conterrà un'impronta del file originale comprensivo di algoritmo con la quale tale impronta viene calcolata (hash) e un riferimento temporale certificato che costituisce evidenza dell'esistenza e dell'esatta composizione del Rapporto collegato all'istante indicato (Tcons).

Apponendo un timestamp al Rapporto di versamento, lo si "sigilla" e contemporaneamente si fissa il riferimento temporale. Tale procedimento costituisce un riferimento temporale certificato per il Rapporto di versamento.

Il Rapporto di versamento attesta la corretta esecuzione del processo di immissione dei Pacchetti, ha la funzione di raccogliere evidenze indirette di tutti i documenti del Pacchetto e garantisce due principali funzioni:

- la possibilità di provare l'integrità dei dati di ogni file contenuto nel pacchetto,
- di permettere il controllo dell'integrità per ogni file in modo separato, senza creare un'interdipendenza tra i file ai fini dell'esibizione e del controllo.

Il Rapporto di versamento è un file in formato XML che riporta, per ognuno dei file inclusi nel Pacchetto, alcune informazioni tra cui un "URN" (unified resource name) e un "hash". L'URN è una stringa univoca che identifica l'oggetto digitale, mentre l'hash è un'impronta del documento, ovvero una sequenza di bit che può essere ricavata dal file in modo ripetibile e standardizzato e che garantisce una corrispondenza esatta col contenuto originale (in modo pratico possiamo dire di avere la garanzia che a due file differenti corrispondono sempre due impronte distinte).

La modalità di conservazione mediante Rapporto di versamento permette di verificare l'integrità di ogni singolo file, a prescindere da tutti gli altri file conservati nello stesso pacchetto. Infatti sarà

sufficiente essere in possesso di un file “candidato” e conoscere il suo URN identificativo per poter eseguire la funzione di hash e confrontare l'impronta ricalcolata con la stringa riportata nel Rapporto. In questa fase vengono associate all'indice tutte le evidenze di autenticità delle firme digitali che verranno verificate all'istante del riferimento temporale:

- i certificati di firma di tutte le firme presenti nel Pacchetto di versamento,
- tutti i certificati appartenenti alle catene di certificazione (trusting chain),
- le liste di revoca dei singoli certificati (CRL).

Il Rapporto di versamento viene conservato all'interno del sistema garantendone l'ininterrotta custodia e la non modificabilità.

[Torna al sommario](#)

7.5 Rifiuto dei Pacchetti di versamento e modalità di comunicazione delle anomalie

Le verifiche effettuate sui Pacchetti di versamento possono risultare negative. Nei casi in cui anche solo su uno dei controlli indicati nella fase 2 si dovesse riscontrare una mancanza o non corrispondenza di informazioni viene generato un file di Comunicazione delle anomalie che verrà comunicato mediante un file di esito al Soggetto produttore. Tale Comunicazione comprenderà i dettagli delle verifiche eseguite sui Pacchetti di versamento comprensive delle precisazioni sulle anomalie.

Le anomalie, in relazione a quanto descritto nella fase 2, possono essere identificate nell'assenza dei metadati obbligatori ovvero nella mancata corrispondenza di ciò che viene versato a quanto dichiarato dal soggetto produttore nella scheda cliente in termini di firma digitale, formati e metadati. Qualora l'anomalia venisse riscontrata soltanto su una parte di documenti inclusi nel Pacchetto di versamento, è facoltà del soggetto produttore decidere se bloccare l'intero pacchetto o soltanto i documenti segnalati. In questo ultimo caso i file conformi vengono inviati in conservazione e gli altri spediti successivamente mediante nuovo Pacchetto di versamento.

[Torna al sommario](#)

7.6 Preparazione e gestione dei Pacchetti di archiviazione

I Pacchetti versati in UniStorage, con la supervisione del Responsabile del servizio di conservazione e del Responsabile della funzione archivistica vengono raggruppati in Pacchetti di archiviazione. Questi pacchetti vengono assemblati dal sistema nei tempi e con i criteri di raggruppamento scelti e concordati con il Soggetto produttore, indicati nella Scheda Cliente (ad es. Pacchetti di archiviazione per tipologie documentali o in base alla cadenza temporale di consegna).

Il processo di costruzione dei Pacchetti di archiviazione, così come previsto dallo standard SInCRO UNI 11386– Supporto all'interoperabilità nella conservazione e nel recupero degli oggetti digitali, avviene con le seguenti modalità:

- individuazione dei documenti destinati a far parte del pacchetto di archiviazione sulla base dei criteri scelti. Tali criteri vengono concordati con il cliente e sono definiti nella scheda cliente e si possono basare sia su caratteristiche legate allo stato del documento, sia sui metadati.
- i Pacchetti di archiviazione vengono chiusi in seguito a due tipi di regole:

- automatiche: collocano nel pacchetto i documenti per i quali ci sia almeno un certificato di firma prossimo alla scadenza. Questa tipologia di regole ha la precedenza su quelle descritte nel punto successivo, le quali riguardano la dimensione massima del Pacchetto di archiviazione e il tempo limite oltre il quale un Pacchetto di archiviazione deve essere forzatamente chiuso,
- attuate dal Responsabile del servizio di conservazione in accordo con il soggetto produttore: definite nella scheda cliente.

Nei casi in cui i Pacchetti di archiviazione contengano referti sanitari, questi vengono crittografati mediante funzione crittografica della suite standard del linguaggio Java. In particolare è definita nel package crypto di JCE e impiega l'algoritmo AES a 128 bit ECB.

I Pacchetti di archiviazione vengono sottoscritti con firma digitale dal Responsabile del servizio di conservazione e marcati temporalmente.

La sottoscrizione dei Pacchetti di archiviazione effettuata da Unimatica-RGI attesta esclusivamente la corretta esecuzione del processo di conservazione secondo la normativa vigente in materia di conservazione. Unimatica-RGI non è responsabile dell'errato contenuto informativo degli oggetti versati.

[Torna al sommario](#)

7.7 Preparazione e gestione dei Pacchetti di distribuzione ai fini dell'esibizione

La gestione dei Pacchetti di distribuzione fa capo al Responsabile del Servizio di Conservazione, al Responsabile della Funzione archivistica e al Privacy manager.

La produzione di Pacchetti di distribuzione avviene in seguito alla richiesta da parte dell'utente.

UniStorage, prevedendo la conservazione dei Pacchetti di archiviazione firmati, implementa un formato di composizione delle marche tale da permettere l'esibizione probatoria di un singolo documento. Quindi, ogni singolo file può essere esibito insieme ai suoi metadati, registrati nel data base, e alle sue prove di conservazione in maniera assolutamente INDIPENDENTE dagli altri documenti.

Unimatica-RGI permette l'accesso ai Pacchetti di distribuzione esclusivamente agli utenti autorizzati. I livelli di accesso vengono definiti in base alle esigenze delle richieste effettuate, rendendo disponibile soltanto il materiale richiesto grazie all'utilizzo di filtri predefiniti che selezionano i canali previsti per la visualizzazione di un determinato pacchetto.

È possibile visualizzare i documenti tramite duplice canale:

- via web: i Soggetti produttori titolari dei documenti potranno ricercare e visualizzare tutti i documenti conservati direttamente sul portale di Unimatica-RGI attraverso l'apposita funzionalità. L'accesso avviene tramite il portale al quale è demandata la sicurezza e la gestione della sessione. I documenti saranno disponibili per l'esibizione on-line per tutto il periodo di conservazione. Per maggiore chiarezza si precisa che al fine di garantire una veloce e corretta visualizzazione dei documenti conservati, tramite ricerca libera il portale permette la visualizzazione di 200 risultati. Per la ricerca di tutti gli altri documenti sarà necessario valorizzare gli appositi campi delle maschere di ricerca con i metadati dichiarati in fase di versamento. La descrizione di dettaglio dell'interfaccia web per le richieste di esibizione dei documenti è contenuta nell'allegato 'Funzionalità_portale'. Vengono inoltre

- resi disponibili servizi web (Web Services) per le eventuali integrazioni con i portali dei Soggetti produttori.
- copia del documento su supporto ottico. La descrizione dettagliata circa la visualizzazione dei Pacchetti di distribuzione mediante supporto ottico è presente nel capitolo 6 Oggetti sottoposti a conservazione, paragrafo 6.5.

La struttura architettuale di UniStorage consente di definire diversi livelli operativi e garantisce che ciascuna Azienda/Ente, Area Organizzativa, Agenzia, Ufficio, Dipartimento, ecc. possa accedere solo ed esclusivamente ai propri documenti, in base alle credenziali e alle politiche di accesso attivate.

[Torna al sommario](#)

7.8 Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento di un pubblico ufficiale

Con la richiesta da parte dell'utente di esibizione dei Pacchetti di distribuzione mediante supporto ottico, viene generata una copia autentica del documento, conforme all'originale. Per i dettagli sulla modalità di richiesta di esibizione dei Pacchetti di distribuzione, fare riferimento al capitolo 6 "Oggetti sottoposti a conservazione" paragrafo 6.5 e al capitolo 7 "Il processo di erogazione del servizio di conservazione", fase 6.

Nei casi in cui, come previsto dall'art. 23-bis, c. 2 del Codice dell'Amministrazione Digitale⁸ il Soggetto produttore richieda la presenza di un pubblico ufficiale, Unimatica-RGI garantirà tale presenza mettendo a disposizione tutte le necessarie risorse che serviranno all'espletamento delle attività, rimandando in ogni caso la scelta al Soggetto produttore al quale saranno addebitate le spese.

Inoltre, in caso di adeguamento del formato dovuto all'evoluzione tecnologica verranno rispettate tutte le procedure elencate nell'Allegato 'Infrastrutture' al presente Manuale. Anche in questo caso, l'eventuale presenza del pubblico ufficiale per l'attestazione di conformità, sarà garantita in seguito alla richiesta del Soggetto produttore a cui vengono attribuiti i costi di gestione.

[Torna al sommario](#)

7.9 Scarto dei Pacchetti di archiviazione

Sette mesi prima della scadenza del periodo di conservazione dei documenti stabilito dal contratto, Unimatica-RGI comunica al Soggetto produttore, in modalità certa, che in assenza di ulteriori comunicazioni, trascorsi i termini previsti, provvederà alla cancellazione dei documenti.

In caso di proroga della conservazione, Unimatica-RGI rinnova la marca temporale sui documenti per il periodo richiesto (uno o più anni).

⁸ "Le copie e gli estratti informatici del documento informatico, se prodotti in conformità alle vigenti regole tecniche di cui all'articolo 71, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale, in tutti le sue componenti, è attestata da un pubblico ufficiale a ciò autorizzato o se la conformità non è espressamente disconosciuta. Resta fermo, ove previsto, l'obbligo di conservazione dell'originale informatico."

Le attività di scarto dei Pacchetti di archiviazione vengono svolte sulla base di accordi tra il Responsabile del servizio di conservazione di Unimatica-RGI e il soggetto produttore. Il responsabile del servizio è tenuto a generare l'elenco dei pacchetti di archiviazione contenenti i documenti destinati allo scarto e ad inviarlo al soggetto produttore che a sua volta, verificato il rispetto dei termini temporali stabiliti dal piano di conservazione, lo comunica al responsabile della gestione documentale o al coordinatore della gestione documentale.

In caso degli archivi pubblici o privati dichiarati di interesse storico particolarmente importante l'autorizzazione finale è rilasciata ai sensi della normativa vigente in materia di beni culturali⁹.

Il Titolare dell'oggetto di conservazione, una volta effettuate le verifiche e/o ricevuta l'autorizzazione da eventuali parti coinvolte, che può essere concessa anche solo su una parte dell'elenco proposto, provvede a trasmetterlo al conservatore affinché provveda alla distruzione dei pacchetti di archiviazione.

Unimatica-RGI provvede a tracciare tutte le operazioni mediante la produzione di informazioni essenziali sullo scarto, inclusi gli estremi della richiesta di nulla osta allo scarto e il conseguente provvedimento autorizzatorio.

I documenti e le aggregazioni documentali informatiche scartate da Unistorage vengono distrutti anche su tutti i sistemi di backup.

Al termine delle operazioni di distruzione dal sistema di conservazione dei pacchetti di archiviazione scartati, Unimatica-RGI provvede a comunicare in via ufficiale il termine delle operazioni al Titolare dell'oggetto che provvederà a sua volta a notificarlo a chi di competenza

[Torna al sommario](#)

7.10 Predisposizione di misure per l'interoperabilità e la trasferibilità ad altri conservatori

Unimatica-RGI, come descritto al par. 6.4 Struttura dati del Pacchetto di archiviazione, genera i PDA applicando le specifiche tecniche dalla norma UNI 11386 - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali. Accoglie, inoltre, formati conformi all'Allegato 2 delle Linee guida o concordati a seguito di opportuna valutazione di interoperabilità, pertanto Unistorage supporta sia l'acquisizione di PDD provenienti da altri conservatori, sia il riversamento verso altro sistema di conservazione.

[Torna al sommario](#)

⁹ L'intervento della Soprintendenza archivistica è previsto anche nel caso di archivi privati per i quali è stato dichiarato l'interesse culturale, secondo quanto disposto dall'art. 21, comma 1, lettera d del Codice dei beni culturali (D. Lgs. 22 gennaio 2004, n. 42).

7.11 Chiusura del contratto

Il Soggetto produttore, in qualsivoglia momento, ha il diritto di rescindere dal contratto. La procedura prevede la compilazione di un apposito modulo, debitamente firmato e timbrato, da inviare ad Unimatica-RGI utilizzando una delle modalità di seguito indicate:

1. Invio dell'originale cartaceo con firma autografa tramite posta all'indirizzo:
Unimatica-RGI S.p.A.
Via Cristoforo Colombo, 21
40131 Bologna
2. Invio dell'originale firmato digitalmente dal rappresentante legale, all'indirizzo di posta elettronica certificata (PEC): fatturaelettronica@pec.unimaticaspa.it

Il soggetto produttore che intende disdire il servizio di conservazione a norma dei documenti informatici affidato alla società Unimatica-RGI può scegliere di:

- mantenere la conservazione a norma dei documenti informatici già versati in conservazione fino al termine precedentemente concordato mantenendo la possibilità di utilizzare le credenziali di accesso al sistema per i soli scopi di consultazione
- non mantenere la conservazione a norma dei documenti informatici già versati in conservazione e di procedere allo scarto degli stessi e quindi disattivare le credenziali di accesso al sistema per i soli scopi di consultazione. L'Utente pertanto, dalla data della disdetta esonera la società Unimatica-RGI da ogni adempimento e responsabilità in merito alla custodia e conservazione dei documenti informatici versati in conservazione ed interessati dal servizio.

I documenti informatici che sono stati oggetto di conservazione a norma possono essere restituiti, a richiesta, all'utente su supporto ottico nel formato standard previsto dalla normativa in vigore (SInCRO – standard UNI 11386 – Supporto all'Interoperabilità nella Conservazione e nel recupero degli Oggetti digitali).

[Torna al sommario](#)

8. Procedure di gestione e di evoluzione

A coordinare la gestione del sistema, l'aggiornamento di questo e le procedure di adeguamento all'evoluzione tecnologica è la figura del Responsabile sviluppo e manutenzione che esegue una costante attività di controllo dell'attività di conservazione in conformità agli standard di qualità e sicurezza ISO 9001 e ISO 27001.

Affinché venga garantito un controllo totale sul sistema e un buon funzionamento di questo, le attività di manutenzione vengono svolte sia sui processi che sulle strutture hardware e software e viene condotta una quotidiana verifica delle attività sulle infrastrutture parallelamente ad una pianificazione delle eventuali procedure straordinarie da condurre in caso di anomalie.

[Torna al sommario](#)

8.1. Misure di sicurezza logica

Il presente paragrafo ha l'obiettivo di descrivere le misure di sicurezza adottate per l'erogazione del Servizio e per la protezione dei dati che fanno riferimento al Piano per la sicurezza del sistema di conservazione di Unimatica-RGI. In particolare, verranno descritte, a titolo esemplificativo ma non esaustivo, le misure di sicurezza tecniche e organizzative adeguate adottate da Unimatica-RGI per garantire un livello di sicurezza adeguato al rischio ai sensi dell'art. 32 del GDPR:

- la gestione utenze,
- la gestione sistemi di protezione,
- la gestione degli incidenti di sicurezza,
- la gestione dei backup,
- la gestione dei supporti di memorizzazione.

[Torna al sommario](#)

8.1.1 Gestione utenze

La policy di riferimento per la gestione delle utenze applicative e di sistema adottata da Unimatica-RGI prevede che le utenze siano rilasciate da un ente (o persona) differente dall'ente o persona che le utilizzerà.

Nell'ambito del servizio di conservazione, le utenze applicative e di sistema sono gestite secondo criteri idonei a garantire il rispetto dell'applicazione di misure di sicurezza tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio ai sensi dell'art. 32 del GDPR. Si riportano di seguito alcune delle misure di sicurezza adottate:

- Utilizzo di password complesse definite secondo i seguenti criteri:
 - la password non deve essere visibile in fase di inserimento nelle sessioni di login e sia criptata all'interno del Data Base;
 - la password:
 - deve avere una lunghezza compresa fra 8 e 25 caratteri,
 - deve contenere almeno un carattere speciale, un carattere maiuscolo, un carattere minuscolo ed un numero
 - non può contenere il nome dell'utente,
 - non può contenere il cognome dell'utente,
 - non può contenere l'username dell'utente,

- non può essere una delle ultime 4 utilizzate;
- la scadenza della password è configurabile attraverso un parametro;
- il sistema deve forzare l'utente a cambiare la password al primo utilizzo;
- il sistema deve avvertire l'utente della necessità di rinnovare la password;
- Applicazione del principio 'segregation of duty' nel rilascio delle credenziali (utente, password e profilo), vale a dire separazione tra chi rilascia e chi utilizza le credenziali di accesso ai dati;
- Applicazione del principio 'need to know' nel rilascio dei profili, vale a dire rilascio dei soli diritti per eseguire le attività di competenza;
- Assegnazione ad ogni utente di credenziali (user e password) personali, uniche e non assegnabili ad altri utenti;
- Revisione periodica degli utenti e dei relativi profili.

[Torna al sommario](#)

8.1.2 Gestione sistemi di protezione

Net Security

La realizzazione logica della rete è fatta secondo i seguenti criteri:

- controllo degli accessi e dei flussi realizzato tramite firewall in cross-mode (doppio Cisco Pix-535) ed utilizzo di software IP Tables per il port e IP filtering;
- filtro sui flussi di traffico da/per Internet costituito da sistemi McAfee Sidewinder ridondati, che effettuano deep packet inspection e forniscono funzionalità di firewall applicativo (livello 7 OSI);
- segregazione della rete e suddivisione della medesima in differenti porzioni dedicate alla rete di Back End dati per i server contenenti i data base, alla rete di Front End per la parte di presentazione, alla rete di gestione per l'amministrazione (funzione di supporto tecnico) della piattaforma;

Gli accessi alla rete sono segregati a livello di porte ed indirizzi IP. Gli accessi agli apparati di rete sono sottoposti a misure rigide di controllo e sono consentiti solamente agli amministratori della medesima.

IDS e IPS

Allo scopo di evitare che eventuali malintenzionati possano forzare le protezioni presenti per accedere in maniera illecita a dati riservati, la barriera di firewall applicativi fornisce anche un costante monitoraggio contro accessi non autorizzati tramite funzionalità IPS (Intrusion Prevention System).

[Torna al sommario](#)

8.1.3 Gestione degli incidenti di sicurezza

Si definisce incident uno stato, in un sistema, un servizio od una rete, che implichi il mancato funzionamento, il possibile mancato rispetto di uno SLA o il mancato funzionamento di contromisure.

Se l'incident coinvolge le proprietà di sicurezza dell'informazione (RID), si configura come incident di sicurezza.

La segnalazione di anomalie può scaturire

- dalle attività di monitoraggio
- da specifica segnalazione da parte di un utente o di personale interno

In entrambi i casi, qualora la segnalazione implichi un problema di sicurezza inficiando quindi l'integrità, riservatezza o disponibilità del dato, la prassi per la gestione degli incident può prevedere l'apertura di un ticket sulla specifica coda OTRS (strumento elettronico di ticketing Open-source Ticket Request System) del servizio di conservazione oppure dell'area sistemi.

Una volta preso in carico il ticket dal Responsabile del settore Conservazione o da un operatore designato egli diventa Incident Owner, cui sono delegate le azioni di: Contenimento¹⁰, Eliminazione delle cause¹¹, Ripristino¹².

La gestione degli incidenti di sicurezza è regolamentata da specifiche procedure dettagliatamente descritte secondo requisiti conformi allo standard ISO 27001:2013. Maggiori dettagli sono descritti nel capitolo 3 del Piano della Sicurezza.

[Torna al sommario](#)

8.1.4 Gestione dei backup e Disaster Recovery

8.1.4.1 Siti Settimo e Firenze

L'architettura del sistema backup è composta da un master server per ogni sito e da differenti media server che hanno il compito di archiviare i dati ed inserirli in una rete dedicata, parallela a quella di erogazione dei singoli servizi, per non impattare sulle prestazioni e sulla disponibilità di questi ultimi, durante la normale esecuzione delle attività di backup.

I singoli agent installati sull'infrastruttura di virtualizzazione e sui server non virtualizzati comunicano con il backup server che esegue il salvataggio dei dati su un appliance Data Domain. Il salvataggio dei dati su un appliance Data Domain viene replicato sul sito secondario. Questo sistema consente:

- Semplicità di integrazione anche con future evoluzioni del software di backup
- De-duplicazione del dato ad alta velocità
- Replica efficiente in rete
- Scalabilità dell'infrastruttura

¹⁰ **Contenimento:** processo che rappresenta la fase di esecuzione delle attività di contrasto, atte a mitigare le compromissioni della sicurezza derivanti da un incidente. Una delle attività principali del processo di contenimento è quella di determinare il patrimonio informativo che viene messo a rischio a seguito di un incidente.

¹¹ **Eliminazione delle cause:** processo che elenca le azioni indirizzate alla rimozione delle cause che scatenano un incidente informatico. E' opportuno sottolineare l'importanza che rappresenta la comprensione del problema che è all'origine dell'incidente; a tale scopo appare determinante descrivere con il maggior dettaglio possibile il modo con cui l'evento di sicurezza si è verificato.

¹² **Ripristino:** processo tramite il quale viene attuato il ritorno alle normali condizioni di operatività aziendale e di chiusura formale dell'incidente. Un obiettivo determinante che emerge dalla corretta applicazione delle misure qui contemplate, è garantire che per i dati e per i sistemi/applicazioni siano ristabilite le funzionalità e performance in essere prima dell'incidente.

L'architettura di backup utilizza le seguenti tecnologie:

- Data Domain DD4200
- Data Domain DD4100
- Data Domain DD2500
- Software di backup NetBackup di Symantec
- Software di backup vRanger di DELL
- Software di backup con modulo di cifratura dei dati
- Rete di backup con throughput a 10 Gbit/s
- Replica dei dati di backup tramite link a 400 Mbit/s fra sito primario e secondario

La funzionalità di backup sulla base dati è implementata utilizzando Oracle RMAN o BARMAN, con cadenza giornaliera e settimanale a seconda delle necessità.

[Torna al sommario](#)

8.1.4.2 Siti di Bologna e Acilia (Roma)

L'architettura di backup si basa sul software open-source bacula, costituito da un modulo director che sovrintende le operazioni di backup, su due unità dischi SATA (una con dischi fissi e una con dischi rimovibili) collegate a server di backup su cui gira il modulo storage di bacula, e su una serie di moduli client (agenti) di bacula disposti sulle macchine contenenti i dati di cui effettuare il backup.

Le categorie di dati oggetto del backup sono:

- Directory di sistema dei sistemi Unimatica-RGI
- DB Postgres[nella modalità export DB]

Nell'ambito del backup dei dati appartenenti alla categoria Directory di sistema, è eseguito anche il backup delle cartelle di rete utilizzate dal personale Unimatica-RGI.

Il backup avviene in due modalità:

- diretto: i dati vengono backuppati direttamente sul server che li contiene tramite un agente bacula
- indiretto: i dati vengono backuppati su NAS da uno script di backup che gira sul server da backuppare, e dal NAS vengono poi prelevati da un agente bacula che li inserisce nel flusso dei backup diretti

Le modalità di backup sono riassumibili in estrema sintesi nei seguenti punti:

- i dati di backup sono conservati per 7 giorni su Dischi, i backup full eseguiti ogni fine settimana sono conservati per 1 mese su dischi;
- vengono eseguiti backup mensili su dischi rimovibili, in singola copia, conservati in cassaforte ignifuga, con retention di un anno;
- l'ultimo backup mensile su disco di ogni anno viene conservato con ritenzione infinita;
- backup su disco di dati con esigenze di retention specifiche (superiori all'anno), sono eseguiti in doppia copia, in base a specifiche degli "owner" dei dati;
- il salvataggio dei documenti su CD-ROM con consegna al Soggetto produttore, può essere eseguito su richiesta;
- il salvataggio dell'applicazione sia server che client è realizzato su supporto fisico esterno (Data tape o CD-ROM) per eseguire una rapida reinstallazione in caso di necessità;
- i supporti di backup hanno rotazione con frequenza settimanale.

Per le attività di salvataggio si eseguono i seguenti controlli:

- monitoraggio e controllo dei log-files dei risultati dei salvataggi (con frequenza quotidiana);
- ripristino periodico a campione dei dati;
- controllo della validità e della funzionalità (leggibilità) dei supporti.

[Torna al sommario](#)

8.1.4.3 Disaster Recovery

I servizi di conservazione di Unimatica-RGI sono erogati tramite due Data Center Primari due Data Center Secondari che svolgono il compito di Backup Remoto e di Disaster Recovery (D/R), al fine di garantire gli opportuni livelli di continuità del servizio.

I Data Center hanno una distanza fra loro superiore 200 e 300 Km e la disponibilità di servizio è H24 per tutti e 4.

I Data Center secondari permettono di usufruire dei servizi in Produzione anche in caso di indisponibilità dei Data Center Primari.

Per questo servizio Unimatica-RGI definisce con il Cliente il livello dei parametri che caratterizzano il servizio di D/R e di continuità operativa.

- Recovery Point Objective (RPO)
Rappresenta il massimo tempo che intercorre tra la produzione di un dato sui siti primari e la sua messa in sicurezza (ad esempio attraverso backup) e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di disastro e che devono essere successivamente ripresi.
- Recovery Time Objective (RTO)
È il tempo necessario per il pieno recupero dell'operatività di un sistema e del relativo processo organizzativo.

[Torna al sommario](#)

8.1.5 Gestione dei supporti di memorizzazione

La gestione dei supporti di memorizzazione, ove richiesti, segue i seguenti criteri:

- i media di memorizzazione elettronica sono correttamente etichettati in modo da fornire le seguenti informazioni: tipologia del media, tecnica della scrittura, data della scrittura, contenuto. Per tecnica della scrittura si intende il formato in cui il media è stato preparato, nel nostro caso formato ISO, dipendentemente dal tipo supporto (CD o DVD);
- in caso di media che vengano riutilizzati per altri dati, essi vengono preventivamente riformattati tramite le tecniche di formattazione a basso livello, allo scopo di evitare che le informazioni ed i dati in essi contenuti possano essere presi e divulgati a soggetti non autorizzati;
- nel caso in cui i dati registrati sui media non più utilizzati non possano essere definitivamente cancellati si procede alla distruzione del media stesso, impedendone quindi il riutilizzo;
- i media sui quali sono eseguiti i salvataggi aziendali sono conservati in una sede differente rispetto a quella dove sono le strumentazioni cui i salvataggi si riferiscono ed in un luogo non accessibile se non al personale autorizzato,
- periodicamente è eseguita una verifica dei media e della disponibilità degli strumenti di accesso ai medesimi. In caso che per qualche media sia verificata la non disponibilità (anche

prevista nel breve futuro) degli strumenti di accesso, si procede allo svecchiamento dei media tramite riversamento del loro contenuto in altro media.

[Torna al sommario](#)

8.2. Procedure di evoluzione e Change management

I cambiamenti che vengono apportati al sistema di conservazione di Unimatica-RGI risultano essere il prodotto di un'adeguata corrispondenza alle procedure di evoluzione tecnologica sia sulle strutture hardware sia su quelle software. Il Responsabile della funzione archivistica e il Responsabile dei sistemi informativi definiscono politiche, priorità e tempistiche affinché vengano garantite nel tempo integrità, disponibilità e sicurezza.

In caso di disservizi causati da problematiche riscontrate durante il processo di aggiornamento, è possibile effettuare il ripristino delle versioni precedenti così da assicurare il corretto e continuo svolgimento delle attività.

Il Responsabile del servizio di conservazione e il Responsabile della sicurezza dei sistemi informativi periodicamente si occuperanno di aggiornare la normativa e gli standard di riferimento in base all'evoluzione di questi.

La descrizione delle procedure di evoluzione e gestione dei cambiamenti è riportata nel paragrafo 3.2.2 del documento "Piano della sicurezza del sistema di conservazione".

[Torna al sommario](#)

8.3. Cessazione del Servizio di conservazione

Il servizio di Conservazione digitale a norma è, dal 2005, uno dei principali asset di Unimatica-RGI e gli obiettivi della Direzione per gli anni futuri sono di continuare ad evolvere il sistema ed il servizio di conservazione per mantenerlo adeguato alla tecnologia ed alla normativa e di espandere sempre più nel mercato target, non solo italiano, la penetrazione dell'azienda.

A fronte dei suddetti obiettivi, è stata comunque stabilita una procedura per definire le modalità secondo le quali dovrà essere gestito l'evento, ad oggi non prevedibile, di cessazione del servizio di Conservazione da parte di Unimatica-RGI

La gestione della cessazione del Servizio di Conservazione, in fase iniziale, è in carico alla Direzione la quale stabilisce un tempo di almeno 10 mesi prima della data di attuazione prevista.

Dal momento della comunicazione, la Direzione, supportata in questo dal Responsabile del servizio di conservazione, provvede a far sì che non vengano stipulati nuovi contratti, in vista della cessazione del servizio.

Alla ricezione della comunicazione suddetta il Responsabile del servizio di conservazione coinvolge i Responsabili delle diverse aree inerenti la Conservazione (Sicurezza, Servizio, Archivistica, Sviluppo) con i quali deve collaborare strettamente per la gestione della cessazione e la relativa pianificazione delle attività.

La procedura e le attività che verranno eventualmente eseguite sono descritte nel dettaglio all'interno del documento PRO_CONS - Piano di Cessazione, qualora venga richiesto, tale procedura viene resa disponibile fornendola al soggetto produttore interessato.

[Torna al sommario](#)

9. Monitoraggio e controlli

L'attività di monitoraggio e controllo viene portata avanti dal Responsabile della sicurezza dei sistemi e dal Responsabile della funzione archivistica, in accordo con il Responsabile del sistema di conservazione. Tale attività è finalizzata alla rilevazione di eventi di sicurezza, identificabili come stati che indicano il mancato rispetto delle politiche di sicurezza, che possano costituire una possibile fonte di rischio per il sistema di conservazione. Nello specifico gli obiettivi delle attività di monitoraggio sono la valutazione del livello del rischio associato agli eventi di sicurezza e la gestione di tali eventi, mediante strumenti come i Report dei controlli, agendo per il contenimento e/o eliminazione delle cause.

Gli eventi di sicurezza sono monitorati tramite il sistema di Log che consente la registrazione degli accessi e degli eventi (operazioni). Il sistema di Log è organizzato per registrare eventi ai vari livelli di astrazione della piattaforma:

- log del sistema operativo (incluso file system) atto ad identificare ingressi, anomalie ed errori;
- log del Data Base atti ad identificare ingressi, anomalie ed errori;
- log dei sistemi di rete (firewall e router) atti ad identificare ingressi, anomalie ed errori;
- log delle applicazioni software utilizzate (realizzati con vista a livello di singolo utente) atti ad identificare ingressi, principali attività svolte dagli utenti, sequenze del processo, accessi ai dati.

I log file degli applicativi contengono almeno le seguenti informazioni:

- utente che ha eseguito l'operazione;
- data e ora dell'operazione;
- operazione eseguita.

I file di log non sono modificabili o eliminabili da parte degli Utenti che usano il sistema (che non dispongono dei diritti di accesso).

I log di sistema sono analizzati da parte dei sistemisti qualora si rendesse necessaria un'indagine a seguito di un malfunzionamento del sistema.

La dettagliata descrizione dei processi relativi alle attività di monitoraggio e controlli è riportata nel documento "Piano della sicurezza del sistema di conservazione", capitolo 3 e nella PRO_CONS - Procedure di conservazione.

I log vengono successivamente inviati in conservazione per mantenere traccia delle comunicazioni tra Soggetto produttore e sistema di conservazione.

[Torna al sommario](#)

9.1 Audit interni e Verifica dell'integrità degli archivi

Le verifiche ispettive interne vengono pianificate dal Responsabile del sistema di gestione per la sicurezza delle informazioni e dal Responsabile della qualità in accordo con il Responsabile sviluppo e manutenzione del sistema di conservazione, dal Responsabile sicurezza dei sistemi per la conservazione e dal Responsabile del servizio di conservazione tenendo conto dello stato e dell'importanza dei processi e delle aree oggetto di verifica, nonché dei risultati delle precedenti verifiche. La frequenza con la quale vengono disposte le verifiche ispettive interne è almeno annuale. Unimatica-RGI si rende disponibile qualora un soggetto produttore volesse richiedere audit di terza parte.

La scelta del personale verificatore viene fatta in modo da garantire obiettività ed imparzialità nel processo di verifica.

Unimatica-RGI prevede in allegato al Manuale “Elenco delle modifiche apportate al Manuale della conservazione e dei documenti obsoleti” tenente traccia delle seguenti informazioni:

- registro delle modifiche al Manuale del sistema di conservazione
- registro dei documenti distrutti

[Torna al sommario](#)

9.2 Reportistica di servizio

Il sistema di conservazione UniStorage gestisce un sistema di tracciatura nel quale vengono registrati tutti i singoli eventi che riguardano sia la gestione dei Pacchetti, dalla fase di versamento a quella di distribuzione, sia i singoli documenti. Questa tracciatura, costruita per implementare un “forensic log”, è in un formato rigido e non disabilitabile. La tracciatura è prerequisito indispensabile per l’esecuzione delle operazioni.

Nel dettaglio, il sistema di log prevede la registrazione di informazioni relative alle diverse funzioni del processo di conservazione per tutte le fasi descritte nel capitolo 7 “Il processo di erogazione del servizio di conservazione”.

La reportistica di servizio che Unimatica-RGI gestisce è di due Tipologie:

1. Reportistica relativa al processo di Conservazione,
2. Reportistica del servizio di Supporto Utente (Service Desk e AM Settore conservazione e Settore sistemi).

Tipologia 1:

vengono prodotti periodicamente i seguenti report:

- Report Consuntivo Pacchetti di archiviazione,
- Report Excel che fornisce la lista dei Pacchetti di archiviazione e che comprende questo set Minimo di informazioni:
 1. Ragione Sociale Cliente;
 2. Numero documenti conservati e spazio occupato nel periodo totali e per tipologia di documento;
 3. Numero documenti conservati e spazio occupato totali e per tipologia di documento.

Tipologia 2:

viene prodotto un report di Servizio che fornirà le seguenti evidenze:

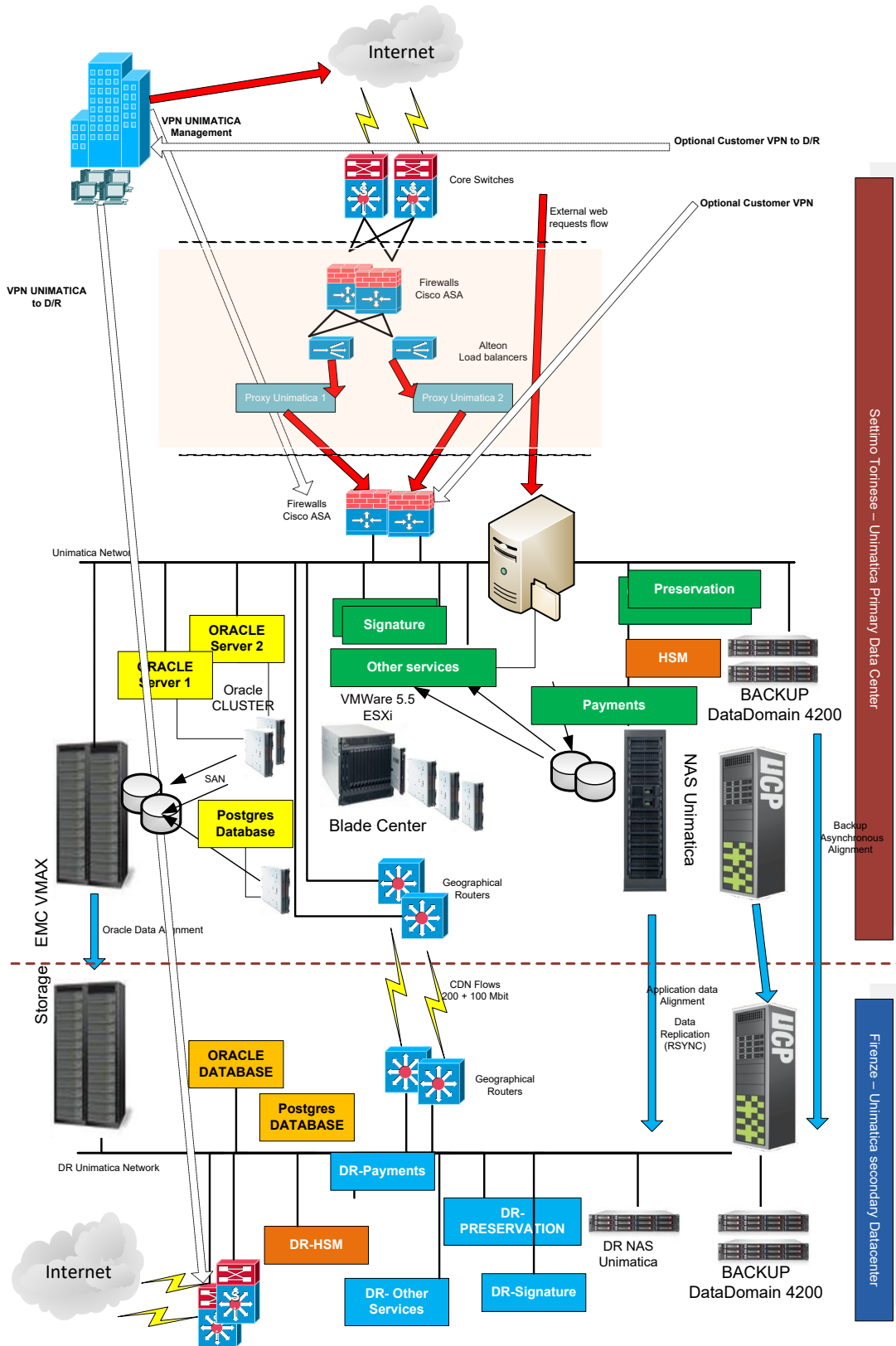
- Numero Incident Segnalati
- Media Tempo di presa in carico Incident
- Media Tempo di chiusura Incident
- Numero Service Request
- Media Tempo di presa in Carico Service Request
- Media Tempo di Chiusura Service Request

[Torna al sommario](#)

10. La server farm di Unimatica-RGI

Dal punto di vista infrastrutturale, i data center dai quali Unimatica-RGI eroga i propri servizi consentono di offrire un servizio di alta qualità in termini di continuità e affidabilità. Tale qualità deriva dalle caratteristiche progettuali che hanno contraddistinto la realizzazione dei Data Center, con criteri focalizzati sempre sull'obiettivo di fornire le massime garanzie di sicurezza, disponibilità e continuità, sia per quanto riguarda l'erogazione di energia elettrica, sia attraverso un opportuno condizionamento climatico, sia attraverso un adeguato meccanismo di sicurezza fisica (impianto antincendio e sorveglianza con allarmi 24x7), sia attraverso la ridondanza architetturale dei sistemi, delle infrastrutture di rete e delle connessioni verso l'esterno.

Lo schema seguente rappresenta l'implementazione hardware/software dell'architettura di conservazione presso i siti di Settimo Torinese e Bologna (siti primari), Firenze, e Acilia (Roma) (siti secondari) nei quali sono allocati i data center:



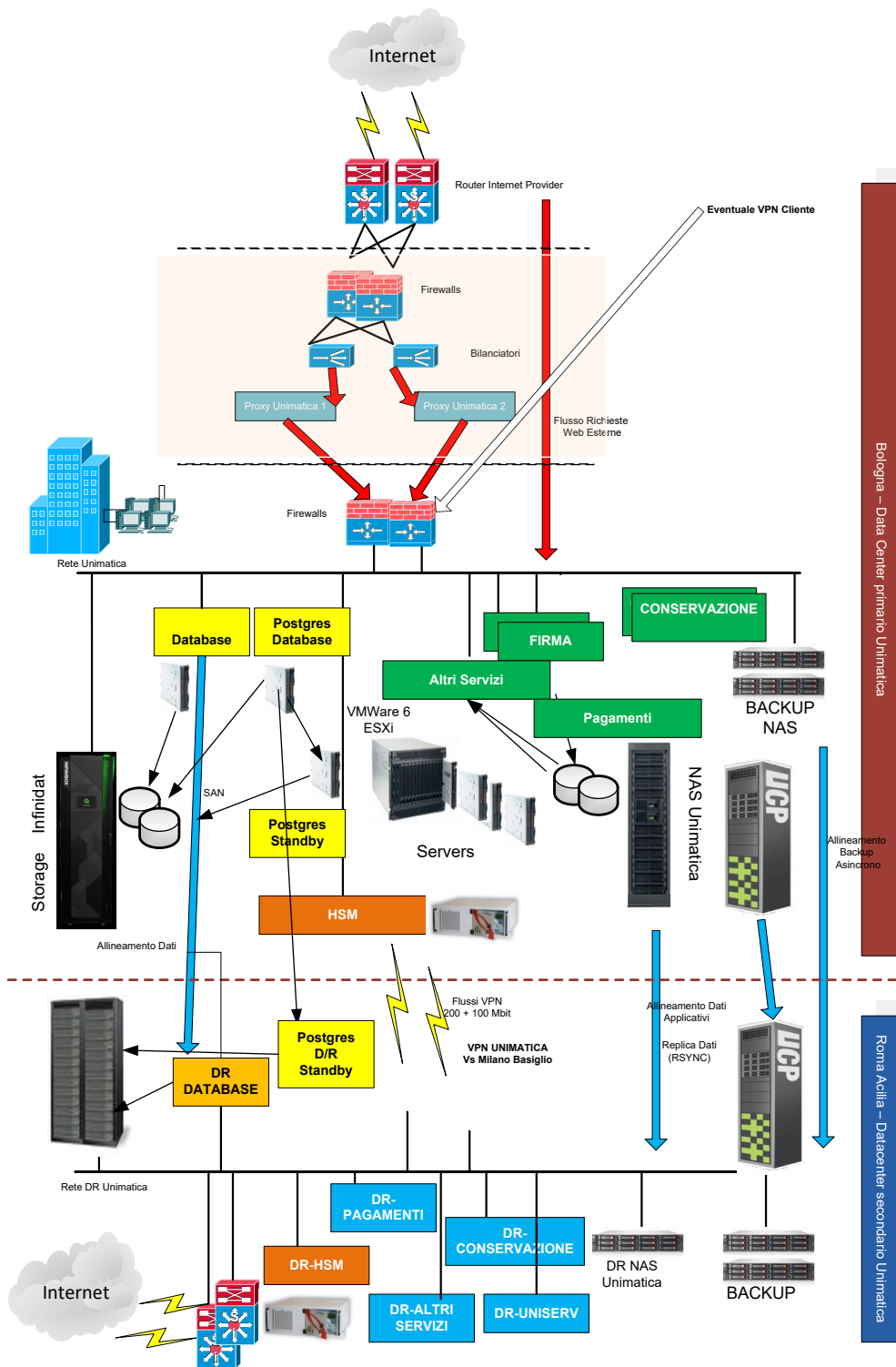


Figura 3 - Architettura di conservazione

[Torna al sommario](#)

10.1 UniStorage - Il sistema per la conservazione

Il sistema software utilizzato per la gestione del processo di conservazione dei documenti informatici è costituito dal prodotto applicativo UniStorage.

UniStorage, sviluppato internamente e totalmente da Unimatica-RGI, è un sistema integrato e completo per la conservazione dei documenti informatici che viene fornito in modalità Outsourcing/ASP/SaaS congiuntamente a tutti i servizi di gestione e supporto correlati, oppure in modalità pacchetto applicativo, installando le applicazioni presso il Data Center del Soggetto produttore.

I servizi offerti, oltre che di tipo applicativo e tecnologico, comprendono tutto il necessario supporto normativo, organizzativo e contrattuale (deleghe, privacy, ecc.).

UniStorage esegue la conservazione nel tempo dei documenti sottoscritti con firma digitale e le seguenti caratteristiche generali:

- completezza - presenza di qualsiasi documento emesso
- robustezza - garanzia di consistenza dei dati inseriti
- sicurezza - protezione dalla manipolazione non autorizzata dei dati
- affidabilità - indipendenza dai guasti dell'hardware
- chiarezza - facilità di consultazione secondo diversi criteri di ricerca

garantendo:

- la completezza e l'inalterabilità delle registrazioni dei Pacchetti documenti inviati in conservazione
- la possibilità di verifica dell'integrità delle registrazioni
- i riferimenti temporali certi.

Il sistema è progettato per partizionare in maniera opportuna i dati gestiti al fine di garantire la separazione per contesto organizzativo e la consistenza dei dati. Il partizionamento opera tra i dati di Aziende diverse o di diversi dipartimenti o uffici afferenti ad una stessa Azienda (Aree Organizzative Omogenee). I Pacchetti versati provenienti anche da flussi diversi di conservazione, vengono mantenuti separati tramite una chiave primaria che li identifica, fin dal loro ingresso in conservazione, come appartenenti ad una data AOO e non ad un'altra. Il sistema di partizionamento è direttamente collegato al sistema di controllo degli accessi e tracciatura, viene quindi garantita la riservatezza dei dati presenti in archivio.

UniStorage è una applicazione Web a tre livelli (desktop, application e database) e utilizzabile da posti di lavoro dotati di sistema operativo Windows o Linux, per mezzo dei principali browser di riferimento sul mercato. Per le postazioni che dovranno operare sulle funzionalità di firma è necessario che localmente siano attivi i driver del dispositivo di firma (lettore, smart card o token USB di firma, tablet per la firma grafometrica, ecc.), oppure che sia utilizzato un dispositivo HSM (Hardware Security Module) raggiungibile via rete.

Il servizio in outsourcing ASP del servizio di conservazione dei documenti informatici prodotti ed inviati dal Soggetto produttore prevede lo svolgimento da parte di Unimatica-RGI, dietro apposita nomina e delega da parte del Soggetto produttore, delle funzioni e responsabilità di conservazione dei documenti.

La descrizione dettagliata delle componenti logiche, tecnologiche e fisiche è riportata nel documento “Infrastruttura” allegato al Manuale del sistema di conservazione.

[Torna al sommario](#)

Appendice A

Allegati al Manuale del sistema di conservazione:

- Allegato 'Infrastrutture'.
- PRO_CONS - Piano di Cessazione

Specificità del contratto e documenti di riferimento:

- Scheda Cliente.
- Flusso per la conservazione dei Documenti in Unistorage
- Specifiche del servizio web per la consegna anticipata di documenti nel Sistema di conservazione.
- 'Funzionalità_portale'.
- Elenco delle modifiche apportate al Manuale della conservazione e dei documenti obsoleti.

[Torna al sommario](#)