ALLEGATO B – MANUALE DI CONSERVAZIONE DEI CONSERVATORI

Manuale di Conservazione

MANUALE DI CONSERVAZIONE DEI CONSERVATORI

Di seguito si riporta l'elenco dei Conservatori Esterni ai quali l'Università degli Studi di Cassino e del Lazio Meridionale ha delegato l'attività di conservazione dei documenti digitali.

CONSERVATORI ESTERNI

1. ARUBA PEC (Servizio Docfly) – Contratto stipulato in data 5/6/2024

2. Consorzio Interuniversitario CINECA – Accordo di versamento del 2/12/2021

Andrea Sassetti
Firmato digitalmente il 25/06/2020 09:56:22 CEST

Aruba PEC S.p.A.

Manuale di Conservazione

Versione: 1.7
Data approvazione: 19/06/2020
Redazione: Alessandro Capobianco
Verificato da: Marco Menonna, Federico Ciofi
Approvato da: Andrea Sassetti
Classificazione documento: pubblico

VERSIONE N°	DATA	NATURA DELLA MODIFICA
1.0	26/11/2014	Prima versione documento
1.1	02/02/2016	Revisione del manuale a seguito della pubblicazione del nuovo schema sul sito istituzionale dell'Agid
1.2	04/04/2016	Modifiche su terminologie utilizzate
1.3	20/09/2017	Par.3.1: aggiornata normativa di riferimento Par.4.1: aggiornati Responsabili del Servizio e date di nomina Par.6.3: rimosso Par.7.6: modificata terminologia (da "materiali" a documenti"); Inserimento Par.7.7.3: Produzione copie o duplicati su supporti rimuovibili Par. 7.11: inserito paragrafo "audit log" Par.8.6: migliorata descrizione della soluzione di conservazione Par.8.6.1: migliorata descrizione change management e inserito riferimento test di Quality Assurance Par.9.2.: modificata cadenza verifica periodica dell'integrità degli archivi. Modificata descrizione procedura leggibilità archivi. Par.9.2.1 modificata frequenza verifica integrità degli archivi Cap.11: Cambiata descrizione specifiche tecniche per "invio in conservazione del PdA" Par.12.7: ridefinite modalità di isolamento delle componenti critiche Par.12.8.3: migliorata descrizione della sicurezza organizzativa e aggiornati riferimenti normativi 12.8.4: aggiornate regole password utente Tutto il documento: aggiornati riferimenti a documenti interni e procedure di sistema

1.4	11/12/2017	Tutto il documento: inseriti testi alternativi per le immagini e verificata accessibilità Par. 1.1: Specificata denominazione societaria del Conservatore Accreditato e inseriti dati identificativi della società Par. 2.1: Uniformata terminologia relativa a IdC, IPdA e IPdV Par. 6.3.2: Aggiornata tabella formati consigliati Par 6.6.1: Aggiornati riferimenti alle specifiche specifiche del Pacchetto di Versamento Par. 6.7.1: Aggiornata terminologia relativa a IdC Par.7.5.2: Inserito paragrafo relativo a gestione PdA incompleti o non validi Par. 7.6.1: Aggiornato paragrafo e corretto refuso di terminologia sul secondo punto Par. 7.8.3: Descritta procedura per scarto immediato Par.9.2: Modificato titolo paragrafo Par. 9.2.1: Rivista descrizione delle attività di verifica dell'integrità degli archvi Par 10.1.2: Aggiornati i contenuti della Scheda di Conservazione Cap. 11: Rivisti ed aggiornati livelli di servizio (SLA)
1.5	11/10/2018	Aggiornamenti Terminologia, Normativa e Standard di Riferimento Par.4.1: Aggiornati Ruoli e Reponsabilità Par.6.4: Precisazione su inserimento delle c.d. extrainfo nell' IdC. Par. 7.1: Aggiornamento modalità di acquisizione dei PdV. Inserito par. 7.5.3 Rettifica dei pacchetti di archiviazione Par.12.5: Rimosso riferimento a protocollo SSL Par. 12.6: Rivisti dettagli gestione dei backup del sistema Tutto il documento: aggiornamenti riferimenti a normativa trattamento dati personali
1.6	17/04/2019	Nuovo Template Cap.1: Aggiornato Rappresentante Legale Par.4.1: Aggiornati Ruoli e Responsabilità
1.7	19/06/2020	Par.4.1: Aggiornati Ruoli e Responsabilità

Sommario

1 Scopo e ambito del documento

Il presente documento è il Manuale del sistema di conservazione (di seguito per brevità chiamato anche "Manuale") del Conservatore Accreditato Aruba PEC S.p.a. (da ora in avanti "ARUBA"). Di seguito i dati identificativi della società:

Denominazione sociale:	**Aruba PEC S.p.A.**
Indirizzo della sede legale ed operativa:	**Via S. Clemente, 53** **24036 Ponte San Pietro (BG)**
Legale rappresentante:	**Giorgio Cecconi** (Amministratore Unico)
N° di iscrizione al Registro Imprese di Bergamo:	**01879020517 (REA n. 445886)**
Codice Fiscale e Partita IVA:	**01879020517**
N° di telefono (centralino):	**+39 0575 050.350**
ISO Object Identifier (OID):	**1.3.6.1.4.1.29741**
Sito web principale:	**https://www.pec.it**
E-mail (generale):	**info@arubapec.it**

Il Manuale illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione dei processi, in particolare le modalità di versamento, archiviazione e distribuzione, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate ed ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione digitale di documenti informatici.

Il Manuale è costituito dalla versione corrente del presente documento.

In particolare, nel presente Manuale sono riportati:

a) i dati dei soggetti che nel tempo hanno assunto la responsabilità del servizio di conservazione, descrivendo in modo puntuale, in caso di affidamento, i soggetti, le funzioni e gli ambiti oggetto dell'affidamento stesso;
b) la struttura organizzativa comprensiva delle funzioni, delle responsabilità e degli obblighi dei diversi soggetti che intervengono nel processo di conservazione;
c) la descrizione delle tipologie dei documenti informatici sottoponibili a conservazione,
d) comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di documenti e delle eventuali eccezioni;
e) la descrizione delle modalità di presa in carico di uno o più pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento e della descrizione dei controlli effettuati su ciascuno specifico formato adottato;
f) la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione;
g) la modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;
h) la descrizione del sistema di conservazione, comprensivo di tutte le componenti tecnologiche, fisiche e logiche, opportunamente documentate e delle procedure di gestione e di evoluzione delle medesime;
i) la descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie;
j) la descrizione delle procedure per la produzione di duplicati o copie;
k) i tempi entro i quali le diverse tipologie di documenti informatici devono essere oggetto di scarto/cancellazione;

l) le modalità con cui viene richiesta la presenza di un pubblico ufficiale, indicando anche quali sono i casi per i quali è previsto il suo intervento;
m) le normative in vigore nei luoghi dove sono conservati i documenti;

Il Manuale recepisce le disposizioni di cui al D.Lgs. 7 marzo 2005, n. 82, e s.m.i. (Codice dell'amministrazione digitale), di seguito per brevità chiamato anche "Codice" o "CAD", oltre alle indicazioni riportate nei provvedimenti di legge o di prassi richiamati nel capitolo "Riferimenti normativi e di prassi" nonché i provvedimenti di natura tecnica richiamati nel capitolo "Riferimenti tecnici".

Il Cliente è tenuto a leggere con la massima attenzione il presente Manuale predisposto da ARUBA. Il Cliente in qualità di unico Responsabile della conservazione approva e fa propri i contenuti del presente Manuale di conservazione. Per una più agevole e scorrevole lettura del presente Manuale si raccomanda la consultazione del capitolo dedicato alle definizioni, abbreviazioni e termini tecnici.
Torna al sommario

2 Terminologia (glossario e acronimi)

Secondo la normativa vigente e ai fini dell'interpretazione del presente Manuale, i termini e le espressioni sotto elencate avranno il significato descritto nelle definizioni in esso riportate. Qualora le definizioni adottate dalla normativa di riferimento non fossero riportate nell'elenco che segue, si rimanda ai testi in vigore per la loro consultazione.
I termini e le espressioni non definiti avranno il significato loro attribuito all'interno del paragrafo o sezione che li contiene.
Ai fini della fruizione del Servizio di conservazione digitale dei documenti informatici descritto nel presente Manuale, valgono ad ogni effetto anche le definizioni contenute nel Contratto, da intendersi, pertanto, qui interamente riportate e trascritte, nonché le seguenti:
Torna al sommario

2.1 Glossario dei termini e acronimi

Glossario dei termini e Acronimi	
AgID	Agenzia per l'Italia Digitale
Accesso	Operazione che consente a chi ne ha diritto di prendere visione dei documenti informatici conservati
Accreditamento	Riconoscimento, da parte dell'Agenzia per l'Italia Digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza, ad un soggetto pubblico o privato che svolge attività di conservazione o di certificazione del processo di conservazione
Agente di alterazione	Qualsiasi codice contenuto in un documento informatico potenzialmente idoneo a modificare la rappresentazione dell'informazione senza alterarne il contenuto binario (in via meramente esplicativa e non esaustiva: macro, codici eseguibili nascosti, formule di foglio di lavoro occulte in tutto o in parte, sequenze di caratteri occultate all'interno dei documenti informatici)
Aggregazione documentale informatica	Raccolta di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente
Archivio	Complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività
Archivio informatico	Archivio intestato dal Cliente al/i Titolare/i nel quale sono conservati costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico e di cui il/i medesimo/i è/sono giuridicamente responsabile/i
Area organizzativa omogenea	Un insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo

	unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.
Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico
Autenticità	Caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico
Base di dati	Collezione di dati registrati e correlati tra loro
Certificatore accreditato	Soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, dell'Agenzia per l'Italia Digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
Ciclo di gestione	Arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo
Chiusura del Pacchetto di Archiviazione	Operazione consistente nella sottoscrizione del Pacchetto di Archiviazione con firma digitale apposta da un Firmatario Delegato di ARUBA e apposizione di una validazione temporale con marca temporale alla relativa impronta
Classificazione	Attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati
Codice o CAD	Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni
Codice eseguibile	Insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici
Conservatore accreditato	Soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia Digitale o da un certificatore accreditato, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
Conservazione	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel Manuale di conservazione
Contrassegno a stampa	Contrassegno generato elettronicamente, apposto a stampa sulla copia analogica di un documento amministrativo informatico per verificarne provenienza e conformità all'originale
Coordinatore della Gestione Documentale	Responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 e s.m.i. nei casi di amministrazioni che abbiano istituito più Aree Organizzative Omogenee
Copia informatica di documento analogico	Il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto
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
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.
Copia di sicurezza	Copia di backup degli archivi del sistema di conservazione.
Descrittore evidenze	Vedi pacchetto informativo.
Destinatario	Identifica il soggetto/sistema al quale il documento informatico è indirizzato.
DIRT	Documenti informatici rilevanti ai fini delle disposizioni tributarie.
Documento analogico	La rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.
Documento analogico originale	Documento analogico che può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi.
Documento originale unico	E' quel documento analogico il cui contenuto non può essere desunto da altre scritture o documenti di cui sia obbligatoria la tenuta, anche presso terzi e che non soddisfa, dunque, alcuna delle condizioni elencate nella definizione di "Documento analogico originale".
Documento informatico	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

Duplicato informatico	Il documento informatico ottenuto mediante la memorizzazione, sullo stesso supporto o su supporti diversi, della medesima sequenza di valori binari del documento originario.
Duplicazione dei documenti informatici	Produzione di duplicati informatici.
Elenco Persone	Elenco delle persone designate dal Cliente ad operare in suo nome, conto e interesse con ARUBA per l'esecuzione del contratto.
Esibizione	Operazione che consente di visualizzare un documento conservato e di ottenerne copia;
Estratto per riassunto	Documento nel quale si attestano in maniera sintetica ma esaustiva fatti, stati o qualità desunti da dati o documenti in possesso di soggetti pubblici
Evidenza informatica	Una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.
Fascicolo informatico	Raccolta, individuata con identificativo univoco, di atti, documenti e dati informatici, da chiunque formati, del procedimento amministrativo, nell'ambito della pubblica amministrazione. Per i soggetti privati è da considerarsi fascicolo informatico ogni aggregazione documentale, comunque formata, funzionale all'erogazione di uno specifico servizio o prestazione.
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.
Fruibilità di un dato	La possibilità di utilizzare il dato anche trasferendolo nei sistemi informativi automatizzati di un'altra amministrazione.
Firmatario delegato	Responsabile del servizio di conservazione o Persona formalmente delegata ad apporre la propria firma digitale sui Pacchetto di Archiviazione per conto di ARUBA; questa persona può essere interna o esterna ad ARUBA, laddove è giuridicamente possibile.
Formato	Modalità di rappresentazione del documento informatico mediante codifica binaria; comunemente è identificato attraverso l'estensione del file e/o il tipo MIME.
Fornitore esterno	Organizzazione che fornisce ad ARUBA servizi relativi al suo sistema di conservazione dei documenti.
Funzionalità aggiuntive	Le ulteriori componenti del sistema di protocollo informatico necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni.
Funzionalità interoperative	Le componenti del sistema di protocollo informatico finalizzate a rispondere almeno ai requisiti di interconnessione di cui all'articolo 60 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.
Funzionalità minime	La componente del sistema di protocollo informatico che rispetta i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.
Funzione di hash	Una funzione matematica che genera, a partire da una evidenza informatica, una sequenza di bit (impronta) in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
Generazione automatica di documento informatico	Formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni.
Identificativo univoco	Sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione.
Indice di Conservazione (IdC)	L'Indice del Pacchetto di Archiviazione (IPdA)
Indice del Pacchetto di Archiviazione (IPdA)	Indice che contiene le informazioni relative al Pacchetto di Archiviazione in formato xml, anche indicato nello standard SInCRO come IdC (Indice di Conservazione)
Indice del Pacchetto di Versamento (IPdV)	Indice che contiene le informazioni relative al pacchetto di versamento in formato xml.
Immodificabilità	Caratteristica che rende la rappresentazione del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso.

Impronta	La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash.
Insieme minimo di metadati del documento informatico	Complesso dei metadati da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta.
Integrità	Insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato.
Interoperabilità	Capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi.
Leggibilità	Insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti.
Log di sistema	Registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati.
Manuale di gestione	Strumento che descrive il sistema di gestione informatica dei documenti.
Memorizzazione	Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici.
Marca temporale	Evidenza informatica che consente di rendere opponibile a terzi un riferimento temporale; la marca temporale prova l'esistenza in un certo momento di una determinata informazione, sotto forma di struttura dati firmata da una Time Stamping Authority.
Metadati	Insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione.
Normativa regolante la conservazione digitale di documenti informatici	Si intende: il D.lgs. 7 marzo 2005, n. 82 e s.m.i. (Codice dell'amministrazione Digitale "CAD") e i relativi decreti attuativi, le regole tecniche e aggiungendo, per il documento informatico a rilevanza tributaria, le disposizioni di cui al DMEF 17 giugno 2014 e s.m.i., il DPR 26 ottobre 1972 n. 633 e s.m.i., il DPR 29 settembre 1973 n. 600 e s.m.i., i provvedimenti interpretativi emessi dagli organi competenti.
Originali non unici	I documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi.
Pacchetto di Archiviazione	Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche e le modalità riportate nel Manuale di conservazione.
Pacchetto di Distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta.
Pacchetto di invio documenti	Pacchetto informativo utilizzato per inviare i documenti fisici al sistema di conservazione a seguito dell'avvenuta accettazione di un pacchetto di versamento.
Pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel Manuale di conservazione;
Pacchetto informativo	Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, documenti amministrativi informatici, documenti informatici rilevanti ai fini tributari, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare.
Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza.
Piano della sicurezza del sistema di gestione informatica dei documenti	Documento, che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi nell'ambito dell'organizzazione di appartenenza.
Piano di conservazione	Strumento, integrato con il sistema di classificazione per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.
Presa in carico	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal Manuale di conservazione;
Processo di conservazione	Insieme delle attività finalizzate alla conservazione dei documenti informatici;

Processo/servizio di marcatura temporale	E' il processo/servizio che associa in modo affidabile un'informazione e un particolare momento, al fine di stabilire prove attendibili che indicano il momento in cui l'informazione esisteva.
Produttore	E' il Cliente, di norma diverso dal Titolare, che in proprio o attraverso le persone fisiche da egli stesso incaricate produce il Pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione; nel caso di Pubblica Amministrazione è identificato nella figura del responsabile della gestione documentale.
Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.
Registrazione informatica	Insieme delle informazioni risultanti da transazioni informatiche o dalla presentazione in via telematica di dati attraverso moduli o formulari resi disponibili in vario modo all'utente.
Registro particolare	Registro informatico specializzato per tipologia o per oggetto; nell'ambito della pubblica amministrazione è previsto ai sensi dell'articolo 53, comma 5 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.;
Registro di protocollo	Registro informatico della corrispondenza in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti.
Referente/i del Cliente	E'/sono le persone fisiche che il Cliente indica ad ARUBA quali punti di riferimento tecnico ed organizzativo per gli aspetti che riguardano le comunicazioni relative all'erogazione del servizio di conservazione.
Repertorio informatico	Registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche che trattano il procedimento, ordinati secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica.
Responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi	Dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.
Responsabile della sicurezza	Soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza.
Riferimento temporale	Informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento.
Scarto	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse culturale.
Scheda/e di conservazione	Elenco dei documenti informatici che il Cliente sottopone a conservazione con il Contratto.
Sistema di classificazione	Strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata.
Sistema di conservazione	Insieme di hardware, software, politiche, procedure, linee guida, regolamenti interni, infrastrutture fisiche e organizzative, volto ad assicurare la conservazione elettronica dei documenti del Cliente per il periodo di tempo specificato nel Contratto. Detto sistema tratta i documenti informatici in conservazione in pacchetti informativi che si distinguono in pacchetti di versamento, pacchetti di archiviazione e pacchetti di distribuzione;
Sistema di gestione informatica dei documenti	Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.; per i privati è il sistema che consente la tenuta di un documento informatico.
Staticità	Caratteristica che indica l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione;
Transazione informatica	Particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche della base di dati.

Testo unico	Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni.
Titolare/i	La/e persona/e fisica/che o giuridica/che o altro tipo di società o ente che è/sono giuridicamente responsabili/e della formazione dei documenti da conservare formati in proprio ovvero formati da terzi in suo/loro nome, conto e interesse.
Ufficio utente	Riferito ad un area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico.
Utente	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.
Validazione temporale	Il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi.
Versamento agli archivi di stato	Operazione con cui il responsabile della conservazione di un'amministrazione statale effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali.

Torna al sommario

2.2 Abbreviazioni e termini tecnici

Abbreviazioni e termini tecnici	
Agenzia per l'Italia Digitale (già DigitPA)	Ente pubblico non economico, con competenza nel settore delle tecnologie dell'informazione e della comunicazione nell'ambito della pubblica amministrazione. L'Ente, opera secondo le direttive per l'attuazione delle politiche e sotto la vigilanza del Ministro per la pubblica amministrazione e l'innovazione, con autonomia tecnica e funzionale, amministrativa, contabile, finanziaria e patrimoniale;
ASP - Application Service Provider	Fornitore di Servizi Applicativi;
CAD	Decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni - "Codice dell'amministrazione digitale";
CA - Certificatore Accreditato	Soggetto autorizzato dall'Agenzia per l'Italia Digitale che garantisce l'identità dei soggetti che utilizzano la firma digitale;
CC - Common Criteria	Criteri per la valutazione della sicurezza nei sistemi informatici, con riconoscimento internazionale in quanto evoluzione dei criteri europei (ITSEC), statunitensi (Federal Criteria), e canadesi (Canadian Criteria);
C.M.	Circolare Ministeriale;
CSCD - contratto di servizio di conservazione dei documenti	Contratto di servizio di conservazione dei documenti, ove sono esplicitate chiaramente l'ambito dell'affidamento conferito, le specifiche funzioni, le attività e le responsabilità affidate dal Cliente ad ARUBA;
D.LGS.	Decreto Legislativo;
D.M.	Decreto Ministeriale;
DNS – Domain Name System	Sistema di gestione dei nomi simbolici associati ad indirizzi di siti e domini Internet. Quando un messaggio di posta elettronica (e-mail), o un applicativo di consultazione di siti internet (browser) punta ad un dominio, il DNS traduce il nome inserito sotto forma di URL (es. http//www.....it)/ in un indirizzo costituito da una sequenza numerica convenzionale (es. 123.123.23.3).
D.P.C.M.	Decreto del Presidente del Consiglio dei Ministri;
D.P.R.	Decreto Presidente della Repubblica;
DPS	Documento Programmatico per la Sicurezza;
ETSI	European Telecommunications Standards Institute;
HSM - Hardware Security Module	Dispositivi hardware dedicati per la sicurezza crittografica e la gestione delle chiavi in grado di garantire un elevato livello di protezione;
HTTP (Hypertext Transfer Protocol)	Protocollo di trasmissione, che permette lo scambio di file (testi, immagini grafiche, suoni, video e altri documenti multimediali) su World Wide Web;
HTTPS (Secure Hypertext Transfer Protocol)	Protocollo di trasmissione, sviluppato da Netscape Communications Corporation, per la cifratura e decifratura dei dati trasmessi durante la consultazione di siti e pagine Internet. Corrisponde ad un'estensione del protocollo Internet standard HTTP (Hypertext Transfer Protocol), attraverso il protocollo SSL;
ICT - Information and Communication Technology	Tecnologia dell'Informazione e delle Telecomunicazioni. Il dipartimento che gestisce i sistemi informatici e telematici;
INTERNET	Un sistema globale di reti informatiche nel quale gli utenti di singoli computer possono ottenere informazioni da luoghi diversi. Lo sua grande diffusione è stata determinata principalmente dall'introduzione dei protocolli di trasmissione di documenti con riferimenti ipertestuali (HTTP) e dallo sviluppo del World Wide Web (WWW);
ISO – International Organization for Standardization	Organizzazione internazionale per la standardizzazione, costituita da organismi nazionali provenienti da più di 75 paesi. Ha stabilito numerosi standard nell'area dei sistemi informativi. L'ANSI (American National Standards Institute) è uno dei principali organismi appartenenti all'ISO;
ITSEC – Information Technology Security Evaluation Criteria	Criteri europei per la valutazione della sicurezza nei sistemi informatici;
MEF	Ministero dell'Economia e delle Finanze;

NTP – Network Time Protocol	Protocollo per la sincronizzazione del tempo;
OID – Object IDentifier	Sequenza numerica univoca che identifica un oggetto (struttura, algoritmo, parametro, sistema) nell'ambito di una gerarchia generale definita dall'ISO;
PdV	Pacchetto di Versamento
PdA	Pacchetto di Archiviazione
PdD	Pacchetto di Distribuzione
PU	Pubblico Ufficiale
PIN – Personal Identification Number	Codice di sicurezza riservato che permette l'identificazione del soggetto abbinato ad un dispositivo fisico. Permette ad esempio l'attivazione delle funzioni del dispositivo di firma;
POP – Point of Presence	Punto di accesso alla rete internet;
PSCD - Prestatore di Servizi di Conservazione dei Dati	Nella fattispecie, ARUBA;
SSL – Secure Socket Layer	Protocollo standard per la gestione di transazioni sicure su Internet, basato sull'utilizzo di algoritmi crittografici a chiave pubblica;
TSA	***Time Stamping Authority;***
TSS	***Time Stamping Service;***
TUDA - DPR 28 dicembre 2000, n. 445, e successive modificazioni -	***"Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa";***
URL – Uniform Resource Locator	Sistema standard di nomenclatura specificante un sito, dominio o altro oggetto (file, gruppo di discussione, ecc.) su Internet. La prima parte dell'URL (http , ftp, file, telnet, news) specifica il protocollo di accesso all'oggetto;
XML	***Extensible Markup language;***
WWW – World Wide Web	Insieme di risorse interconnesse da hyperlink accessibili tramite Internet

Torna al sommario

3 Normativa e standard di riferimento

3.1 Normativa di riferimento

Il sistema di conservazione digitale di ARUBA, è stato realizzato in conformità alla normativa vigente in materia di conservazione dei documenti informatici. Alla data l'elenco dei principali riferimenti normativi italiani in materia, ordinati secondo il criterio della gerarchia delle fonti, è costituito da:

- **Codice Civile** [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- **Legge 7 agosto 1990**, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- **Decreto del Presidente della Repubblica 28 dicembre 2000**, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- **Regolamento (UE) 2016/679** del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.
- **Regolamento (UE) N. 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
- **Decreto Legislativo 30 giugno 2003, n. 196** e s.m.i. – Codice in materia di protezione dei dati personali;
- **Decreto Legislativo 22 gennaio 2004, n. 42** e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- **Decreto Legislativo 7 marzo 2005 n. 82** e s.m.i. – Codice dell'amministrazione digitale (CAD);
- **Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013** – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
- **D.M. 17 giugno 2014** - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005;
- **Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013** - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- **Circolare AGID 10 aprile 2014, n. 65** - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.
- **Il DPR nr. 1409 del 30 settembre 1963 -** (Legge archivistica) all'art. 30 prevede che le cartelle cliniche siano conservate illimitatamente. Secondo le norme vigenti, inoltre, gli originali cartacei delle cartelle cliniche in quanto originali unici, non possono essere distrutti;
- **Circolare Ministero della Sanità 19 dicembre 1986, n. 61 -** Circolare avente per oggetto il periodo di conservazione della documentazione sanitaria presso le istituzioni sanitarie pubbliche e private di ricovero e cura
- **DM 14.2.1997 -** Norma di attuazione del D.lgs n.230/95, "Determinazione delle modalità affinché i documenti radiologici e di medicina nucleare e i resoconti esistenti siano resi tempestivamente disponibili per successive esigenze mediche, ai sensi dell'art. 111, comma 10, del decreto legislativo 17 marzo 1995, n. 230"
- **D.lgs 26 maggio 2000, n. 187 -** Attuazione della direttiva 97/43/Euratom in materia di protezione sanitaria delle persone contro i pericoli delle radiazioni ionizzanti connesse ad esposizioni mediche
- **Prontuario di selezione per gli archivi delle aziende sanitarie locali e delle aziende ospedaliere, 2005**
  Atto di indirizzo che reca indicazioni sui tempi di conservazione dei documenti generati e/o custodita Aziende Sanitarie pubbliche ed accreditate, redatto dal Ministero per i Beni e la Attività Culturali
- **Consiglio dei Ministri – Conferenza Stato Regioni 02 Marzo 2012 -** Linee Guida per la dematerializzazione della documentazione clinica in diagnostica per immagini. Normativa e prassi.

Torna al sommario

3.2 Standard di riferimento

Dove non sono indicate una versione e/o una data specifica, si intende fare riferimento alla più recente versione disponibile del documento citato:

- **ISO 14721:2012 OAIS** (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- **ISO/IEC 27001:2013**, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- **ETSI TS 101 533-1 V1.3.1 (2012-04)** Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- **ETSI TR 101 533-2 V1.3.1 (2012-04)**Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- **UNI 11386:2010 Standard SInCRO** - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- **ISO 15836:2009** Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.
- **Dicom 3.0** (Digital Imaging and Communications in Medicine, immagini e comunicazione digitali in medicina)
- **Health Level 7 (HL7)** versione 2.3.1 e 2.5
- Integrating the Healthcare Enterprise (IHE)
- **UNI ISO 15489-1: 2006** Information and documentation -- Records management -- Part 1: General
- **UNI ISO 15489-2: 2007** Information and documentation—Records management. Part 2: Guidelines
- **ISO 9001:2015** – Quality management systems – Requirements;

Torna al sommario

4 Ruoli e responsabilità

Nel sistema di conservazione si individuano i seguenti ruoli principali:

Ruolo	Organizzazione di appartenenza
Produttore	Cliente
Responsabile della conservazione	Cliente
Referenti del Cliente	Cliente
Responsabile del servizio di conservazione	ARUBA
Utente	Cliente/Terzi autorizzati

ARUBA, quale **Responsabile del servizio di conservazione** digitale dei documenti informatici del Cliente, agisce nei limiti dell'affidamento conferito e nell'osservanza degli obblighi ivi previsti nonché nel rispetto della normativa regolante la conservazione digitale di documenti informatici e delle presenti prescrizioni; in particolare, essa agirà attraverso persone fisiche dalla stessa formalmente incaricate.
L'attività di ARUBA riguarda la sola conservazione digitale dei documenti informatici del Cliente, senza alcuna responsabilità e possibilità di intervento ed accesso al contenuto degli stessi.
A carico del Responsabile del servizio di conservazione, non è posto alcun obbligo/dovere di elaborare i documenti informatici versati in conservazione al fine di estrarre i relativi metadati che, pertanto, dovranno essere forniti e associati ai rispettivi documenti a cura e carico del Cliente.
Il Responsabile del servizio di conservazione opera altresì nell'osservanza di quanto stabilito nel presente *Manuale*, al quale, se necessario, è sin da ora autorizzato ad apportare le modifiche, le integrazioni e gli aggiornamenti ritenuti necessari e/o conseguenti al mutato contesto tecnico-giuridico della normativa in materia.

L'utente è il soggetto che richiede al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge. Tali informazioni vengono fornite dal sistema di conservazione secondo le modalità previste nel presente *Manuale*.
Come già anticipato, il processo di conservazione impone al Cliente l'istituzione di una struttura ed una organizzazione interna, coerente con le proprie politiche di efficienza gestionale, che garantisca la piena osservanza alle disposizioni normative di riferimento e di quanto previsto dal presente *Manuale,* dal *Contratto* e dai rispettivi allegati.
A tale scopo, in base alle specifiche necessità, il Cliente deve, sia dal punto di vista dell'impostazione operativa delle

attività propedeutiche alla conservazione digitale dei propri documenti informatici sia dal punto di vista della scelta delle risorse coinvolte nel processo, organizzare il lavoro all'interno della propria organizzazione affinché esso venga svolto secondo i principi stabiliti dalla normativa in materia nonché dalle specifiche regole tecniche.
Tutto il personale di ARUBA è stato assunto nel rispetto di politiche rigorose volte ad accertarne, tra l'altro, l'alto grado di professionalità nonché i requisiti morali e di onorabilità.
Torna al sommario

4.1 Profili professionali all'interno della struttura organizzativa ARUBA

Qui di seguito si da conto della struttura organizzativa del processo di conservazione adottato evidenziando, nel contempo, le funzioni, le responsabilità e gli obblighi dei diversi soggetti che intervengono nel suddetto processo. Il processo di conservazione prevede una serie di attività che implicano il concorso di numerosi soggetti, a differenti livelli e con diverse responsabilità.

Qui di seguito vengono dettagliate per singola attività i diversi compiti e responsabilità delle figure preposte alla gestione e controllo del sistema di conservazione.

Il processo di conservazione, prevede, le seguenti **figure responsabili** :

1. Responsabile del servizio di conservazione;
2. Responsabile della funzione archivistica di conservazione;
3. Responsabile del trattamento dei dati personali, ora Responsabile della protezione dei dati personali (DPO)
4. Responsabile della sicurezza dei sistemi per la conservazione;
5. Responsabile dei sistemi informativi per la conservazione;
6. Responsabile dello sviluppo e della manutenzione del sistema di conservazione

Qui di seguito si riportano le **attività associate a ciascuna delle figure sopra elencate**:

- **Responsabile del servizio di conservazione**

Le attività affidate dal Responsabile della conservazione con l'Atto di Affidamento.

- **Responsabile della funzione archivistica di conservazione**

Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte del Cliente, 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 col Cliente 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.

- **Responsabile del trattamento dei dati personali, ora Responsabile della protezione dei dati personali (DPO)**

Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.

In particolare tenuto a:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento UE 2016/679 nonché da altre disposizioni relative alla protezione dei dati;
b) sorvegliare l'osservanza del Regolamento UE 2016/679, di altre disposizioni relative alla protezione dei dati nonché delle politiche del titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del Regolamento UE 2016/679;
d) cooperare con l'autorità di controllo; e
e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento UE 2016/679, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al

trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

- **Responsabile della sicurezza dei sistemi per la conservazione**

Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.

- **Responsabile dei sistemi informativi per la conservazione**

Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione; monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con il fornitore e 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.

- **Responsabile dello sviluppo e della manutenzione del sistema di conservazione**

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 col Cliente 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.

Ciascuno dei responsabili sopra elencati può avvalersi, per lo svolgimento delle attività al medesimo attribuite, di addetti ed operatori formalmente incaricati.
Nella pagina seguente sono riportati i dati dei soggetti che nel tempo hanno assunto particolari funzioni e responsabilità con riferimento al sistema di conservazione.
Torna al sommario

Ruoli e responsabilità					
Ruolo	**Cognome**	**Nome**	**Responsabilità**	**Data nomina**	**Data cessazione**
Responsabile del servizio di conservazione	Sassetti	Andrea	Definizione e attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione; definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente; corretta erogazione del servizio di conservazione al Cliente; 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.	04/01/2019	
	Braccagni	*Simone*	*Come sopra*	*01/09/2014*	*03/01/2019*
Responsabile della funzione archivistica di conservazione	Boschi	Serena	Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte del Cliente, 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 col Cliente ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.	01/09/2014	

Responsabile del trattamento dei dati personali, ora Responsabile della protezione dei dati personali (DPO)	Giommoni	Roberta	Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.In particolare tenuto a: a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento UE 2016/679 nonché da altre disposizioni relative alla protezione dei dati; b) sorvegliare l'osservanza del Regolamento UE 2016/679, di altre disposizioni relative alla protezione dei dati nonché delle politiche del titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del Regolamento UE 2016/679; d) cooperare con l'autorità di controllo; e e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento UE 2016/679, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.	24/05/2018	
Responsabile del trattamento dei dati personali	*Braccagni*	*Simone*	*Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.*	*01/09/2014*	*23/05/2018*
Responsabile della sicurezza dei sistemi per la conservazione	Tacconi	Nicola	Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.	13/05/2020	
	Corsi	*Matteo*	*Come sopra*	*06/09/2017*	*13/05/2020*
	Santoni	*Adriano*	*Come sopra*	*01/09/2014*	*05/09/2017*
Responsabile dei sistemi informativi per la conservazione	Gaverini	Angelo	Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione; monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con il fornitore; 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.	06/09/2017	
	Ravazza	*Roberto*	*Come sopra*	*01/09/2014*	*05/09/2017*

Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Mauro	Manetti	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 col Cliente 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.	06/09/2017	
	Pulvirenti	*Salvatore*	*Come sopra*	*01/09/2014*	*05/09/2017*

Torna al sommario

5 Struttura organizzativa per il servizio di conservazione

In questo capitolo sono indicate le strutture organizzative coinvolte nel servizio di conservazione comprese le responsabilità, che intervengono nelle principali funzioni che riguardano il servizio di conservazione
Torna al sommario

5.1 Organigramma

La figura in basso riporta le strutture organizzative coinvolte nel servizio di conservazione:

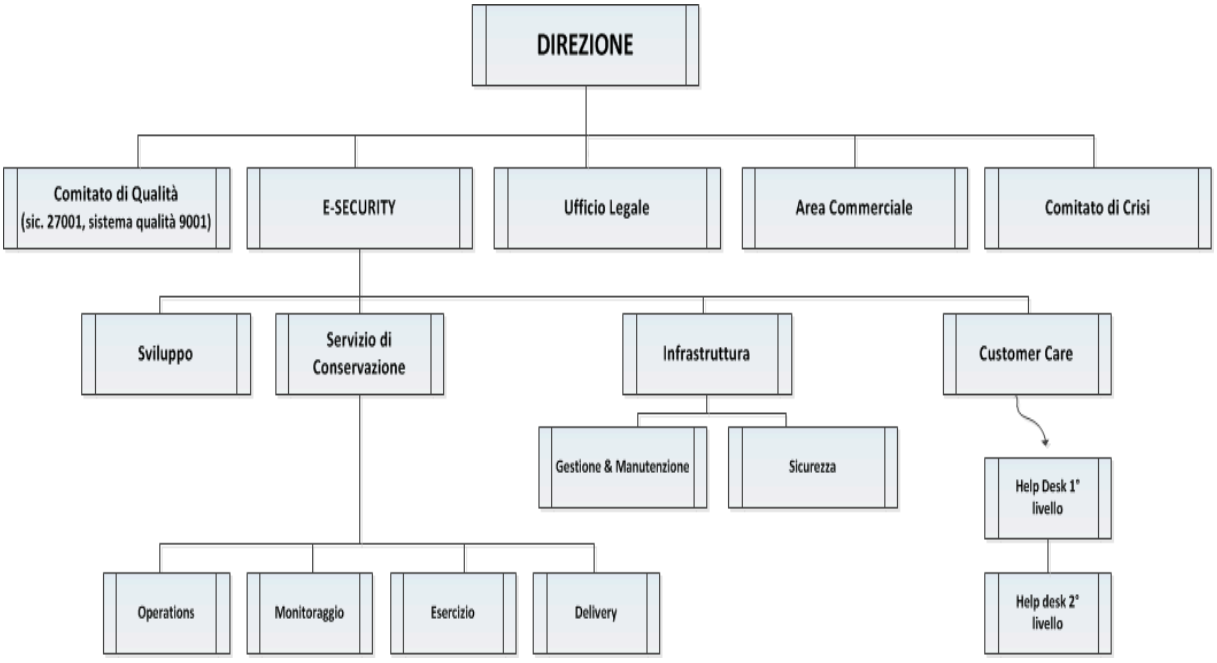


Figura 1: Rappresentazione delle strutture organizzative coinvolte nel servizio di conservazione

Torna al sommario

5.2 Strutture organizzative

Nello specifico le strutture funzionali dell'organizzazione operano in sinergia come segue:

- **Direzione**
  - ✓ la Direzione Aziendale garantisce la continuità generale dell'organizzazione
- **Comitato di Qualità**
  - ✓ garantisce la qualità operativa dei servizi ed il miglioramento di processi/procedure
- **E-Security**
  - ✓ rappresenta la Business Line che si occupa dei servizi e soluzioni di sicurezza in ambito digitale
- **Ufficio legale e Compliance**
  - ✓ garantisce la verifica periodica di conformità a normativa e standard di riferimento
- **Area Commerciale**
  - ✓ promuove il servizio di conservazione ai clienti
  - ✓ fornisce il supporto ai clienti in fase di prevendita (pre-sales)
  - ✓ partecipa attivamente al miglioramento dei servizi erogati in termini di definizione dell'offerta

- **Infrastruttura**
  - ✓ garantisce la sicurezza degli accessi logici e fisici, predisponendo appositi asset nel perimetro del data center
  - ✓ garantisce la sicurezza dell'infrastruttura tramite sistemi dedicati (video-sorveglianza, anti-intrusione, anti-incendio, etc)
  - ✓ designa, gestisce e provvede alla manutenzione delle aree sicure
- **Sviluppo**
  - ✓ fornisce know-how e supporto per lo sviluppo dei sistemi informativi
  - ✓ provvede alla progettazione di nuovi servizi e fornisce supporto per la manutenzione dei servizi attivi
  - ✓ si occupa dello studio di fattibilità per l'implementazione di nuovi servizi
  - ✓ fornisce interventi di analisi ed attività di assistenza nella fase di pre-vendita dei servizi
- **Servizio di Conservazione**
  - ✓ garantisce la gestione degli asset (hardware e software), occupandosi dell'intero processo di supply-chain del servizio di conservazione
  - ✓ provvede alla gestione delle informazioni, per l'intero ciclo di vita (dalla classificazione, al monitoraggio del sistema, fino alla protezione dei log)
  - ✓ si occupa della manutenzione ed assistenza, a garanzia della continuità operativa del servizio di conservazione
  - ✓ garantisce l'esecuzione del processo di conservazione in conformità ai requisiti tecnici normativi
  - ✓ provvede alla gestione operativa degli accessi logici e fisici, seguendo apposite procedure e mantenendo aggiornata la documentazione
  - ✓ garantisce l'attivazione e consegna dei servizi ai clienti, rispettando KPI e SLA concordati
- **Customer Care**
  - ✓ provvede all'assistenza tecnica rivolta ai clienti proprietari dei servizi
  - ✓ fornisce il supporto operativo sui servizi dei clienti
  - ✓ partecipa al miglioramento dei processi di comunicazione verso i clienti

Torna al sommario

5.3 Responsabilità e funzioni nel processo di conservazione

Di seguito sono indicati i compiti, le responsabilità e le funzioni di firma in relazione alle diverse fasi del processo di conservazione digitale.

Fasi del processo	Descrizione delle fasi del processo di conservazione		COMPITI	RESPONSABILITA'	FIRMA
FASE 1	**Acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico**				
	Descrizione sintetica	Il sistema di conservazione riceve l'indice del pacchetto di versamento contenente le informazioni sugli oggetti digitali che saranno inviati in conservazione.	**SC**	**RMGO**	**==**
FASE 2	**Verifica che il pacchetto di versamento e gli oggetti contenuti siano coerenti con le modalità previste nel presente Manuale di conservazione e con i formati di conservazione**				
	Descrizione sintetica	Viene verificato che l'oggetto ricevuto sia formalmente un indice xml in linea con lo standard DocFly. Viene verificato che il PdV è versato nei termini contrattuali e di servizio stabiliti col produttore	**SC**	**RMGO**	**==**
FASE 3	**Preparazione del rapporto di conferma**				
	Descrizione sintetica	Il sistema, una volta effettuate le verifiche dell'idPdV rimane in attesa dell'invio dei documenti	**SC**	**RMGO**	**==**
FASE 4	**Eventuale rifiuto del pacchetto di versamento, nel caso in cui le verifiche di cui alla FASE 2 abbiano evidenziato anomalie e/o non conformità**				
	Descrizione sintetica	Il sistema scarta l'intero pacchetto e invia notifica in automatico	**SC**	**RMGO**	**==**
FASE 5	**Ricezione e verifica dei documenti**				
	Descrizione sintetica	Per ognuno di documenti inviati viene verificato che l'hash del documento informatico sia corrispondente all'hash dichiarato all'interno del medesimo indice del pacchetto al fine di avere garanzia che la trasmissione del pacchetto sia avvenuta correttamente e che l'integrità del documento informatico ricevuto sia assicurata. Vengono inoltre effettuati controlli di leggibilità, integrità e che i documenti non siano già presenti a sistema	**SC**	**RMGO**	**==**
FASE 7	**Generazione automatica del rapporto di versamento relativo a ciascun pacchetto di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo Universale Coordinato (UTC), e una o più impronte, calcolate sull'intero contenuto del pacchetto di versamento, secondo le modalità di seguito descritte**				
	Descrizione sintetica	Il sistema genera in automatico il rapporto di versamento per ognuno dei PdV che ha superato i controlli qualitativi	**SC**	**RMGO**	**==**
FASE 8	**Sottoscrizione del rapporto di versamento con firma digitale apposta da ARUBA**				
	Descrizione sintetica	Il sistema provvede in automatico alla sottoscrizione digitale del rapporto di versamento con certificato del RSC e alla marcatura temporale del rapporto.	**SC**	**RMGO**	**RSC**
FASE 9	**Preparazione e gestione del Pacchetto di Archiviazione (c.d. Pacchetto di Archiviazione)**				

	Descrizione sintetica	Il sistema genera il Pacchetto di Archiviazione secondo le modalità descritte al cap. 7	**SC**	**RMGO**	**==**
FASE 10	**Sottoscrizione del Pacchetto di Archiviazione con firma digitale apposta da ARUBA e apposizione di una validazione temporale con marca temporale alla relativa impronta. Tale operazione viene in breve chiamata anche "Chiusura del Pacchetto di Archiviazione"**				
	Descrizione sintetica	Come previsto da normativa l'Indice di Conservazione, viene sottoscritto digitalmente dal RSC, una volta passato nello stato "conservato".	**SC**	**RMGO**	**RSC**
FASE 11	**Preparazione e sottoscrizione con firma digitale del Responsabile del servizio di conservazione del Pacchetto di Distribuzione ai fini dell'esibizione richiesta dall'utente**				
	Descrizione sintetica	Come previsto da normativa il PdD viene sottoscritto digitalmente dal RSC	**SC**	**RER**	**RSC**
FASE 12	**Produzione di duplicati informatici o di copie informatiche effettuati su richiesta del Cliente in conformità a quanto previsto dalle regole tecniche in materia di formazione del documento informatico**				
	Descrizione sintetica	Richieste di duplicati o copie informatiche vengono sottoscritte digitalmente dal RSC in modo da attestarne l'autenticità rispetto al documento sorgente	**SC**	**RER**	**RSC**
FASE 13	**Eventuale scarto del Pacchetto di Archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dal contratto di servizio, dandone preventiva informativa al Cliente al fine di raccoglierne il consenso**				
	Descrizione sintetica	Una volta scaduti i termini di conservazione previsti dal contratto, il sistema provvede a inviare una mail di notifica al client, il quale potrà decidere in autonomia se cancellarli dal sistema.	**SC**	**RCD** **DPO**	**==**

Legenda:
- **RMGO** - responsabile del monitoraggio della gestione ordinaria del sistema e dei processi di base di conservazione
- **RER** - responsabile dell'esibizione/restituzione dei documenti informatici conservati
- **RIS** - responsabile dell'infrastruttura sistemistica, del piano di Disaster Recovery / Piano di continuità operativa (Business Continuity Plan) e della sicurezza
- **RCD** - responsabile della cancellazione dei documenti e dei dati digitali
- **DPO** - responsabile della protezione dei dati personali
- **RSC** - responsabile del servizio di conservazione
- **SC** - Sistema di conservazione

Torna al sommario

6 Oggetti sottoposti a conservazione

6.1 Descrizione delle tipologie dei documenti sottoposti a conservazione

Come chiaramente esplicitato nel *Contratto*, il servizio di conservazione digitale dei documenti informatici non riguarda la conservazione di documenti analogici di alcun tipo e genere.

Prima dell'attivazione del servizio il Cliente esplicita la tipologia di documenti che intende sottoporre a conservazione mediante il servizio offerto da ARUBA, evidenziandone le caratteristiche nell'apposito allegato del *Contratto*.

Per ogni formato definito viene individuato anche il **software necessario per la visualizzazione** del documento informatico.

ARUBA configura sul servizio un profilo di conservazione per ogni tipologia/classe di documenti su indicazione del Cliente, classificato come omogeneo in base ai dati da utilizzare per l'indicizzazione ed i termini di conservazione (vedi apposito allegato al *Contratto*).

Ogni variazione di formato di documento e di software associato per la visualizzazione oppure dei dati utilizzati per l'indicizzazione deve essere preventivamente concordato con ARUBA e configurato sul servizio.

Il sistema di conservazione digitale è impostato per accettare le seguenti tipologie di documento:

- **documenti informatici** sono la "rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti" come definito dal Codice dell'Amministrazione Digitale;
- **documenti amministrativi** costituenti atti amministrativi con rilevanza interna al procedimento amministrativo;
- **documenti rilevanti ai fini tributari** come stabilito nel DM del MEF del 17 giugno 2014;
- **documenti clinici** che possono contenere informazioni su osservazioni cliniche dirette, quali rivelazioni di anamnesi, segni vitali o sintomi, osservazioni indirette, derivanti, ad esempio da diagnostica strumentale, esami di laboratorio o rappresentazione iconografica di resoconti radiologici, oppure opinioni mediche quali valutazioni di osservazioni cliniche, consulti e consulenze, obiettivi da raggiungere o piani diagnostico terapeutici, azioni di natura clinico-sanitaria atte a generare osservazioni cliniche ed opinioni mediche;
- **altri documenti in genere**

Le diverse tipologie di documenti sono prodotti/formati/emessi a cura e sotto l'esclusiva responsabilità del Cliente mediante una delle seguenti principali modalità:

a) redazione tramite l'utilizzo di appositi strumenti software;
b) 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;
c) registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari;
d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

Al fine di garantire l'identificazione certa del soggetto che ha formato il documento, i documenti informatici posti in conservazione saranno in genere sottoscritti con firma digitale del Cliente e dovranno essere identificati in modo univoco e persistente.

E' prevista la possibilità di depositare in conservazione documenti informatici non sottoscritti. In tal caso deve necessariamente essere preventivamente dichiarata, per ogni classe/tipo di documento, nell'apposito allegato del *Contratto*.

Torna al sommario

6.2 Copie informatiche di documenti analogici originali unici

Come noto, l'art. 22 del CAD stabilisce che:

a) (comma 2) le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico hanno la stessa efficacia probatoria degli originali da cui sono estratte, se la loro conformità è attestata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e

asseverata secondo le regole tecniche stabilite ai sensi dell'articolo 71.

b) (comma 3) le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico nel rispetto delle regole tecniche di cui all'articolo 71 hanno la stessa efficacia probatoria degli originali da cui sono tratte se la loro conformità all'originale non è espressamente disconosciuta.

Pertanto, alla luce di quanto sopra, il Cliente qualora intendesse depositare in conservazione copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico è tenuto, a propria cura e spese, a predisporre quanto necessario per ottemperare a quanto previsto dalle richiamate disposizioni.

In particolare, sarà cura e carico del Cliente:

a) produrre la copia per immagine su supporto informatico del documento analogico mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto;

successivamente:

b) (ai fini di quanto stabilito dall'articolo 22, co. 3, del CAD), dovrà sottoscrivere con firma digitale la copia per immagine del documento analogico;

oppure

c) laddove richiesto dalla natura dell'attività, (art. 22, comma 2, del CAD), dovrà inserire nel documento informatico contenente la copia per immagine, l'attestazione di conformità all'originale analogico. Il documento informatico così formato dovrà poi essere sottoscritto con firma digitale del notaio o con firma digitale o firma elettronica qualificata di pubblico ufficiale a ciò autorizzato.

Si tenga presente che l'attestazione di conformità delle copie per immagine su supporto informatico di uno o più documenti analogici, effettuata per raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia, può essere prodotta, sempre a cura e carico del Cliente, come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. Tale documento informatico separato dovrà essere sottoscritto con firma digitale del notaio o con firma digitale o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato.

In sostanza, in questi casi il Cliente dovrà alternativamente depositare in conservazione:

- la copia per immagine su supporto informatico dell'originale analogico contenente l'attestazione di conformità all'originale analogico debitamente sottoscritto come sopra riportato;

oppure

- le copie per immagine su supporto informatico unitamente all'attestazione di conformità prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni singola copia per immagine, debitamente sottoscritto come sopra riportato.

Torna al sommario

6.3 Formati gestiti

Come noto, la leggibilità di un documento informatico dipende dalla possibilità e dalla capacità di interpretare ed elaborare correttamente i dati binari che costituiscono il documento, secondo le regole stabilite dal formato con cui esso è stato rappresentato. Il formato di un documento informatico è la convenzione usata per rappresentare il contenuto informativo mediante una sequenza di byte.

Il sistema di conservazione ARUBA garantisce la conservazione dei documenti prodotti nei formati previsti dall'allegato 2 "Formati" del DPCM 03-12-2013.

I formati ammessi alla conservazione, devono essere specificati dal Cliente prima del versamento in conservazione e per tale ragione vengono esplicitati all'interno di uno specifico allegato, facente parte del Contratto di servizio stipulato con ARUBA (come descritto al par 10.1.2).

Torna al sommario

6.3.1 Caratteristiche generali dei formati

I formati scelti devono essere, puntualmente richiamati nell'apposito allegato al *Contratto.* ARUBA, comunque raccomanda un insieme di formati che sono stati dalla stessa valutati in funzione di alcune caratteristiche quali:

CARATTERISTICA		DESCRIZIONE DELLA CARATTERISTICA
1	**APERTURA**	Un formato si dice "aperto" quando è conforme a specifiche pubbliche, cioè disponibili a chiunque abbia interesse ad utilizzare quel formato. La disponibilità delle specifiche del formato rende sempre possibile la decodifica dei documenti rappresentati in conformità con dette specifiche, anche in assenza di prodotti che effettuino tale operazione automaticamente. Questa condizione si verifica sia quando il formato è documentato e pubblicato da un produttore o da un consorzio al fine di promuoverne l'adozione, sia quando il documento è conforme a formati definiti da organismi di standardizzazione riconosciuti. In quest'ultimo caso tuttavia si confida che quest'ultimi garantiscono l'adeguatezza e la completezza delle specifiche stesse. In relazione a questo aspetto, ARUBA ha privilegiato formati già approvati dagli Organismi di standardizzazione internazionali quali ISO e OASIS.
2	**SICUREZZA**	La sicurezza di un formato dipende da due elementi: - il grado di modificabilità del contenuto del file; - la capacità di essere immune dall'inserimento di codice maligno.
3	**PORTABILITÀ**	Per portabilità si intende la facilità con cui i formati possano essere usati su piattaforme diverse, sia dal punto di vista dell'hardware che del software, inteso come sistema operativo. Di fatto si ottiene mediante l'impiego fedele di standard documentati e accessibili e dalla loro diffusione sul mercato.
4	**FUNZIONALITÀ**	Per funzionalità si intende la possibilità da parte di un formato di essere gestito da prodotti informatici, che prevedono una varietà di funzioni messe a disposizione del Cliente per la formazione e gestione del documento informatico.
5	**SUPPORTO ALLO SVILUPPO**	Il supporto allo sviluppo è la modalità con cui si mettono a disposizione le risorse necessarie alla manutenzione e sviluppo del formato e i prodotti informatici che lo gestiscono (organismi preposti alla definizione di specifiche tecniche e standard, società, comunità di sviluppatori, ecc.).
6	**DIFFUSIONE**	La diffusione è l'estensione dell'impiego di uno specifico formato per la formazione e la gestione dei documenti informatici. Questo elemento influisce sulla probabilità che esso venga supportato nel tempo, attraverso la disponibilità di più prodotti informatici idonei alla sua gestione e visualizzazione.

Torna al sommario

6.3.2 Formati consigliati per la conservazione

Oltre al soddisfacimento delle caratteristiche suddette, nella scelta dei formati idonei alla conservazione, ARUBA è stata estremamente attenta affinché i formati stessi fossero capaci a far assumere al documento le fondamentali caratteristiche di immodificabilità e staticità.

Pertanto, alla luce delle suddette considerazioni, i formati indicati dalla normativa per la conservazione delle diverse tipologie di documenti informatici sono i seguenti:

FORMATO	DESCRIZIONE	
PDF - PDF/A	Il PDF (Portable Document Format) è un formato creato da Adobe nel 1993 che attualmente si basa sullo standard ISO 32000. Questo formato è stato concepito per rappresentare documenti complessi in modo indipendente dalle caratteristiche dell'ambiente di elaborazione del documento. Il formato è stato ampliato in una serie di sotto-formati tra cui il PDF/A.	
	Caratteristiche e dati informativi	
	Informazioni gestibili	Testo formattato, immagini, grafica vettoriale 2D e 3D, filmati.
	Sviluppato da	Adobe Systems - http://www.adobe.com/
	Estensione	.pdf
	Tipo MIME	Application/pdf
	Formato aperto	SI
	Specifiche tecniche	Pubbliche
	Standard	ISO 32000-1 (PDF) ISO 19005-1:2005 (vers. PDF 1.4) ISO 19005-2:2011 (vers. PDF 1.7)
	Altre caratteristiche	Assenza di collegamenti esterni
		Assenza di codici eseguibili
		Assenza di contenuti crittografati
		Il file risulta indipendente da codici e collegamenti esterni che ne possono alterare l'integrità e l'uniformità nel lungo periodo
		Le più diffuse suite d'ufficio permettono di salvare direttamente i file nel formato PDF/A
		Sono disponibili prodotti per la verifica della conformità di un documento PDF al formato PDF/A.
	Software necessario alla visualizzazione	Adobe Reader

FORMATO	DESCRIZIONE	
TIFF	Il TIFF è un formato utilizzato per la rappresentazione delle immagini mediante grafica raster (l'immagine digitale è formata da un insieme pixel, ordinate secondo linee e colonne).	
	Caratteristiche e dati informativi	
	Informazioni gestibili	Immagini
	Sviluppato da	Aldus Corporation in seguito acquistata da Adobe
	Estensioni	.tif
	Tipo MIME	image/tiff
	Formato aperto	NO
	Specifiche tecniche	Pubbliche
	Ultime versioni	TIFF 6.0 del 1992 TIFF Supplement 2 del 2002
	Standard	ISO 12639 (TIFF/IT) ISO 12234 (TIFF/EP)
	Altre caratteristiche	Formato immagine raster, in versione non compressa o compressa senza perdita di informazione
		Formato utilizzato per la conversione in digitale di documenti cartacei
		Esistono parecchie versioni, alcune delle quali proprietarie (che ai fini della conservazione nel lungo periodo sarebbe bene evitare)
		In genere le specifiche sono pubbliche e non soggette ad alcuna forma di limitazione
	Software necessario alla visualizzazione	ImageGlass

FORMATO	DESCRIZIONE
JPG	Il JPG è un formato utilizzato per la rappresentazione delle immagini mediante grafica raster (l'immagine digitale è formata da un insieme pixel, ordinate secondo linee e colonne).
	Caratteristiche e dati informativi

Informazioni gestibili	Immagini
Sviluppato da	Joint Photographic Experts Group
Estensioni	.jpg, .jpeg
Tipo MIME	image/jpeg
Formato aperto	SI
Specifiche tecniche	Pubbliche
Ultima versione	2009
Standard	ISO/IEC 10918:1
Altre caratteristiche	Formato immagine raster, in versione compressa. Può comportare una perdita di qualità dell'immagine originale.
	JPG è il formato più utilizzato per la memorizzazione di fotografie ed è quello più comune su World Wide Web.
	Lo stesso gruppo che ha ideato il JPG ha prodotto il JPEG 2000 con estensione .jp2 (ISO/IEC 15444-1) che può utilizzare la compressione senza perdita di informazione. Il formato JPEG 2000 consente, inoltre, di associare metadati ad un'immagine. Nonostante queste caratteristiche la sua diffusione è tutt'oggi relativa.
Software necessario alla visualizzazione	ImageGlass

FORMATO	**DESCRIZIONE**	
Office Open XML (OOXML)	Offine Open XML, comunemente abbreviato in OOXML, è un formato di file, sviluppato da Microsoft, basato sul linguaggio XML per la creazione di documenti di testo, fogli di calcolo, presentazioni, grafici e database.	
	Caratteristiche e dati informativi	
	Informazioni gestibili	Documenti di testo, fogli di calcolo, presentazioni, grafici e database
	Sviluppato da	Microsoft
	Estensioni principali	.docx, .xlsx, .pptx
	Tipo MIME	*application/vnd.openxmlformats-officedocument.wordprocessingml.document,application/x-tika-ooxml,application/zip* *application/vnd.ms-powerpoint,application/vnd.openxmlformats-officedocument.presentationml.template,application/vnd.ms-powerpoint.addin.macroEnabled.12,application/vnd.ms-powerpoint.presentation.macroEnabled.12,application/vnd.ms-powerpoint.template.macroEnabled.12,application/vnd.ms-powerpoint.slideshow.macroEnabled.12* *application/vnd.ms-excel,application/vnd.openxmlformats-officedocument.spreadsheetml.template,application/vnd.ms-excel.sheet.macroEnabled.12,application/vnd.ms-excel.template.macroEnabled.12,application/vnd.ms-excel.addin.macroEnabled.12,application/vnd.ms-excel.sheet.binary.macroEnabled.12,application/x-tika-msoffice* *application/vnd.openxmlformats-officedocument.spreadsheetml.sheet,application/x-tika-ooxml*
	Formato aperto	SI
	Specifiche tecniche	Pubblicate da Microsoft dal 2007
	Ultima versione	1.1
	Standard	ISO/IEC DIS 29500:2008
	Altre caratteristiche	Open XML è adottato dalla versione 2007 della suite Office di Microsoft
		MS Office 2007 legge e scrive file conformi a ECMA-376 Edition 1
		MS Office 2010 legge e scrive file conformi a ISO/IEC 29500:2008 transitional (norme transitorie) e legge file conformi a ISO/IEC 29500:2008 strict (indicazioni fondamentali)
		Documenti conformi ad ISO/IEC 29500:2008 strict sono supportati da diversi prodotti informatici disponibili sul mercato

		Il formato Office Open XML dispone di alcune caratteristiche che lo rendono adatto alla conservazione nel lungo periodo, tra queste l'embedding dei font, la presenza di indicazioni di presentazione del documento, la possibilità di applicare al documento la firma digitale XML.
		I metadati associabili ad un documento che adotta tale formato sono previsti dallo standard ISO 29500:2008
	Software necessario alla visualizzazione	https://openxmlviewer.codeplex.com/

FORMATO	**DESCRIZIONE**	
Open Document Format	ODF (Open Document Format, spesso referenziato con il termine OpenDocument) è uno standard aperto, basato sul linguaggio XML, sviluppato dal consorzio OASIS per la memorizzazione di documenti corrispondenti a testo, fogli elettronici, grafici e presentazioni.	
	Caratteristiche e dati informativi	
	Informazioni gestibili	Documenti di testo, fogli di calcolo, presentazioni e grafici.
	Sviluppato da	OASIS
	Estensioni principali	.ods, .odp, .odg, .odb
	Tipo MIME	application/vnd.oasis.opendocument.text
	Formato aperto	SI
	Specifiche tecniche	Pubblicate da OASIS dal 2005
	Ultima versione	1.0
	Standard	ISO/IEC 26300:2006 UNI CEI ISO/IEC 26300
	Altre caratteristiche	Formato basato sul linguaggio XML
		Un documento è descritto da più strutture XML, relative a contenuto, stili, metadati ed informazioni per l'applicazione
		Lo standard ISO/IEC IS 26300:2006 è ampiamente usato come standard documentale nativo, oltre che da OpenOffice.org, da una ampia serie di altri prodotti disponibili sulle principali piattaforme: Windows, Linux. Mac.
		È stato adottato come standard di riferimento da moltissime organizzazioni governative e da diversi governi ed ha una "penetrazione" di mercato che cresce giorno per giorno.
	Software necessario alla visualizzazione	Open Office

FORMATO	**DESCRIZIONE**	
XML	Extensible Markup Language (XML) è un formato di testo flessibile derivato da SGML (ISO 8879). Su XML si basano numerosi linguaggi standard utilizzati nei più diversi ambiti applicativi. Ad esempio: SVG usato nella descrizione di immagini vettoriali, XBRL usato nella comunicazione di dati finanziari, ebXML usato nel commercio elettronico, SOAP utilizzato nello scambio dei messaggi tra Web Service	
	Caratteristiche e dati informativi	
	Informazioni gestibili	Contenuto di evidenze informatiche, dei pacchetti di versamento, archiviazione e distribuzione, ecc.
	Sviluppato da	W3C - http://www.w3.org/
	Estensione	.xml
	Tipo MIME	Application/xml Text/xml
	Formato aperto	SI
	Specifiche tecniche	Pubblicate da W3C – http://www.w3.org/XML/
	Altre caratteristiche	Formato di testo flessibile derivato da SGML (ISO 8879).
	Software necessario alla visualizzazione	Qualsiasi editor di testo. Inoltre è possibile, concordando con il Cliente le caratteristiche di un opportuno file xslt, produrne una copia human readable con Microsoft Internet Explorer / Firefox / Google Chrome o altri browser

FORMATO	**DESCRIZIONE**

TXT	File di testo semplice, non strutturato, è adatto a contenuti puramente testuali e non richiede particolari possibilità di strutturazione o informazioni aggiuntive sulla struttura o la formattazione. Non contiene quindi indicazioni di formattazione nascoste o visibili (p. es. grassetto, rientri, colori ecc.) o indicazioni strutturali (p. es. titoli, sezioni, sottosezioni, indice ecc.). Questi file molto semplici offrono, sul lungo periodo, ottime garanzie per la conservazione e leggibilità dei dati.	
	Caratteristiche e dati informativi	
	Informazioni gestibili	Testo
	Estensione	.txt
	Tipo MIME	text/plain
	Formato aperto	SI
	Specifiche tecniche	Pubbliche
	Standard	ISO 646 RFC 3629 ISO/ IEC 10646
	Altre caratteristiche	Sono ammessi i seguenti set di caratteri: • US-ASCII; • ISO 8859-1 e 8859-15 (Latin-1 e Latin-9); • Unicode (UTF-8, UTF-16)
		Ai fini della conservazione nell'uso di tale formato, è importante specificare la codifica del carattere (Character Encoding) adottata.
	Software necessario alla visualizzazione	Notepad++

FORMATO	**DESCRIZIONE**	
EML	Electronic Mail Message (EML) è un formato di testo che definisce la sintassi di messaggi di posta elettronica scambiati tra utenti	
	Caratteristiche e dati informativi	
	Informazioni gestibili	Messaggi di posta elettronica e PEC
	Sviluppato da	Internet Engineering Task Force (IETF) - http://www.ietf.org/
	Estensione	.eml
	Tipo MIME	Message/rfc2822
	Formato aperto	SI
	Specifiche tecniche	Pubblicate da IETF - http://www.ietf.org/rfc/rfc2822.txt
	Altre caratteristiche	è un formato di testo flessibile derivato da SGML (ISO 8879).
	Software necessario alla visualizzazione	La maggior parte dei client di posta elettronica supportano la visualizzazione di file eml

Per quanto concerne il formato degli allegati al messaggio di posta elettronica, valgono le indicazioni di cui sopra. I formati XML ed EML sono accettati solamente per le classi documentali di tipo "PEC".
Torna al sommario

6.3.3 Identificazione

L'associazione del documento informatico al suo formato può avvenire, attraverso varie modalità, tra cui le più impiegate sono:

1. l'estensione: una serie di lettere, unita al nome del file attraverso un punto, ad esempio [nome del file].doc identifica un formato sviluppato dalla Microsoft;
2. il magic number: i primi byte presenti nella sequenza binaria del file, ad esempio 0xffd8 identifica i file immagine di tipo .jpeg;
3. verifica della corrispondenza tra il tipo MIME ricavato dall'estensione del file ed il tipo MIME ricavato dal magic number;
4. l'utilizzo di tool automatici specifici come Apache TIKA

Per identificare il formato dei files posti in conservazione occorre procedere all'analisi di ogni singolo documento

informatico contenuto all'interno dei pacchetti di versamento. ARUBA procede come segue:

1	**Fase di IDENTIFICAZIONE**	Ogni documento che viene inviato al sistema di conservazione deve essere stato precedentemente ed espressamente indicato dal sistema versante. In questo modo tutti i documenti non noti vengono automaticamente non riconosciuti e quindi rifiutati
2	**Fase di RICEZIONE**	Il sistema Aruba, una volta noti i documenti che il Cliente vuole mettere in conservazione si mette in attesa, secondo i canali concordati, della loro ricezione
3	**Fase di VALIDAZIONE**	Una volta che i documenti vengono recepiti dal sistema di conservazione la prima elaborazione effettuata sugli stessi è quella del rilevamento della tipologia corretta del documento. Solo se questo esame restituisce esito positivo vengono realizzate ulteriori validazioni atte a garantire la correttezza formale del documento, secondo gli standard qui esposti e gli accordi convenuto col Cliente

Torna al sommario

6.4 Metadati da associare alle diverse tipologie di documenti

Con il termine "metadati" si indicano tutte le informazioni significative associate al documento informatico, escluse quelle che costituiscono il contenuto del documento stesso. I metadati riguardano principalmente, ma non esclusivamente, i modi, i tempi ed i soggetti coinvolti nel processo della formazione del documento informatico, della sua gestione e della sua conservazione.

Metadati sono anche le informazioni riguardanti gli autori, gli eventuali sottoscrittori e le modalità di sottoscrizione e la classificazione del documento. I metadati devono essere associati al documento dal Cliente prima del versamento in conservazione e per tale ragione vengono esplicitati all'interno di uno specifico allegato, facente parte del Contratto di servizio stipulato con ARUBA (come specificato al par 10.1.2).
I metadati forniti dal Cliente restano di proprietà del Cliente medesimo.

I metadati, seppur chiaramente associati al documento informatico, possono essere gestiti indipendentemente dallo stesso. In relazione ai diversi tipi di documenti informatici posti in conservazione, è previsto un "**set minimo"** di metadati.

Oltre al set minimo di metadati, il Cliente potrà decidere di associare al documento informatico eventuali ulteriori metadati c.d. "*extrainfo*". Le extra info verranno inserite, al pari degli altri metadati, nell'indice di conservazione che. I metadati *extrainfo* dovranno essere puntualmente individuati nello spazio ad essi riservato nell'apposito allegato del *Contratto* e verranno opportunamente gestiti da Aruba come in esso concordato.

Torna al sommario

6.5 Modalità di assolvimento dell'imposta di bollo sui documenti posti in conservazione

Il Cliente è tenuto al pagamento dell'imposta di bollo eventualmente dovuta sui documenti depositati in conservazione.

Pertanto, il versamento dell'imposta dovuta dovrà essere effettuata dal Cliente nei termini previsti dall'art. 6 del DMEF 17 giugno 2014 e nei modi di cui all'art. 17 del D.Lgs. 9 luglio 1997, n. 241 e loro successive modificazioni e/o integrazioni.

Tutti i relativi e conseguenti obblighi, adempimenti e formalità per l'assolvimento dell'imposta di bollo sui documenti informatici posti in conservazione sono ad esclusivo onere e carico del Cliente, il quale dovrà attenersi alle disposizioni di legge ed ai documenti di prassi emanati ed emanandi.

Allo stesso modo, sono ad esclusivo onere e carico del Cliente tutte le comunicazioni da presentare al competente Ufficio delle entrate in forza di quanto stabilito dalla normativa regolante la conservazione digitale di documenti informatici.

Torna al sommario

6.6 Pacchetto di versamento

In questo paragrafo sono fornite le tipologie di pacchetto di versamento gestite e per ciascuna di esse descritta la struttura dati.
Il nostro standard prevede l' indice di un pacchetto di versamento che si caratterizza per le seguenti parti:

- area di identificazione del PDV
- area di identificazione dei documenti costituenti il pacchetto e composta dai seguenti elementi:

- metadato obbligatori
- metadati extra-info

Nella prima parte il dato importante e obbligatorio è il *pdvid* ovvero l'identificativo del PDV. Esso deve essere unico all'interno dello spazio gestito dal produttore, quindi indipendentemente dall'archivio.

La seconda parte prevede una lista di elementi, uno per ogni documento da versare. Ogni singolo file deve essere per prima cosa identificato. A questo scopo sono necessari i seguenti dati:
- nome file
- algoritmo di hashing per la generazione dell'impronta
- impronta del documento

Inoltre, poiché il sistema deve controllare la tipologia di documento per valutarne l'aderenza alle condizioni espresse in fase di contratto, deve essere indicato il MIME type del documento.
Per rimanere poi aderenti alla norma vigente devono essere passati anche un id unico dei singoli documenti del pacchetto e la data di chiusura degli stessi.

L'ultima parte dell'Indice contiene un insieme di metadati extra-info, così come definiti in fase contrattuale col Produttore
Torna al sommario

6.6.1 Specifiche Pacchetto di Versamento

Le specifiche del Pacchetto di Versamento secondo lo standard definito da ARUBA, sono disponibili all'interno di specifiche sezioni pubblicate sui siti web www.pec.it e guide.pec.it.
Torna al sommario

6.7 Pacchetto di Archiviazione

In questo paragrafo viene resa la struttura del Pacchetto di Archiviazione nonché il trattamento dei pacchetti di archiviazione.
Torna al sommario

6.7.1 Specifiche Pacchetto di Archiviazione

Il Pacchetto di Archiviazione è composto da varie parti:

- l'insieme degli elementi (documenti e/o altri PdA) che compongono il pacchetto
- l'Indice del Pacchetto di Archiviazione (IPdA) che elenca tutti gli elementi del pacchetto. Il formato dell'indice è aderente allo standard UNI SInCRO (nel quale è indicato come IdC – Indice di Conservazione) ed è marcato temporalmente e firmato elettronicamente con certificato del Responsabile del Sistema di Conservazione.

Torna al sommario

6.8 Pacchetto di Distribuzione

Il Pacchetto di Distribuzione contiene l'insieme degli elementi (documenti e/o PdA) precedentemente ricercati e selezionati dall'utente.

Viene offerto sotto forma di un archivio .zip che per ogni elemento contiene:

- una cartella contenente l'elemento stesso. Nel caso di un documento il documento stesso, nel caso di un PdA l'intero PdA, ovvero tutti gli elementi di cui è costituito
- un'altra cartella che contiene l'indice relativo all'elemento individuato, marcato temporalmente e firmato elettronicamente con certificato del Responsabile del Sistema di Conservazione

Torna al sommario

6.9 Documenti rilevanti ai fini delle disposizioni tributarie

In considerazione di quanto previsto dall'art. 21, co. 5, del CAD[1], i documenti informatici rilevanti ai fini delle disposizioni tributarie (di seguito, per brevità chiamati anche "**DIRT**") sono conservati nel rispetto di quanto previsto dalle disposizioni in materia, attualmente riconducibili al Decreto del 17 giugno 2014 del Ministero dell'Economia e delle Finanze e successive modificazioni ed integrazioni.

Il Cliente, pertanto, è tenuto a conoscere le disposizioni relative alla normativa regolante la conservazione digitale di documenti informatici in vigore ed a controllare l'esattezza dei risultati ottenuti con l'utilizzo del Servizio di conservazione fornito da ARUBA.

Formazione, emissione e trasmissione dei documenti fiscalmente rilevanti

Ai fini tributari, la formazione, l'emissione, la trasmissione, la copia, la duplicazione, la riproduzione, l'esibizione, la validazione temporale e la sottoscrizione dei documenti informatici, deve avvenire a cura del Cliente nel rispetto delle regole tecniche adottate ai sensi dell'art. 71 del decreto legislativo 7 marzo 2005, n. 82, e dell'art. 21, comma 3, del decreto del Presidente della Repubblica 26 ottobre 1972, n. 633, in materia di fatturazione elettronica

Immodificabilità, integrità, autenticità e leggibilità dei documenti fiscalmente rilevanti

I documenti informatici rilevanti ai fini tributari devono avere le caratteristiche dell'immodificabilità, dell'integrità, dell'autenticità e della leggibilità, e devono essere utilizzati i formati previsti dal decreto legislativo 7 marzo 2005, n. 82 e dai decreti emanati ai sensi dell'art. 71 del predetto decreto legislativo nonché quelli individuati nel presente Manuale. Detti formati devono essere idonei a garantire l'integrità, l'accesso e la leggibilità nel tempo del documento informatico.

Pertanto, tutti i DIRT che vengono versati in conservazione devono essere statici ed immodificabili, ossia privi di qualsiasi agente di alterazione.

Il Cliente dovrà assicurarsi e garantire che i DIRT che versa in conservazione abbiano le suddette caratteristiche sin dalla loro formazione e, in ogni caso, prima che siano depositati nel sistema di conservazione.

A tale fine, i DIRT, salvo diverso e circostanziato accordo col Responsabile del servizio di conservazione, devono essere prodotti nel formato PDF/A in conformità a quanto previsto nel capitolo 12 del presente *Manuale*.

Ordine cronologico e non soluzione di continuità per periodo di imposta

Posto che l'art. 3 del Decreto MEF 17.06.2014 stabilisce che i documenti informatici devono essere conservati in modo tale da rispettare le norme del codice civile, le disposizioni del codice dell'amministrazione digitale e delle relative regole tecniche e le altre norme tributarie riguardanti la corretta tenuta della contabilità, il Cliente deve farsi carico di versare in conservazione i propri documenti informatici assicurando, ove necessario e/o previsto dalle norme e/o dai principi contabili nazionali, l'ordine cronologico dei medesimi e senza che vi sia soluzione di continuità in relazione a ciascun periodo d'imposta o anno solare.

In altre parole, gli obblighi richiamati dall'art. 3 del DM 17.06.2014, essendo riferibili a norme riguardanti la corretta tenuta della contabilità, sono posti a completo ed esclusivo carico del Cliente.

Ciò comporta che il Cliente, nell'eseguire il versamento in conservazione dei DIRT, dovrà rispettare le regole di corretta tenuta della contabilità e procedere secondo regole uniformi, nell'ambito del medesimo periodo d'imposta o anno solare.

Funzioni di ricerca

ARUBA non fornisce, in fase di formazione dei documenti, alcuna funzionalità di indicizzazione degli stessi che, quindi, è posta ad esclusivo carico e sotto la responsabilità del Cliente il quale al documento informatico immodificabile il Cliente dovrà associare, in relazione ad ogni classe/tipologia documentale, i metadati previsti dalla legge (anche tributaria) e dalle regole tecniche di cui all'art. 71 del CAD e, più in generale, dalla vigente normativa in materia o gli eventuali ulteriori metadati riportati nell'Elenco documenti in conservazione; i suddetti metadati dovranno essere generati dal Cliente durante la fase di produzione/formazione/emissione dei documenti informatici.

Pertanto, è il Sistema di Gestione documentale del Cliente che deve assicurare l'indicizzazione dei DIRT in merito al formato, allo stato, alle caratteristiche (fiscali) di ogni singolo DIRT ed ai metadati "minimi" previsti dal Decreto MEF del 17 giugno 2014 (nome, cognome, denominazione, codice fiscale, partita IVA, data e associazioni logiche di questi) e dal

[1] Art. 21, co. 5 del CAD: "Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con uno o più decreti del Ministro dell'economia e delle finanze, sentito il Ministro delegato per l'innovazione e le tecnologie.";

presente *Manuale* nel capitolo 12.

Per sfruttare appieno le potenzialità del processo di conservazione dei DIRT non è sufficiente attenersi alle regole tecniche previste dalla norma, ma è necessario che il Cliente si attenga scrupolosamente ad un progettato ciclo di gestione dei DIRT, con il fine di predisporli ed organizzarli sin dalla loro formazione in modo tale da massimizzare la facilità del loro reperimento, prestando particolare attenzione alla fase di classificazione ed organizzazione. Dal puntuale svolgimento di quanto sopra dipende la facilità del loro reperimento.

A tale fine, è necessario che, in relazione ad ogni classe documentale, il Cliente associ ad ogni DIRT i metadati previsti dal presente *Manuale* (ed, eventualmente, degli ulteriori previsti nell'apposito allegato del *Contratto*) necessari per adempiere agli obblighi imposti dalle disposizioni in materia.

Il sistema di conservazione garantisce, come riportato nel capitolo 16, le necessarie funzioni di ricerca dei DIRT conservati sulla scorta dei metadati ad essi associati.

Classificazione dei DIRT secondo aggregazioni per "Tipo documento"

Il Sistema di Gestione documentale del Cliente, oltre ad assicurare il formato, l'indicizzazione, l'apposizione del riferimento temporale, la sottoscrizione con firma digitale di ogni DIRT dallo stesso prodotto, deve provvedere altresì alla classificazione per tipologia di documento in conformità a quanto previsto dall'Allegato 1 al presente Manuale.

Torna al sommario

6.9.1 Modalità di assolvimento dell'imposta di bollo sui DIRT

Come precisato nel precedente capitolo 12, l'imposta di bollo nonché tutti gli obblighi e le formalità per l'assolvimento dell'imposta sui DIRT, qualora dovuta, sono ad esclusivo onere e carico del Cliente, il quale dovrà attenersi alle disposizioni di legge (art. 6, del DMEF del 17 giugno 2014) ed ai documenti di prassi emanati ed emanandi.

Torna al sommario

6.10 Trattamento dei pacchetti di archiviazione contenenti documenti rilevanti ai fini delle disposizioni tributarie

Il processo di conservazione dei DIRT è effettuato nel rispetto delle regole di cui al DMEF del 17 giugno 2014 e successive modificazioni ed integrazioni.

Nello specifico, il processo di conservazione, prende avvio con il versamento in conservazione del pacchetto di versamento prodotto dal Cliente e termina (ergo, "viene chiuso in conservazione") termina con l'apposizione di una marca temporale sul Pacchetto di Archiviazione.

Con riferimento ai DIRT, il processo di conservazione, in forza di quanto stabilito dall'art. 3 del DMEF del 17 giugno 2014, è effettuato entro il termine previsto dall'art. 7, comma 4-ter, del decreto-legge 10 giugno 1994, n. 357, convertito con modificazioni dalla legge 4 agosto 1994, n. 489 e s.m.i..

Pertanto, il Cliente dovrà provvedere a trasmettere ad ARUBA il pacchetto di versamento, contenente i DIRT da sottoporre a conservazione, rigorosamente entro i termini stabiliti nell'apposito allegato del Contratto; tale termine è necessario ad ARUBA per "chiudere" in conservazione il Pacchetto di Archiviazione entro i termini perentori previsti dalla legge.

Torna al sommario

7 Il processo di conservazione

In questo capitolo sono riportate tutte le fasi inerenti il processo di conservazione dei documenti informatici
Torna al sommario

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

Come già anticipato in altre parti del presente *Manuale*, unico responsabile del contenuto del pacchetto di versamento è il Cliente (Produttore), che deve formarlo, sottoscriverlo con firma digitale (ove previsto) e trasmetterlo al sistema di conservazione secondo le modalità operative di versamento definite nel presente *Manuale,* nel *Contratto* e nei rispettivi allegati.
L'operazione di versamento consiste nella trasmissione dei documenti da conservare e dei metadati che li specializzano, così come già accennato precedentemente.
La ricezione e presa in carico di un pacchetto di versamento segue uno schema logico di funzionamento che si articola in due fasi distinte: ricezione dell'Indice del Pacchetto di Versamento (IPdV) e ricezione dei documenti che fanno parte del Pacchetto di Versamento (PdV).

L'uno e gli altri possono essere trasmessi al sistema di conservazione attraverso canali diversi. Alternativamente essi possono essere:

- interfaccia web
- invocazione di metodi tramite web service REST
- trasferimento via protocollo FTP

Ogni canale messo a disposizione è provvisto di opportuni accorgimenti per la trasmissione dei dati in modalità sicura:

- l'interfaccia web viaggia su protocollo HTTPS
- il web service REST è contattabile tramite protocollo HTTPS
- la PEC nativamente garantisce autenticità della provenienza e notifica di consegna in modalità sicura
- il server FTP è raggiungibile via FTPS

Per il completamento delle operazioni di conservazione di un PdV non è necessario scegliere esclusivamente uno dei canali sopra citati. La ricezione, anche in maniera asincrona, dei singoli componenti di un PdV possono arrivare anche da canali diversi.

Il sistema di conservazione prende in carico un PdV solo dopo che tutte le sue parti (IPdV e relativi documenti) vengono correttamente ricevuti e superano con esito positivo i relativi controlli.

Tale operazione viene ufficialmente sancita dalla produzione del cosiddetto Rapporto di Versamento (RdV) che viene consegnato al cliente all'indirizzo PEC fornito nella fase contrattuale.

Poiché la produzione del RdV rappresenta formalmente la presa in carico del PdV da parte del sistema di conservazione, il RdV viene marcato temporalmente e firmato digitalmente direttamente o via delega dal Responsabile del servizio di Conservazione.

Torna al sommario

7.1.1 Ricezione dell'indice del pacchetto di versamento

L'IPdV è un'evidenza informatica, ovvero un file, che descrive il versamento stesso e i documenti che ne fanno parte attraverso l'uso di metadati. Questi sono di carattere diverso a seconda che descrivano proprietà e qualità del pacchetto in genere o dei singoli documenti.

E' bene sottolineare che ogni PdV può contenere esclusivamente documenti della stessa tipologia, ovvero della stessa Classe Documentale. In questo senso l'elenco dei metadati dei singoli documenti è in qualche modo omogeneo.

Per consentire l'elaborazione automatica dei metadati il sistema di conservazione Aruba richiede l'incapsulamento degli stessi in un determinato formato XML, che di fatto costituisce l'IPdV.

In tale file sono contenute sezioni diverse che identificano la qualità dei metadati. Essi infatti possono essere caratteristici del PdV e del soggetto versante, rappresentare direttive speciali di elaborazione per la conservazione, descrittivi dei singoli documenti che si vogliono conservare, a loro volta distinti in standard, come indicato nel paragrafo 12.4, o definiti insieme al Cliente in fase di stipula del contratto e infine caratteristici del formato del documento.

La struttura dell'indice del pacchetto di versamento è definita nel paragrafo 6.6.1.
La funzione di ricezione degli indici dei pacchetti di versamento nel sistema di conservazione effettua, per ogni indice, i seguenti controlli:

- abilitazione alla conservazione da parte del sistema di gestione documentale versante e in particolare dell'utente che effettua il versamento. In caso di esito negativo il sistema rifiuta il tentativo di versamento
- controllo formale dell'indice versato. In particolare viene verificato che sia un formato XML valido per una elle Classi Documentali registrate a sistema. In caso di esito negativo il sistema rifiuta il tentativo di versamento
- verifica, tramite l'id univoco contenuto nell'indice, dell'eventuale presenza del PdV già nel sistema. In caso di esito positivo il nuovo indice sostituisce in toto il vecchio. Di conseguenza vengono aggiornati tutti i metadati, tutti i documenti eventualmente versati e non più presenti nel nuovo indice vengono cancellati dal sistema
- controllo sulla completezza e correttezza formale dei metadati, in relazione alla Classe Documentale rilevata. In caso di esito negativo il sistema rifiuta il tentativo di versamento
- controllo sulla tipologia di documenti che si vuole versare. Ogni documento deve appartenere ad almeno uno dei formati ammessi dalla tipologia di Classe Documentale. In caso di esito negativo il sistema rifiuta il tentativo di versamento
- eventuali controlli supplementari definiti insieme al Cliente. La gestione degli esiti negativi va formalizzato in sede contrattuale

Torna al sommario

7.1.2 Ricezione documenti associati ad un pacchetto di versamento

La ricezione dell'IPdV permette al sistema di conservazione di registrare i metadati del PdV e di mettersi in attesa dei documenti per la conservazione del pacchetto.
Relativamente al singolo documento tra i metadati indicati nell'IPdV sono di particolare importanza quelli utili all'identificazione dello stesso. Essi sono principalmente due: un identificativo univoco utile all'identificazione human readable del documento e un hash del file stesso, ovvero una stringa di caratteri che normalizza con un particolare algoritmo in maniera univoca il documento stesso.
In particolare l'hash, che per il sistema di conservazione Aruba deve essere in formato SHA256 base64, garantisce la riconoscibilità e incorruttibilità del documento in forma automatica e univoca.
Nel momento in cui un documento viene ricevuto da uno qualsiasi dei canali esposti precedentemente, ne viene calcolato l'hash in SHA265 e base64. Se il risultato è tra quelli precedentemente comunicati in uno dei IPdV ricevuti e non ancora in conservazione, allora il file viene accettato.
Successivamente la funzione di ricezione dei documenti informatici nel sistema di conservazione effettua una serie di controlli atti a verificare formalmente leggibilità, integrità e la corrispondenza del documento alle regolamentazioni stabilite per la Classe Documentale di appartenenza. Per operare ciò il sistema determina il formato dello stesso sulla base di quanto esposto in precedenza (estensione e mimetype).
La mancata identificazione del formato del file causa il rifiuto dello stesso con conseguente restituzione di un errore.
Una volta individuato il formato del documento viene controllato che questo sia tra i formati ammessi per la Classe Documentale di appartenenza. Nel caso di esito negativo il file viene rifiutato e viene restituito un errore. Superati i primi controlli, ne vengono operati degli altri relativamente alla qualità dello stesso.
In relazione a ciascun documento informatico infine:

- viene verificato che non sia già presente nel sistema di conservazione;
- viene verificato che il salvataggio avvenga correttamente all'interno del sistema di conservazione.

Tutti i documenti informatici che non superano anche uno solo dei precedenti controlli **vengono rifiutati**. In questo caso non viene salvata alcuna informazione sul sistema di conservazione ed il documento non conforme viene immediatamente eliminato.

Quando tutti i documenti di un pacchetto di versamento vengono ricevuti correttamente viene reso disponibile il rapporto di versamento sottoscritto con firma digitale dal Responsabile del servizio di Conservazione.

Tale rapporto viene anche inviato via email da un indirizzo PEC all'indirizzo PEC fornito dal cliente in fase contrattuale.
Torna al sommario

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

Le funzionalità attivate nel processo di versamento/acquisizione del pacchetto di versamento prevedono dei controlli sia nella fase di ricezione dell'indice del PdV che sui singoli documenti inviati e corrispondenti a quanto previsto nell'indice stesso. La tabella riportata in basso elenca le diverse tipologie di controlli effettuati e per ognuna di esse indica l'azione prevista da sistema. Quest'ultima può tradursi in una operazione di scarto o notifica di un warning.

Controlli dell'indice del Pacchetto di versamento

Il deposito di un pacchetto di versamento è distinto per ciascun pacchetto di documenti informatici omogenei (documenti omogenei, ossia aventi la stessa classe documentale). Pertanto, a classi documentali diverse corrispondono diversi PdV e versamenti, uno per ogni classe.

Controlli nella fase di ricezione dell'indice del PdV

ID	Oggetto del controllo	Azione in caso di check negativo
Verifica Autorizzazioni		
1.01	viene verificato che l'utente che effettua il versamento sia abilitato all'invio dei Pdv	Il sistema scarta l'intero pacchetto
Verifica formale indice del PdV		
2.01	viene verificato che l'oggetto ricevuto sia formalmente un indice xml in linea con lo standard DocFly	Il sistema scarta l'intero pacchetto
2.02	viene verificato che il PdV è versato nei termini contrattuali e di servizio stabiliti col produttore	WARNING: Il sistema accetta il PdV ma non garantisce la conservazione nei termini concordati
Verifica presenza dati-documenti nell'indice del PdV		
3.01 **3.02**	viene verificato che l'indicazione del sistema di conservazione sia corretta viene verificato che l'identificativo specificato nel Pdv non sia già presente nel sistema di conservazione	Il sistema scarta il PdV poiché il metadato contenuto nell'indice indica un sistema di conservazione diverso da DocFly Il sistema verifica se il PdV (che contiene lo stesso ID) non sia già stato conservato. In questo caso il sistema considera il nuove indice in sostituzione del precedente. Viene invece scartato qualora il PdV risulta essere in stato 'conservato'.
3.04	viene effettuato un controllo semantico sui metadati presenti nell'indice del PdV	Il sistema scarta il PdV poiché uno o più metadati non rispettano il formato condiviso nel contratti di servizio
3.05	viene controllato che per ciascun documento dichiarato e descritto all'interno dell'indice del Pdv: a. tutti i metadati minimi obbligatori siano presenti e nel formato corretto; b. il formato del documento è un formato ammesso c. l'estensione del documento sia tra quelle ammesse per il tipo documento; d. il formato dichiarato sia corrispondente all'estensione del nome file	Il sistema scarta il PdV perché le verifiche formali sui documenti dichiarati nell'indice del PdV hanno avuto esito negativo
Verifiche Paternità		
4.01	viene verificato che il Pdv, nel caso abbia estensione P7M, sia firmato con certificato valido	Il sistema scarta il PdV perché le verifiche formali sui certificati di firma hanno avuto esito negativo
4.02	viene verificato che tutte le firme apposte al Pdv siano valide	Il sistema scarta il PdV perché le verifiche formali sui certificati di firma hanno avuto esito negativo

Controlli nella fase di ricezione dei documenti

A seguito della corretta ricezione dell'indice del PdV, il sistema di conservazione è pronto per la ricezione dei relativi documenti informatici (files) descritti nel pacchetto stesso

Controlli nella fase di ricezione dei documenti (files)

ID	Oggetto del controllo	Azione in caso di check negativo
Controllo ricezione documenti		
1.01	viene verificato che l'hash del documento informatico inviato sia corrispondente all'hash dichiarato all'interno del medesimo indice del pacchetto al fine di avere garanzia che la trasmissione del pacchetto sia avvenuta correttamente e che l'integrità del documento informatico ricevuto sia assicurata	Il sistema scarta il documento poiché non atteso
1.02	in caso di file P7M viene verificata la validità della firma apposta su ogni singolo documento: • Controllo di conformità. • Controllo Crittografico. • Controllo Catena Trusted. • Controllo Certificato. • Controllo CRL	Il sistema scarta il documento qualora il certificato di firma non sia valido WARNING: in caso di documenti firmati e il certificato di firma utilizzato è prossimo alla scadenza, il sistema evidenzia un warning.
1.03	viene verificato che il documento sia leggibile	Il sistema scarta il documento nel caso questo non sia leggibile
1.04	viene verificato che il formato del documento informatico sia effettivamente valido e corrispondente a quanto dichiarato nel pacchetto di versamento. In tal caso i controlli eseguiti variano in funzione del formato atteso per ciascuno specifico documento.	Il sistema scarta il documento poiché il formato non è quello atteso
1.05	viene verificato che i documenti ricevuti non siano già presenti nel sistema di conservazione;	WARNING: il documento viene accettato e il sistema invia una notifica
1.06	viene verificato che la ricezione dei documenti si sia correttamente conclusa entro la data limite di ricezione stabilita col produttore nel contratto di servizio	WARNING: il documento viene accettato ma il sistema non garantisce la conservazione nei termini concordati

Le eventuali anomalie e/o scarti riscontrate durante le verifiche effettuate sull'indice del pacchetto di versamento e documenti contenuti al suo interno, saranno comunicate via PEC sia al responsabile della conservazione indicato dal cliente (nel contratto di servizio) che all'utente che ha effettuato l'operazione di versamento.

Tali comunicazioni saranno conservate all'interno del sistema di posta per tutta la durata del contratto sottoscritto dal cliente.

Torna al sommario

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

Il sistema di conservazione predispone, per ciascun pacchetto di versamento, un **rapporto di versamento** che viene firmato dal Responsabile del Sistema di Conservazione. Lo schema del rapporto di versamento è illustrato nel paragrafo successivo (par. 7.3.1).

In particolare il rapporto di versamento contiene, tra l'altro, le seguenti informazioni:

- identificativo unico del PdV, come indicato nel relativo IPdV
- identificativo unico del PdV fornito dal sistema di conservazione
- data di ricezione dell'IPdV
- per ogni documento accettato viene indicato:
  - id univoco, come indicato nell'IPdV
  - id univoco fornito dal sistema di conservazione
  - hash
  - data di ricezione
  - esito della ricezione (accettato o warning)
  - descrizione warning, ove necessario

Torna al sommario

7.3.1 Specifiche rapporto di versamento

Il Rapporto di Versamento è basilare nel processo di conservazione, in quanto è documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.

Esso viene prodotto nel momento in cui tutti gli elementi utili per la conservazione del pacchetto di versamento sono stati consegnati al sistema.

In esso sono presenti sempre i seguenti dati:

- id del Pacchetto di Versamento
- id del Rapporto di Versamento
- riferimento temporale (UTC) di generazione del Rapporto di Versamento
- lista dei documenti afferenti al pacchetto. Per ognuno di essi sono distinguibili:
- id come indicato nell'Indice del PdV
- id assegnato dal sistema
- impronta del documento
- nome del documento
- data di ricezione del file
- esito controllo firma digitale (ove previsto)
- esito controllo marca temporale (ove previsto)

Il Rapporto di Versamento viene sempre firmato digitalmente con certificato del Responsabile di Conservazione. In questo modo viene reso non modificabile.

Torna al sommario

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

Per la gestione dei rifiuti dei pacchetti di versamento e modalità di comunicazione delle anomalie si rimanda al par. 7.2.

Torna al sommario

7.5 Preparazione e gestione del Pacchetto di Archiviazione

Il Pacchetto di Archiviazione (PdA) è quello conservato dal sistema di conservazione e possiede un insieme completo di metadati utili alla conservazione a lungo termine.

Il Pacchetto di Archiviazione viene realizzato secondo lo standard di riferimento SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010), che rappresenta lo standard nazionale riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione.

Uno più pacchetti di versamento vengono trasformati in un Pacchetto di Archiviazione (PdA) in base alle regole tecniche standard del sistema conservazione previste e agli accordi contrattuali.

Il sistema di conservazione a lungo termine ha, fra le altre, la prerogativa di conservare l'autenticità dei documenti in esso contenuti.

La preservazione della suddetta autenticità non può però basarsi tout court sulla firma digitale in quanto quest'ultima:

- ha una validità slegata dall'architettura e dalla struttura del sistema di conservazione;
- ha una validità limitata nel tempo e pari al certificato emesso dalla CA;
- vede la propria sicurezza legata ad algoritmi soggetti ad obsolescenza tecnologica.

È pertanto fondamentale che il sistema di conservazione a lungo termine verifichi la validità ed il valore delle firme digitali apposte dal Cliente sui documenti informatici oggetto di conservazione.

A tale fine, il Cliente dovrà accertarsi che le firme digitali apposte sui documenti informatici inviati in conservazione:

a) siano valide al momento di sottoscrizione del documento informatico;

b) e mantengano piena validità sino al termine ultimo convenuto con ARUBA per la "chiusura" del Pacchetto di Archiviazione.

Con la sottoscrizione dei pacchetti di archiviazione ARUBA non sottoscrive il contenuto e la semantica dei documenti conservati ma asserisce solamente che il processo di conservazione è stato eseguito correttamente, nel rispetto della normativa regolante la conservazione digitale di documenti informatici

Torna al sommario

7.5.1 Chiusura anticipata (in corso d'anno) del Pacchetto di Archiviazione

In caso di accessi, verifiche ed ispezioni in corso d'anno, il sistema consente, dietro specifica richiesta del Cliente, l'anticipata chiusura del Pacchetto di Archiviazione rispetto ai tempi programmati.

Torna al sommario

7.5.2 Gestione dei Pacchetti di Archiviazione non validi o non completi

Nel caso di versamento di un PdA che non viene completato entro 4 ore dalla sua creazione, il sistema invia una email al Responsabile della Conservazione per avvertire l'utente e chiedere il completamento o la modifica del PdA.

Qualora il PdA non venga completato entro 7 giorni dalla sua creazione, il sistema provvederà a:

a) Rimuovere i PdV incompleti presenti nel PdA e/o documenti non collegati a nessun IPdV;
b) Conservare il PdA con i soli PdV completi e validi (con conseguente RdC);
c) Eliminare l'intero PdA nel caso in cui non contenga alcun PdV valido;
d) Inviare una mail di notifica all'utente dell'avvenuta cancellazione dei PdV incompleti ed eventuale conservazione del PdA con i soli PdV validi e completi;
e) Registrare sui log il dettaglio di tutte le operazioni e dei file cancellati.

Torna al sommario

7.5.3 Rettifica dei pacchetti di archiviazione

Il sistema di conservazione prevede la possibilità di eseguire la rettifica del pacchetto di archiviazione, inviando un documento successivo rispetto a quello inviato in precedenza in conservazione. Tale operazione, riservata solamente al produttore o titolare con diritti di scrittura sulla classe documentale relativa, permette al cliente di sostituire un documento inviato in conservazione con un nuovo documento dello stesso tipo, lasciandone invariati i metadati.

Il cliente, una volta indicato il PDA sul quale applicare la rettifica, potrà procedere alla sostituzione di uno o più documenti ed inserire la motivazione relativa all'operazione. Il documento sarà sottoposto ai medesimi controlli di verifica previsti dal processo di conservazione sui documenti originariamente inviati al servizio di conservazione. Una volta sostituiti i documenti, il sistema mostrerà a video l'esito della rettifica: in caso di errori riscontrati, verrà indicato per ciascun documento la tipologia di errore, permettendo al cliente di apportare le modifiche necessarie per concludere l'operazione, altrimenti sarà confermato l'esito positivo della rettifica.

Il PDA rettificato conterrà l'IPDV ed i documenti modificati, mentre il PDA originale rimarrà a disposizione sul sistema di conservazione nel PDD e consultabile dal cliente in qualsiasi momento.

Le operazioni di rettifica verranno registrate nei log di sistema.

Torna al sommario

7.6 Preparazione e gestione del Pacchetto di Distribuzione ai fini dell'esibizione

Nel modello OAIS e in linea con la normativa vigente, il Pacchetto di Distribuzione è strutturato nel modello dati come il Pacchetto di Archiviazione. La differenza sta nella sua destinazione in quanto esso viene concepito per essere fruito ed utilizzato dall'utente finale (esibizione).

In questo caso, un PdD può anche non coincidere con il Pacchetto di Archiviazione originale conservato: anzi, molto spesso, ragioni di opportunità inducono a distribuire pacchetti informativi che sono un'estrazione del contenuto informativo di un PdA. Può anche verificarsi il caso di Pacchetto di Distribuzione che sono il frutto di più PdA che vengono "spacchettati" e reimpacchettati per un più fruibile utilizzo da parte dell'utente.

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

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

- I file/documenti richiesti così come sono stati archiviati dal sistema al momento della messa in conservazione
- Indici dei Pacchetti di Archiviazione, marcati temporalmente e firmati come all'origine, con cui sono stati conservati i documenti richiesti. Al loro interno sono contenuti tutti i metadati di tutti i documenti messi in conservazione nello stesso PdA

A fronte di una richiesta di produzione del Pacchetto di Distribuzione, il sistema effettua delle verifiche di coerenza e correttezza del pacchetto e dei documenti in esso contenuti. A tal proposito, il sistema di conservazione verifica che le impronte dei documenti restituiti nel PdD corrispondano a quelle presenti nel relativo indice del Pacchetto di Archiviazione; in modo da garantire che i documenti stessi non abbiano subito alterazioni o modifiche nei contenuti.

La richiesta di produzione di un PdD implica l'invio di una comunicazione via PEC all'utente finale e altri destinatari eventualmente comunicati dal cliente nel contratto di servizio. Le comunicazioni via PEC, relative alle ricevute di invio e consegna, vengono conservate al fine di tracciare l'intera trasmissione.

La richiesta di esibizione può avvenire da due tra i canali messi a disposizione: interfaccia web e web service.

In entrambi i casi il flusso di selezione dei documenti da esibire è il medesimo:

1. ricerca dei documenti attraverso opportuni filtri
2. selezione e spostamento dei riferimenti dei documenti individuati all'interno di un area di lavoro
3. richiesta di esibizione a partire dai documenti nell'area di lavoro
4. produzione del link di download da cui scaricare il Pacchetto di Distribuzione

La ricerca dei documenti avviene tramite la selezione di filtri sui metadati. Una volta individuata la classe documentale di interesse l'utente può effettuare le ricerche inserendo i valori su cui filtrare per uno o più metadati di riferimento.

La ricerca contemporanea su più metadati implica un filtro più forte, ovvero una restrizione del numero dei documenti risultanti.

Inoltre è possibile effettuare una ricerca tra documenti di classi documentali differenti ma che sono accomunati per un particolare metadato.

Se ad esempio si volessero cercare tutti i documenti afferenti a un determinato numero pratica, dotando classi documentali di tipo differente dello stesso metadato "numero pratica" è possibile effettuare una ricerca di questo tipo.

Tutti i documenti di interesse risultanti dalle ricerche vengono quindi spostati in un'area di lavoro. Finita l'operazione di selezione l'utente può ulteriormente chiedere di esibire solo una parte dei documenti messi nell'area di lavoro.

Il Pacchetto di Distribuzione risultante dalla richiesta di esibizione contiene:

- i documenti da esibire
- gli indici dei PdA, marcati temporalmente e firmati elettronicamente così come al momento della conservazione, del flusso di conservazione relativo ai documenti scelti

Nel caso in cui tra i documenti figurino interi PdA, il Pacchetto di Distribuzione contiene tutti i documenti che lo compongono.

Torna al sommario

7.6.1 Attività conseguenti alla cessazione del contratto

In tutti i casi di cessazione del rapporto contrattuale, ARUBA consente al Cliente, nei termini previsti dalle Condizioni di

fornitura, il recupero dei propri documenti.

Non incombe su ARUBA alcun obbligo di provvedere alla materiale restituzione dei documenti informatici conservati, dal momento che l'attività di recupero dovrà essere effettuata dal Cliente con le modalità descritte di seguito:

1. Accedendo al sistema, il Cliente effettua esplicita richiesta di chiusura dell'intero Archivio
2. Il sistema in automatico genera il Pacchetto di Distribuzione contenente tutte le evidenze dei PdA (Pacchetti di Archiviazione) conservati.
3. Il Cliente riceve comunicazione via mail PEC del buon esito della procedura
4. Il Cliente, da sistema, richiede la produzione del Pacchetto di Distribuzione relativo all'intero archivio
5. Entro i termini stabiliti da contratto, il sistema rende disponibile il Pacchetto di Distribuzione che potrà essere scaricato dal cliente

Torna al sommario

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

Nei successivi paragrafi vengono descritte le procedure adottate per la produzione di duplicati o copie.

Torna al sommario

7.7.1 Produzione di duplicati

La produzione di duplicati informatici dei documenti conservati può avvenire a seguito di una richiesta proveniente dal dipartimento tecnico oppure da una richiesta effettuata direttamente all'interno del sistema di conservazione.

In entrambe le situazioni, il passo iniziale consiste nella ricerca del documento informatico di interesse sfruttando le funzionalità messe a disposizione dal sistema di conservazione. Individuato il documento informatico di interesse, una apposita funzione consente di effettuare il download del documento stesso, producendo quindi un duplicato.

Il documento informatico richiesto viene infatti estratto dal sistema in formato binario controllando che l'estrazione sia eseguita senza errori e quindi inviata all'utente che ne ha fatto richiesta.

Torna al sommario

7.7.2 Produzione di copie

La produzione di copie si rende necessaria solamente a seguito di obsolescenza tecnologica di un formato accettato in conservazione e determina, quale diretta conseguenza, l'avvio di una procedura di riversamento sostitutivo.

In tale contesto ARUBA, previo perfezionamento di specifico accordo scritto (dove saranno concordati ruoli, modalità, tempi e corrispettivi), si renderà disponibile a collaborare col Cliente nell'effettuare le copie informatiche dei documenti informatici depositati in conservazione secondo quanto stabilito dalle regole tecniche vigenti.

Torna al sommario

7.7.3 Produzione copie o duplicati su supporti rimuovibili

In caso di richiesta di produzione di copie o duplicati su supporto rimuovibile, viene prodotto un insieme di DVD (o altro supporto), ognuno autoconsistenze, e consegnati al responsabile della conservazione che ne ha fatto richiesta.

Il processo prevede l'uso di un apposito applicativo che permette la generazione di immagini complete o parziali degli archivi di conservazione che poi vengono riversate su supporto ottico da un operatore. Il software richiede in input l'identificativo dell'archivio di conservazione, le classi documentali desiderate e il periodo temporale coinvolto. L'output generato è dato dal contenuto selezionato dagli archivi di conservazione, lottizzato in pacchetti di dimensione compatibile alla capienza del supporto ottico. I supporti creati vengono etichettati con una codifica generata automaticamente che in nessun modo riporta informazioni sul contenuto.

In ogni singolo pacchetto sono presenti i documenti protetti con criptazione e il software di ricerca e accesso. Il software di ricerca e accesso permette previo inserimento di una password da parte dell'utente, di poter visionare l'indice di quanto contenuto nei pacchetti prodotti, eseguire ricerche su metadati e decriptare e visionare i singoli documenti. Qualora il cliente desiderasse anche l'evidenza della conservazione verrà consentito lo scarico, ovviamente decriptando in linea, del documento con il relativo Indice di Conservazione e tutte le evidenze necessarie.

La protezione dei documenti è quindi ottenuta tramite criptazione con un certificato pubblico, generato allo scopo. La decriptazione è eseguita tramite la chiave privata, abbinata al certificato, rilasciata col software di ricerca e accesso, e un PIN che viene recapitato a mezzo telematico al responsabile della conservazione. Insieme al PIN viene anche recapitata una descrizione del contenuto di ogni supporto: codice del supporto, evidente sull'etichetta dello stesso, archivio, classi documentali data conservazione primo Pacchetto di Archiviazione, data conservazione ultimo Pacchetto di Conservazione.

Torna al sommario

7.7.4 Intervento del Pubblico Ufficiale

ARUBA richiede la presenza di un pubblico ufficiale nei casi in cui sia previsto il suo intervento assicurando allo stesso l'assistenza tecnica necessaria per l'espletamento delle attività al medesimo attribuite.

Ogni risorsa, comprese quelle di natura economica, necessaria per l'espletamento delle attività attribuite al pubblico ufficiale dovranno essere garantite e sostenute dal Cliente; pertanto, qualora il Cliente non se ne sia fatto carico direttamente, ARUBA è sin da ora autorizzata ad addebitare al Cliente tutti i costi e le spese, compresi gli onorari inerenti le attività prestate dal Pubblico Ufficiale, qualora la normativa ne richieda obbligatoriamente la presenza.

Torna al sommario

7.8 Scarto dei pacchetti di archiviazione

7.8.1 Trasferimento dei documenti informatici in conservazione

Nella scheda di conservazione, parte integrante del contratto di servizio e sottoscritta dal cliente, sono indicati i tempi entro i quali le diverse tipologie di documenti devono essere trasferite in conservazione, ove, nel caso delle pubbliche amministrazioni, non già presenti nel Manuale di gestione.

Torna al sommario

7.8.2 Scarto dei documenti informatici conservati

Relativamente alla possibilità di scarto, ossia di eliminare legalmente i documenti informatici conservati digitalmente a norma di legge, occorre distinguere preliminarmente la tipologia dei soggetti (Clienti) produttori, pubblici o privati.

Va preliminarmente osservato che in ambito privato, con l'eccezione degli archivi "dichiarati di notevole interesse storico", che divengono archivi specificatamente disciplinati, l'obbligo di conservazione dei documenti è disciplinato dall'ordinamento vigente e, in particolare, dai termini prescrittivi del codice civile nonché, per le scritture contabili, le fatture, le lettere e i telegrammi ricevuti e le copie delle fatture, delle lettere e dei telegrammi spediti, segnatamente dall'art. 2220 del c.c., il quale stabilisce l'obbligo di conservazione di dieci anni dalla data dell'ultima registrazione.

In ambito pubblico, oltre alle prescrizioni civilistiche, si rendono applicabili una serie di altre disposizioni specifiche, una su tutte, il Codice dei beni culturali e ambientali, emanato con il D.Lgs. 10 gennaio 2004, n. 42.

Inoltre, con riferimento agli archivi pubblici o privati, che rivestono interesse storico-artistico particolarmente importante, lo scarto del Pacchetto di Archiviazione avviene previa autorizzazione del Ministero per i beni e le attività culturali rilasciata al produttore secondo quanto previsto dalla normativa vigente in materia.

Pertanto, alla luce di quanto sopra sinteticamente rappresentato, una volta scaduti i termini previsti dalla legge il Cliente riceve una notifica via PEC dal sistema di conservazione e in autonomia può decidere di eliminare i documenti conservati attraverso le funzionalità previste dal sistema di conservazione.

Torna al sommario

7.8.3 Richiesta di scarto immediato

I clienti possono richiedere ad ARUBA lo scarto di alcuni Pacchetti di Archiviazione dal sistema di conservazione. Fermo quanto definito nel precedente paragrafo, riguardante il rispetto della normativa vigente in materia, il Responsabile della Conservazione potrà, previa compilazione della modulistica messa a disposizione da ARUBA, richiedere lo scarto di uno o più PdA.

Il richiedente dovrà indicare nel modulo i riferimenti all'archivio ed ai pacchetti di archiviazione che intende scartare, unitamente alle motivazioni dello scarto ed alla conferma di disporre di tutte le autorizzazioni necessarie per l'operazione.

Il modulo dovrà essere accompagnato da firma valida ed inviato tramite email all'indirizzo pec scarto@docfly.it.

Le operazioni di scarto verranno registrate nei log di sistema.

Torna al sommario

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

In analogia allo standard SInCRO, la struttura prevista per il PdV prevede una specifica al fine di raggiungere un soddisfacente grado d'interoperabilità nei processi di migrazione, la struttura dell'Indice di Conservazione viene realizzata da ARUBA in conformità con quanto previsto dallo standard "*Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali*", (c.d. SInCRO), ossia dalla norma UNI 11386 dell'ottobre 2010.

I pacchetti di archiviazione generati dal sistema di conservazione vengono trattati al solo scopo di soddisfare i requisiti della conservazione digitale dei documenti ed al soddisfacimento delle richieste di produzione di pacchetti di distribuzione e di esibizione.

Il soddisfacimento dei requisiti della conservazione digitale implica che i pacchetti di archiviazione vengano firmati digitalmente dal responsabile del servizio di conservazione o da un suo delegato e marcati temporalmente per assicurarne la validità nel corso del tempo.

La produzione di pacchetti di distribuzione o l'esibizione di pacchetti di archiviazione comporta invece la produzione di duplicati degli stessi che sono successivamente utilizzati nei processi. Il Pacchetto di Archiviazione memorizzato all'interno del sistema non subisce più alcuna modifica successiva alla firma digitale e all'apposizione della marca temporale.

Torna al sommario

7.10 Tabella riepilogativa delle fasi del processo di conservazione

Il processo di conservazione si articola nelle seguenti fasi:

FASE 1	**Acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico**	
	Descrizione sintetica	Consiste nella ricezione dell'IPdV
FASE 2	**Verifica che il pacchetto di versamento e gli oggetti contenuti siano coerenti con le modalità previste nel presente Manuale di conservazione e con i formati di conservazione**	
	Descrizione sintetica	In questa fase vengono condotti i controlli sull'IPdV
FASE 3	**Preparazione del rapporto di conferma**	
	Descrizione sintetica	A seconda dell'esito del controllo sull'IPdV viene prodotto un rapporto di conferma che viene restituito al sistema versante. **NOTA BENE:** il rapporto di conferma non implica la presa in carico del versamento da parte del sistema
FASE 4	**Eventuale rifiuto del pacchetto di versamento, nel caso in cui le verifiche di cui alla FASE 2 abbiano evidenziato anomalie e/o non conformità**	
	Descrizione sintetica	Alternativamente alla fase 3 viene restituito al sistema versante l'indicazione di eventuali anomalie. In tale caso il versamento viene rifiutato
FASE 5	**Ricezione dei documenti**	
	Descrizione	Il sistema si mette in attesa dei documenti del PdV

	sintetica	
FASE 6	**Verifica dei documenti**	
	Descrizione sintetica	In questa fase vengono condotti i controlli specifici del documento ricevuto
FASE 7	**Generazione automatica del rapporto di versamento relativo a ciascun pacchetto di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo Universale Coordinato (UTC), e una o più impronte, calcolate sull'intero contenuto del pacchetto di versamento, secondo le modalità di seguito descritte**	
	Descrizione sintetica	Una volta ricevuti correttamente, o con warning, tutti i documenti del PdV viene prodotto il PdV
FASE 8	**Sottoscrizione del rapporto di versamento con firma digitale apposta da ARUBA**	
	Descrizione sintetica	Il RdV viene firmato digitalmente dal Responsabile del servizio di Conservazione o da un suo delegato. Infine il RdV viene inviato al Cliente via email PEC. In questa fase Aruba prende in carico il versamento ufficialmente
FASE 9	**Preparazione e gestione del Pacchetto di Archiviazione (c.d. Pacchetto di Archiviazione)**	
	Descrizione sintetica	Il Pacchetto di Archiviazione è un insieme di metadati in grado di fornire prova dell'integrità dell'insieme dei documenti, ad esso correlati la cui conservazione decorre da una data determinata, la cui prova di integrità è fornita tramite una firma elettronica qualificata, corroborata da una marca temporale. La struttura del Pacchetto di Archiviazione è costruita sulla base delle specifiche della struttura dati (UNI 11386:2010) contenute nell'allegato 4 alle regole tecniche e secondo le modalità riportate nel manuale della conservazione
FASE 10	**Sottoscrizione del Pacchetto di Archiviazione con firma digitale apposta da ARUBA e apposizione di una validazione temporale con marca temporale alla relativa impronta. Tale operazione viene in breve chiamata anche "Chiusura del Pacchetto di Archiviazione"**	
	Descrizione sintetica	Il Pacchetto di Archiviazione (PdA), che viene costruito dal versamento di uno o più PdV, viene "chiuso" nel momento in cui tutti i PdV sono stati presi in carico dal sistema. La chiusura viene sancita dall'apposizione di opportuna marca temporale, per stabilirne l'istante di creazione, e firma digitale del Responsabile del servizio di Conservazione o di un suo delegato, per garantirne l'immodificabilità. Con la suddetta firma apposta in calce al Pacchetto di Archiviazione e la suddetta dichiarazione il conservatore NON SOTTOSCRIVE il contenuto e la semantica dei documenti conservati ma asserisce solamente che il processo di conservazione è stato eseguito correttamente, nel rispetto delle norme giuridiche e delle indicazioni contrattuali di servizio.
FASE 11	**Preparazione e sottoscrizione con firma digitale di ARUBA del Pacchetto di Distribuzione ai fini dell'esibizione richiesta dall'utente**	
	Descrizione sintetica	Il Pacchetto di Distribuzione (PdD) è definito in base alle esigenze del richiedente e può contenere anche un set parziale di metadati. È generato a partire dai pacchetti di archiviazione. Nel caso più semplice il PdD contiene dei duplicati del PdA. In alternativa esso può essere costituito da una scelta di documenti conservati selezionati attraverso una o più interrogazioni. I risultati di tali ricerche possono essere raccolti in un'area di lavoro e da qui può essere prodotto il PdD voluto.
FASE 12	**Produzione di duplicati informatici effettuati su richiesta del Cliente in conformità a quanto previsto dalle regole tecniche in materia di formazione del documento informatico**	
	Descrizione sintetica	Per duplicato informatico si intende il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario. I duplicati informatici hanno il medesimo valore giuridico, ad ogni effetto di legge, del documento informatico da cui sono tratti, se prodotti in conformità alle regole tecniche in materia di formazione del documento informatico, ovvero se contiene la stessa sequenza di bit del documento informatico di origine.
FASE 13	**Eventuale scarto del Pacchetto di Archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dal *Contratto* di servizio, dandone preventiva informativa al Cliente al fine di raccoglierne il consenso**	
	Descrizione sintetica	Alla scadenza dei termini di conservazione, il cliente in autonomia può decidere di cancellar ei documenti in conservazione.

Torna al sommario

7.11 Audit Log

Il sistema di conservazione registra per ogni evento rilevante a quanto definito nella normativa relativa al processo di conservazione.

In particolare sono gestiti i seguenti eventi:

- Creazione PDA
- Conservazione PDA
- Invio Rapporto di Versamento
- Invio Rapporto di Conservazione
- Esibizione PDD
- Download Documento
- Scarto PDA
- Verifica Integrità PDA

Il log di audit è consultabile tramite applicativo dal produttore e attraverso il sistema di back office a chi gestisce il servizio o a pubblico ufficiale che ne faccia richiesta.
Il log viene salvato in apposito database e rimane disponibile nel tempo per consultazione. Oltre al log di audit sono presenti altri log di servizio relativi ad altri eventi generati dal sistema durante il processo di conservazione.
Torna al sommario

8 Il sistema di conservazione

8.1 Infrastruttura informatica datacenter

I Data Center dal quale sono erogati i servizi si trovano sul territorio nazionale e sono conformi ai requisiti della normativa ISO/IEC 27001:2013.

Nelle due strutture che verranno messe a disposizione per l'erogazione dei servizi viene data grande importanza alla sicurezza degli ambienti e dei dati in essi contenuti. Per questo sono presenti tutta una serie di sistemi che permettono di garantire integrità degli ambienti e dei servizi.

Torna al sommario

8.2 Caratteristiche generali della soluzione di conservazione

La soluzione, come meglio descritto in seguito, presenta le seguenti caratteristiche peculiari:

- architettura di produzione implementata su infrastruttura virtuale e storage dedicati predisposta totalmente ridondata (HA) presso il Data Center di proprietà del gruppo Aruba, certificato **ANSI/TIA 942-A Rating IV (ex Tier)**, sito in via Gobetti 96, Arezzo;
- architettura secondaria predisposta per consentire la doppia scrittura del dato, effettuata attraverso procedura applicativa, e la replica sincrona storage based della piattaforma virtuale, inclusi i DB documentali e gestionali, situata presso il Data Center di proprietà del gruppo Aruba, sito in via Ramelli, Arezzo;

Il Sistema di Conservazione è sviluppato in modo modulare consentendo una facile scalabilità semplicemente aggiungendo unità e potenza elaborativa ai moduli sottoposti al maggior carico. Vista l'esperienza del Gruppo Aruba nell'ambito della gestione di grandi volumi di dati è sempre stato un obiettivo per il Gruppo creare architetture che possiamo definire elastiche: "espandibili" in caso di aumento del carico di lavoro oppure "limitabili" nel caso di una riduzione delle necessita.

L'intera soluzione è stata progettata per essere quindi in grado di gestire l'elaborazione di grandi volumi di dati, scalando sia verticalmente che orizzontalmente in ognuna delle sue singole componenti, con un elevato livello di affidabilità, distribuendo su più server fisici nodi con il medesimo ruolo ed evitando single point of failure.

L'architettura modulare del sistema è implementata al 100% su infrastruttura di virtualizzazione con hypervisor VMware e garantisce i sintesi i seguenti vantaggi:

Affidabilità - Totale ridondanza ai guasti HW

- Funzionalità di HA implementata dall'architettura virtuale.
- Almeno due moduli con il medesimo ruolo posizionati su server fisici separati.
- DBMS in configurazione Master-Master.
- Utilizzo di sistemi di firma e marca ad alte prestazioni in HA

Architettura scalabile

- Nodi di Front-End ed Application multipli e contemporaneamente attivi.

- Storage di livello Enterprise ad alte prestazioni per la piattaforma VMware e le componenti DB
- Funzionalità di replica

Torna al sommario

8.3 Componenti Logiche

Di seguito riportiamo l'immagine rappresentativa delle componenti logiche del sistema di conservazione:

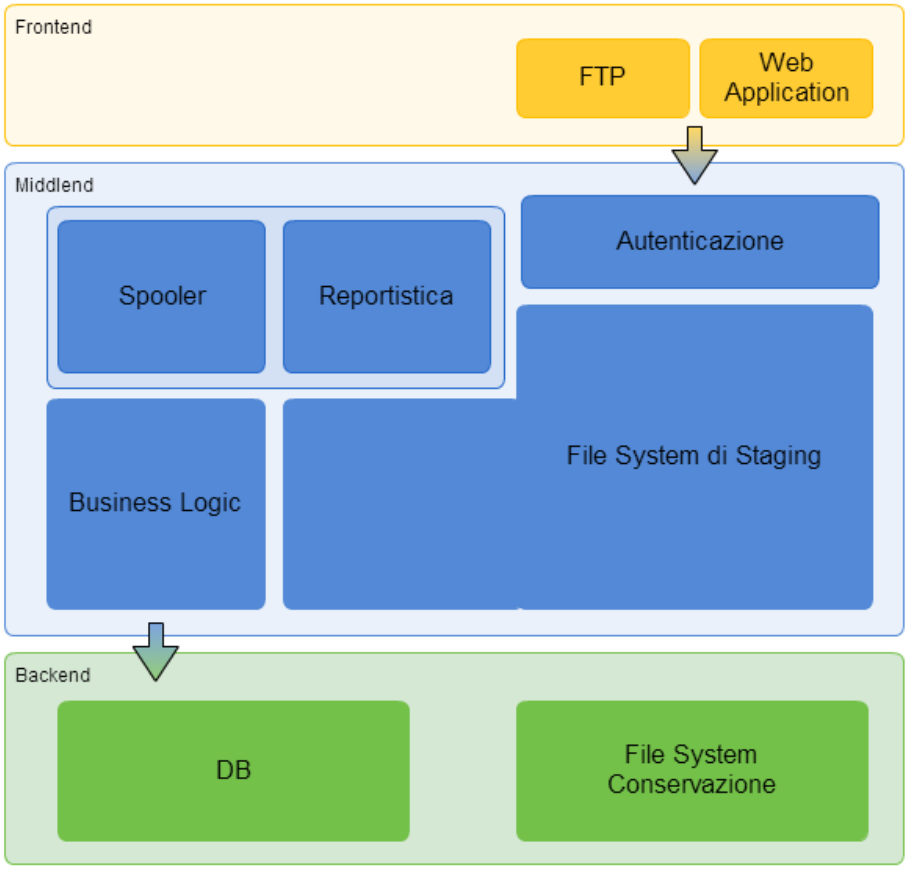


Figura 2: Rappresentazione delle componenti logiche

Come si evince dalla figura l'architettura è basata su una soluzione multi-tier a 3 livelli:

- **Presentation layer**: L'applicazione è pensata per essere scalabile, aumentando il numero dei Web container attraverso una logica di server clustering, gestita automaticamente dal sistema, che, a seconda del livello di carico di ciascun server, distribuirà al meglio le richieste dei client

- **Business logic (o application) layer**: La Business Logic implementa l'intelligenza necessaria per gestire le varie istanze di backend sia in scrittura, sia in fase di ricerca, distribuendo le query sulle varie istanze disponibili. Tutte le istanze backend sono sempre disponibili almeno in lettura

- **Store (& Database) layer**: la parte di back end è composta da diverse istanze. Ogni istanza è costituita dal DB e dal relativo file system. Il DB è duplicato in modalità Master-Master su due nodi predisposti sull'ambiente virtuale e contiene i metadati conservati; il FS contiene l'archivio (dati conservati) e viene replicato con strumenti di basso livello.

Torna al sommario

8.4 Componenti tecnologiche

Il sistema di conservazione Aruba PEC è composto da varie parti e tecnologie, con l'obiettivo di trarre il meglio dalla loro sinergia.

Le principali componenti software che interagiscono all'interno del sistema sono:

- Sistema documentale quale CMS di riferimento
- DB per la gestione dei dati di sistema e dei metadati legati ai materiali in conservazione
- Sistema LDAP per le operazioni di registrazione, autenticazione e controllo degli accessi degli utenti al sistema, indipendentemente dall'interfaccia scelta
- Web server e servlet container per le interfacce di frontiera (Web e Web Service)
- Un sistema di message broker per la gestione delle code in ingresso dei documenti in conservazione sulle interfacce di caricamento massivo (FTP e Web Service)
- Motore di Ricerca per la gestione dei dati di audit

Torna al sommario

8.5 Componenti fisiche

La soluzione è composta da due infrastrutture fra loro interconnesse:

- un sito di Produzione completamente autosufficiente e con tutte le componenti ridondate in HA e collegato tramite fibre ottiche dedicate e di proprietà, con doppia via, al sito secondario,
- un sito Secondario di DR predisposto alla replica dei dati e con le componenti necessarie ad una ripartenza del servizio.

Tutte le componenti utilizzate sono di tipologia enterprise e, come tutte le soluzioni implementate da ARUBA, utilizzano prodotti di marche ampliamente riconosciute e leader del mercato di riferimento.

Torna al sommario

8.5.1 Sito Primario (Produzione)

Il sito di produzione ospita una infrastruttura virtuale basata su soluzione VMware sul quale vengono istallati:

- i nodi di Front-End (almeno due) per le interfacce di caricamento, esibizione e gestione,
- gli Application o Business Logic server (almeno due),
- i backend server, un singolo nodo per ogni istanza,
- un nodo virtuale dedicato al DB server di ogni istanza di backend, la seconda copia in Master-Master è installata sul sito secondario,
- un nodo virtuale per la gestione delle code del sistema di caricamento,
- un nodo virtuale che implementa il DB che contiene tutte le informazioni per la gestione dell'infrastruttura (configurazione, accounting, etc.), la seconda copia in Master-Master è installata sul sito secondario,
- Storage di livello enterprise per l'archiviazione dei documenti;
- Link ed interfacce verso i sistemi di Firma e Marcatura presenti nel medesimo data Center

La figura sottostante schematizza quanto implementato sul sito principale senza entrare nelle specifiche modalità di replica.

Al fine di garantire i ridondanza e bilanciamento del traffico vengono utilizzati dispositivi di load balancing in grado di distribuire il carico di lavoro su un numero di macchine virtualmente illimitato. Questo meccanismo permette di risolvere oltre a problemi prestazionali con la semplice aggiunta a caldo di nuove macchine, anche problemi relativi ad eventuali guasti delle componenti bilanciate, nonché la manutenzione programmata dei singoli nodi.

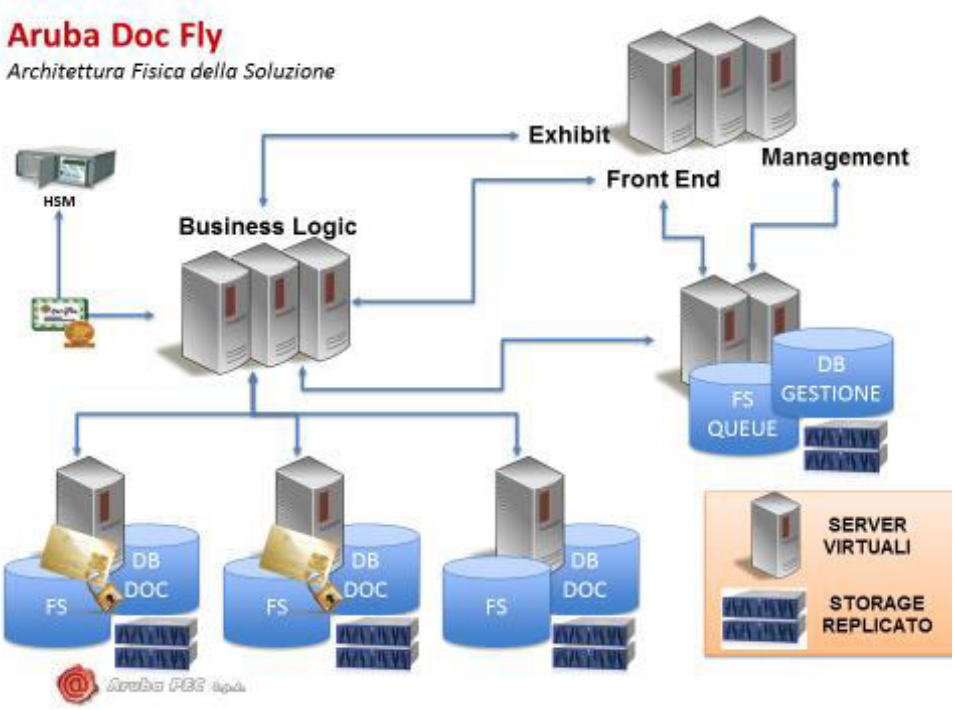


Figura 3: Rappresentazione architettura fisica della soluzione

Torna al sommario

8.5.2 Sito Secondario (DR)

Il sito secondario ospita un'infrastruttura virtuale basata su VMWare sulla quale vengono installati:

- Server di backend corrispondente ad uno dei nodi ridondati dell'ambiente di produzione
- Server DB sincronizzato in maniera sincrona (master-master) con i DB di produzione
- Storage enterprise su cui vengono sincronizzati i dati in maniera asincrona che saranno resi disponibili ai server del sito secondario per ripristinare il servizio
- Collegamenti verso i sistemi esterni di firma e Marcatura temporale (sempre situati nel sito secondario)
- Macchine virtuali replicate dal sito primaro (1 per ciascuna tipologia)

Nello specifico le macchine replicate dal sito primario sono quelle che forniscono i seguenti servizi:

- Frontend Web
- Frontend WS
- Business Logic
- Indicizzazione
- Audit
- Autenticazione

La procedura di switch tra il sito primario ed il secondario è basata tramite il cambio dei puntamenti a livello di DNS.

La figura sottostante schematizza la modalità di replica delle componenti non replicate applicativamente, ad esclusione quindi dei dati archiviati, replicati con doppia scrittura e DB, configurati in Master-Master.

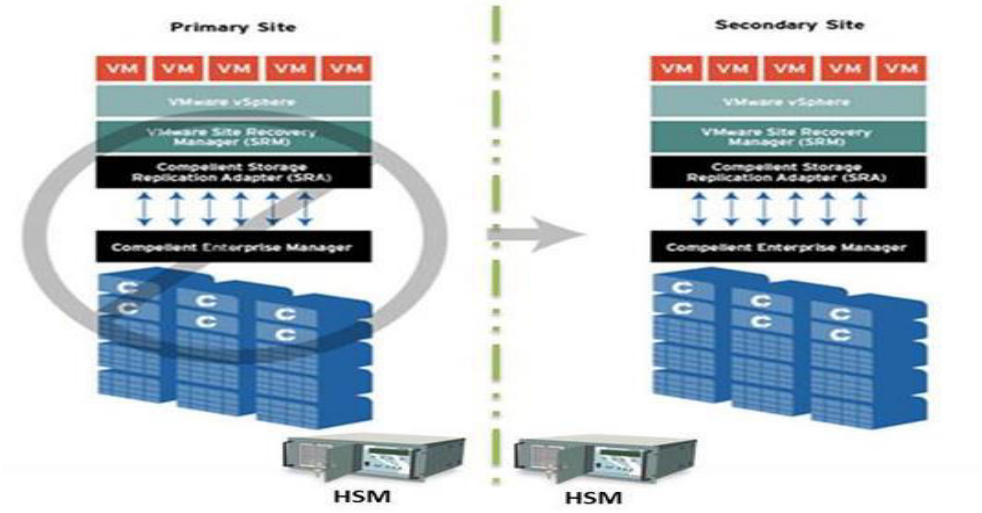


Figura 4 Schema logico della soluzione di Disaster Recovery

In caso di problemi sul sito di Produzione è possibile effettuare la riattivazione del servizio, senza perdita di dati entro 24 ore.

Torna al sommario

8.6 Procedure di gestione e di evoluzione

In linea con quanto previsto dalla circolare n° 65, nell'allegato "REQUISITI DI QUALITÀ E SICUREZZA PER L'ACCREDITAMENTO E LA VIGILANZA, sono descritte le procedure in riferimento a:

- conduzione e manutenzione del sistema di conservazione;
- gestione degli audit-log e loro conservazione;
- monitoraggio del sistema di conservazione:
- change management;
- verifica periodica di conformità a normativa e standard di riferimento

Riguardo i primi tre aspetti, si richiama il documento "MGA_A_38-01 Politica per la gestione dei beni, delle capacità e delle modifiche" I documenti in oggetto descrivono strategie di continuità, considerando tutte le componenti organizzative, operative, del business, tecnologiche, infrastrutturali che contribuiscono all'intero sistema e processo di conservazione.

Torna al sommario

8.6.1 Change management

Qualsiasi operazione di upgrade per evoluzione o bug fixing di una qualsiasi componente del sistema di conservazione Aruba PEC segue una procedura standardizzata atta a operare per garantire il minimo impatto su eventuali fermo servizio e la massima sicurezza possibile riguardo ai dati e documenti a sistema.

Tale procedura si basa sui seguenti assunti:

- ogni componente sviluppata è conservata in opportuno sistema di versionamento del codice
- i file di configurazione di ogni componente sono separati dai compilati in maniera da garantire un accesso più flessibile e veloce al personale addetto
- sono state predisposte apposite macchine di deploy per la compilazione e creazione dei pacchetti delle varie componenti da installare

Ogni aggiornamento del sistema passa da un flusso ben definito che consente contemporaneamente di mantenere stabile e sicura l'intera soluzione in uso dall'esterno e di sviluppare senza ostacoli nuove funzionalità.

Tale procedura risulta di particolare importanza anche per garantire l'accesso controllato e limitato a pochi addetti agli ambienti di produzione.

In particolare vengono messi a disposizione 4 ambienti di lavoro: sviluppo, test, collaudo e produzione.

Tutti gli sviluppi vengono condotti e testati nell'ambiente sviluppo che è di uso esclusivo agli sviluppatori per le sue caratteristiche di continua trasformazione.

Qualsiasi altro attore esterno al team di sviluppo non ha nessun accesso a tale ambiente.

Il codice sviluppato viene conservato all'interno di un sistema di versionamento organizzato in maniera da permettere qualora sia necessario l'estrazione di una qualsiasi versione del software. Una volta che un nuovo modulo software è pronto, esso viene registrato nel sistema di versionamento associandogli un tag/versione.

Per operare l'installazione sull'ambiente di test, deputato ai test pre-collaudo, i sorgenti vengono scaricati su un ambiente di deploy, esterno all'ambiente di test stesso, direttamente dal sistema di versionamento, insieme a eventuali script automatici di compilazione, installazione e configurazione.

Sull'ambiente di test il team della QA (Quality Assurance) effettua i test per verificare la corretta implementazione dei moduli rilasciati ed effettua anche i test regressione.

Solo se il processo di testing va a buon fine si procede con il rilascio dei nuovi moduli nell'ambiente di collaudo e produzione con la medesima procedura utilizzata per l'ambiente di test.

Torna al sommario

8.6.2 Verifica periodica di conformità a normativa e standard di riferimento

Aruba, in qualità di conservatore, svolge una verifica periodica della conformità alle normative ed agli standard. di riferimento. A tal proposito, viene effettuata una volta l'anno, una verifica sulla rispondenza ai requisiti di qualità e sicurezza avvalendosi dello strumento di check list, sulla base dell'allegato della circolare n° 65, attraverso il quale viene registrata l'aderenza o meno alla conformità richiesta.

Torna al sommario

9 Monitoraggio e controlli

In questo capitolo si riporta la descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie.

Torna al sommario

9.1 Procedure di monitoraggio

ARUBA assicura la verifica periodica del funzionamento, nel tempo, del sistema di conservazione. Tali verifiche, descritte in "MGA_A_38-01 Politica per la gestione dei beni, delle capacità e delle modifiche", sono riportate in maniera dettagliata all'interno dei documenti "MGA_A_25-03 Layout Logico" e "MGA_A_35-03 Politica di Backup".

Il controllo della buona funzionalità del sistema di conservazione avviene tramite apposite funzionalità di monitoraggio del software. Esse mostrano l'esito delle operazioni automatiche eseguite sul sistema di conservazione come la generazione dei pacchetti di archiviazione, la chiusura dei pacchetti di archiviazione e la verifica dell'integrità degli archivi.

Unitamente all'esito delle predette operazioni vengono controllati anche i log delle operazioni medesime al fine di avere maggiore certezza di quanto effettivamente eseguito dal sistema di conservazione. Tutte queste informazioni sono controllate per ciascun singolo cliente.

Il monitoraggio avviene inoltre anche a livello di processi di elaborazione sul sistema di conservazione. Questo permette di individuare eventuali casi di processi bloccati che potrebbero inficiare il funzionamento del sistema stesso.

Un ultimo controllo del buon funzionamento del sistema può avvenire tramite il monitoraggio delle tracciature che vengono effettuate a livello di database. Tutte le operazioni eseguite determinano infatti la creazione di apposite revisioni che registrano tutte le modifiche intervenute sul sistema permettendo eventualmente di ripristinare i dati a seguito di situazioni anomale.

Torna al sommario

9.2 Verifiche sugli archivi

ARUBA assicura la verifica periodica, con cadenza non superiore a 36 mesi, dell'integrità degli archivi e della leggibilità degli stessi; assicura, inoltre, agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza.

Il sistema di conservazione esegue periodicamente ed automaticamente le operazioni di controllo dell'integrità degli archivi. Tali operazioni vengono eseguite solo su una certa percentuale dell'archivio che viene definita nella configurazione del sistema di conservazione.

Il controllo eseguito è di due tipologie:

- **controllo di leggibilità:** consiste nel rendere disponibile attraverso una macchina virtuale un viewer per la visualizzazione dei documenti conservati. Il viewer specifico viene fornito sulla base dell'estensione del documento (mime type) e della versione del formato associato. Il dettaglio di tutte. La lista delle tipologie supportate è definita nella procedura "Registro dei formati supportati da DocFly2". Per ogni formato presente nel registro è individuato il relativo programma che ne permette la corretta visualizzazione(viewer). Il registro viene tenuto aggiornato sulla base dei nuovi formati o di quelli che diventano obsoleti. Conseguentemente sono aggiornati i viewer presenti sulla macchina virtuale per la corretta leggibilità dei documenti conservati. Ulteriori dettagli operativi sulla verifica della leggibilità sono disponibili sulla procedura MGA_A_77-01_Procedura leggibilità documenti in conservazione a norma.
- **controllo di integrità:** consiste nel ricalcolare l'hash di ciascun oggetto e verificare che corrisponda all'hash memorizzato nel sistema. Questo fornisce una ragionevole certezza dell'integrità degli oggetti dato che la funzione di hash restituisce un valore differente anche a seguito della modifica di un solo bit dell'oggetto.

La combinazione dei due tipi di controllo descritti non fornisce però garanzia di poter visualizzare correttamente il documento e che lo stesso sia effettivamente intellegibile dall'uomo.

Infatti questa garanzia non può essere fornita senza entrare nel merito del documento stesso. La garanzia della corretta visualizzazione del documento è d'altro canto garantita dalla scelta del formato PDF/A per i documenti conservati. Questo formato possiede infatti la caratteristica intrinseca di fornire leggibilità a lungo termine oltre all'ulteriore garanzia di essere basato su specifiche pubbliche (ISO 19005:2005).

Torna al sommario

9.2.1 Pianificazione delle verifiche periodiche da effettuare

La verifica dell'integrità degli archivi viene effettuata sui filesystems in cui i documenti sono replicati, controllando tutti i file presenti in nei PdA conservati.

Viene verificato che i file distribuiti nei filesystems siano identici mediante:

- controllo del nome e della dimensione dei file presenti sui filesystems;
- calcolo dell'hash di ogni singolo file. Il valore viene confrontato con l'hash del corrispondente file censito nell'IPdV del PdA.

Il controllo su ciascun PdA conservato viene effettuato a intervalli temporali. La prima dell'integrità del PdA verifica viene effettuata entro 36 mesi dalla conservazione del PdA. Le successive verifiche vengono effettuate entro 36 mesi dalla conclusione dell'ultima verifica effettuata.

Torna al sommario

9.2.2 Mantenimento della firma per il periodo di conservazione

Il sistema di conservazione si avvale di un fornitore terzo (Certificatore accreditato) per le attività di firma digitale e di marcatura temporale. Questo fornitore garantisce che gli elaboratori che offrono il servizio di marcatura temporale e di firma digitale sono protetti da livelli di protezione logica estremamente elevati. La medesima collocazione fisica del sistema garantisce gli elaboratori dalla possibilità di compromissioni fisiche grazie agli accorgimenti tecnici atti ad impedire accessi non autorizzati da persone e danneggiamenti da eventi accidentali. Non è infatti consentito l'accesso e la permanenza di una sola persona. I locali ove si svolgono le procedure di firma e marca sono dotati di sofisticati impianti di allarme, telecamere, microfoni, rilevatori di movimento (che si attivano soltanto quando nessuna persona vi è presente), al fine di controllare ogni movimento all'interno degli stessi.

Torna al sommario

9.3 Soluzioni adottate in caso di anomalie

In caso di anomalie riscontrate a seguito del monitoraggio delle funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi, sono presenti apposite procedure di emergenza (contingency) e piani di Business Continuity da applicare in attesa del ripristino del servizio (così come descritto dal Disaster Recovery Plan del Gruppo Aruba)

Torna al sommario

10 Specifiche contrattuali

I documenti costituenti l'impianto contrattuale del servizio di conservazione a norma sono riportati nelle condizioni/accordo di fornitura.

ARUBA, in linea con la normativa vigente, garantisce contratti o accordi scritti che specificano e disciplinano diritti e responsabilità delle Parti, versamento e acquisizione, mantenimento, accesso, ritiro, deposito, diritti e responsabilità di conservazione sui i documenti che tratta, natura economica e di servizio

Ai fini dell'attivazione ed erogazione del servizio di conservazione il Cliente sottoscrive e perfeziona il relativo Contratto. SI tratta del contratto con il quale il Cliente affida ad ARUBA la conservazione digitale dei documenti informatici di cui è titolare nonché dei documenti informatici di titolarità di terzi soggetti dallo stesso prodotti, sottoscritti digitalmente e versati in conservazione in virtù di specifico affidamento a tal fine sottoscritto dai suddetti terzi in favore del Cliente.

Torna al sommario

10.1.1 Nomina di Aruba quale responsabile del servizio di conservazione e del trattamento dei dati

Ai fini dell'erogazione del servizio di conservazione digitale a norma, il Cliente nomina e affida ad ARUBA quale Responsabile del Servizio di Conservazione e Responsabile esterno del trattamento dei dati come previsto dalla vigente normativa in materia di protezione dei dati personali (Regolamento (UE) 2016/679 e D.Lgs. 196/2003 e s.m.i.) e indicato all'art 6 co. 8 delle nuove regole tecniche (DPCM del 3 Dic 2013). Pertanto, i ruoli di Responsabile della conservazione e di Titolare del trattamento sono ricoperti dal Cliente, mentre i ruoli di Responsabile del servizio di conservazione e di Responsabile del trattamento dei dati saranno ricoperti da ARUBA.

Torna al sommario

10.1.2 Scheda di conservazione

Il documento denominato "Scheda di conservazione" costituisce parte integrante e sostanziale del Contratto.

Il Produttore condivide con ARUBA le caratteristiche, le modalità ed i termini di versamento dei documenti informatici da sottoporre a conservazione digitale, approvando espressamente quanto indicato nelle scheda conservazione.

Il contenuto della Scheda di conservazione è volto a precisare:

- le tipologie di documenti da conservare;
- i metadati minimi riferiti ad ogni classe/tipo documento
- eventuali (metadati) extrainfo riferiti ad ogni classe/tipo documento sui quali effettuare specifici controlli;
- i formati da adottare per ogni classe/tipo documento.

Torna al sommario

10.1.3 Elenco Persone

Ai fini dell'affidamento del servizio di conservazione digitale di documenti informatici, il Cliente comunica l'identità delle persone fisiche dallo stesso ufficialmente incaricate di mantenere i rapporti con ARUBA e titolate ad operare in nome e per conto del Produttore medesimo, precisandone funzione e ruolo.

Torna al sommario

10.2 Modello di funzionamento del servizio

L'obiettivo ed il compito di ARUBA è quello di conservare i documenti informatici del Cliente con sistemi coerenti alla normativa regolante la conservazione digitale dei documenti informatici.

In particolare, il servizio di conservazione digitale di ARUBA soddisfa le seguenti funzioni d'uso:

- salvaguardia dell'integrità dei documenti informatici conservati mediante apposizione della firma digitale al Pacchetto di Archiviazione. Nel suddetto Pacchetto di Archiviazione è presente, fra l'altro, l'impronta di ogni singolo documento sottoposto a conservazione;
- prolungamento della validità del documento mediante apposizione della marca temporale al Pacchetto di Archiviazione;

- accesso diretto tramite interfaccia Web ai documenti informatici conservati;
- semplicità di invio e versamento dei documenti informatici da sottoporre a conservazione;
- totale sicurezza nella trasmissione dei documenti informatici da sottoporre a conservazione.

Il sistema di conservazione opera secondo un modello organizzativo che garantisce la sua distinzione logica dal sistema di gestione documentale, qualora esistente presso il Cliente.

In particolare, la conservazione è svolta affidando ad ARUBA il ruolo ed i compiti fissati nell'Atto di Affidamento.

A tal fine, ARUBA ed il Cliente hanno adottato il presente *Manuale* ove sono illustrati dettagliatamente l'organizzazione, i soggetti coinvolti ed i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione dei processi, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate ed ogni altra informazione utile alla gestione ed alla verifica del funzionamento, nel tempo, del sistema di conservazione.

Pertanto, al fine di attivare il servizio di conservazione digitale dei documenti informatici è necessario che il Cliente abbia sottoscritto il *Contratto* e gli allegati ad esso relativi, all'interno dei quali vengono, fra l'altro, specificati:

a) i contenuti e le caratteristiche generali del Servizio di conservazione digitale;
b) i termini di decorrenza e la durata del Servizio di conservazione digitale;
c) gli eventuali Servizi Estesi erogati su richiesta del Cliente;
d) le responsabilità e gli obblighi del Cliente;
e) le responsabilità e gli obblighi di ARUBA;
f) le modalità di produzione/formazione/emissione/sottoscrizione dei documenti informatici;
g) la descrizione delle tipologie e delle classi dei documenti informatici da sottoporre a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di documenti e delle eventuali eccezioni;
h) la definizione dell'intervallo di conservazione ossia dell'intervallo di tempo intercorrente tra la presa in carico del pacchetto di versamento e la chiusura del Pacchetto di Archiviazione.
i) Le modalità di distribuzione/esibizione dei documenti informatici conservati;

Torna al sommario

10.2.1 Obblighi del Cliente

Il processo di conservazione impone al Cliente l'istituzione di un'organizzazione interna idonea, che garantisca la piena osservanza delle disposizioni normative in tema di gestione documentale[2] e delle procedure da osservare per la corretta produzione/formazione/emissione e sottoscrizione dei documenti informatici destinati alla conservazione digitale in conformità alle regole tecniche di cui all'art. 71 del CAD ed a quanto stabilito dal presente *Manuale* e dal *Contratto*.

A tale scopo, in base alle specifiche necessità, il Cliente deve, sia dal punto di vista dell'impostazione operativa delle attività propedeutiche alla conservazione digitale dei documenti informatici che dal punto di vista della scelta delle risorse coinvolte nel processo, organizzare il lavoro affinché esso venga svolto secondo i principi stabiliti dalla normativa regolante la conservazione digitale dei documenti informatici.

Il Cliente, quindi, all'interno della propria struttura organizzativa, dovrà aver definito:

a) le procedure propedeutiche alla conservazione digitale a lungo termine dei documenti informatici;
b) le funzioni e le attività affidate, con particolare attenzione alla verifica della congruità e continuità dei processi di produzione/formazione/emissione dei documenti informatici destinati alla conservazione digitale a lungo termine;
c) la gestione delle responsabilità derivanti dalle funzioni ed attività affidate;
d) la documentazione delle deleghe ed il relativo mantenimento;
e) le misure organizzative e tecniche idonee ad evitare danno ad altri.

Il Cliente deve attenersi scrupolosamente alle regole previste dal presente *Manuale*, alle prescrizioni previste nel *Contratto* e negli allegati ad esso relativi.

Il Cliente deve altresì prendere visione del presente *Manuale* prima di inoltrare i pacchetti di versamento e/o qualsiasi altra richiesta a ARUBA.

[2] Si veda, a puro titolo di esempio, il DPR 28.12.2000, n. 445, il DPCM 3.12.2013 sul protocollo informatico, ove applicabili;

Torna al sommario

10.2.2 Obblighi di ARUBA

ARUBA, come analiticamente descritto nel *Contratto*, limitatamente alle attività ad essa affidate, è responsabile verso il Cliente per l'adempimento degli obblighi discendenti dall'espletamento delle attività previste dalla normativa vigente in materia di conservazione digitale di documenti informatici.

In particolare, ARUBA, ai fini dell'erogazione del Servizio oggetto del *Contratto*, svolge le attività ad essa affidate dal Cliente come in dettaglio riportate nel documento "*Atto di Affidamento*", nei modi e nei termini specificati nel presente *Manuale* e negli allegati ad esso relativi.

Pertanto è obbligo di ARUBA conservare digitalmente i documenti informatici del Cliente allo scopo di assicurare, dalla presa in carico e fino all'eventuale cancellazione, la loro conservazione a norma, garantendone, tramite l'adozione di regole, procedure e tecnologie, le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità.

Il Sistema di conservazione di ARUBA è in grado di esibire tutti i documenti informatici in esso conservati in qualsiasi momento del periodo di conservazione; a tal fine, ARUBA ha in essere procedure adeguate a soddisfare, senza indebiti ritardi, le richieste di accesso, esibizione o consegna dei documenti conservati, effettuate dai soggetti debitamente autorizzati.

Oltre alla restituzione dei documenti informatici trasferiti e conservati presso ARUBA, viene garantita anche la restituzione delle relative evidenze informatiche che comprovano la corretta conservazione degli stessi, fornendo gli elementi necessari per valutare la loro autenticità e validità giuridica.

Non rientra fra i Servizi offerti da ARUBA la conservazione di documenti analogici.

Torna al sommario

10.2.3 Compiti organizzativi

ARUBA provvede alla realizzazione di una base di dati relativa ai documenti informatici che il Cliente versa in conservazione, gestita secondo i principi di sicurezza illustrati nel presente *Manuale* e nel *Contratto* attuati adottando procedure di tracciabilità tali da garantire la corretta conservazione, l'accessibilità a ogni singolo documento e la sua esibizione.

ARUBA si occupa altresì di definire:

a) le caratteristiche ed i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare e organizzare gli stessi in modo da garantire la corretta conservazione e la sicurezza dei dati, anche al fine di poterli prontamente produrre, ove necessario;

b) le procedure di sicurezza e tracciabilità che consentano di risalire in ogni momento alle attività effettuate durante l'esecuzione operativa di conservazione.

c) le procedure informatiche ed organizzative per la corretta tenuta dei supporti su cui vengono memorizzati i documenti informatici oggetto di conservazione.

d) le procedure informatiche ed organizzative atte ad esibire la documentazione conservata, in caso di richieste formulate da chi ne abbia titolo.

ARUBA si occupa di redigere e sottoporre a revisione il presente *Manuale*. Il Cliente si dovrà dotare di un proprio Manuale della Conservazione costituito dalla descrizione di componenti, processi ed organizzazione propri, integrato e completato, se ritenuto necessario, dal presente *Manuale*.

Torna al sommario

10.2.4 Compiti di manutenzione e controllo

ARUBA provvede a:

- mantenere un registro cronologico del software dei programmi in uso nelle eventuali diverse versioni succedute nel tempo ed un registro cronologico degli eventi di gestione del sistema di conservazione comprensivo delle risoluzioni adottate per rimuovere eventuali anomalie;
- implementare specifici controlli di sistema per individuare e prevenire l'azione di software che possano alterare i programmi ed i dati;

- verificare la corretta funzionalità del sistema e dei programmi in gestione;
- analizzare e valutare periodicamente la registrazione degli eventi rilevanti ai fini della sicurezza (analisi del log di sistema);
- definire e documentare le procedure di sicurezza da rispettare per l'apposizione del riferimento temporale;
- mantenere e gestire i dispositivi di firma in conformità con le procedure stabilite dal certificatore qualificato che ha rilasciato i relativi certificati;
- verificare la validità delle marche temporali utilizzate dal sistema di conservazione;
- verificare il buon funzionamento del file system

Torna al sommario

10.2.5 Compiti operativi

ARUBA effettua le seguenti attività:

- supervisione dell'intero sistema di conservazione digitale, verificando accuratamente i processi di apposizione delle firme digitali, dei riferimenti temporali e delle marche temporali, in modo che la procedura rispetti la normativa, assicurandosi che tutto il processo si realizzi secondo le procedure descritte nel presente *Manuale*;
- sincronizzazione dell'ora di sistema di tutti i sistemi utilizzati, verifica e controllo della sincronizzazione del clock di sistema per consentire registrazioni accurate e comparabili tra loro;
- mantenimento della documentazione descrittiva del processo di conservazione aggiornata nel corso del tempo;

Torna al sommario

10.2.6 Fasi del processo di conservazione e responsabilità

Il servizio di conservazione digitale dei documenti informatici è erogato e sviluppato per rispondere alle esigenze di qualsiasi soggetto che abbia l'esigenza di conservare documenti informatici come imprese, professionisti, associazioni, Pubblica Amministrazione centrale e locale. Il servizio permette di conservare i documenti informatici del Cliente, garantendone l'integrità e la validità legale nel tempo nonché la loro "esibizione a norma".

Come già fatto osservare, il sistema di conservazione opera secondo i modelli organizzativi esplicitamente concordati con il Cliente e formalizzati nel Contratto e negli allegati ad esso relativi che garantiscono la sua distinzione logica dal sistema di gestione documentale del Cliente, qualora esistente.

Pertanto, la conservazione non viene svolta all'interno della struttura organizzativa del Cliente (soggetto titolare dei documenti informatici da conservare), ma è affidata ad ARUBA, che espleterà le attività per le quali ha ricevuto formale affidamento, nei limiti della stessa e per le quali opera in modo autonomo e ne è responsabile.

La sequenza di attività che vanno dalla fase propedeutica alla formazione dei documenti informatici alla fase di conservazione degli stessi è di seguito schematicamente rappresentata:

SISTEMI	FASE	DESCRIZIONE E MACRO FASI DEL PROCESSO DI CONSERVAZIONE	ATTIVITÀ A CARICO DI:	
			CLIENTE	ARUBA
Sistema di gestione documentale del Cliente	1	Produzione/formazione/emissione a norma dei documenti informatici e contestuale generazione dei relativi metadati	X	
	2	Produzione del pacchetto di versamento	X	
	3	Deposito in conservazione del pacchetto di versamento e dei relativi documenti informatici completi di metadati	X	
Servizio di Fatturazione Elettronic	1a	Produzione/formazione/emissione a norma dei documenti informatici e contestuale generazione dei relativi metadati		X
	2a	Produzione del pacchetto di versamento		X

	3a	Deposito in conservazione del pacchetto di versamento e dei relativi documenti informatici completi di metadati		X
Sistema di Firma Digitale	4	Servizio di Firma Automatica e di eventuale apposizione marca temporale, da effettuare sui documenti tributari prima dell'invio al sistema di conservazione.	X	X
Sistema di conservazione digitale dei documenti informatici	5	Acquisizione da parte del sistema di conservazione del pacchetto di versamento prodotto dal Cliente per la sua presa in carico		X
	6	Verifica che il pacchetto di versamento ed i documenti informatici in esso descritti siano coerenti e conformi alle prescrizioni stabilite dal Contratto di servizio		X
	7	Eventuale rifiuto del pacchetto di versamento o dei documenti informatici, nel caso in cui le verifiche di cui alla fase 6 abbiano evidenziato delle anomalie		X
	8	Generazione, in modo automatico, del rapporto di versamento relativo a ciascun pacchetto di versamento		X
	9	Invio al Cliente del rapporto di versamento		X
	10	Preparazione e gestione del Pacchetto di Archiviazione		X
	11	"Chiusura" del Pacchetto di Archiviazione mediante sottoscrizione con firma digitale di ARUBA e apposizione di marca temporale		X
	12	Richieste di esibizione dei documenti informatici conservati	X	
	13	Preparazione del Pacchetto di Distribuzione ai fini dell'esibizione richiesta dall'utente con tutti gli elementi necessari a garantire l'integrità e l'autenticità degli stessi		X
	14	Richiesta del Cliente di duplicati informatici	X	
	15	Produzione di duplicati informatici su richiesta del Cliente		X

Dal prospetto di cui sopra emerge chiaramente come ogni singola fase del processo è propedeutica alle altre.

In ogni caso, prima di dare corso al processo di conservazione, il Cliente e ARUBA dovranno definire, attraverso il perfezionamento del Contratto e degli allegati ad esso relativi, come configurare il servizio in base alle specifiche esigenze del Cliente concordando le modalità di gestione e fruizione oltre alla quantità e tipologia di documenti da conservare.

Torna al sommario

11 Livelli di servizio (SLA)

I livelli di servizio relativi all'offerta standard, sono riportati nella tabella in basso e rappresentano le metriche di servizio che devono essere rispettate dal conservatore ARUBA nei confronti dei propri clienti/utenti.

CARATTERISTICHE GENERALI DEL SERVIZIO	**SPECIFICHE TECNICHE**
Disponibilità complessiva del servizio	99,95%
Assistenza	Sistema di ticketing e canale telefonico
Periodo di fatturazione	Annuale
Durata minima contratto	Un anno (eventuali upgrade richiesti in seguito alla stipula del contratto vanno ad allinearsi alla scadenza riportata sul contratto stesso)
Datacenter su cui è attivabile il servizio	DC1-IT (http://datacenter.aruba.it)
FASI ELABORAZIONE PACCHETTI DI VERSAMENTO	**SPECIFICHE TECNICHE**
Presa in carico del PdV (Generazione del Rapporto di versamento)	Entro 48h dal ricevimento dell'ultimo documento contenuto nel pacchetto di versamento

Invio in conservazione del PdA	Entro 72h dalla presa in carico dell'ultimo PdV valido e completo contenuto nel PdA, nel caso in cui tutti i PdV contenuti nel PdA siano validi e completi[3].
RICHIESTA DI ESIBIZIONE	**SPECIFICHE TECNICHE**
Produzione del Pacchetto di Distribuzione	Entro 4h dalla richiesta di produzione del PdD

Torna al sommario

12 Sicurezza del sistema di conservazione

Aruba PEC ed il Gruppo Aruba hanno implementato un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) conforme alla norma ISO 27001. Nell'ambito del Sistema di Conservazione proposto sono adottate misure di sicurezza fisica, logica e organizzativa coerenti con tale SGSI e con la normativa vigente in tema di protezione dei dati personali (Regolamento (UE) 2016/679 e D.lgs. 196/2003 e s.m.i.).

Torna al sommario

12.1 Privacy e requisiti di sicurezza dei dati

Aruba PEC tutela la riservatezza dei dati personali e garantisce ad essi la protezione necessaria da ogni evento che possa metterli a rischio di violazione, trattandoli secondo le specifiche previsioni della vigente normativa in materia.

Come previsto dal Regolamento dell'Unione Europea n. 2016/679 ("GDPR"), ed in particolare all'art. 13, sono fornite all'utente ("Interessato") tutte le informazioni richieste dalla normativa relative al trattamento dei propri dati personali mediante apposita, specifica e preventiva informativa, resa altresì sempre disponibile all'interno del proprio sito istituzionale. Con specifico riferimento ai compiti affidati con la nomina a Responsabile del trattamento dei dati personali, ARUBA comunica di ottemperare a quanto previsto dalla normativa vigente in materia ed alle prescrizioni di cui all'art. 28 del Regolamento (UE) 2016/679.

In conformità con le proprie politiche di sicurezza delle informazioni e del suo sistema di gestione ISO 27001, ARUBA s'impegna a non divulgare, comunicare o diffondere le informazioni e i dati dei quali verrà a conoscenza durante l'espletamento delle attività. Inoltre si impegna a rispettare, nello svolgimento delle attività oggetto del servizio di conservazione, tutti i principi, contenuti nelle disposizioni normative vigenti, relativi al trattamento dei dati personali e in particolare quelli contenuti nel Regolamento (UE) 2016/679 e garantisce che le informazioni personali, patrimoniali, statistiche, anagrafiche, e/o di qualunque altro genere, di cui verrà a conoscenza in conseguenza dei servizi resi, in qualsiasi modo acquisite, vengano considerati riservati e come tali trattati. Si impegnerà infine a dare istruzioni al proprio personale affinché tutti i dati e le informazioni vengano trattati nel rispetto della normativa di riferimento.

Torna al sommario

12.2 Analisi dei Rischi

Il Gruppo Aruba ha svolto un'analisi dei rischi sul Sistema di Conservazione estesa agli aspetti di sicurezza fisica, logica ed organizzativa, incluso il coinvolgimento di enti esterni (fornitori); l'analisi è riportata nel relativo **Piano della Sicurezza** .

Torna al sommario

12.3 Controllo Accessi

Gli utenti possono accedere – previa identificazione ed autenticazione – solamente alle risorse (es. sistemi, funzionalità, informazioni) per cui sono stati esplicitamente autorizzati in base al ruolo ricoperto. I permessi sono attribuiti alle utenze secondo il principio del "least privilege" e rivisti periodicamente per mitigare il rischio di abuso di privilegi. Ad ogni persona (interna od esterna) viene assegnata un'utenza personale e univoca. Le utenze di gruppo sono usate solo per esigenze particolari ed espressamente autorizzate.

Torna al sommario

[3] La gestione dei PdA non validi o non completi è descritta al paragrafo 0

12.4 Monitoraggio Eventi e Vulnerabilità di Sicurezza

Nell'ambito del Servizio di Conservazione, viene conservata e periodicamente esaminata una traccia (audit log) delle operazioni svolte dagli utenti e dai processi, in modo che tali azioni possano essere documentate ed attribuite a chi le ha eseguite o causate (accountability), anche allo scopo di rilevare eventi di sicurezza, incidenti e vulnerabilità associati ai sistemi coinvolti nel processo di conservazione. Tali log vengono archiviati su supporto permanente e non è permesso agli utenti non autorizzati di accedervi.

Torna al sommario

12.5 Cifratura

Come previsto dal Piano della Sicurezza del Servizio di Conservazione di Aruba PEC, tutte le comunicazioni tra il Sistema e gli utenti (interattivi o applicativi) sono protette col protocollo sicuro TLS e pertanto sono cifrate. Per la cifratura del canale, si utilizzano algoritmi di cifratura con chiavi di lunghezza ≥ 128 bit.

Torna al sommario

12.6 Backup

Nell'ambito della gestione operativa del Servizio di Conservazione, sono definite ed applicate procedure di backup finalizzate alla creazione e conservazione di copie di sicurezza dei dati, dei software applicativi, delle loro configurazioni e di ogni altra informazione necessaria per ripristinare il servizio in caso di necessità (per es. a fronte di guasti hardware o incidenti più severi).

I dati vengono scritti e salvati sempre in duplice copia sincrona sui sistemi di storage distribuiti geograficamente con la garanzia dell'effettiva scrittura su entrambi i siti. Sui due storage utilizzati inoltre vengono effettuate copie di sicurezza attraverso meccanismi di snapshot per garantire la massima salvaguardia del dato.

I metadati e i dati utenti sono salvati su istanze dedicate distribuite su due siti geografici distinti e configurate in mirror transazionale in modo da avere una duplicazione non solo del dato ma anche di tutti i metadati necessari alla propria reperibilità e ricerca.

Per quanto riguarda i documenti, si fa presente che essi sono sempre conservati in doppia copia, ciascuna presso un data center separato (per i documenti, dunque, non vi è una reale distinzione tra copia di produzione e copia di backup).

Torna al sommario

12.7 Isolamento delle componenti critiche

I sistemi utilizzati per il Servizio di Conservazione, da un punto dell'architettura fisica, sono posti all'interno di rack dedicati ai servizi eSecurity di Aruba PEC e isolati dagli altri sistemi del datacenter.

In particolare i server e le componenti software del Sistema di Conservazione sono separati logicamente dagli altri Servizi per mezzo di macchine virtuali ed istanze dedicate.

Per quanto concerne il livello organizzativo, questo è parzialmente separato, coerentemente coi requisiti indicati nel Piano della Sicurezza e nel Manuale della Conservazione.

Torna al sommario

12.8 Sicurezza fisica datacenter del Gruppo Aruba

Nelle due strutture che verranno messe a disposizione per l'erogazione dei servizi viene data grande importanza alla sicurezza degli ambienti e dei dati in essi contenuti. Per questo sono presenti tutta una serie di sistemi che permettono di garantire integrità degli ambienti e dei servizi.

Figura 5: Immagine esterna del Datacenter

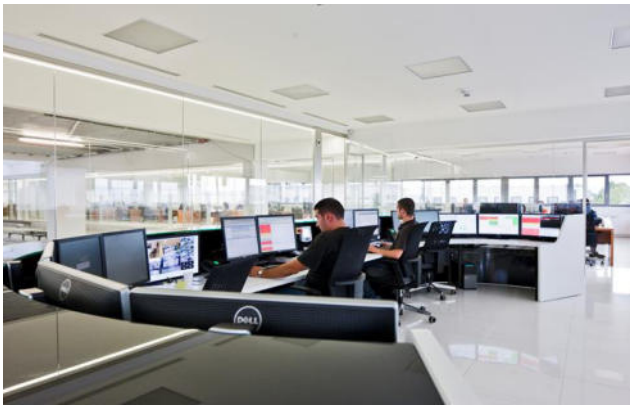


Figura 6: Immagine del Network Operations Center

I datacenter sono situati in un'area classificata come di "basso rischio idrogeologico", inoltre l'edificio è completamente antisismico ed è posto ad un piano rialzato dal livello stradale, in modo da risultare maggiormente protetto alle calamità naturali.

Sia il datacenter primario che quello secondario, sono continuamente monitorati e dotati delle soluzioni di sicurezza più avanzate descritte in seguito.

Torna al sommario

12.8.1 Sicurezza Fisica Data Center Primario

L'edificio primario è situato ad Arezzo in via Gobetti ed è certificato ANSI/TIA 942-A Rating IV (ex Tier). Il datacenter è stato progettato ponendo la massima attenzione alla **sicurezza fisica degli accessi**:

- le **porte esterne** sono di tipo blindato;
- le **finestre** e le **superfici vetrate esterne** a piano terra sono dotate di vetro antiproiettile dello spessore di 21 mm;
- le **griglie per il passaggio dell'aria** necessaria al raffreddamento della sala dati sono protette da sbarre trasversali in acciaio del diametro di 20 mm.

L'**accesso dei visitatori** avviene attraverso una "**bussola**" a due ante rotanti e interbloccate, analoga a quelle normalmente utilizzate negli istituti bancari - anch'essa dotata di vetri anti-proiettile da 21 mm di spessore. Una volta avuto accesso all'interno, è presente una seconda barriera, costituita da varchi motorizzati. Per attraversare tali varchi è necessario essere accreditati alla antistante Reception, con lo scopo di ottenere un badge abilitato. Per la registrazione dei visitatori, è istituito un apposito registro conservato in conformità con quanto previsto dalla **normativa ISO 27001**.

Superata la barriera dei varchi motorizzati, si trova davanti la sala dati principale, delimitata da una parete in vetro antiproiettile da 21 mm. L'accesso, consentito solo al personale abilitato, avviene tramite porte scorrevoli di sicurezza assoggettate al controllo accessi. L'intero stabile è circondato da una resede che lo separa su tutti i lati dalle altre proprietà, e protetto da una recinzione rigida in metallo dell'altezza di 260 cm. La struttura è presidiata e sorvegliata 24x7x365.

Il **data center** è dotato di un **sistema di controllo accessi** esteso a tutti i varchi, sia esterni (ingresso principale, uscite di sicurezza, magazzini, locali tecnici) che interni (sale dati, locali tecnici, uffici). Il riconoscimento è basato su un doppio criterio di autenticazione, mediante l'utilizzo di una tessera di prossimità e la digitazione di un pin. Il sistema di gestione degli accessi prevede la possibilità di abilitare e disabilitare le singole tessere in base alle aree, agli orari ed ad altri parametri, in modo da garantire sia la massima sicurezza degli ambienti che la necessaria fluidità degli accessi. E' possibile generare dettagliati report (per utente, per varco, per data) in modo da ricostruire con la massima precisione - se necessario - i percorsi effettuati da ogni singolo visitatore.

L'edificio è dotato di un **sistema anti-intrusione** che utilizza sensori volumetrici a doppia tecnologia, assieme a sensori a contatti su infissi e sensori di vibrazione sui vetri delle sale dati.

L'impianto è integrato da sistemi evoluti di analisi delle immagini rese disponibili dall'impianto di video-sorveglianza (trattato di seguito). La resede esterna è protetta tramite barriere a raggi infrarossi applicate lungo tutto il perimetro della recinzione esterna. L'impianto anti-intrusione è integrato con il sistema di controllo accessi.

L'**impianto di video-sorveglianza** è costituito da un cospicuo numero di telecamere (oltre 120) posizionate sia all'interno dell'edificio (lungo tutti i punti di passaggio e all'interno dei locali sensibili) che all'esterno (lungo la recinzione, sulla copertura dell'edificio e nella zona dove sono ubicati i gruppi elettrogeni). Le telecamere utilizzate sono di tipologie diverse in base alle diverse esigenze derivanti dai singoli posizionamenti (angolo e distanza di visuale, tipologia di illuminazione, ecc). Le immagini vengono rese disponibili in real-time al personale di presidio mediante appositi monitor presenti all'interno del **NOC**.

Tutte le immagini acquisite vengono immagazzinate tramite videoregistratori digitali, situati in ambienti protetti e conservate per 24H, come previsto dalle vigenti **normative in ambito Privacy**.

Tutto l'edificio è dotato di un **sistema di rilevamento dei fumi** costituito da sensori ottici posizionati in ambiente, sotto al pavimento flottante e sopra il controsoffitto. I sensori sono collegati tra loro in loop e mediante cavo antifiamma, in modo da garantire il loro funzionamento anche in caso di interruzione di un collegamento. Sono stati previsti opportuni sensori in grado di verificare la presenza di fumo all'interno delle condotte per il ricambio dell'aria degli ambienti.

La gestione dell'impianto è demandata ad una centrale a 6 loop, con il compito di rilevare i segnali provenienti dai sensori, attivando gli allarmi ottici e acustici, nonché provvedendo all'attivazione dell'impianto di spegnimento mediante apposite unità di spegnimento. Le aree sensibili e/o a maggiore rischio (2 sale dati, 2 sale tlc, 6 power center, 6 sale trasformatori MT e 2 sale quadri MT) sono dotate di sistema di spegnimento a gas inerte (Azoto).

Il **metodo di spegnimento** è quello della diluizione d'ossigeno, ottenuto mediante una scarica di un'adeguata quantità di azoto in grado di ridurre la percentuale di ossigeno dal 23% presente normalmente in atmosfera al 12% circa, valore che non consente la combustione. Tale scarica non rappresenta un pericolo per la salute delle persone eventualmente ancora presenti nell'ambiente al momento della scarica (comunque annunciata con un anticipo di 60 secondi da allarmi acustici e ottici) e preserva gli apparati consentendo la continuità nell'erogazione dei servizi.

I gruppi elettrogeni di emergenza presenti, posizionati all'esterno, sono dotati di impianti di rilevazione e di spegnimento incendi (ad anidride carbonica) dedicati e autonomi. Tali gruppi sono dotati inoltre di sistema di intercettazione del carburante, in grado di interrompere l'afflusso in caso di incendio. E' inoltre presente la normale dotazione di estintori portatili e carrellati.

I vari locali dell'edificio sono dotati di sensori per il **rilevamento della presenza di liquidi**, posizionati sotto il pavimento flottante. Per quanto riguarda la possibilità di allagamento derivante da rottura delle tubazioni per l'acqua dei servizi igienici (o dalla dimenticanza di rubinetti aperti), è stato previsto un sistema costituito da sensori (flussostati e rilevatori di presenza) e da una logica che, nel caso in cui venga rilevato il flusso di acqua in assenza di persone all'interno dei singoli servizi igienici, provvede all'interruzione dell'erogazione dell'acqua nel medesimo ambiente tramite l'attivazione di una elettrovalvola, eliminando la possibilità di riversamento di acqua a terra.

Le eventuali problematiche derivanti da alluvioni sono scongiurate, in quanto la struttura è ubicata in zona pianeggiante ed in posizione rilevata di circa un metro rispetto al piano di campagna. In fase progettuale si è provveduto inoltre a evitare il posizionamento di impianti strategici o di parte di essi a quota inferiore a tale valore: ciò esclude la necessità di sistemi anti-allagamento dotati di pompe idrauliche.

I server dislocati presso il Centro Servizi saranno dotati di meccanismi di sicurezza fisica utili ad impedire il furto locale dei dati. Gli armadi rack sono tutti dotati di sportelli metallici con serratura a chiave e i supporti di memorizzazione contenenti dati sono conservati in luogo sicuro. Gli apparati attivi di rete saranno posizionati in armadi di cablaggio con chiusura a chiave che inibisce l'accesso fisico ai dischi locali e ne impedisce la rimozione.

Tutti gli impianti sopradescritti, assieme agli impianti e sistemi strategici (gruppi elettrogeni, ups, quadri elettrici, condizionamento di potenza) e agli impianti standard (illuminazione, condizionamento uffici) sono supervisionati da un sistema **BMS** (**Building Management System**) a mappe, in grado di gestire tutti gli eventi e gli allarmi, di interpretarli e di assegnare loro le opportune priorità, generando le conseguenti notifiche in modo da ridurre al massimo i tempi di interpretazione e individuazione degli eventi. Il **BMS** - controllato dal personale di presidio del **NOC** (**Network Operation Center**) - è accessibile anche da remoto ed in grado di provvedere alla notifica degli allarmi tramite i consueti canali (e-mail, SMS, ecc).

La pavimentazione flottante è realizzata mediante pannelli in conglomerato ad alta resistenza appoggiate su struttura composta da tubolari in acciaio ed offre adeguate capacità di carico e di resistenza. Al fine di verificare la corrispondenza con i dati del fornitore sono state eseguite prove di carico in laboratorio.

Torna al sommario

12.8.2 Sicurezza fisica Data Center Secondario

La **sicurezza fisica** del **data center** secondario viene garantita attraverso:

- un sistema di video-sorveglianza che utilizza telecamere motorizzate per tenere sotto controllo i punti nevralgici della struttura;
- un sistema di allarme che rileva automaticamente eventuali vibrazioni o aperture non autorizzate di ingressi e di infissi;
- un impianto anti-intrusione – monitorato dal NOC - che utilizza rilevatori di presenza a doppia tecnologia (micro-onde e raggi infrarossi), contatti magnetici e barriere a raggi infrarossi per proteggere le zone in cui gli ambienti sono suddivisi e prevenire l'apertura non autorizzata di ingressi ed infissi;
- sistema di controllo accessi che permette l'accesso al solo personale autorizzato, dotato di badge con tecnologia RFID e codice PIN personale;
- un sistema anti-incendio a gas inerti (non tossici) - connesso a rilevatori di fumo posti sopra e sotto al pavimento flottante – che si attiva automaticamente inondando di gas solo la zona colpita;
- un sistema di rilevazione liquidi che permette di intercettare - dal NOC e tramite appositi allarmi acustici in loco - eventuali fuoriuscite di liquido dagli impianti tecnologici;
- un sistema centrale server per archiviare e consultare (da personale autorizzato tramite accesso protetto) qualsiasi accesso ai locali, che solo avviene attraverso RFID associato a codice numerico.

Anche nel sito secondario, i server saranno dotati di meccanismi di sicurezza fisica utili ad impedire il furto locale dei dati: gli armadi rack sono provvisti di sportelli metallici con serratura a chiave; i supporti di memoria dati sono conservati in un luogo sicuro ed i server sono protetti da un apposito sportello con chiusura a chiave (come inibizione dell'accesso fisico e della rimozione).

Torna al sommario

12.8.3 Sicurezza organizzativa comune ai due data center

Aruba garantisce inoltre la sicurezza organizzativa delle strutture, che viene continuamente adeguata in caso di evoluzioni delle normative. Il sistema di registrazione dei log per tutti i servizi erogati è infatti conforme alle normative vigenti ed adeguato in caso di evoluzioni.

A tale proposito viene garantito che:

- i processi attuati per il monitoraggio e la rilevazione di eventuali intrusioni o anomalie sono definiti ed attuati
- l'accesso alle informazioni riservate dell'Amministrazione viene permesso solo a personale autorizzato, in conformità al Regolamento (UE) 2016/679;

Aruba garantisce che tutti gli apparati necessari all'erogazione dei servizi vengano gestiti solo da personale univocamente individuato e che gli aspetti di sicurezza siano attuati in base a procedure documentate. Le procedure di sistema del Gruppo Aruba, redatte sulla base dello standard ISO27001 per la gestione della sicurezza delle informazioni, garantiscono che siano documentati:

- gli accessi fisici delle persone agli edifici in cui sono situati apparati;
- gli accessi fisici delle persone ai locali contenenti apparati;
- le regole per l'accesso da parte di personale esterno (fornitori, addetti alla manutenzione, visitatori, etc.);
- le modalità di gestione degli strumenti per l'accesso ad eventuali casseforti ed armadi blindati (combinazioni delle casseforti, chiavi degli armadi, etc.);
- le modalità di gestione degli archivi cartacei (regole per la conservazione, modalità di consultazione, eventuale registrazione degli accessi, etc.);
- la gestione di situazioni anomale;
- le modalità di ripristino a seguito di interruzione dell'erogazione di energia elettrica;
- le procedure di backup e di restore;
- le procedure di escalation.

Le **postazioni di lavoro** si trovano in uffici interdetti all'accesso del pubblico. Le postazioni condivise, messe a disposizione della clientela, risiedono su reti e uffici separati (sale riunioni attrezzate), e sono dotate di opportune limitazioni di accesso.

Per l'**accesso alle postazioni di lavoro**, i dipendenti dispongono di token hardware personali protetti da apposito **PIN** associato a credenziali nella forma nome.cognome e password, di tipo strong, conosciute solo dagli stessi. Attraverso l'**Active Directory aziendale** è possibile offrire cambio password con obbligo di password in base a policy standard condivise.

L'accesso ai server viene garantito attraverso le stesse credenziali personali sia per ambienti windows che per ambienti linux. Le password vengono mantenute nella massima riservatezza e non possono essere trascritte.

Torna al sommario

12.8.4 Sicurezza Logica dei sistemi e degli apparati

I protocolli ed i servizi utilizzati per la gestione degli apparati (SNMP, RADIUS, NTP, Log, LDAP) vengono erogati solo verso le reti di management mediante l'utilizzo di ACL (Access Control List). All'interno delle reti dedicate, se il protocollo/servizio lo supporta, è in ogni caso necessario autenticarsi.

Tutti i protocolli previsti per l'accesso ed il controllo dei sistemi sono di tipo sicuro cifrato, prevedendo ssh, https o rdp.

All'interno dei singoli apparati i servizi non necessari vengono disattivati e quelli necessari vengono erogati solo verso le interfacce che richiedono che tali servizi vengano resi disponibili.

Le politiche e le conseguenti architetture e configurazioni di rete adottate garantiscono fra l'altro:

- L'impossibilità di effettuare IP spoofing da un qualsiasi utente connesso direttamente alla rete
- L'impossibilità di effettuare attacchi smurf, fraggle, land tramite limitazione nell'accesso agli indirizzi di broadcast e filtraggio dei pacchetti che riportano un indirizzo sorgente palesemente scorretto
- La capacità di reagire tempestivamente a qualsiasi tipo di attacco alle proprie infrastrutture anche tramite la possibilità di configurare in qualsiasi punto della rete qualsiasi regola di filtraggio atta a mitigare il fenomeno evidenziato

Gli enti/gruppi che operano sulla configurazione dei sistemi hanno diverse esigenze in termini di necessità d'accesso alle classi d'apparati. L'autorizzazione all'accesso alla configurazione di un apparato è nominale, non di gruppo. L'accesso ad una specifica classe d'apparati dipende dall'appartenenza dell'utente ad uno specifico gruppo. L'associazione dell'utenza al Gruppo permette di confinare l'accesso degli utenti ai soli apparati la cui gestione è in carico al Gruppo. Sulla base di tale appartenenza, l'utente potrà autenticarsi sull'apparato utilizzando una login ed una password personali nel caso di apparati con tecnologia IP mentre per quanto riguarda apparati di trasporto (SDH e DWDM) l'autenticazione si esegue a livello dei sistemi di gestione. Sono stati inoltre introdotti dei meccanismi di gestione delle password (lunghezza minima,

presenza di caratteri numerici, ecc.) di enable e delle password locali in modo da ottenere un bilanciamento tra l'esigenza di avere un adeguato livello di sicurezza e le esigenze di implementazione/gestione delle linee guida.

L'inserimento di un nuovo utente in un gruppo deve essere richiesto dal responsabile del gruppo stesso. La richiesta deve pervenire via e-mail all'apposita casella di posta nel caso della rete IP o all'amministratore di rete nel caso di accesso agli apparati di rete di Trasporto.

Successivamente alla configurazione dell'utente, sarà inviata e-mail di conferma all'utente stesso ed al responsabile del gruppo. La rimozione di un utente da un gruppo deve essere richiesta dal responsabile del gruppo stesso. La richiesta deve pervenire via e-mail all'apposita casella di posta nel caso della rete IP o all'amministratore di rete nel caso di accesso agli apparati di rete di trasporto.

Successivamente alla rimozione dell'utente, sarà inviata e-mail di conferma all'utente stesso ed al responsabile del gruppo. Le password utilizzate dagli utenti dovranno seguire le seguenti regole:

- Non inferiori agli 8 caratteri.
- Non devono essere facilmente identificabili. Nomi propri, nomi di prodotti, nomi di Clienti ecc. sono da evitare
- Devono contenere caratteri misti: minuscole, maiuscole, numeri, spazi, caratteri speciali (@, %, $ ecc.)

L'utente viene invitato a cambiare con regolarità la sua password utente. Nel caso l'utente decidesse di non cambiare la propria password, riceverà quotidianamente, nelle ultime due settimane di validità della stessa, un avviso di richiesta di modifica password.
Torna al sommario

12.9 Piano di Disaster Recovery e Continuità operativa

Aruba ha sviluppato e adotta appositi piani di Disaster Recovery e Business Continuity allo scopo di gestire e mediare i rischi cui può essere soggetta.

Tali documenti definiscono ed elencano le azioni da intraprendere prima, durante e dopo una condizione di emergenza per assicurare il ripristino (Disaster Recovery) e la continuità (Business Continuity) dei servizi erogati. Essi forniscono indicazioni e dove possibile istruzioni passo-passo atte ad assicurare la continuità dei servizi critici di Aruba anche in presenza di eventi indesiderati che possano causare il fermo prolungato dei sistemi informatici.

I Piani di Disaster Recovery sono stati redatti tenendo presente le "Linee Guida per il disaster recovery delle PA" dell'Agenzia per l'Italia Digitale,ed è dunque ispirato al ciclo di Deming (Plan, Do, Check, Act) prevedendo, dopo la fase iniziale di studio/analisi del contesto, il disegno della soluzione tecnologico-organizzativa che meglio risponde alle esigenze di continuità richieste, la realizzazione e il mantenimento della soluzione. Tale piano viene dettagliato maggiormente in fase di setup dell'infrastruttura.

La continuità operativa sarà garantita anche in caso di blocchi prolungati, quali, a titolo esemplificativo:

- distruzione o inaccessibilità di una struttura nella quale sono allocate unità operative o apparecchiature critiche;
- indisponibilità di personale essenziale per il funzionamento dell'azienda;
- interruzione del funzionamento delle infrastrutture (tra cui energia elettrica, reti di telecomunicazione, ecc.);
- alterazione dei dati o indisponibilità dei sistemi a seguito di attacchi perpetrati dall'esterno attraverso reti telematiche;
- danneggiamenti gravi provocati da dipendenti

Torna al sommario

12.9.1 Business Impact Analisys (BIA)

Come prima cosa si valutano gli elementi che più risentirebbero dell'interruzione del servizio, ovvero si valuterà con il cliente quali sono gli aspetti maggiormente critici del servizio offerto.
La BIA valuta normalmente l'impatto di un evento sull'operatività economica, nel caso della conservazione documentale però l'interruzione dei servizi erogati comporta danni non immediatamente "monetizzabili". Le perdite (e dunque l'impatto) saranno valutate assieme al cliente tenendo conto dell'insieme dei seguenti aspetti:

- Aspetti economici
- Aspetti sociali
- Aspetti reputazionali;
- Aspetti normativi.

Torna al sommario

12.9.2 Analisi dei Rischi

In questa fase si identificheranno quali siano gli scenari di rischio che insistono sul patrimonio informativo attraverso i quali si qualificano gli eventi / minacce che presentano maggior probabilità di concretizzarsi (e.g. in funzione dei livelli di vulnerabilità, delle contromisure in essere, dell'appetibilità dei servizi offerti), generando un danno per il cliente. Si individueranno pertanto le possibili cause di indisponibilità quali ad esempio diffusione di virus, interruzione dell'alimentazione elettrica, incendio alla sala CED, etc...

Torna al sommario

12.9.3 Classificazione dei Sistemi e delle Risorse

Allo scopo di indirizzare le priorità di ripristino in caso di disastro, nonché realizzare un efficiente utilizzo delle risorse, si ritiene indispensabile classificare i sistemi presenti all'interno delle infrastrutture di ARUBA a seconda della loro criticità in caso di disastro.

Sono stati individuati quattro livelli di criticità, così definiti:

- **Sistemi critici:**
  Sono quei sistemi indispensabili per fornire un minimo ed accettabile livello di servizio in caso di evento disastroso e/o necessari per il funzionamento degli altri sistemi a minore criticità.
- **Sistemi importanti**:
  Sono quei sistemi necessari per garantire un livello standard di servizi, che quindi hanno una significativa importanza operativa.
- **Sistemi semi-importanti:**
  Si tratta di sistemi necessari per le normali operazioni, tuttavia risultano avere una minore importanza operativa rispetto a quelli del punto precedente.
- **Sistemi non-critici:**
  Sono i sistemi che rivestono la minore importanza (quali servizi accessori ecc.) operativa per cui il ripristino non riveste carattere di priorità.

Verrà inoltre fornito l'elenco del personale, il responsabile della Continuità Operativa e le procedure di escalation da utilizzare per dichiarare lo stato di disastro.

Torna al sommario

12.9.4 Modalità tecniche per la Business Continuity ed il Disaster Recovery

Come descritto nell'architettura fisica della soluzione il sistema implementa i seguenti livelli di sicurezza:

1) Il sistema di produzione è completamente ridondato senza alcun Single Point of Failure. Alcune componenti sono per convenienza distribuite sui due Data Center connessi in ambito metropolitano in modo tale da essere

totalmente resilienti a qualsiasi guasto HW o SW che possa colpire un singolo nodo fisico o virtuale. Per come è costruito il sistema inoltre l'impatto sulle performance dovuto alla rottura di un singolo componente può essere considerato irrilevante e comunque la configurazione normale ripristinata nel giro di pochi minuti.

2) La presenza di un sito collegato in ambito metropolitano e già parzialmente attivo garantisce la piena operatività della soluzione anche nel caso di fermo del data center principale. Le uniche operazioni necessarie sono la riconfigurazione della rete, per il corretto raggiungimento del sistema, e la riattivazione dei nodi di Front-end ed Application sull'apposita infrastruttura virtuale. Per tutti gli eventi che abbiano impatto sul data center di produzione, che ricordiamo essere certificato **ANSI/TIA 942-A Rating IV (ex Tier)**, la riattivazione del servizio senza perdita di dati è prevista entro 24 ore. Nel caso di attivazione del sito secondario, questa viene eseguita manualmente seguendo apposite procedure, a seguito della dichiarazione di crisi prevista dalle procedure.

Torna al sommario

13 Disposizioni finali

13.1 Nullità o inapplicabilità di clausole

Se una qualsivoglia disposizioni del presente Manuale, o relativa applicazione, risulti per qualsiasi motivo o in qualunque misura nulla o inapplicabile, il resto del presente Manuale (così come l'applicazione della disposizione invalida o inapplicabile ad altre persone o in altre circostanze) rimarrà valido e la disposizione nulla o inapplicabile sarà interpretata nel modo più vicino possibile agli intenti delle parti.

Torna al sommario

13.2 Interpretazione

Salvo disposizioni diverse, questo Manuale dovrà essere interpretato in conformità alla correttezza, buona fede ed a quanto ragionevole anche in virtù degli usi commerciali nazionali.

Torna al sommario

13.3 Nessuna rinuncia

In nessun caso eventuali inadempimenti e/o comportamenti del Cliente difformi rispetto al Manuale potranno essere considerati quali deroghe al medesimo o tacita accettazione degli stessi, anche se non contestati da ARUBA. L'eventuale inerzia di ARUBA nell'esercitare o far valere un qualsiasi diritto, clausola o disposizione del Manuale, non costituisce rinuncia a tali diritti o clausole.

Torna al sommario

13.4 Comunicazioni

Qualora ARUBA o il Cliente desiderino o siano tenuti ad effettuare delle comunicazioni, domande o richieste in relazione al presente Manuale, tali comunicazioni dovranno avvenire nelle modalità ed ai riferimenti indicati nel Contratto.

Torna al sommario

13.5 Intestazioni e Appendici e Allegati del presente Manuale Operativo

Le intestazioni, sottotitoli e altri titoli del presente Manuale sono utilizzati solo per comodità e riferimento, e non saranno utilizzati nell'interpretazione o applicazione di qualsiasi disposizione ivi contenuta.

Le appendici, gli allegati, comprese le definizioni del presente Manuale, sono parte integrante e vincolante del presente Manuale a tutti gli effetti.

Torna al sommario

13.6 Modifiche del Manuale di conservazione

ARUBA si riserva il diritto di aggiornare periodicamente il presente Manuale in modo estensibile al futuro e non retroattivo. Le modifiche sostituiranno qualsiasi disposizione in conflitto con la versione di riferimento del Manuale di conservazione.

Torna al sommario

13.7 Violazioni e altri danni materiali

Il Cliente rappresenta e garantisce che i documenti oggetto di conservazione e le informazioni in essi contenute non interferiscano, danneggino e/o violino diritti di una qualsiasi terza parte di qualunque giurisdizione.

Torna al sommario

13.8 Norme Applicabili

Le attività di conservazione contenute nel presente Manuale sono assoggettate alle leggi dell'ordinamento italiano.

Il presente documento informatico è formato nel rispetto delle regole tecniche di cui all'art. 71 del D.Lgs. 7 marzo 2005 n. 82 e s.m.i. (Codice dell'amministrazione digitale) e sottoscritto con firma digitale del Sig. Andrea Sassetti.

Torna al sommario

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
2.4	10/04/2024	6.4 8 8.4.3.1	Indicato Soggetto firmatario dei PdD Specifiche sulle modalità di accesso al servizio Aggiornati type Issue	M. Mingrone	-	A. De Angelis
2.3	05/06/2023	5	Cambiamento dei ruoli e aggiornamento storico dei ruoli	M. Mingrone	-	A. De Angelis
2.2	09/01/2023	5	Cambiamento dei ruoli e aggiornamento storico dei ruoli	Massimiliano Valente	N. Carofiglio	M. Valente
2.1	26/10/2022	Intestazione	Modificato ente certificatore e rispettivo logo	M. Mingrone	-	M. Valente
2.00	29/11/2021	2.1 2.2 3.1 3.2 4 5.1 5.2 7.1	Glossario Acronimi Normativa di riferimento Standard di riferimento Ruoli e responsabilità Organigramma Matrice RACI attività del servizio	M. Mingrone N. Carofiglio	A. De Angelis	M. Valente

			Aggiunto capitolo "Redazione Accordi di versamento"			
1.12	12/05/2021	5	Cambiamento dei ruoli e aggiornamento storico dei ruoli	Massimiliano Valente		M. Valente
1.11	11/01/2021	5	Cambiamento di ruoli	Riccardo Righi		R. Righi
1.10	08/04/2020	4 5 6.1	Definito meglio il ruolo del Responsabile del trattamento dei dati personali Recepite modifiche organigramma Definita meglio la proprietà degli oggetti conservati	Riccardo Righi		R. Righi
1.9	03/05/2019	Tutto 3.1 6.1 6.3, 6.4 5.1 8.1 8.2 8.3 9.3	Sistemazione Layout Adeguata Normativa Esplicitati formati conservati Revisione PdA e PdV Revisione organigramma Revisione Componenti Logiche Revisione Componenti Tecnologiche Revisione Componenti Fisiche Revisione politiche di Conservazione dei log	Stefano Capelli Laura Nisi		R. Righi
1.8	08/02/2018	5	Inserimento storico dei ruoli	Stefano Capelli Laura Nisi		R. Righi
1.7	15/12/2017	5	Cambiamento di ruoli	Stefano Capelli		R. Righi
1.6	06/11/2017	5 5.1	Cambiamento di ruoli Aggiornamento dell'organigramma	Laura Nisi	R. Righi	R. Righi
1.5	11/08/2017	8.3	Variazione struttura base dati	Laura Nisi		R. Righi
1.4	22/06/2017		Cambiamento di ruoli	Laura Nisi		R. Righi
1.3	10/10/2016		Revisione a seguito delle osservazioni dell'AGID	Laura Nisi	A. De Angelis	P. Vandelli

1.2	16/06/2016		Revisione a seguito delle osservazioni dello Studio Lisi	Laura Nisi	A. De Angelis	P. Vandelli
1.1	22/04/2016		Revisione a seguito delle osservazioni dello Studio Lisi	Laura Nisi	A. De Angelis	P. Vandelli
1.0	01/12/2015		Emissione	Laura Nisi	P. Tentoni F. Merighi A. De Angelis P. Vandelli	P. Vandelli

Sommario

1 Scopo e ambito del documento

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

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

La struttura del manuale è la seguente:

- il presente elaborato che costituisce la sezione generale del manuale di conservazione;
- 8 allegati tecnici:
  - Allegato 1 - Modello accordo di versamento
  - Allegato 2 - Pacchetto di versamento
  - Allegato 3 - Indice UNISinCRO
  - Allegato 4 - Mezzi di trasmissione
  - Allegato 5 - Rapporto di versamento
  - Allegato 6 - Controlli sul pacchetto di versamento
  - Allegato 7 – Organigramma
  - Allegato 8 – Formati accettati

Torna al sommario

2 Terminologia

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

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

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

Torna al sommario

2.1 Glossario

Accesso	Operazione che consente di prendere visione dei documenti informatici.	LLGG
Accordo di versamento	Accordo firmato dal cliente e dal conservatore che descrive le condizioni di versamento di oggetti informativi dal sistema informativo del cliente al sistema di conservazione. Le condizioni di versamento formalizzano sia i	OAIS

	dettagli tecnici della procedura di versamento - quali il protocollo di comunicazione, lo standard di firme, i controlli sul buon esito del versamento - che gli aspetti archivistici come la descrizione della tipologia del documento, del contesto, della provenienza.	
Affidabilità	Caratteristica che, con riferimento a un sistema di gestione documentale o conservazione, esprime il livello di fiducia che l'utente ripone nel sistema stesso, mentre con riferimento al documento informatico esprime la credibilità e l'accuratezza della rappresentazione di atti e fatti in esso contenuta.	LLGG
Aggregazione documentale informatica	Insieme di documenti informatici o insieme di fascicoli informatici riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente.	LLGG
AgID	Agenzia per l'Italia digitale. Ha il compito di garantire la realizzazione degli obiettivi dell'Agenda digitale italiana in coerenza con l'Agenda digitale europea.	CAD
Archival Information Package (AIP)	Denominazione in OAIS del pacchetto di archiviazione. Per l'accezione utilizzata in questo manuale cfr. Pacchetto di archiviazione.	OAIS
Archivio	Complesso dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività.	LLGG

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

Classificazione	Attività di organizzazione di tutti i documenti secondo uno schema costituito da un insieme di voci articolate in modo gerarchico e che individuano, in astratto, le funzioni, competenze, attività e/o materie del soggetto produttore.	LLGG
Cliente	Il soggetto che per legge ha l'obbligo di conservare.	CINECA
Comunità di riferimento	Un gruppo ben individuato di potenziali utenti che dovrebbero essere in grado di comprendere un particolare insieme di informazioni. La comunità di riferimento può essere composta da più comunità di utenti.	OAIS
Controllo forzabile	Sono forzabili i controlli il cui mancato superamento rimette la responsabilità del versamento dell'unità al Responsabile della conservazione.	CINECA
Controllo non forzabile	Sono non forzabili i controlli il cui mancato superamento comporta il rifiuto inderogabile dell'unità di versamento controllata.	CINECA
CONSERVA	Sistema di conservazione Cineca	CINECA
Conservatore	Soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici.	LLGG
Conservazione	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato garantendo nel tempo le caratteristiche di	LLGG

	autenticità, integrità, leggibilità, reperibilità dei documenti.	
Consumer	Denominazione in OAIS di utente. Per l'accezione utilizzata in questo manuale cfr. Utente.	OAIS
Contenuto informativo	L'insieme di informazioni che costituisce l'obiettivo originario della conservazione**.** È un oggetto informativo composto dal suo oggetto-dati e dalle sue informazioni sulla rappresentazione.	OAIS
Convenzioni di denominazione del file	Insieme di regole sintattiche che definisce il nome dei file all'interno di un filesystem o pacchetto. (Anche ***Naming convention)***	LLGG
Coordinatore della Gestione Documentale	Soggetto responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 nei casi di amministrazioni che abbiano istituito più Aree Organizzative Omogenee.	LLGG
Copia informatica di documento analogico	Il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto.	CAD
Copia informatica di documento informatico	Il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari. Modifiche ed integrazioni al CAD.	CAD

Copia per immagine su supporto informatico di documento analogico	Il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto.	CAD
Destinatario	Il soggetto/sistema al quale il documento informatico è indirizzato.	LLGG
Digest	Vedi impronta crittografica.	LLGG
Dissemination Information Package (DIP)	Denominazione in OAIS del pacchetto di distribuzione. Per l'accezione utilizzata in questo manuale cfr. Pacchetto di distribuzione.	OAIS
Documento amministrativo informatico	Gli atti formati dalle pubbliche amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse.	LLGG
Documento analogico	La rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.	CAD
Documento elettronico	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva.	LLGG
Documento informatico	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.	LLGG
Duplicato informatico	Il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario.	CAD
eIDAS - electronic IDentification Authentication and Signature	Regolamento (UE) № 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel	

	mercato interno e che abroga la direttiva 1999/93/CE.	
Esibizione	Operazione che consente di visualizzare un documento conservato.	LLGG
Evidenza informatica	Una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.	
Fascicolo informatico	Aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento.	LLGG
File	Insieme di informazioni, dati o comandi logicamente correlati, raccolti sotto un unico nome e registrati, per mezzo di un programma di elaborazione o di scrittura, nella memoria di un computer.	LLGG
Filesystem	Sistema di gestione dei file, strutturato mediante una o più gerarchie ad albero, che determina le modalità di assegnazione dei nomi, memorizzazione e organizzazione all'interno di uno storage.	LLGG
Firma digitale	Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di	CAD

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

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

	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 hash crittografica a un'evidenza informatica.	LLGG
Indice di conservazione	File associato ad ogni volume di conservazione, contenente un insieme di informazioni organizzate conformemente allo Schema XML fornito in questo documento.	UNISINCRO
Informazioni descrittive	L'insieme delle informazioni, composto essenzialmente dalla descrizione del pacchetto per coadiuvare l'utente nella ricerca, nella richiesta e nel recupero di informazioni in un OAIS. Sono riportate all'interno degli Accordi di Versamento. Compongono il pacchetto insieme alle informazioni sulla conservazione.	OAIS
Informazioni sul contesto	Le informazioni che documentano le relazioni del contenuto informativo con il suo ambiente, ivi inclusi i motivi della creazione del contenuto informativo e il modo in cui è in relazione con altri contenuti informativi. Sono riportate all'interno degli Accordi di Versamento.	OAIS
Informazioni sull'accesso	Le informazioni che identificano le restrizioni di accesso. Sono riportate all'interno degli Accordi di Versamento.	OAIS
Informazioni sull'identificazione	Le informazioni che identificano, e se necessario descrivono, uno o più meccanismi di attribuzione di identificatori al contenuto informativo. Tali informazioni forniscono anche	OAIS

	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.	
Informazioni sull'impacchettamento	Le informazioni usate per collegare e identificare le componenti di un pacchetto informativo. Sono riportate all'interno degli Accordi di Versamento.	OAIS
Informazioni sull'integrità	Le informazioni che documentano i meccanismi di autenticazione e forniscono le chiavi di autenticazione per garantire che l'oggetto contenuto Informativo non sia stato alterato senza una documentazione dell'evento. Sono riportate all'interno degli Accordi di Versamento.	OAIS
Informazioni sulla conservazione	Le informazioni necessarie per un'adeguata conservazione del contenuto informativo. Includono le informazioni sull'identificazione, provenienza, contesto, integrità e accesso.	OAIS
Informazioni sulla provenienza	Le informazioni che documentano la storia del contenuto informativo, sui cambiamenti avvenuti dal momento della sua creazione e su chi ne ha curato la custodia sin dall'origine. Sono 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 conservazione.	LLGG
Oggetto digitale	Oggetto informativo digitale, che può assumere varie forme tra le quali quelle di documento informatico, fascicolo informatico, aggregazione documentale informatica o archivio informatico.	LLGG
Oggetto informativo	Un oggetto dati insieme con le sue informazioni sulla rappresentazione.	OAIS
Originali non unici	I documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi.	CAD
Pacchetto di archiviazione	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di	LLGG

	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.	LLGG
Pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione.	LLGG
Pacchetto informativo	Contenitore logico che racchiude uno o più oggetti di conservazione con i relativi metadati, oppure anche i soli metadati riferiti agli oggetti di conservazione.	LLGG
Path	Informazioni relative alla localizzazione virtuale del file all'interno del filesystem espressa come concatenazione ordinata del nome dei nodi del percorso. (anche *Percorso*)	LLGG
Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di 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	LLGG

	conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445.	
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 i documenti ricevuti e spediti da un ente e per tutti i documenti informatici dell'ente stesso.	LLGG
Registro particolare	Registro informatico individuato da una pubblica amministrazione per la memorizzazione delle informazioni relative a documenti soggetti a registrazione particolare.	LLGG
Repertorio informatico	Registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche con cui si formano altri atti e documenti o indici di atti e documenti secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica.	CINECA

Resoconto di versamento	Documento informatico che comunica al Produttore, immediatamente dopo il versamento, lo stato del pacchetto di versamento (*interamente_versato, parzialmente_versato o rifiutato)* con il dettaglio dell'esito di tutti i controlli sulle singole unità.	CINECA
Responsabile del servizio di conservazione	Soggetto che coordina il processo di conservazione all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID.	LLGG
Responsabile della conservazione	Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.	LLGG
Responsabile della funzione archivistica di conservazione	Soggetto che coordina il processo di conservazione dal punto di vista archivistico all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID	LLGG
Responsabile della gestione documentale	Soggetto responsabile della gestione del sistema documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445.	LLGG
Responsabile della protezione dei dati	Persona con conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, in grado di assolvere i compiti di cui all'articolo 39 del Regolamento (UE) 2016/679.	LLGG

Riferimento temporale	Insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC).	LLGG
Riversamento	Procedura mediante la quale uno o più documenti informatici sono convertiti da un formato di file (ovvero di busta, ovvero di pacchetto di file) ad un altro, lasciandone invariato il contenuto per quanto possibilmente permesso dalle caratteristiche tecniche del formato (ovvero dei formati) dei file e delle codifiche di destinazione.	LLGG
Scarto	Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico-culturale.	LLGG
Serie	Raggruppamento di documenti con caratteristiche omogenee (vedi anche aggregazione documentale informatica).	LLGG
Sigillo elettronico	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi.	LLGG
Sistema di conservazione	Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, comma 1, del CAD.	LLGG
Sistema di gestione informatica dei documenti	Insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure	CAD

	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.	
Submission Information Package (SIP)	Denominazione in OAIS del pacchetto di versamento. Per l'accezione utilizzata in questo manuale cfr. Pacchetto di versamento.	OAIS
Tag library	Dizionario dei marcatori contenente le definizioni in ordine alfabetico di tutti gli elementi, i tipi e gli attributi individuati da uno Schema XML, mirato a definire la loro semantica.	UNISINCRO
Tipologia documentale	Categoria di documenti omogenei per natura e funzione giuridica, modalità di registrazione o di produzione, che hanno comuni caratteristiche formali e/o intellettuali.	CINECA
Titolare dell'oggetto di conservazione	Soggetto produttore degli oggetti di conservazione. Nel contesto Cineca corrisponde al Cliente. (Nel testo anche Titolare)	LLGG
Trasferimento	Passaggio di custodia dei documenti da una persona o un ente ad un'altra persona o un altro ente.	LLGG
TUDA	Testo Unico della Documentazione Amministrativa, Decreto del Presidente della Repubblica 28 dicembre 2000, n.445, e successive modificazioni.	LLGG
Ufficio	Riferito ad un'area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi	LLGG

	a disposizione dal sistema di protocollo informatico.	
UNI SinCRO	Norma UNI che definisce, tramite uno Schema XML, la struttura dell'insieme dei dati a supporto del processo di conservazione. Essa individua la struttura del cosiddetto indice 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 divisibile, di cui è composto un archivio, per esempio, una lettera, un memorandum, un rapporto, una fotografia, una registrazione sonora. Può essere composta da più file.	CINECA
Utente abilitato	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.	LLGG

Versamento	Passaggio di custodia, di proprietà e/o di responsabilità dei documenti. Nel caso di un organo giudiziario e amministrativo dello Stato operazione con la quale il responsabile della conservazione trasferisce agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali.	LLGG
Volume di conservazione	Unità logica risultato finale di un processo mirato a conservare un insieme di oggetti digitali.	UNISINCRO
Web Service	Sistema software progettato per supportare l'interoperabilità tra diversi elaboratori su di una medesima rete ovvero in un contesto distribuito.	CINECA

Torna al sommario

2.2 Acronimi

AGID	Agenzia per l'Italia Digitale
AIP	Archival Information Package (OAIS) anche PdA
DIP	Dissemination Information Package (OAIS) anche PdD
ETSI	European Telecommunications Standards Institute
IPA	Indice Pubblica Amministrazione
ISO	International Standard Organization

OAIS	Open Archival Information System
PAIMAS	Space Data and Information Transfer Systems - Producer-Archive Interface - Methodology Abstract Standard (ISO 20652)
PDI	Preservation Descriptive Information
PdA	Pacchetto di Archiviazione
PdD	Pacchetto di Distribuzione
PdV	Pacchetto di Versamento
PEC	Posta Elettronica Certificata
RdC	Responsabile della conservazione
SIP	Submission Information Package (OAIS) anche PdV
UNI	Ente Nazionale Italiano di Unificazione
URL	Uniform Resource Locator
WebDAV	Web-based Distributed Authoring and Versioning: protocollo che consente di trasformare il web in mezzo di lettura e scrittura analogo al disco locale. In particolare WebDAV si riferisce a un set di istruzioni del protocollo HTTP, che permettono all'utente di gestire in modo collaborativo dei file in un server remoto.
XML	EXtensible Markup Language

Torna al sommario

3 Normativa e standard di riferimento

3.1 Normativa

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

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

- **Codice Civile** – R.D del 16 marzo 1942 n. 262;
- **Legge 241/1990** - Nuove norme sul procedimento amministrativo;
- **DPR 445/2000** - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- **DPR 37/2001** - Regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli uffici dello Stato;
- **D.lgs 196/2003** - recante il Codice in materia di protezione dei dati personali;
- **D.lgs 42/2004** - Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n.137;
- **D.lgs 82/2005** e ss.mm.ii. - Codice dell'amministrazione digitale;
- **D.lgs 33/2013** - Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni;
- **DPCM 22 febbraio 2013** - Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;
- **DPCM 21 marzo 2013** - Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a

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

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

Torna al sommario

3.2 Standard di riferimento

Si riportano di seguito gli standard di riferimento:

- **ISO 14721 OAIS -** (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- **ISO/IEC 27001 -** Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- **UNI 11386 -** Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- **ISO 15836 -** Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.
- **ISO 20652 -** Paimas, Space data and information transfer systems – Methodology abstract standard;
- **ISO 15489 -1 -** Information and documentation – Records Management – part 1: General;
- **ISO 13008** - Information and documentation — Digital records conversion and migration process;
- **ETSI EN 319 401** - Electronic Signatures and Infrastructures (ESI) General Policy Requirements for Trust Service Providers (laddove applicabile);
- **ETSI TS 119 511** - Electronic Signatures and Infrastructures (ESI) Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques;
- **ETSI TS 101 533-1 V1.3.1 (2012-04)** Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- **ETSI TR 101 533-2 V1.3.1 (2012-04)** Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for

Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.

Torna al sommario

4 Ruoli e responsabilità

Il presente capitolo richiama quanto previsto dalla normativa per quanto riguarda le attività di competenza dei soggetti responsabili e presenti nel processo di conservazione.
Di seguito l'elenco dei profili richiesti e/o ritenuti utili al fine di una corretta gestione del processo di conservazione:

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

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

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

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

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

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

- il ***Responsabile del servizio di conservazione*** si occupa della:
  - Definizione e attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione;
  - definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente;
  - corretta erogazione del servizio di conservazione all'ente produttore;
  - gestione delle convenzioni, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.

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

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

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

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

- il ***Responsabile della sicurezza dei sistemi per la conservazione*** si occupa del/della:
  - rispetto dei requisiti e monitoraggio della sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza;
  - segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.

- il ***Responsabile dei sistemi informativi per la conservazione*** si occupa del/della:
  - gestione dell'esercizio delle componenti hardware e software del sistema di conservazione;
  - monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con il cliente;
  - segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive;
  - pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione;
  - controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.

- il ***Responsabile dello sviluppo e della manutenzione del sistema di conservazione*** si occupa del/della:

- coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione;
- pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione;
- monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione;
- interfaccia con il produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche;
- gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.

Torna al sommario

5 Struttura organizzativa per il servizio di conservazione

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo	Eventuali deleghe
Responsabile del servizio di conservazione (RSERV)	Alessandro De Angelis	Cfr. Capitolo 2 - Ruoli e Responsabilità	Giugno 2023	Nessuna
Responsabile Sicurezza dei sistemi per la conservazione (RSIC)	Paola Tentoni	Cfr. Capitolo 2 - Ruoli e Responsabilità	Gennaio 2015	Nessuna
Responsabile funzione archivistica di conservazione (RARCH)	Mariagrazia Mingrone	Cfr. Capitolo 2 - Ruoli e Responsabilità	Gennaio 2023	Nessuna
Responsabile sistemi informativi per la conservazione (RSINF)	Angelo Neri	Cfr. Capitolo 2 - Ruoli e Responsabilità	Aprile 2015	Nessuna
Responsabile sviluppo e manutenzione del sistema di conservazione (RSVIL)	Alessandro De Angelis	Cfr. Capitolo 2 - Ruoli e Responsabilità	Giugno 2023	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	Massimiliano Valente	Cfr. Capitolo 2 - Ruoli e Responsabilità	Da maggio 2021 a maggio 2023
	Riccardo Righi	Cfr. Capitolo 2 - Ruoli e Responsabilità	Da luglio 2017 ad aprile 2021
	Paolo Vandelli	Cfr. Capitolo 2 - Ruoli e Responsabilità	Da luglio 2015 a luglio 2017

Responsabile trattamento dati personali	Emilio Ferrari	Cfr. Capitolo 2 - Ruoli e Responsabilità	Da gennaio 2014 a febbraio 2018
Responsabile sviluppo e manutenzione del sistema di conservazione	Massimiliano Valente	Cfr. Capitolo 2 - Ruoli e Responsabilità	Da ottobre 2017 a maggio 2023
	Francesca Merighi	Cfr. Capitolo 2 - Ruoli e Responsabilità	Da aprile 2015 a ottobre 2017
Responsabile funzione archivistica di conservazione	Massimiliano Valente	Cfr. Capitolo 2 - Ruoli e Responsabilità	Da maggio 2021 a dicembre 2022
	Riccardo Righi	Cfr. Capitolo 2 - Ruoli e Responsabilità	Da ottobre 2020 ad aprile 2021
	Laura Federica Nisi	Cfr. Capitolo 2 - Ruoli e Responsabilità	Da luglio 2015 a ottobre 2020

Torna al sommario

5.1 Organigramma

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

Torna al sommario

5.2 D Strutture organizzative

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

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

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

6 Oggetti sottoposti a conservazione

6.1 Oggetti conservati

Il servizio di conservazione Conserva, in ottemperanza alla normativa segue il modello informativo dello standard ISO 14721 OAIS[1] (di seguito solo OAIS).
Lo standard OAIS ha la peculiarità di organizzare gli oggetti informativi da conservare in pacchetti informativi tipizzati in base alla fase del processo di conservazione. I tipi di pacchetto sono tre e racchiudono gli oggetti informativi inviati in conservazione assieme alla relativa metadatazione utile ai fini conservativi:

- il **pacchetto di versamento (PdV)**: pacchetto versato dal produttore e utilizzato per l'acquisizione degli oggetti informativi e dei metadati da parte del sistema di conservazione;
- il **pacchetto di archiviazione (PdA)**: pacchetto finalizzato alla memorizzazione a lungo termine degli oggetti informativi digitali nel sistema di conservazione;
- il **pacchetto di distribuzione (PdD)**: pacchetto costituito da una o più unità documentali o da un pacchetto di archiviazione, generato dal Sistema su richiesta dell'utente in una forma idonea alle specifiche esigenze di utilizzo.

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

- la grande rapidità di aggiornamento delle tipologie di oggetti informativi da conservare;
- gli oggetti informativi da conservare variano da un Titolare a un altro ed è possibile che le stesse tipologie di oggetti informativi da conservare possano variare sia dal punto di vista del contenuto informativo che della metadatazione.

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

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

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

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

Torna al sommario

6.2 Pacchetto di versamento

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

A livello generale il pacchetto di versamento è costituito da:

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

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

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

L'invio al sistema di conservazione Conserva può avvenire tramite due modalità:

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

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

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

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

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

Il sistema di conservazione si avvale di librerie open source per il riconoscimento dei formati dei file ricevuti all'interno dei pacchetti di versamento. Queste librerie non si limitano a verificare l'estensione dei file, ma ne verificano il contenuto, dando quindi un livello di sicurezza superiore rispetto al reale formato dei file giunti in conservazione.

Torna al sommario

6.3 Pacchetto di archiviazione

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

A livello generale il pacchetto di archiviazione è costituito da:

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

I pacchetti di archiviazione possono essere costruiti seguendo due criteri:

- serie di unità documentarie omogenee;
- unità archivistiche.

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

In linea con la normativa, l'indice del pacchetto di archiviazione è conforme allo standard UNI 11386 SInCRO, al fine di facilitare l'interoperabilità tra i sistemi di conservazione. La descrizione puntuale della valorizzazione dei singoli elementi dello standard SInCRO è riportata nell'allegato 3 dedicato all'implementazione di UNISInCRO in Conserva.

Torna al sommario

6.4 Pacchetto di distribuzione

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

A livello generale il pacchetto di distribuzione è costituito da:

- 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 dal responsabile del servizio di conservazione. L'intero pacchetto viene fornito all'utente in formato compresso, firmato digitalmente e marcato temporalmente dal responsabile del servizio di conservazione.

Torna al sommario

7 Il processo di conservazione

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

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

La fase di versamento è la prima fase del processo di conservazione che disciplina formalmente il passaggio di custodia e gestione degli oggetti informativi dal Titolare al Conservatore.
Per strutturare questa fase di acquisizione degli oggetti informativi è stato preso come modello di riferimento lo standard ISO 20652 Paimas[2] (di seguito chiamato Paimas), il cui scopo è quello di definire la metodologia da seguire dal primo contatto tra il Titolare e il Conservatore, fino alla ricezione e validazione dell'unità di versamento nel sistema di conservazione.
Il suddetto standard struttura la fase di versamento in:

- **fase preliminare**: include i primi contatti tra il Titolare e il Conservatore in cui si definiscono gli interlocutori e l'obiettivo della conservazione; in questa fase si dà inizio alla redazione della relativa documentazione e si individuano gli oggetti informativi che il Titolare intende inviare al sistema di conservazione;
- **fase di definizione formale**: permette di entrare nel merito dei dettagli dell'intero processo di conservazione per stilare l'accordo di versamento la cui sottoscrizione è a cura del Responsabile della conservazione del Titolare e del Responsabile del servizio di conservazione (*"Allegato 1 Modello di Accordo di versamento"*);
- **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 titolare dell'oggetto di conservazione e descritti nell'accordo di versamento.

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

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

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

Torna al sommario

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

Il rapporto di versamento è un documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.

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

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

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

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

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

Il fine del rapporto di versamento è di dare evidenza dei risultati del processo di versamento, sia che il pacchetto e le relative unità siano state versate o rifiutate, sia che una volta versate risultino esser le stesse concordate con il Titolare.

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

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

Torna al sommario

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

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

Il rifiuto in fase di trasferimento viene comunicato in maniera sincrona al Titolare e normalmente avviene nel caso in cui il pacchetto di versamento inviato non corrisponda, in toto o in parte, al pacchetto di versamento ricevuto da CONSERVA, oppure che il pacchetto stesso non sia stato costruito secondo le regole concordate in fase di accordo di versamento. È possibile consultare tutti i messaggi di errore che il servizio comunica al Titolare in fase di trasferimento, nell'allegato relativo ai controlli.

In fase di versamento, invece, i controlli vengono eseguiti in modalità asincrona. Il sistema, dopo aver ricevuto il pacchetto di versamento, tramite servizio temporizzato elabora il pacchetto stesso effettuando una serie di controlli (alcuni comuni a tutti i pacchetti di versamento, altri diversi a seconda della tipologia dell'unità di versamento, altri ancora richiesti dal Titolare e quindi diversi da ente a ente). La fase di versamento, qualsiasi sia l'esito, si conclude con la notifica del *resoconto di versamento* e del *rapporto di versamento* al Titolare. Nel resoconto di versamento, viene comunicato lo stato del pacchetto di versamento (*interamente_versato, parzialmente_versato o rifiutato)* con il dettaglio dell'esito di tutti i controlli sulle singole unità. Nel Rapporto di Versamento sono presenti informazioni simili assieme ad altre più dettagliate relative al pacchetto di versamento

per verificarne l'integrità nel tempo; il rapporto di versamento viene firmato digitalmente dal Responsabile del servizio di Conservazione tramite firma automatica. Tutti i rapporti di versamento vengono sottoposti a procedura di conservazione. È possibile consultare tutti i messaggi di errore che il servizio comunica al Titolare in fase di versamento nell'allegato relativo ai controlli.

Torna al sommario

7.6 Preparazione e gestione del pacchetto di archiviazione

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

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

Ai fini dell'interoperabilità tra i sistemi di conservazione e come previsto dalla norma, l'indice del pacchetto di archiviazione deve corrispondere allo standard UNI SInCRO.

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

La generazione dell'indice del pacchetto di archiviazione avviene al momento della chiusura del pacchetto di archiviazione. Il pacchetto, normalmente, viene chiuso al momento di chiusura dell'unità archivistica o della serie a cui corrisponde. Il tempo che intercorre tra il popolamento del pacchetto e il momento della chiusura non aumenta il rischio di corruzione della documentazione conservata: grazie al monitoraggio periodico e all'infrastruttura di sicurezza è possibile garantirne l'autenticità, ossia la sua identità ed integrità, documentabile tramite una chiara catena di evidenze.

Al fine di render stabile l'indice, questo viene firmato digitalmente dal Responsabile del servizio di conservazione, su affidamento del Responsabile della conservazione, e vi appone una marca temporale rilasciata da una CA secondo la normativa vigente.

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

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

Tutte le unità presenti in un pacchetto di archiviazione, sia chiuso che aperto, possono essere aggiornate; tutti gli aggiornamenti sono tracciati e le singole unità versionate. In caso di aggiornamento di un'unità presente in un pacchetto di archiviazione chiuso, quest'ultimo viene migrato e la migrazione viene tracciata nell'indice del pacchetto di archiviazione.

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

1. se la perdita o la corruzione di dati è dovuta ad un incidente si attiva la procedura di Disaster Recovery;
2. in altri casi si ricreano, grazie alle informazioni presenti sul sistema, i pacchetti di versamento originali con cui gli oggetti digitali corrotti sono entrati in CONSERVA al fine di riversarli nuovamente nel sistema;
3. se l'attività descritta al punto 2 non fosse possibile, a causa della perdita definitiva di informazioni, si concorderebbe una procedura con il Titolare al fine di controllare sui sistemi produttori la possibilità di risalire agli oggetti digitali originali; la perdita definitiva dei dati è, ad ogni modo, improbabile, in quanto l'accesso al database è limitato al solo team di CONSERVA.

Torna al sommario

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

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

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

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

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

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

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

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

Torna al sommario

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

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

La figura del pubblico ufficiale è necessaria nei seguenti casi:

- dichiarazione di conformità di una copia informatica di un documento informatico conservato nel sistema di conservazione;
- dichiarazione di conformità di copia informatica di documento informatico conservato nel sistema di conservazione nei casi di obsolescenza di formato.

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

Torna al sommario

7.9 Scarto dei pacchetti di archiviazione

All'interno dell'accordo di versamento vengono riportati anche i tempi di conservazione dell'oggetto informativo, stabiliti negli appositi massimari di selezione e scarto dei singoli Titolari. L'accordo, ove possibile, farà anche riferimento alla normativa che disciplina lo scarto di specifiche tipologie di oggetti informativi (ad esempio norme fiscali).

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

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

Nel caso di archivi pubblici o privati di particolare interesse culturale, le procedure di scarto avvengono previa autorizzazione del Ministero della cultura.

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

Torna al sommario

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

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

Il Conservatore è in grado di acquisire pacchetti di distribuzione provenienti da altri conservatori aderenti 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 nei paragrafi che seguono.

Agli utenti autorizzati ad accedere al servizio, Cineca rilascia apposite credenziali di accesso composte da username e password; il servizio garantisce l'autenticazione anche tramite SPID (l'utente può accedere a Conserva utilizzando le credenziali rilasciate dal proprio gestore di identità digitale) e tramite CIE (l'utente può accedere utilizzando la propria Carta d'Identità Elettronica).

Torna al sommario

8.1 Componenti logiche

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

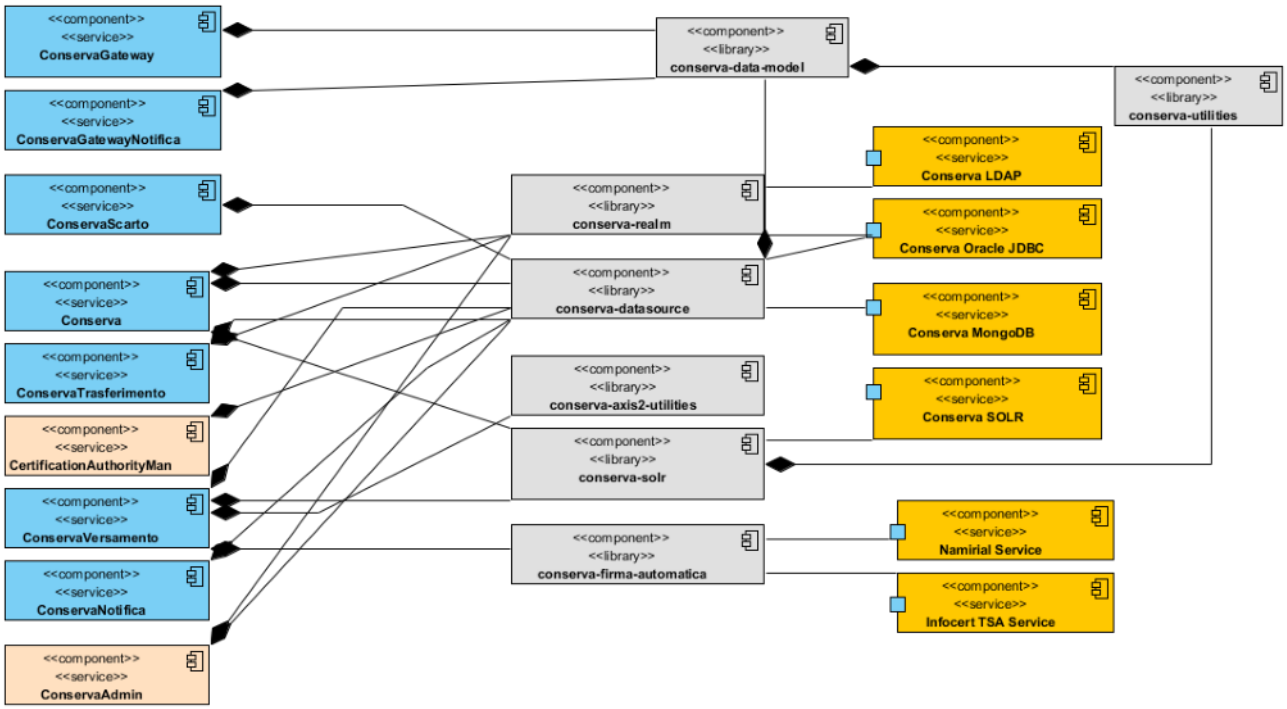


Figura 1- Schema delle componenti logiche che compongono il servizio

- **Conserva servizio** - Componente che si occupa dell'accesso degli utenti al sistema. È un'applicazione web basata su un'architettura MVC (Model View Controller). Rende disponibili funzioni di ricerca ed esibizione (pacchetti di distribuzione), di consultazione di audit, di amministrazione e di recupero dati di versamento.
- **ConservaTrasferimento servizio** - Componente che riceve tramite *web service* i pacchetti di versamento inviati dai sistemi produttori. Comprende anche una serie di controlli che riguardano l'integrità e la correttezza formale del pacchetto di versamento.
- **ConservaVersamento servizio** – Componente Web che elabora i pacchetti di versamento ricevuti, li verifica ed effettua le operazioni necessarie affinché gli oggetti informativi in esso contenuti vengano presi in carico dal sistema di conservazione. Crea, popola, chiude e infine distribuisce i pacchetti di archiviazione in cui gli oggetti informativi vengono conservati.
- **Conserva-datasource libreria** – Libreria che si occupa di tutte le comunicazioni tra i componenti software e le basi di dati.
- **Conserva-data-model libreria** - Componente software dove vengono descritti gli oggetti che vengono elaborati e popolati da tutti gli altri componenti.

- **Conserva-utilities libreria** - Componente che mette a disposizione dell'intero sistema di conservazione metodi di utilità comuni a tutti gli altri componenti.
- **Conserva-axis2-utilities libreria** - Componente che mette a disposizione metodi che riguardano le connessioni tramite *web service*.
- **Conserva-solr libreria** - Componente che mette a disposizione metodi che consentono di indicizzare e ricercare elementi indicizzati.
- **Conserva-realm libreria** - Componente che mette a disposizione metodi che consentono di dialogare con il sistema di autenticazione e il sistema di autorizzazione.
- **Conserva-firma-automatica libreria** - Componente che si occupa dell'interazione con il Gateway di firma per l'apposizione delle firme automatiche necessarie al funzionamento di CONSERVA.
- **ConservaNotifica servizio** – Componente che gestisce le notifiche push dei rapporti e dei resoconti di versamento ai webservice registrati dei produttori.
- **CertificationAuthority servizio** – Componente che gestisce l'aggiornamento del repository locale dei certificati e delle CRL.
- **ConservaAdministration servizio** - Componente che permette l'amministrazione del sistema e della maggior parte dei componenti precedentemente descritti: ad esempio la creazione e la gestione di tutte le utenze che possono accedere a Conserva, la gestione dei servizi temporizzati, la creazione e gestione degli enti produttori e la creazione e gestione di nuovi accordi di versamento.
- **ConservaScarto servizio** – Componente che gestisce l'interazione fra il componente Conserva (interfaccia web di consultazione dell'archivio) e il componente conserva-versamento per la gestione dell'attività di scarto di oggetti informativi con la conseguente revisione dei pacchetti di archiviazione.

Torna al sommario

8.2 Componenti tecnologiche

8.2.1 Software e strumenti software utilizzati

Partendo dal diagramma seguente, si descrivono le tecnologie utilizzate per il corretto funzionamento di CONSERVA:

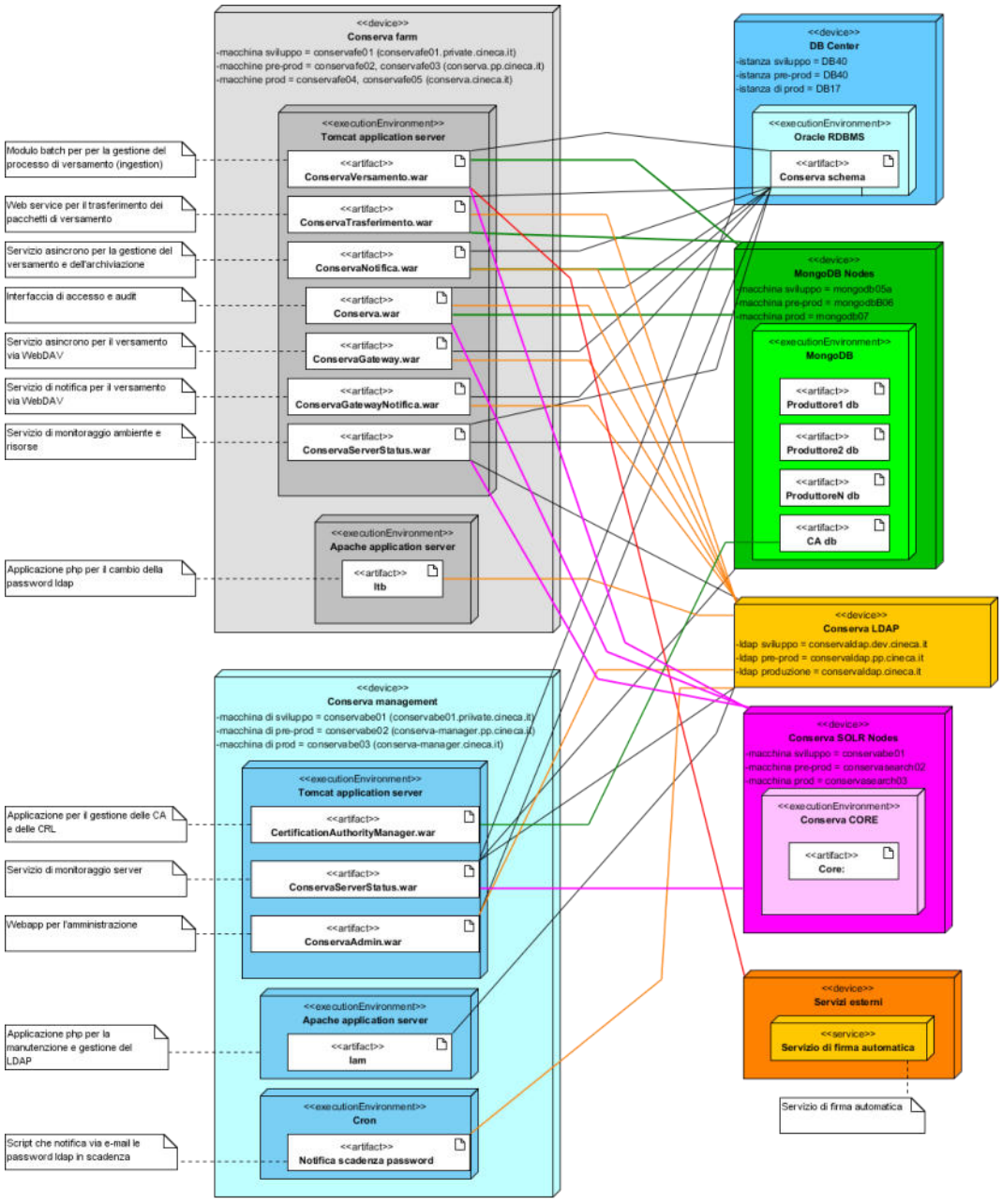


Figura 2 - Diagramma descrittivo dei componenti di Conserva

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

Torna al sommario

8.2.2 Disaster recovery

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

- il sito primario del servizio di hosting è ubicato presso la sede Cineca di Casalecchio di Reno, mentre il sito secondario è ubicato presso la sede Cineca di Roma. Cineca si impegna a comunicare ai Titolari, con adeguato preavviso, ogni variazione all'ubicazione dei siti.
- La frequenza di copia dei dati – ovvero la freschezza del dato sul sito DR – è detta RPO (Recovery Point Objective) ed è di 24H. La ripartenza del servizio sul sito di Disaster Recovery - RTO (Recovery Time Objective) è di 48H.

- I dati dei Titolari, gestiti nell'ambito del servizio di hosting, risiedono all'interno del territorio italiano, nella fattispecie presso i siti primario e secondario previsti per il servizio. Cineca si impegna a comunicare al Titolare, con adeguato preavviso, ogni variazione all'ubicazione dei siti, pur garantendo sempre l'ubicazione interna al territorio italiano.
- Cineca garantisce i servizi per la riattivazione e il ripristino del sistema informativo primario, in presenza di un evento catastrofico, di una condizione di emergenza o di un disastro. I criteri per la definizione di tali eventi e la responsabilità per l'attivazione del Piano di Disaster Recovery rimangono in carico a Cineca, che provvederà a darne visibilità ai Titolari. A fronte di eventuali integrazioni fra l'applicazione e sistemi terzi del Titolare, Cineca si impegnerà nel coordinamento con lo stesso per la gestione in fase di emergenza dei rispettivi Piani di Disaster Recovery.
- Cineca si impegna ad eseguire test periodici (almeno una volta l'anno) per simulare il funzionamento del sito di Disaster Recovery in caso di disastro del sito primario, al fine di verificare che sia assicurato il corretto ripristino del funzionamento del sistema informativo di produzione.

Torna al sommario

8.3 Componenti fisiche

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

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

Lo schema che segue rappresenta la distribuzione dei componenti nell’ambiente di produzione

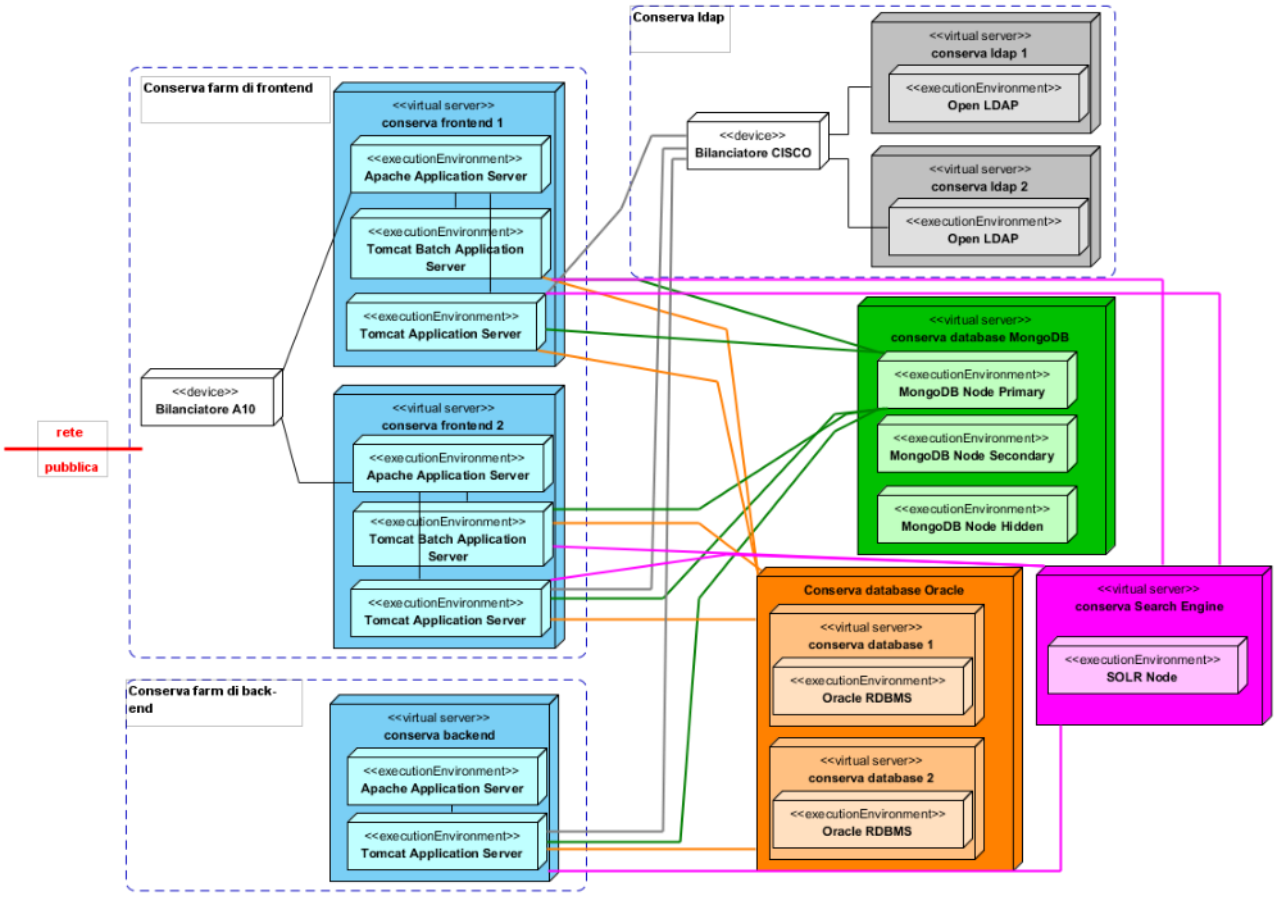


Figura 3 - Distribuzione componenti di Conserva

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

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

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

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

- **Sistema di front end (business logic)**: due server in farm dietro bilanciatore, visibili da rete pubblica, con Apache e Tomcat Application Server.
- **Sistema di back end (business logic)**: un server singolo, visibile solo da rete privata, con Apache e Tomcat Application Server.

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

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

Le sedi CINECA coinvolte sono:

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

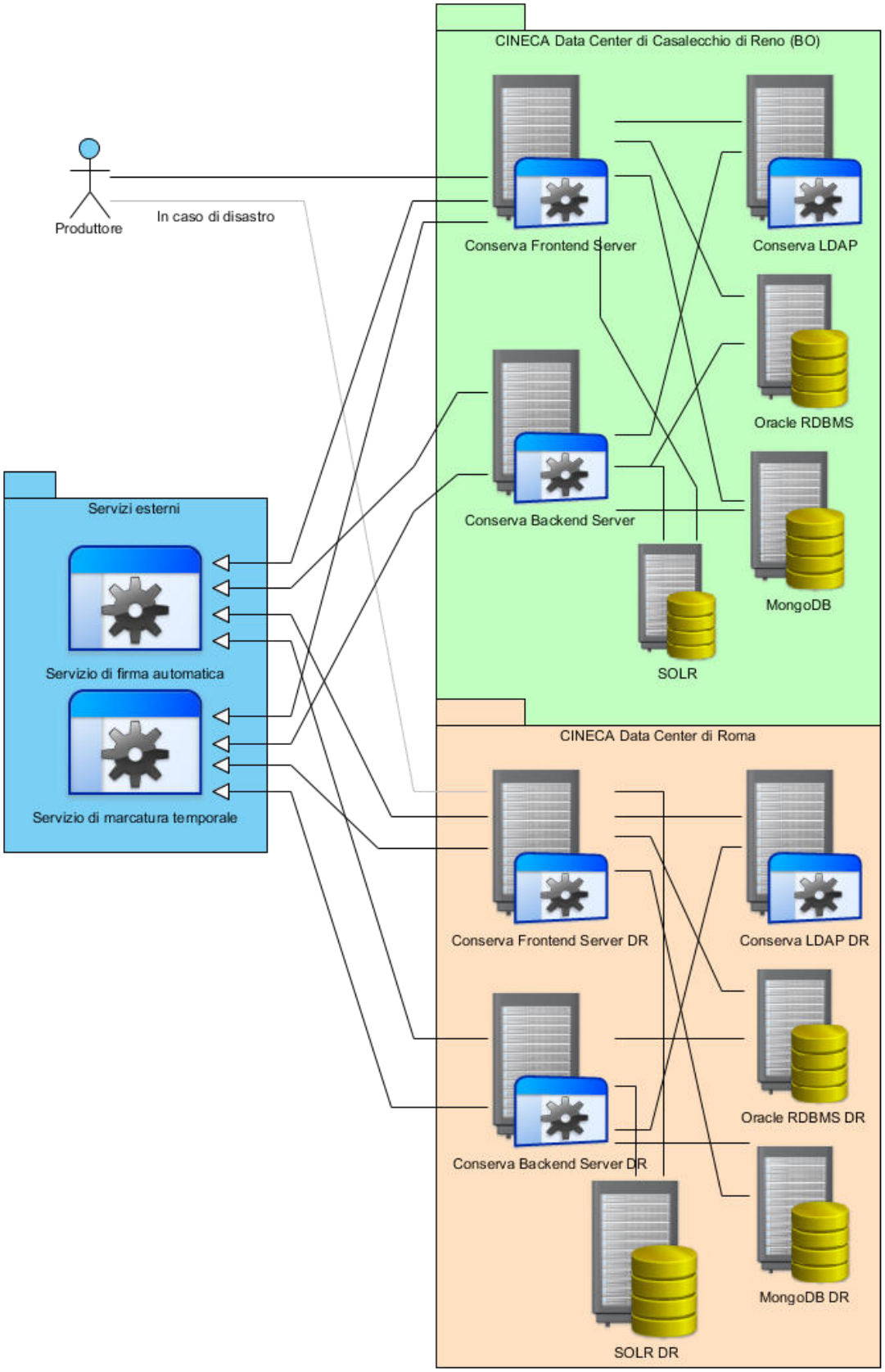

CINECA Data Center di Casalecchio di Reno (BO)
Produttore
In caso di disastro
Conserva Frontend Server
Conserva LDAP
Oracle RDBMS
Conserva Backend Server
MongoDB
SOLR
Servizi esterni
Servizio di firma automatica
Servizio di marcatura temporale
CINECA Data Center di Roma
Conserva Frontend Server DR
Conserva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

Figura 4 - Distribuzione topologica delle componenti fisiche di Conserva

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

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

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

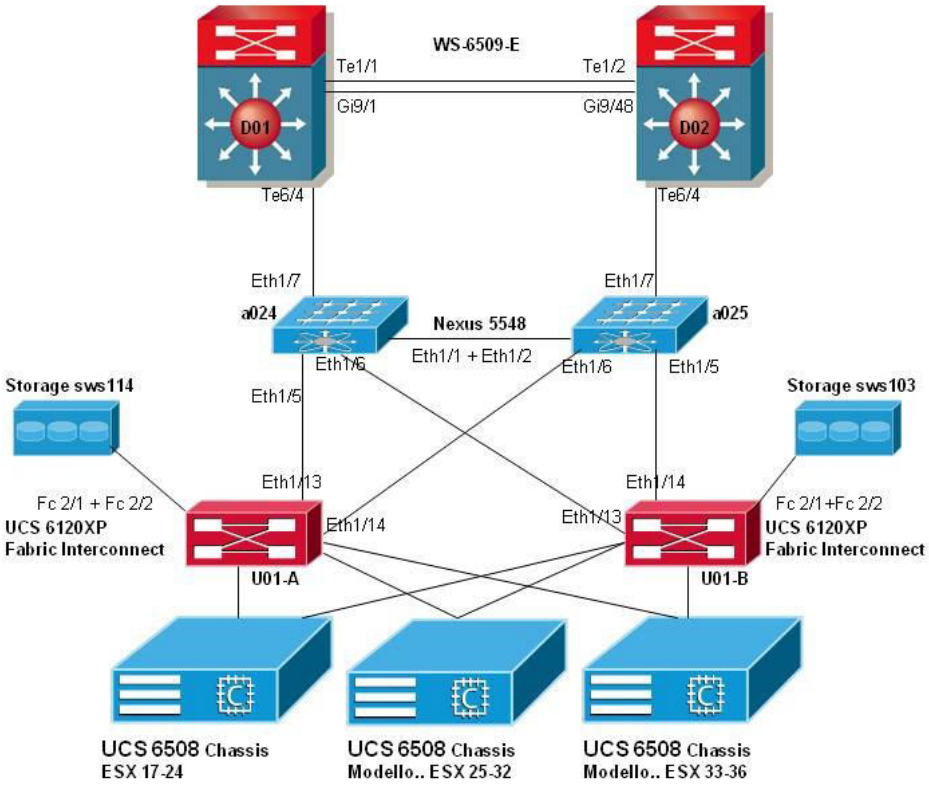


Figura 5 - Schema interconnessioni degli apparati di Conserva

Torna al sommario

8.4 Procedure di gestione e di evoluzione

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

In particolare ogni fase tiene conto dei principi di sicurezza descritti nella pubblicazione del NIST (National Institute of Standards and Technology) "*Engineering Principles for Information Technology Security*"[3].

Torna al sommario

8.4.1 Strategia di sviluppo e ciclo di vita del sistema Conserva

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

- **Caratteristiche del prodotto:** un sistema di conservazione deve essere conforme alla normativa vigente e agli standard di riferimento (in particolare OAIS).
- **Modalità di rilascio del prodotto:** il sistema di conservazione può essere reso disponibile in più rilasci, tutti auto-consistenti e testati, che consistono in un arricchimento e miglioramento delle funzionalità precedenti.
- **Coinvolgimento del cliente del progetto:** a causa delle norme cogenti di conservazione, il cliente del servizio partecipa solo parzialmente alle scelte progettuali. In particolare rende chiari e manifesti i propri requisiti attraverso documentazione appositamente redatta e sottoscritta (accordo di versamento) che costituisce la base per la configurazione e personalizzazione del sistema, piuttosto che per lo sviluppo.

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

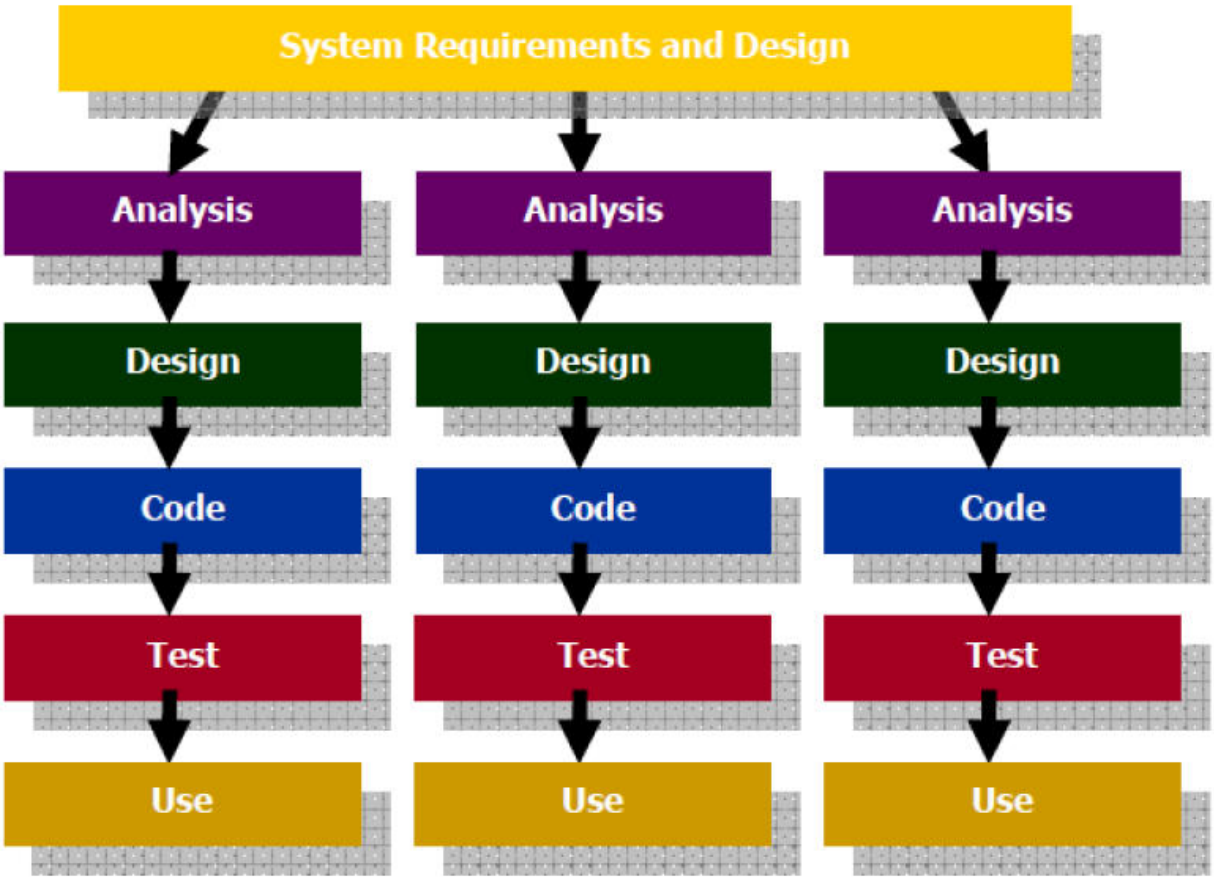


Figura 6 - Ciclo di vita iterativo-incrementale dello sviluppo del software

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)).

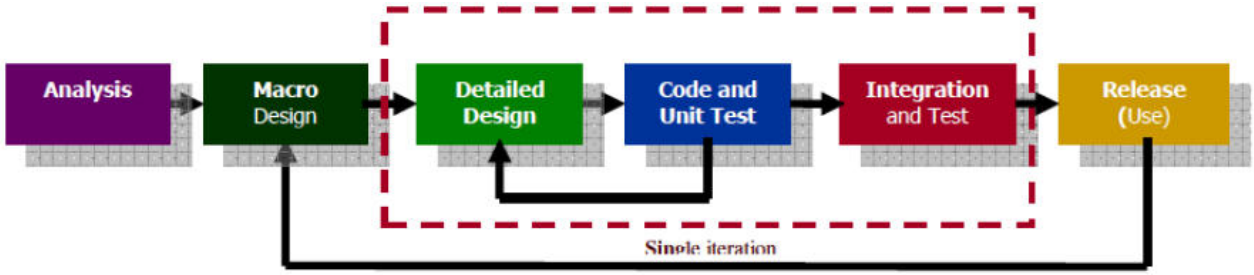


Figura 7 - Dettaglio del ciclo di vita iterativo-incrementale dello sviluppo del software

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

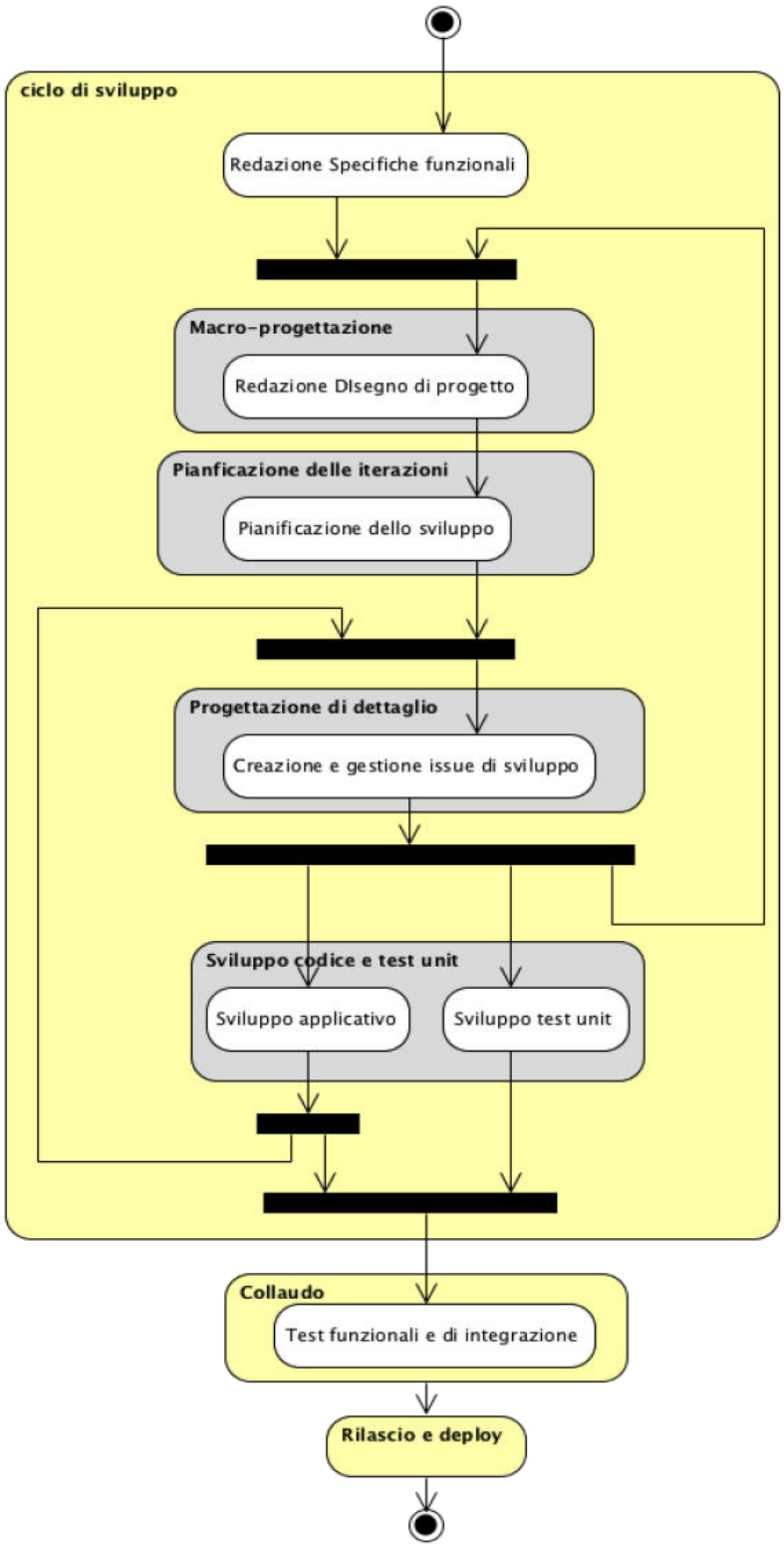


Figura 8 - Fasi di produzione e rilascio del software

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

Torna al sommario

8.4.3.1 Issue

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

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

- possono essere specificate altre informazioni generali.

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

- **Bug -** Segnalazione di errore sul sistema o su uno specifico componente.
- **Story -** Descrizione di una nuova funzionalità da implementare. Utilizzato soprattutto nella fase di macro-analisi.
- **Requirement -** Specifica di requisiti da implementare. Utilizzato per i requisiti dettagliati.
- **Epic -** Utilizzata per raggruppare più issue afferenti allo stesso macro ambito.
- **Task -** Compito generico non classificabile come uno dei precedenti.

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

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

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

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

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

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

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

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

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

Di seguito il workflow che seguono gli stati della issue:

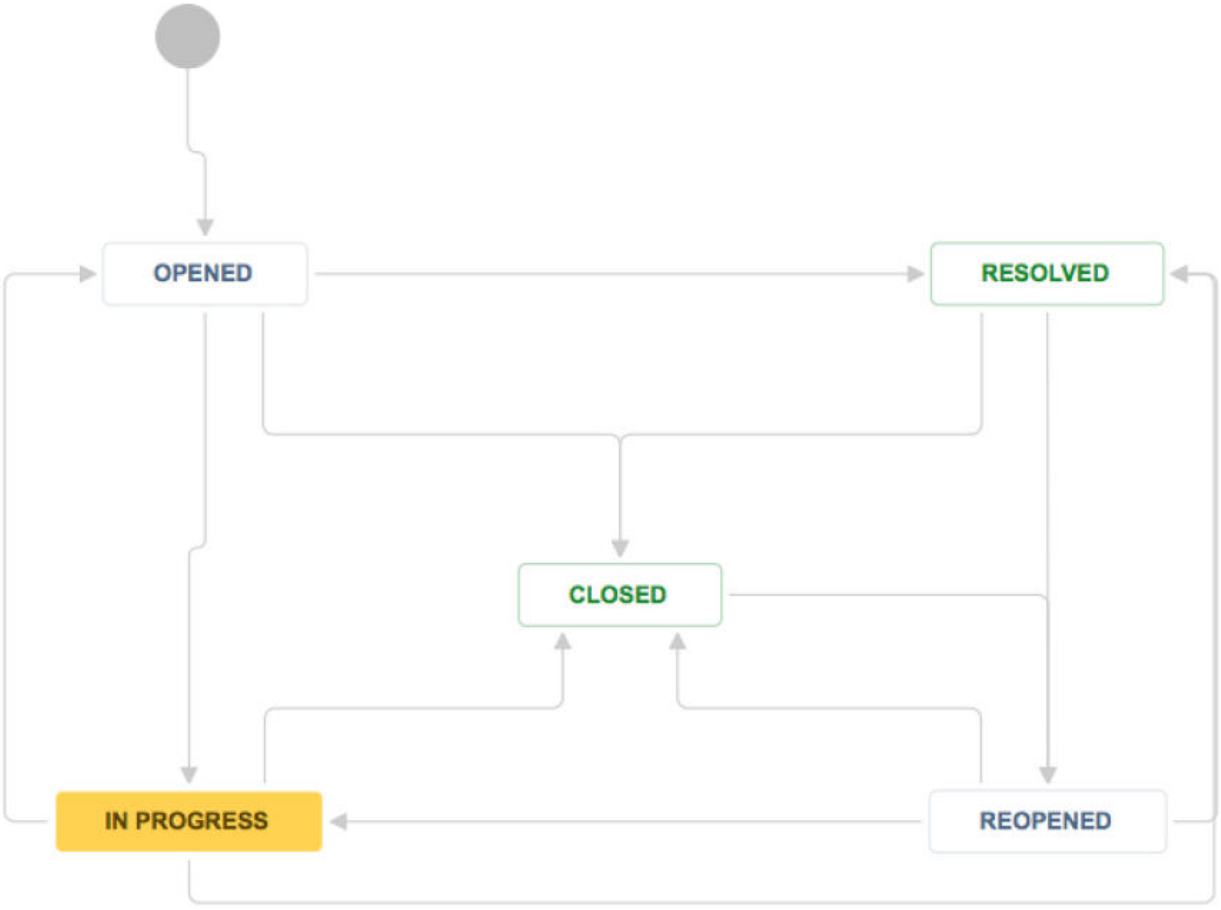


Figura 9 - Workflow degli stati delle singole issue

Torna al sommario

8.4.3.2 Progetti

Le issue in JIRA sono organizzate in progetti.

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

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

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

Sono stati predisposti due progetti speciali Jira:

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

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

Torna al sommario

8.4.3.3 Backlog

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

Torna al sommario

8.4.3.4 Sprint

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

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

Torna al sommario

8.4.4 Versionamento semantico dei componenti

Il numero di ogni versione dei componenti di CONSERVA è costituito da 3 cifre:
MAJOR.MINOR.PATCH.

- L'incremento della *prima cifra (MAJOR)* è a fronte di modifiche sostanziali all'applicazione, che rendono il componente non retro-compatibile con le versioni precedenti.
- L'incremento della *seconda cifra (MINOR)* è a fronte di modifiche sostanziali all'applicazione, che mantengono il componente retro-compatibile con le versioni precedenti.
- L'incremento della *terza cifra (PATCH)* indica una release contenente correzioni di bug e interventi minori con un basso impatto sulla stabilità dell'applicazione e sulla sua usabilità.

Torna al sommario

8.4.5 Gli ambienti di esercizio

8.4.5.1 Separazione degli ambienti

Per CONSERVA sono attivi tre ambienti distinti e separati:

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

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

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

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

Torna al sommario

8.4.5.2 Gestione e validazione degli ambienti

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

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

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

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

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

Torna al sommario

8.4.5.3 Sicurezza dei servizi e delle transazioni applicative

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

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

Torna al sommario

9 Monitoraggio e controlli

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

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

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

Torna al sommario

9.1 Procedure di monitoraggio

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

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

Il monitoraggio consente di misurare lo stato e le metriche di funzionamento della maggior parte dei sistemi applicativi, ed è in grado di dialogare secondo i protocolli più diffusi delle applicazioni quali https, pop3/s, imap/s, smtp, snmp, ed è in grado di intercettare le metriche di funzionamento quali CPU, uso della memoria, della rete, I/O, disco, stato complessivo del sistema operativo, raggiungibilità IP, icmp ecc… di ogni sistema e/o servizio applicativo. In particolare consente:

- la rilevazione degli incidenti;
- il monitoraggio del funzionamento dei servizi e degli oggetti informativi relative ai "livelli funzionali";

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

Ogni anomalia rilevata viene gestita secondo i processi di event, incident, problem management e secondo le procedure che si ispirano alle linee guida ITILv3[4].

Torna al sommario

9.2 Verifica dell'integrità degli archivi

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

Torna al sommario

9.2.1 Monitoraggio a campione degli archivi

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

- Oggetti informativi;
- Pacchetti di archiviazione.

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

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

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

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

Torna al sommario

9.2.2 Controllo integrità unità a seguito di richiesta di esibizione

A seguito di una richiesta di esibizione, Conserva allega al pacchetto di distribuzione un rapporto in cui viene riportato l'esito delle procedure di verifica effettuate sull'integrità del pacchetto generato. Nel caso in cui la verifica di integrità del contenuto del pacchetto di distribuzione desse esito negativo, oltre a produrre il rapporto il sistema notifica l'errore a chi ha richiesto l'esibizione, al Responsabile della conservazione del Titolare coinvolto ed agli eventuali suoi delegati, al Responsabile del servizio di Conservazione, al Responsabile della funzione archivistica di conservazione e al Responsabile dello sviluppo. Questi ultimi avvieranno la procedura di gestione

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

Torna al sommario

9.3 Politiche di conservazione dei log

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

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

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

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

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

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

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

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

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

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

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

Di seguito sono elencate le diverse componenti logiche di Conserva.

Torna al sommario

9.3.1 ConservaTrasferimento

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

- data del trasferimento;

- classe che sta effettuando il log;
- ente Titolare che ha inviato il pacchetto di versamento;
- id del pacchetto di versamento per riconoscerlo all'interno di Conserva;
- nome macchina Conserva che ha elaborato il pacchetto di versamento;
- indirizzo IP della macchina da cui è partito il versamento;
- tipo di azione richiesta;
- tempo impiegato ad effettuare l'azione richiesta;
- livello del log (INFO, WARN, ERROR);
- risultato del trasferimento (es.: "Pacchetto di versamento trasferito con successo").

Torna al sommario

9.3.2 ConservaVersamento

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

- elaborazione controlli versamento (JOB_VERSAMENTO, JOB_RECUPERO_VERSAMENTO);
- elaborazione delle attività riguardanti l'archiviazione (JOB_ARCHIVIAZIONE);
- elaborazione delle attività riguardanti la distribuzione (JOB_DISTRIBUZIONE);
- aggiornamento delle statistiche (JOB_STATISTICHE_GIORNALIERE)
- registrazione delle statistiche di fine anno (JOB_STATISTICHE_ANNUALI)

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

- data dell'evento;
- livello del log (INFO, WARN, ERROR);
- tipo di job che genera il log;
- nome della macchina Conserva che ha gestito l'attività;
- informazioni riguardanti unità di versamento, unità documentale e/o unità archivistica, pacchetto di versamento e/o pacchetto di archiviazione interessati dall'attività.

Torna al sommario

9.3.3 ConservaNotifica

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

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

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

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

Torna al sommario

9.3.4 Conserva

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

- registra il login e il logout;
- registra le ricerche effettuate;

- registra la visualizzazione di unità archivistiche/unità documentali;
- registra il download di file;
- registra le richieste di esibizione dei documenti.

Le informazioni registrate sono riguardo le attività sono:

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

Torna al sommario

9.4 Soluzioni adottate in caso di anomalie

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

- **anomalie di sistema:** sono anomalie legate all'infrastruttura *hardware* e *middleware* che ospita Conserva;
- **anomalie applicative:** sono anomalie legate ai componenti applicativi, in particolare:
  - accesso degli utenti alle interfacce web;
  - richieste dell'utente pervenute attraverso interfacce web o chiamate a *web service,* quali ad esempio: trasferimento dei pacchetti di versamento e richiesta di pacchetti di distribuzione, ecc.;
  - modifiche dello stato degli oggetti durante le fasi di versamento e archiviazione operate automaticamente dal sistema di conservazione (versamento o rifiuto unità, generazione e notifica rapporti di versamento, ecc.);

- eccezioni causate da malfunzionamenti del software o dell'infrastruttura sottostante rilevabili dagli applicativi (indisponibilità dei database o di servizi esterni, esaurimento della memoria, errori di lettura/scrittura su *filesystem*, ecc.);
- verifiche del controllo di consistenza degli oggetti conservati: sia su richiesta, sia come risultato dell'operazione automatica a campione, sia come verifica in fase di esibizione.

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

Torna al sommario

9.4.1 Gestione segnalazione delle anomalie

Lo strumento per il tracciamento e la gestione degli incidenti è il sistema di *issue tracking* Jira, a sua volta collegato ad un'interfaccia web semplificata per le utenze del Titolare, detta *Customer Portal*.
La segnalazione di un'anomalia può provenire:

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

Una volta notificata l'anomalia tramite il sistema di *Customer Portal*, questa deve essere formalmente registrata da parte del team di Conserva con l'apertura di una *issue* su Jira, collegata a quella di notifica, in cui deve essere specificato il tipo *Bug*, devono essere aggiunti i componenti *Sistema*, *Incidente* e, eventualmente, *Lesione SLA* (solo se l'anomalia riscontrata può comportare una potenziale lesione dei livelli del servizio stabiliti). Se possibile vanno specificati anche il/i, Titolare (*Customer*) su cui si riflette l'incidente e l'ambiente (*Environment*) coinvolto (componente software e sua versione).
Se la segnalazione dell'anomalia è effettuata da personale CINECA, la procedura di registrazione appena specificata è eseguita contestualmente all'apertura della *issue* di segnalazione su Jira.
Una volta avvenuta la registrazione l'incidente deve essere trattato.

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

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

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

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

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

Torna al sommario

Manuale di Conservazione

Allegato 1 – Modello accordo di versamento

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**	**01/01/2014**	**P. Vandelli**	**Titolari dell'oggetto di conservazione, Personale Cineca**

STATO/STORIA DELLE REVISIONI

Versione	Data	Paragrafo rev.	Oggetto dalla revisione	Autore/i principale della revisione	Altri contributi	Validato
1.5	16/10/2023	esempio modello accordo di versamento Intero documento	Aggiornato modello Refusi	M. Mingrone	-	A. De Angelis
1.4	26/10/2022	Intestazione	Modificato ente certificatore e relativo logo	M. Mingrone	-	M.Valente
1.3	29/11/2021	Intero Doc.	Modello Accordo, sostituto in tutto il documento "Produttore" con "Titolare"	M. Mingrone N. Carofiglio	-	M.Valente

1.2	24/06/2016		Revisione	Laura Nisi	P. Vandelli	P. Vandelli
1.1	22/04/2016		Revisione a seguito delle osservazioni dello Studio Lisi	Laura Nisi	P. Vandelli	P. Vandelli
1.0	01/12/2015		Emissione	Laura Nisi	P. Vandelli	P. Vandelli

Descrizione Modello accordo di versamento

L'accordo di versamento è un documento Word strutturato con delle property da precompilare e che si trovano in File/Informazioni/Proprietà.

L'accordo di versamento è un modello al quale corrisponde un determinato codice sulla base della tipologia di oggetto da conservare. Gli accordi di versamento stipulati con il Titolare dell'oggetto di conservazione[1] sono delle istanze del modello prestabilito a monte.

Il frontespizio deve essere compilato con:

- **logo** del Titolare e del Conservatore;
- **denominazione** del Titolare e del Conservatore;
- **nome** e **cognome** del Responsabile della Conservazione e del Responsabile del Servizio di Conservazione o del Responsabile della funzione archivistica;
- **oggetto** dell'accordo: l'oggetto dell'accordo viene costruito da parti fisse e parti variabili (indicate tra parentesi quadre in corsivo): Conservazione de *[nome della tipologia o delle tipologie da conservare]* archiviati in fascicolo *[descrizione del fascicolo]* prodotti da *[denominazione del sistema produttore]* e inviati in conservazione da *[denominazione del sistema mittente]*'.

Sia l'indicazione di appartenenza ad un fascicolo che la presenza di un sistema produttore sono opzionali.

ESEMPIO: Conservazione [*dei verbali di esame elettronici]* archiviati in fascicolo [di *studente]* prodotti da [*Esse3]* ed *inviati* in conservazione da *[Titulus].*

- **codice accordo**: composto da [codice della tipologia] + [.TTS]+ [.codIPA] / [codice Ente]
  - il codice della tipologia è determinato dal conservatore;
  - [.TTS] spesso è presente se la tipologia proviene da Titulus;
  - [.codIPA] è presente se il Titolare è una pubblica amministrazione.
  - [codice Ente] è presente se il Titolare NON è una pubblica amministrazione

ESEMPIO: codice accordo dei verbali di esame dell'Università XXXX che arrivano da Titulus VERB.ESAMI.TTS.XXXX. Il modello dell'accordo da cui deriva l'accordo con il Titolare nel caso sia un'Università ha codice VERB.ESAMI.TTS.UNIV

- **versione accordo**: è composta da tre coppie di numeri. La prima riguarda la struttura del modello dell'Accordo, la seconda riguarda le modifiche effettuate dell'istanza del modello nel corso del tempo

[1] Di seguito Titolare

per ciascuna tipologia (queste versioni sono riportate nella parte *Versioni precedenti dell'accordo*, nella quale viene riportata la data e il codice di definizione del modello), la terza coppia riguarda la versione dell'istanza del modello concordata con il Titolare. Le versioni dell'istanza sono riportate nella parte *Storia del documento*, nella quale viene riportata la data e il codice di definizione dell'istanza.

ESEMPIO: l'accordo di versamento dei verbali di esame che arrivano da Titulus dell'università di XXXX ha versione 01.02.01 perché è la prima versione pattuita con l'Università XXXX, derivata dalla seconda versione del modello.

- **data** dell'accordo: deve essere la stessa della relativa versione dell'accordo presente nella *Storia del documento*;
- **stato** di *bozza* dell'accordo è presente fino all'approvazione della versione da entrambe le parti; in seguito alla approvazione lo stato diventa *definitivo*;
- codici di possibili **allegati** seguono la stessa regola del codice accordo con l'aggiunta di [.A*n*] dove per *n* si intende il numero progressivo dell'allegato**.** Se cambia la versione dell'allegato, non cambia la versione dell'accordo a cui è allegato e quindi nel quale viene citato.

ESEMPIO: il codice del primo allegato dell'accordo di versamento dei verbali di esame che arrivano da Titulus dell'Università XXXX è VERB.ESAMI.XXXX.A1. Da notare che [.TTS] non c'è in quanto il contenuto dell'allegato è indipendente dal sistema mittente;

- l'accordo può esser firmato con firma autografa, digitale o elettronica. Si preferisce che alla definizione dell'accordo tra le parti sia il Conservatore a firmare digitalmente e poi spedire al Titolare l'accordo per la controfirma sempre con firma digitale.

Di seguito viene riportato il modello di accordo di versamento sulla base del quale viene predisposto ogni singolo accordo di versamento sottoscritto da Titolare e Conservatore.

Esempio Modello accordo di versamento

[Logo Titolare]	CINECA

ACCORDO DI VERSAMENTO

TRA

TITOLARE DELL'OGGETTO DI CONSERVAZIONE	CONSERVATORE
[NOME DEL TITOLARE]	**CINECA CONSORZIO INTERUNIVERSITARIO**
nella figura del RESPONSABILE DELLA CONSERVAZIONE	nella figura della RESPONSABILE DELLA FUNZIONE ARCHIVISTICA
[Nome cognome del RdC]	**[Nome cognome del RSERV o RARCH]**

OGGETTO DELL'ACCORDO
CONSERVAZIONE [TIPOLOGIA OGGETTO INFORMATIVO]

CODICE ACCORDO	VERSIONE	DATA	STATO (BOZZA/DEFINITIVO)
[CodTipologia].[CodIPA]	**01.00.00**	**GG/MM/AAAA**	**BOZZA**

MODALITÀ DI SOTTOCRIZIONE DELL'ACCORDO		
[ ] Firma autografa	[x] Firma digitale	[ ] Firma elettronica

VERSIONI PRECEDENTI DELL'ACCORDO (versione, data, tipo di intervento)		
01.00	GG/MM/AAAA	Versione standard redatta da CINECA

STORIA DEL DOCUMENTO (versione, data, tipo intervento)		
01.00.01	GG/MM/AAAA	Versione approvata dalle parti

PREMESSA	
[premesse]	
INFORMAZIONI GENERALI	
Rappresentanti Conservatore	Per tutti i profili professionali inerenti al servizio di conservazione si può far riferimento al manuale di conservazione del conservatore Cineca.
Comunità di riferimento	[Categorie di riferimento per l'accesso]
Sistemi coinvolti	[Elenco dei sistemi coinvolti nella produzione della documentazione] Conserva – sistema di conservazione
DESCRIZIONE DEL PACCHETTO DI VERSAMENTO	
Tipologia e descrizione della struttura dell'oggetto informativo	[Descrizione della tipologia documentaria dal punto di vista giuridico e diplomatistico]
Generazione dell'oggetto informativo	[Descrizione dell'intero processo di generazione dell'oggetto informativo]
Informazione sulla rappresentazione	[Descrizione sia dal punto di vista semantico che strutturale dell'oggetto informativo]
Informazioni sulla conservazione	[Descrizione del set di metadati finalizzato alla descrizione degli oggetti informativi da conservare]
Informazioni descrittive	[Descrizione delle chiave di ricerca tramite le quali è possibile al Responsabile della conservazione e ai suoi delegati trovare l'oggetto informativo di interesse]
Informazioni sull'impacchettamento	[Informazioni su come vengano impacchettati gli oggetti informativi da conservare]
Classi di oggetti e istanze	[Descrizione delle classi di oggetti previste e delle relative istanze].
TRASFERIMENTO	
Protocolli di versamento	[Descrizione del protocollo di versamento utilizzato]
Criteri di formazione del Pacchetto di Versamento (SIP)	[Descrizione della formazione del pacchetto di versamento]

Descrizione del processo di trasferimento	[Descrizione di tutte le procedure finalizzate al completo passaggio di custodia]
VERSAMENTO	
Procedura di validazione	[Descrizione delle procedure di validazione standard]
Controlli aggiuntivi	[Descrizione dei controlli aggiunti in base alla tipologia dell'oggetto da conservare o di esigenze del Titolare]
Rapporto di versamento	[Descrizione del processo di formazione e consegna del Rapporto di Versamento]
CONSERVAZIONE	
Criteri e modalità di formazione del Pacchetto di Archiviazione	[Descrizione delle modalità di formazione del Pacchetto di Archiviazione]
Criteri e tempistiche di chiusura del Pacchetto di Archiviazione	[Descrizione della modalità di chiusura del Pacchetto di Archiviazione]
Tempi di conservazione	[Descrizione delle modalità e dei tempi di selezione e scarto]
Eventuali accordi per la selezione	[Descrizione di eventuali accordi per la selezione]
Attività di monitoraggio periodico	[Periodicità del monitoraggio degli oggetti conservati]
ESIBIZIONE	
Consultazione da interfaccia	[Descrizione della modalità di presentazione dei risultati].
Modalità di esibizione	[Descrizione delle caratteristiche del pacchetto di distribuzione].

[data topica], [data cronica]

[Nome del Titolare]
Il r*esponsabile della conservazione*
[Nome cognome RdC]

CINECA Consorzio Interuniversitario
La r*esponsabile della funzione archivistica*
[nome e cognome RARCH o RSERV]

Manuale di Conservazione

Allegato 2 – Pacchetto di versamento

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	**X**	**01/01/2014**	**P. Vandelli**	**Personale Cineca e Kion, Studio Legale Lisi AGID**
Ad uso interno				
Di dominio pubblico				

STATO/STORIA DELLE REVISIONI

Versione	Data	Paragrafo revisionato	Oggetto dalla revisione	Autore/i principale della revisione	Altri contributi	Validato
1.3	08/04/2024	Intero documento		Alessandro De Angelis	Mariagrazia Mingrone Nicola Carofiglio	Alessandro De Angelis
1.2	27/09/2023	Intestazione Intero documento	Aggiornato logo Cineca Modificato certificatore ed aggiornato il relativo logo	Mariagrazia Mingrone	Nicola Carofiglio	Alessandro De Angelis

			Aggiornata la descrizione del IPdV e inseriti i relativi xsd sulla base della versione 2.0 dell'IPdV			
1.1	22/04/2016		Revisione a seguito delle osservazioni dello Studio Lisi	Laura Federica Nisi		Paolo Vandelli
1.0	01/12/2015			Laura Federica Nisi	Francesca Merighi Alessandro De Angelis Paolo Vandelli	Paolo Vandelli

Sommario

1 Allegato 2 – Descrizione della struttura del pacchetto di versamento

In ottemperanza all'allegato 5 delle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici, le unità vengono descritte nell'indice del pacchetto attraverso i metadati indicati nell'allegato stesso.

Oltre ai metadati delineanti dalla normativa si è ritenuto opportuno corredare l'indice del pacchetto di versamento con metadati integrativi trattati dal sistema di gestione documentale e utili al perfezionamento della ricerca delle unità nel sistema di conservazione.

Nel caso in cui il sistema produttore del pacchetto di versamento non fosse un sistema di gestione documentale potrebbero non essere presenti i sopracitati metadati integrativi.

L'invio al sistema di conservazione Conserva può avvenire tramite due modalità:

- Tramite l'uso di web services;
- Tramite interfaccia web in Conserva.

Per il dettaglio dei metodi di trasmissione a Conserva dei pacchetti di Versamento si rimanda al relativo allegato al Manuale di Conservazione "*Mezzi di trasmissione*".

1.1 Struttura pacchetto di versamento

Di seguito si riporta la struttura prevista per la trasmissione del pacchetto di versamento a Conserva.

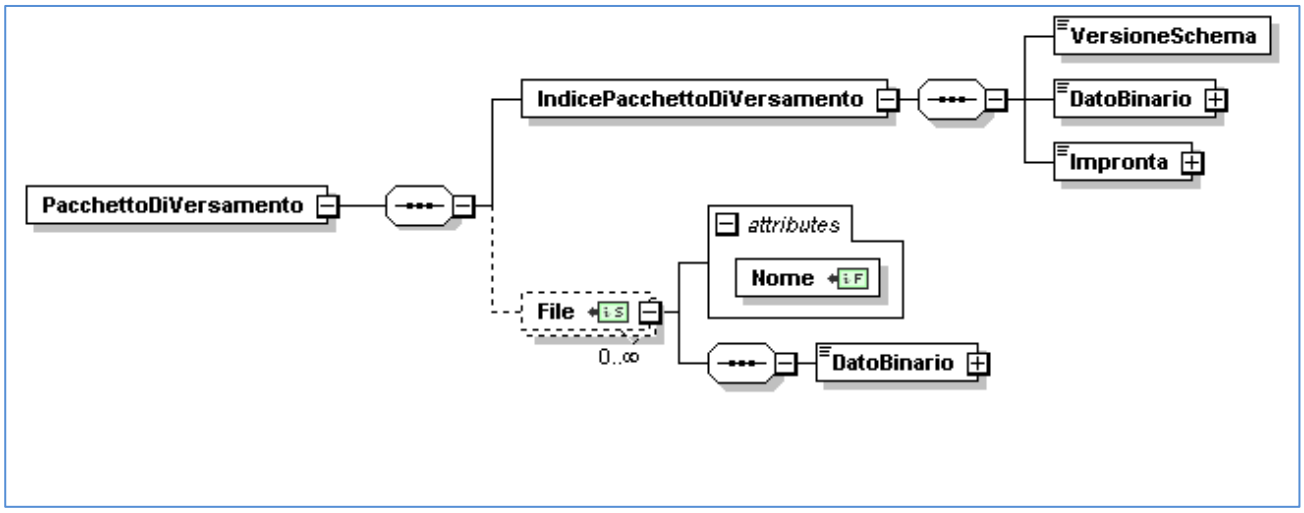


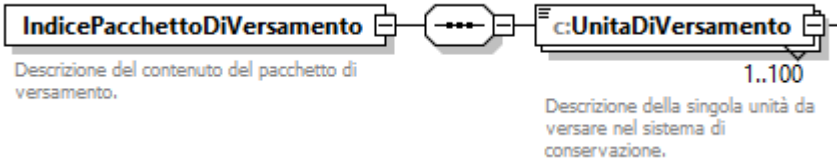
Figura 1 - Pacchetto di versamento

La struttura del *PacchettoDiVersamento*, trasmessa a Conserva è costituita da:

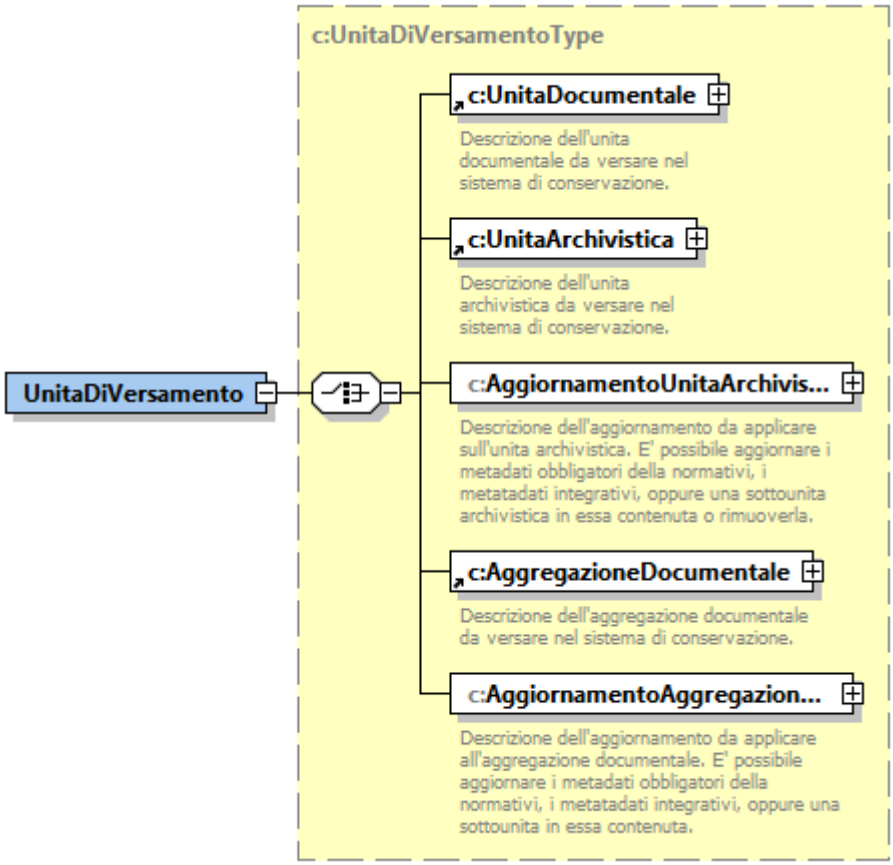
- *IndicePacchettoDiVersamento*: elemento che contiene i metadati descrittivi degli oggetti digitali trasmessi in conservazione;
- *Impronta dell' IndicePacchettoDiVersamento:* sequenza alfanumerica ottenuta applicando un particolare algoritmo di calcolo alla sequenza di bit che formano il file;
- *File*: elemento ricorsivo che contiene fisicamente i file relativi ai documenti (unità documentali) inviati in conservazione.

Il pacchetto di versamento può essere trasferito in modalità compressa [zip da massimo 20MB, se il pacchetto è di dimensioni maggiori è possibile inviare più file compressi] o non compressa.

1.2 IndicePacchettoDiVersamento

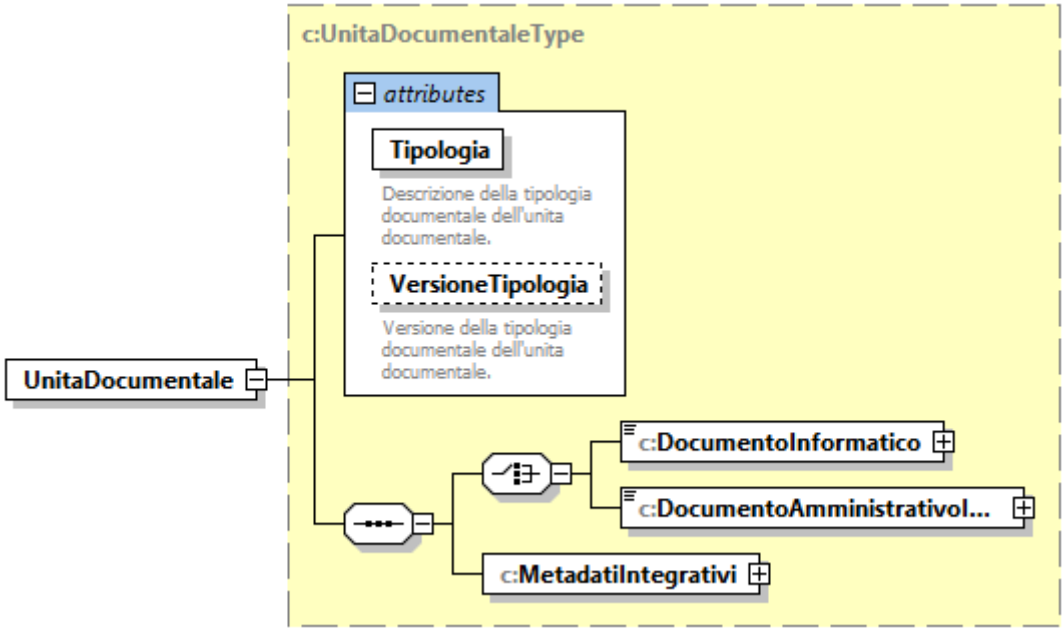
elemento ***IndicePacchettoDiVersamento***	
Descrizione	L'indice del pacchetto di versamento contiene l'insieme dei metadati delle unità inviate in conservazione attraverso il pacchetto medesimo.
Diagramma	
Elementi	Informazione
	c:UnitaDiVersamento: si veda elemento c:UnitaDiVersamento

elemento c:***UnitaDiVersamento***

Descrizione	L'unità di versamento rappresenta la singola unità versata.
Diagramma	

Elementi	Informazione
	c:UnitaDocumentale: si veda elemento UnitaDocumentale
	c:UnitaArchivistica: si veda elemento UnitaArchivistica
	c:AggiornamentoUnitaArchivistica: si veda elemento AggiornamentoUnitaArchivistica
	c:AggregazioneDocumentale: si veda elemento c:AggregazioneDocumentale
	c:AggiornamentoAggregazioneDocumentale: si veda elemento c:AggiornamentoAggregazioneDocumentale

elemento c:***UnitaDocumentale***

Descrizione	All'interno di un elemento UnitaDocumentale vengono riportati i metadati descrittivi di un documento trasmesso al sistema di conservazione. L'elemento può essere contenuto in un fascicolo (in tal caso sarà contenuto a sua volta in un elemento UnitaArchivistica o AggiornamentoUnitaArchivistica) o parte di una aggregazione documentale (in tal caso sarà contenuto a sua volta in un elemento AggregazioneDocumentale o Aggiornamento AggregazioneDocumentale); il documento può anche essere riportato direttamente all'interno dell'elemento UnitaDiVersamento.
Diagramma	

Attributi	Informazione	Valori ammessi	Tipo dato	Default
	Tipologia: codifica della tipologia di documento come concordato nell'accordo di versamento	Testo libero	Alfanumerico	-
	VersioneTipologia: versione della tipologia documentale. Se omesso Conserva assegna la versione citata nell'ultimo accordo di versamento sottoscritto fra Produttore e Conservatore	Testo libero	Alfanumerico	-

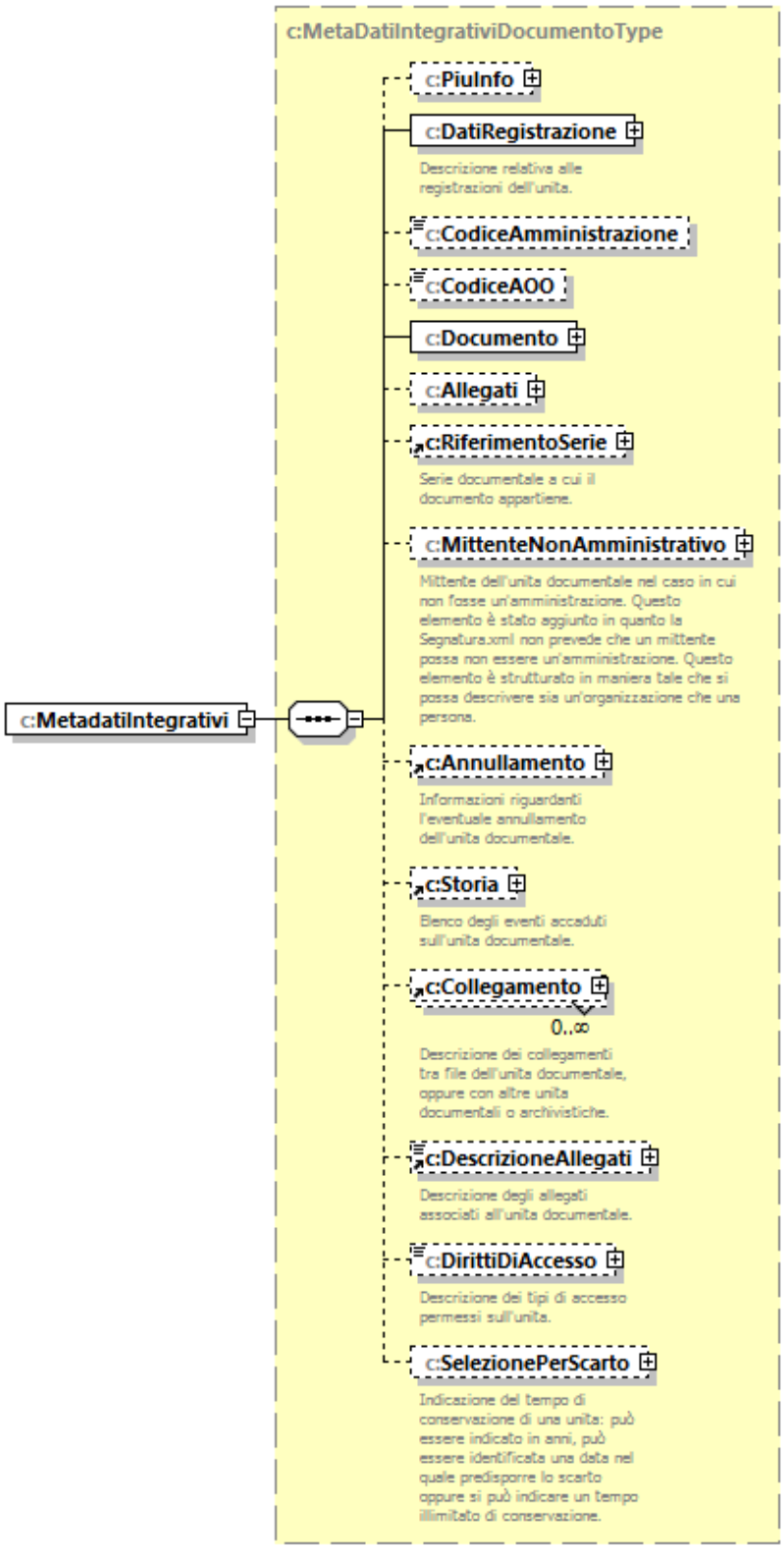
Elementi	Informazione
	c:DocumentoInformatico: si veda elemento c:DocumentoInformatico
	c:DocumentoAmministrativoInformatico: si veda **Errore. L'origine riferimento**

	non è stata trovata.
	c:MetatadiIntegrativi: si veda **Errore. L'origine riferimento non è stata trovata.**
Elementi sovraordinati	UnitaDiVersamento, SottoUnita, AggiornamentoSottoUnita

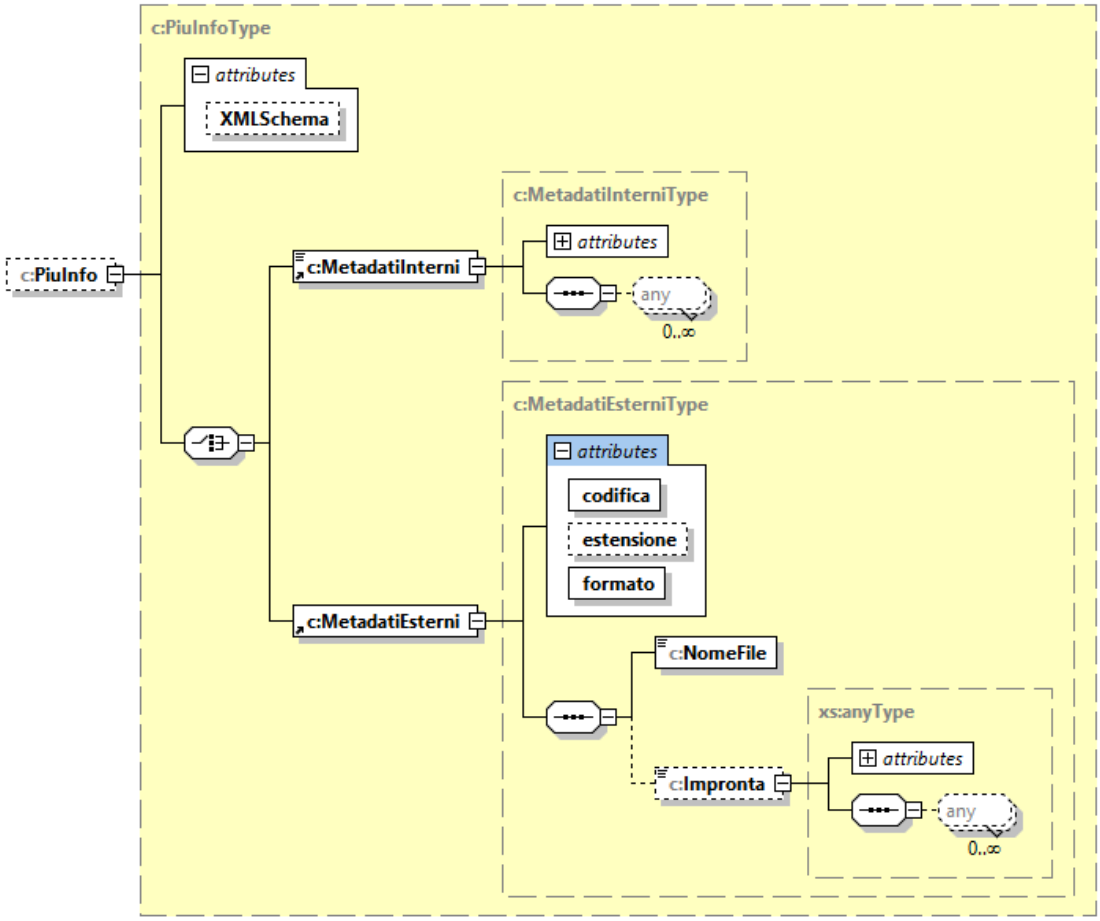
elemento ***c:DocumentoInformatico***	
Descrizione	Metadati documento informatico (vedi paragrafo '2. METADATI DEL DOCUMENTO INFORMATICO' dell'Allegato 5 al documento "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici").
Elementi	Informazione
	vedi paragrafo '2. METADATI DEL DOCUMENTO INFORMATICO' dell'Allegato 5 al documento "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici")
Elementi sovraordinati	UnitaDocumentale

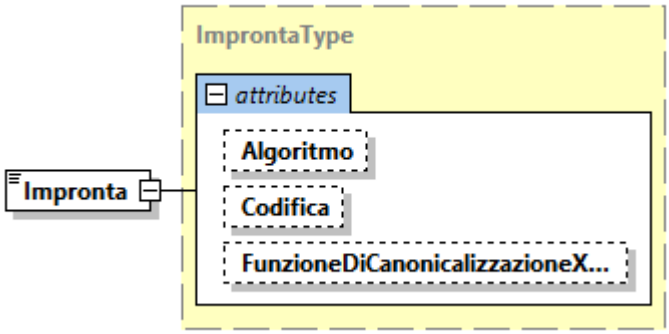
elemento ***c:DocumentoAmministrativoInformatico***	
Descrizione	Metadati documento informatico (vedi paragrafo '3. METADATI DEL DOCUMENTO AMMINISTRATIVO INFORMATICO' dell'Allegato 5 al documento "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici").
Elementi	Informazione
	vedi paragrafo '3. METADATI DEL DOCUMENTO AMMINISTRATIVO INFORMATICO' dell'Allegato 5 al documento "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici")
Elementi sovraordinati	UnitaDocumentale

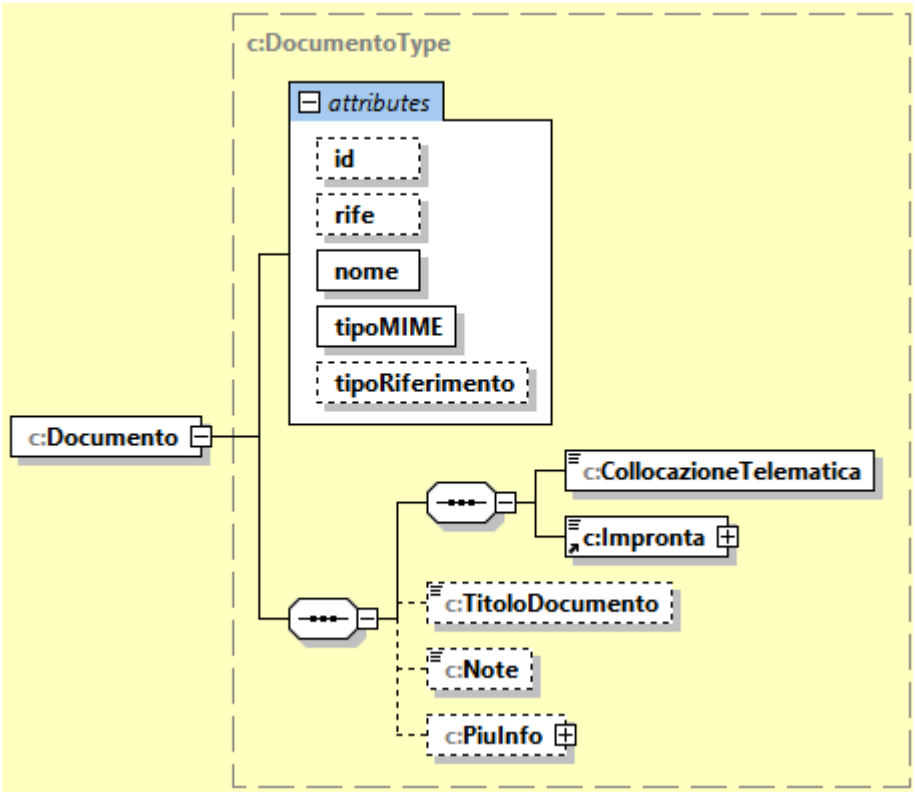
elemento ***c:MetadatiIntegrativi (Documento)***	
Descrizione	Metadati integrativi che consentono di estendere la descrizione del documento informatico.

Diagramma	
Elementi	**Informazione**

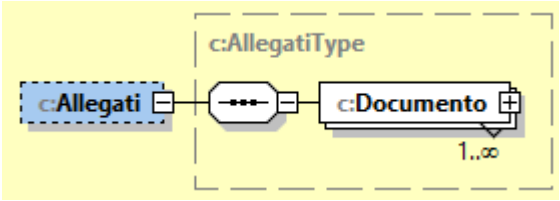
	c:PiuInfo: Informazioni aggiuntive sul documento. Per dettagli si veda elemento PiuInfo.
	c:DatiRegistrazione: Descrizione del tipo di registrazione. Per dettagli si veda elemento elemento c:DatiRegistrazione.
	c:CodiceAmministrazione: Identificativo univoco dell'amministrazione per il sistema che ha generato il documento (Stringa).
	c:CodiceAOO: Identificativo univoco dell'AOO per il sistema che ha generato il documento (Stringa).
	c:Documento: Elemento che descrive il file principale del documento.
	c:Allegati: contiene i dati telematici ed amministrativi di un destinatario per conoscenza del documento secondo la sintassi dell'elemento Segnatura.
	c:RiferimentoSerie: serie documentale a cui il documento appartiene (facoltativo, normalmente le serie documentali vengono create automaticamente da Conserva leggendo metadati relativi alla repertoriazione o in base alla tipologia). Per dettagli si veda elemento RiferimentoSerie
	c:MittenteNonAmministrativo: Mittente dell'unità documentale nel caso in cui non fosse un'amministrazione. Si veda elemento c:MittenteNonAmministrativo
	c:Annullamento: Informazioni riguardanti l'eventuale annullamento del documento. Per dettagli si veda elemento Annullamento
	c:Storia: si veda elemento Storia.
	c:Collegamento: si veda elemento Collegamento.
	c:DescrizioneAllegati: si veda elemento DescrizioneAllegati.
	c:DirittiDiAccesso: si veda elemento c:DirittiDiAccesso.
	c:SelezionePerScarto: si veda elemento c:SelezionePerScarto.
Elementi sovraordinati	DocumentoInformatico, DocumentoAmministrativoInformatico

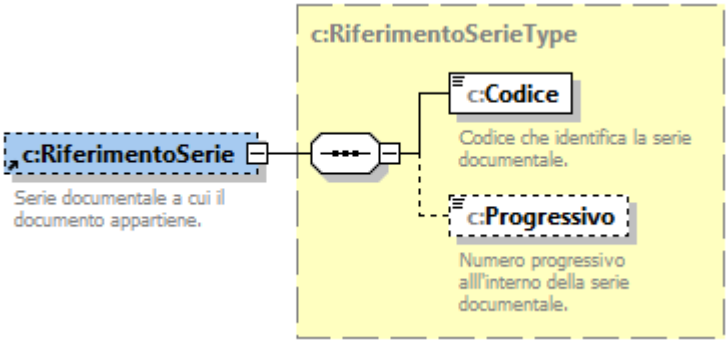
<table>
<tr><td colspan="5">elemento c:PiuInfo</td></tr>
<tr><td>Descrizione</td><td colspan="4">Elemento in cui inserire eventuali informazioni aggiuntive che riguardano il documento; queste informazioni possono essere presenti su un file esterno che deve essere collegato tramite l’elemento NomeFile e su cui va calcolata l’impronta o possono essere inserite all’interno dell’indice nell’elemento c:MetadatiInterni.</td></tr>
<tr><td>Diagramma</td><td colspan="4"> 
</td></tr>
<tr><td>Attributi</td><td>Informazione</td><td>Valori ammessi</td><td>Tipo dato</td><td>Default</td></tr>
<tr><td></td><td>XMLSchema: schema per validare l’elemento MetadatiInterni</td><td>Testo libero</td><td>Alfanumerico</td><td>-</td></tr>
<tr><td>Elementi</td><td colspan="4">c:MetadatiInterni: Metadati aggiuntivi del documento descritti all’interno dello stesso indice seguendo lo schema dell’attributo XMLSchema
c:MetadatiEsterni: Metadati aggiuntivi del documento descritti in un file esterno riconosciuto dall’elemento NomeFile</td></tr>
<tr><td>Elementi sovraordinati</td><td colspan="4">MetadatiIntegrativi (Documento), MetadatiIntegrativiFascicolo, MetadatiIntegrativiAggregazioneDocumentale</td></tr>
</table>

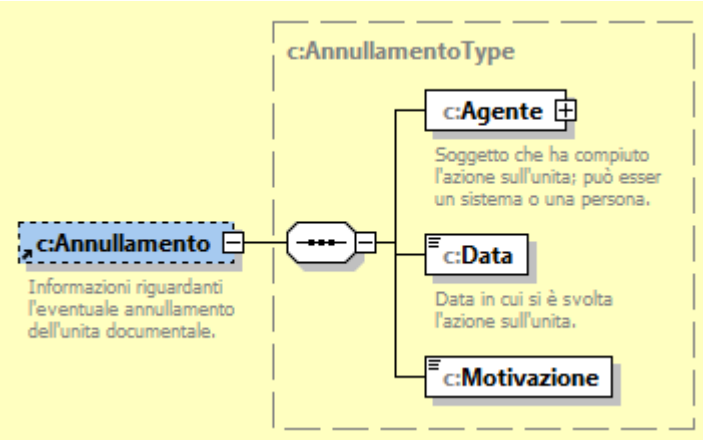
elemento ***c:Impronta***				
Descrizione	Impronta del file.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	Algoritmo: tipologia di algoritmo utilizzato per il calcolo dell'impronta. Al momento prevediamo solo l'impronta SHA256.	SHA256	Tipo algoritmo	-
	Codifica: encoding dell'impronta. Fisso a base64.	base64	encoding	-
	FunzioneDiCanonicalizzazioneXML: funzione di canonicalizzazione per i file xml		String	-
Elementi sovraordinati	Documento			

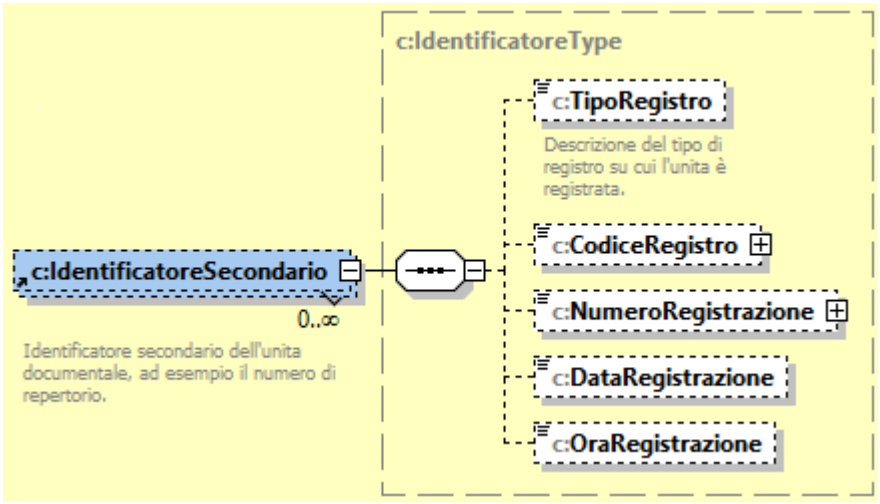
<table>
<tr><td colspan="3">elemento c:Documento</td></tr>
<tr><td>Descrizione</td><td colspan="2">Elemento in cui inserire le informazioni riguardanti il file principale del documento.</td></tr>
<tr><td>Diagramma</td><td colspan="2"> 
</td></tr>
<tr><td>Attributi</td><td colspan="2"><table>
<tr><th>Informazione</th><th>Valori ammessi</th><th>Tipo dato</th><th>Default</th></tr>
<tr><td>id: id del file (facoltativo)</td><td>Identificatore univoco</td><td>ID</td><td>-</td></tr>
<tr><td>rife: riferimento per l’id del file (facoltativo)</td><td>Riferimento</td><td>IDREF</td><td>-</td></tr>
<tr><td>nome: nome del file</td><td>Testo libero</td><td>anySimpleType</td><td>-</td></tr>
<tr><td>tipoMIME: content type del file</td><td>Testo libero</td><td>anySimpleType</td><td>-</td></tr>
<tr><td>tipoRiferimento:</td><td>Testo libero</td><td>String</td><td>telematico (valori ammessi MIME, telematico, cartaceo)</td></tr>
</table></td></tr>
<tr><td>Elementi</td><td colspan="2">c:CollocazioneTelematica: Posizione all’interno del pacchetto di versamento del file (normalmente i file sono nella stessa cartella dell’indice del pacchetto di versamento)
c:Impronta: Impronta del file. Per dettagli si veda elemento Impronta
c:TitoloDocumento: Descrizione del file (Stringa, facoltativo)
c:Note: Note che riguardano il file (Stringa, facoltativo)
c:PiuInfo: Informazioni aggiuntive sul documento. Per dettagli si veda elemento PiuInfo.</td></tr>
<tr><td>Elementi</td><td colspan="2">Allegati, MetadatiIntegrativi (Documento), MetadatiIntegrativiFascicolo,</td></tr>
</table>

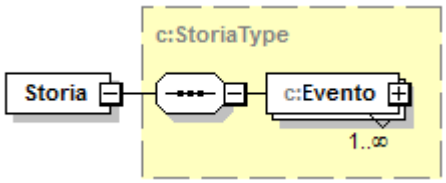
sovraordinati	MetadatiIntegrativiAggregazioneDocumentale

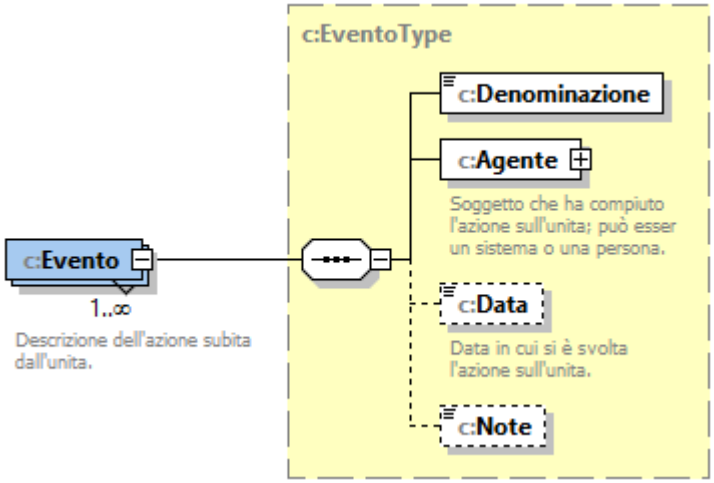
elemento ***c:Allegati***	
Descrizione	Elemento ripetibile in cui riportare eventuali allegati al documento principale.
Diagramma	
Attributi e elementi	**c:Documento:** elemento che descrive il singolo file. Per dettagli si veda elemento c:Documento
Elementi sovraordinati	MetadatiIntegrativi (Documento)

elemento ***c:RiferimentoSerie***	
Descrizione	Elemento in cui specificare informazioni che riguardano la serie a cui appartiene il documento.
Diagramma	
Elementi	**c:Codice:** Codice serie (max 100 caratteri). **c:Progressivo**: Numero identificativo del documento all'interno della serie.
Elementi sovraordinati	MetadatiIntegrativi (Documento)

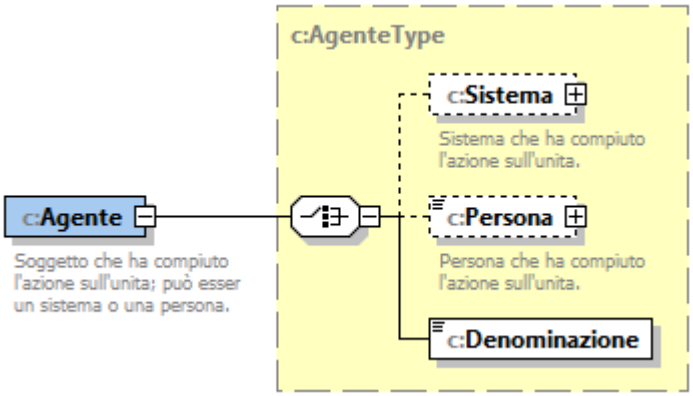
elemento ***c:Annullamento***	
Descrizione	Informazioni riguardanti l'eventuale annullamento del documento.
Diagramma	
Elementi	**c:Agente*:*** si veda elemento c:Agente **c:Data:** Indica la data dell'annullamento espressa secondo il formato ISO 8601 esteso (aaaa-mm-gg) **c:Motivazione:** Descrizione motivazione dell'annullamento (String)
Elementi sovraordinati	MetadatiIntegrativi (Documento)

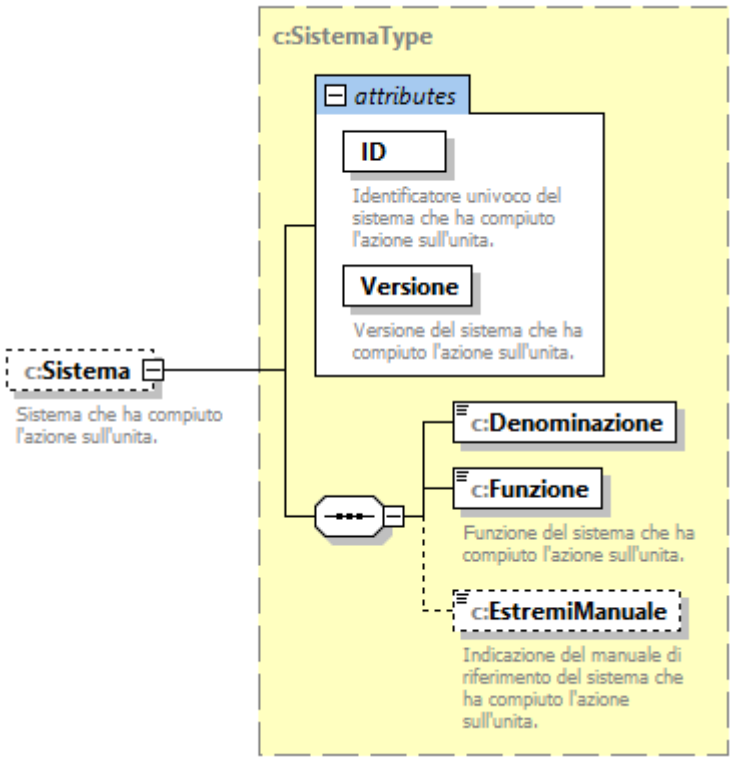
elemento ***IdentificatoreSecondario***	
Descrizione	Elemento ripetibile in cui riportare eventuali ulteriori elementi che identificano il documento, secondari rispetto a quelli principali inseriti DocumentoInformatico, DocumentoAmministrativoInformatico e AggregazioneDocumentaliInformatiche.
Diagramma	
Elementi	**c:TipoRegistro:** Descrizione del tipo di registro su cui l'unità è registrata.
	c:CodiceRegistro: Contiene il codice identificativo del registro di protocollo, degli altri registri di cui all'articolo 53, comma 5, del Testo unico, dei repertori e degli archivi gestiti nell'ambito del sistema unico di gestione documentale e protocollo informatico. È attribuito dalla amministrazione al registro nell'ambito della AOO in cui è stato definito. Il codice è codificato mediante un sottoinsieme dei caratteri previsti dalla specifica US-ASCII a 8 bit; il codice è composto da lettere maiuscole ([A-Z]), lettere minuscole ([a-z]), caratteri numerici ([0-9]) e dai caratteri "-" e "_" e ".". Deve avere una lunghezza non superiore a 16 caratteri.
	c:NumeroRegistrazione: Contiene il numero della registrazione di protocollo formato da almeno sette cifre decimali, con giustificazione mediante zeri (es. il numero 1 deve essere codificato come 0000001).
	c:DataRegistrazione: Indica la data della registrazione di protocollo espressa secondo il formato ISO 8601 esteso (aaaa-mm-gg).
	c:OraRegistrazione: Indica l'ora della registrazione espressa secondo il formato "hh:mm:ss".
Elementi sovraordinati	DatiRegistrazione

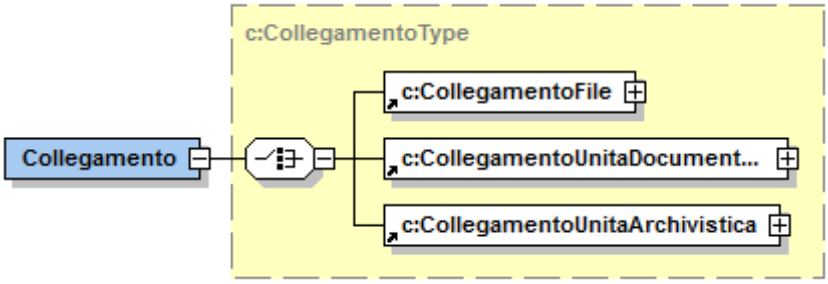
elemento ***Storia***	
Descrizione	Elemento in cui riportare la storia dei principali eventi manifestatisi sul documento informatico, documento amministrativo informatico o fascicolo. Questi eventi vengono trasmessi dal Produttore al Conservatore.
Diagramma	
Elementi	**Informazione**
	c:Evento: si veda elemento c:Evento
Elementi sovraordinati	MetadatiIntegrativi (Documento)

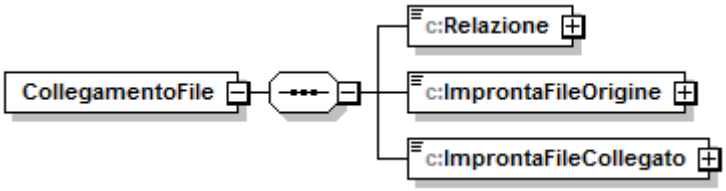
elemento c:***Evento***	
Descrizione	Elemento in cui viene rappresentato il singolo evento storicizzato dal Produttore e manifestatosi su un documento o un fascicolo (unità). Ogni istanza rappresenta un evento manifestato sull'unità.
Diagramma	
Elementi	**Informazione**
	c:Denominazione: descrizione sintetica dell'evento registrato (campo testo libero)
	c:Agente: si veda elemento c:Agente
	c:Data: data e ora in cui si è manifestato l'evento secondo lo standard ISO 8601
	c:Note: Contiene delle note che descrivono in maniera più dettagliata il tipo di evento. Al suo interno non è consentito l'inserimento di un testo altrimenti strutturato (es. un frammento di codice XML).
Elementi sovraordinati	Storia

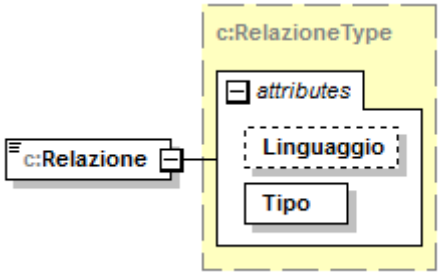
elemento c:***Agente***

Descrizione	Soggetto che ha compiuto l'azione sull'unità; può esser un sistema o una persona.
Diagramma	
Elementi	**Informazione**
	c:Sistema: sistema che ha compiuto l'azione sull'unità. Si veda elemento c:Sistema
	c:Persona: riporta i dati della persona fisica che ha compiuto l'azione sull'unità, secondo la sintassi dell'elemento Segnatura:Persona
	c:Denominazione: descrizione del sistema/elemento che scatena l'evento. Campo testuale, secondo la sintassi dell'omonimo elemento in Segnatura.
Elementi sovraordinati	c:Evento

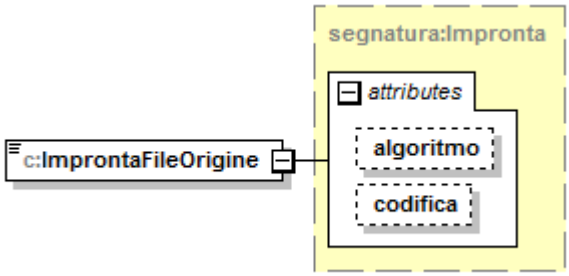
<table>
<tr><td colspan="5">elemento c:Sistema</td></tr>
<tr><td>Descrizione</td><td colspan="4">Sistema che ha compiuto l’azione sull’unità.</td></tr>
<tr><td>Diagramma</td><td colspan="4"> 
</td></tr>
<tr><td>Attributi</td><td>Informazione</td><td>Valori ammessi</td><td>Tipo dato</td><td>Default</td></tr>
<tr><td></td><td>ID: identificatore univoco del sistema che ha compiuto l'azione sull'unità.</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td></td><td>Versione: versione del sistema che ha compiuto l’azione sull’unità.</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td>Elementi</td><td colspan="4">Informazione</td></tr>
<tr><td></td><td colspan="4">c:Denominazione: denominazione del sistema produttore che ha compiuto l’azione</td></tr>
<tr><td></td><td colspan="4">c:Funzione: Nome della funzione che ha generato la storicizzazione dell’azione</td></tr>
<tr><td></td><td colspan="4">c:EstremiManuale: Indicazione del manuale di riferimento del sistema che ha compiuto l'azione sull'unità.</td></tr>
<tr><td>Elementi sovraordinati</td><td colspan="4">Agente</td></tr>
</table>

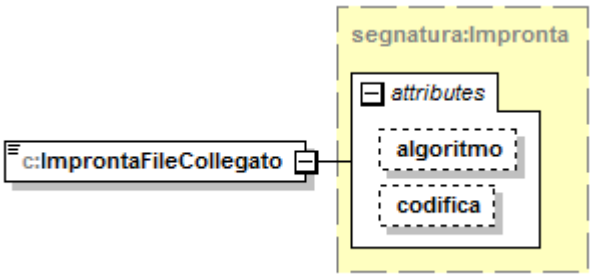
elemento **Collegamento**	
Descrizione	Descrizione dei collegamenti tra file dell'unità documentale, oppure con altre unità documentali o archivistiche.
Diagramma	
Elementi	**Informazione**
	c:CollegamentoFile: si veda elemento CollegamentoFile
	c:CollegamentoUnitaDocumentale: si veda elemento CollegamentoUnitaDocumentale
	c:CollegamentoUnitaArchivistica: si veda elemento CollegamentoUnitaArchivistica
Elementi sovraordinati	MetadatiIntegrativi (Documento), MetadatiIntegrativiFascicolo

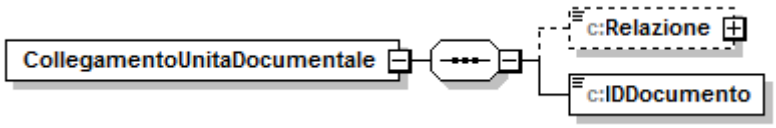
elemento ***CollegamentoFile***	
Descrizione	Descrizione del collegamento tra i file dell'unità documentale. Ad esempio, versioni differenti dello stesso file: - per formato: ad esempio versione XML e versione PDF; - per contenuto: ad esempio versione integrale e versione con omissis.
Diagramma	
Elementi	**Informazione**
	c:Relazione: si veda elemento c:Relazione
	c:ImprontaFileOrigine: si veda elemento c:ImprontaFileOrigine
	c:ImprontaFileCollegato: si veda elemento c:ImprontaFileCollegato
Elementi sovraordinati	Collegamento

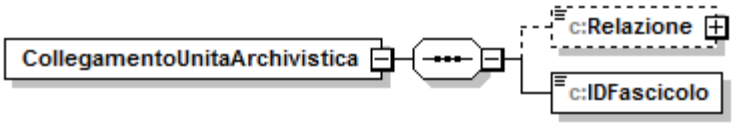
<table>
<tr><td colspan="6">elemento c:Relazione</td></tr>
<tr><td>Descrizione</td><td colspan="5">Descrizione della relazione che intercorre tra il file principale ed il file derivato messi in relazione fra di loro. Esempi di relazione:
- Fra file della medesima unità documentale:
○ versione XML
○ versione PDF
○ versione PDF/A
○ versione integrale
○ versione con omissis
- Fra unità (documentali o archivistiche)
○ Collegamento
- Fra unità documentali
○ revocato da
○ sostituito da
○ dichiarazione di conformità</td></tr>
<tr><td>Diagramma</td><td colspan="5"> 
</td></tr>
<tr><td rowspan="3">Attributi</td><td>Informazione</td><td>Valori ammessi</td><td>Tipo dato</td><td>Default</td></tr>
<tr><td>Linguaggio: lingua in cui è descritto il tipo di relazione</td><td>Codifica ISO 639-1</td><td>alfanumerico</td><td>it</td></tr>
<tr><td>Tipo: elemento testuale che descrive il tipo di relazione</td><td>Stringa</td><td>Es: versione XML, versione PDF/A, versione PDF versione con omissis versione integrale, master editabile (es. file word) , dichiarazione di</td><td></td></tr>
</table>

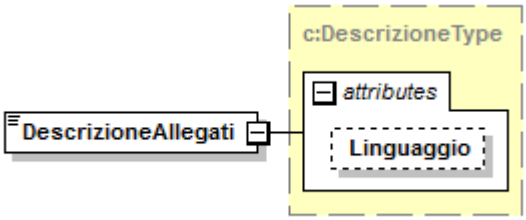
			conformità…	
Elementi sovraordinati	CollegamentoFile CollegamentoUnitaDocumentale CollegamentoUnitaArchivistica			

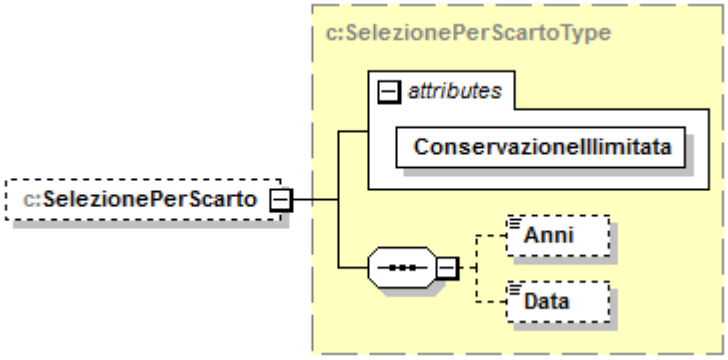
elemento c:***ImprontaFileOrigine***				
Descrizione	Impronta del file a cui si riferisce il collegamento (master), secondo l'algoritmo indicato come attributo.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	algoritmo: tipologia di algoritmo utilizzato per il calcolo dell'impronta. Al momento le specifiche sulla segnatura di protocollo prevedono solo l'impronta SHA256.	SHA256	Tipo algoritmo	-
	codifica: encoding dell'impronta. Fisso a base64.	base64	encoding	-
Elementi sovraordinati	CollegamentoFile			

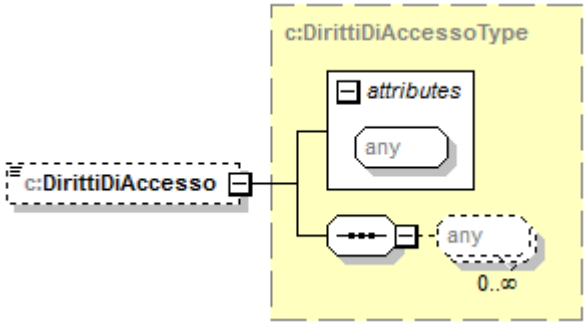
<table>
<tr><td colspan="5">elemento c:ImprontaFileCollegato</td></tr>
<tr><td>Descrizione</td><td colspan="4">Impronta del file da collegare (slave) al file principale (master) in base alla relazione descritta.</td></tr>
<tr><td>Diagramma</td><td colspan="4"> 
</td></tr>
<tr><td rowspan="3">Attributi</td><td>Informazione</td><td>Valori ammessi</td><td>Tipo dato</td><td>Default</td></tr>
<tr><td>algoritmo: tipologia di algoritmo utilizzato per il calcolo dell’impronta. Al momento utilizziamo l’impronta SHA256.</td><td>SHA256</td><td>Tipo algoritmo</td><td></td></tr>
<tr><td>codifica: encoding dell’impronta. Fisso a base64.</td><td>base64</td><td>encoding</td><td></td></tr>
<tr><td>Elementi sovraordinati</td><td colspan="4">CollegamentoFile</td></tr>
</table>

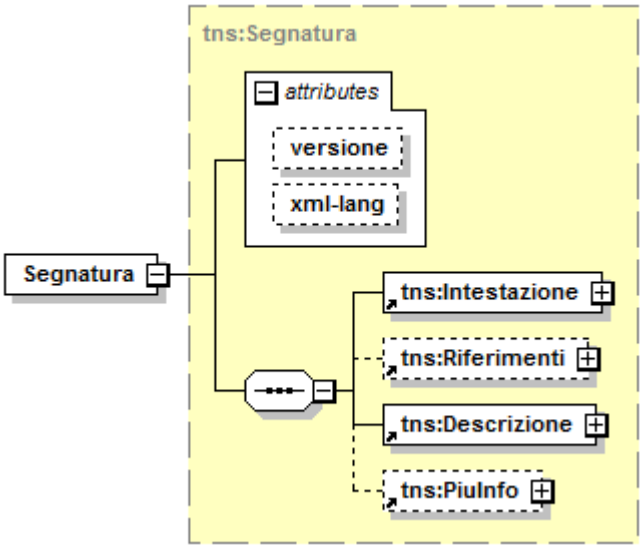
<table>
<tr><td colspan="2">elemento CollegamentoUnitaDocumentale</td></tr>
<tr><td>Descrizione</td><td>Descrive il collegamento dell’unità corrente con un’unità documentale, secondo una relazione definita.</td></tr>
<tr><td>Diagramma</td><td> 
</td></tr>
<tr><td rowspan="3">Elementi</td><td>Informazione</td></tr>
<tr><td>c:Relazione: si veda elemento c:Relazione.</td></tr>
<tr><td>c:IDDocumento: Identificativo univoco dell’unità documentale, nel sistema produttore.</td></tr>
<tr><td>Elementi sovraordinati</td><td>Collegamento</td></tr>
</table>

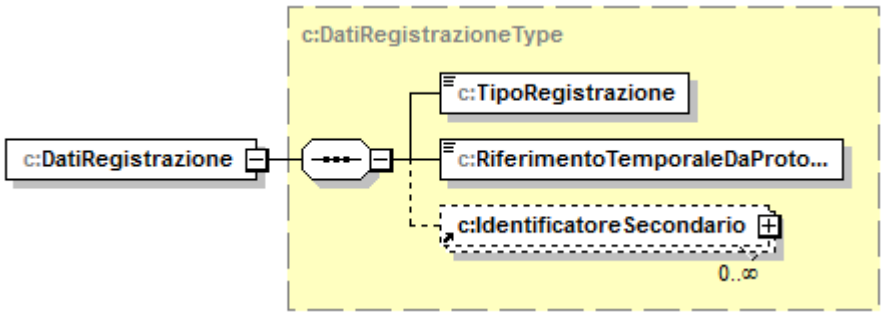
elemento ***CollegamentoUnitaArchivistica***	
Descrizione	Descrive il collegamento dell'unità corrente con un'unità archivistica, secondo una relazione definita.
Diagramma	
Elementi	**Informazione**
	c:Relazione: si veda elemento c:Relazione
	c:IDFascicolo: identificativo univoco del fascicolo, nel sistema produttore.
Elementi sovraordinati	Collegamento

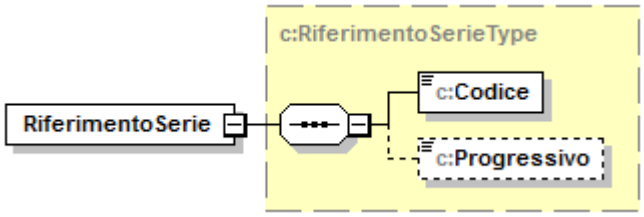
elemento ***DescrizioneAllegati***				
Descrizione	Descrizione sommaria degli allegati al documento. Se ad esempio il sistema mittente è Titulus, in questo elemento viene riportata la descrizione degli allegati, obbligatoria e non modificabile in Titulus.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	Linguaggio: lingua in cui è descritto il tipo di relazione	Codifica ISO 639-1	alfanumerico	**it**
Elementi sovraordinati	MetadatiIntegrativi (Documento)			

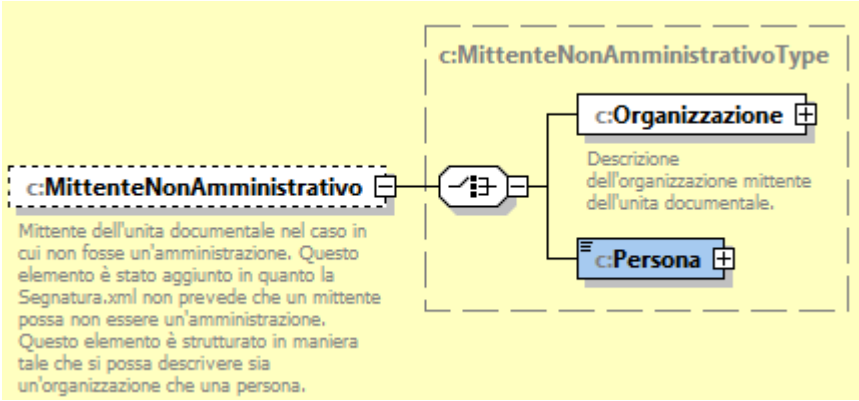
elemento c:***SelezionePerScarto***				
Descrizione	Indicazione del periodo oltre al quale verificare se procedere allo scarto dell'unità. L'unità può essere a conservazione perenne, oppure può essere soggetta a valutazione per lo scarto una volta decorso un certo periodo. Decorso il periodo di conservazione, l'unità viene evidenziata al Responsabile della conservazione per le valutazioni del caso e per attuare eventuali politiche di scarto. Se questo elemento non viene valorizzato, fa fede quanto definito nell'accordo di versamento, oppure nell'unità archivistica.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	ConservazioneIllimitata: indica che l'unità non è soggetta a scarto. Se 'true' non sarà necessario indicare un periodo per lo scarto.	true/false	boolean	-
Elementi	**Informazione**			
	Anni: numero di anni oltre i quali l'unità sarà valutata per lo scarto. Tipicamente la valutazione sarà effettuata al termine dell'anno di scadenza. Assume tipicamente i valori 1, 5, 10 20.			
	Data: data oltre la quale valutare se scartare questa unità. Questa opzione è stata inserita per comodità, anche se tipicamente si fa riferimento ad un periodo dello scarto espresso in anni e non con date esplicite.			
Elementi sovraordinati	MetadatiIntegrativi (Documento)			

elemento c:***DirittiDiAccesso***	
Descrizione	Descrizione dei tipi di accesso permessi sull'unità. Da definire.
Diagramma	
Elementi sovraordinati	MetadatiIntegrativi (Documento)

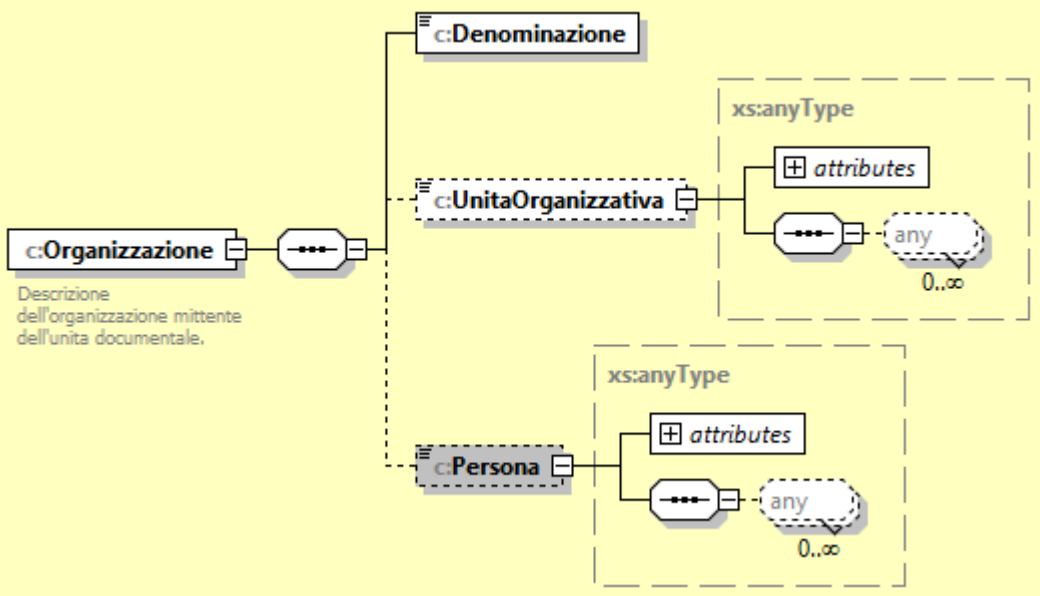
elemento ***Segnatura***	
Descrizione	I metadati della segnatura sono quelli definiti nell'allegato 6 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici.
Diagramma	
Elementi sovraordinati	DocumentoAmministrativoInformatico

elemento c:***DatiRegistrazione***	
Descrizione	Descrizione relativa alle registrazioni del documento amministrativo informatico. Tipicamente si fa riferimento ad un registro di protocollo e ad eventuali ulteriori repertoriazioni del documento.
Diagramma	
Elementi	**Informazione**
	c:TipoRegistrazione: nel caso di registrazione di protocollo riporta la tipologia di registrazione, quindi: “Arrivo”, “Partenza”, “Interno”, “Non protocollato”
	c:RiferimentoTemporaleDaProtocollo: Indicazione se il riferimento temporale opponibile a terzi ai fini della validità della firma digitale sia la registrazione di protocollo. Può assumere i valori ‘true’ o ‘false’
	c:IdentificatoreSecondario: si veda elemento IdentificatoreSecondario
Elementi sovraordinati	MetadatiIntegrativi (Documento)

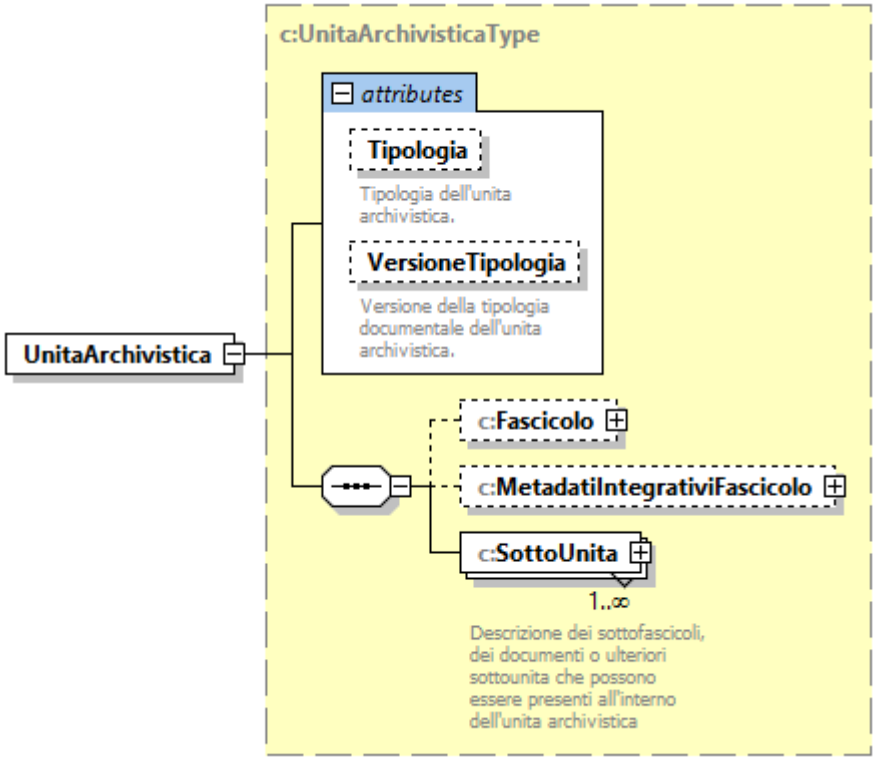
elemento ***RiferimentoSerie***	
Descrizione	Serie documentale a cui il documento appartiene. Si fa uso di questo elemento in vece dell'IdentificatoreSecondario, quando si vuole che il sistema di conservazione archivi in una serie automatica documenti omogenei non gestiti in tal senso dal sistema produttore. Inoltre, si può istruire Conserva perché operi controlli specifici su queste particolari serie (ad esempio nel caso di fatture attive, si può istruire Conserva ad impedire l'inoltro di pacchetti per i quali la sequenzialità della serie non sia garantita).
Diagramma	
Elementi	**Informazione**
	c:Codice: codice che identifica la serie documentale
	c:Progressivo: numero progressivo all'interno della serie documentale
Elementi sovraordinati	DocumentoAmministrativoInformatico / MetadatiIntegrativi

elemento c:***MittenteNonAmministrativo***	
Descrizione	Mittente dell'unità documentale nel caso in cui non fosse un'amministrazione. Questo elemento è stato aggiunto in quanto la vecchia Segnatura non prevedeva che un mittente potesse non essere un'amministrazione. Questo elemento è strutturato in maniera tale che si possa descrivere sia un'organizzazione che una persona. L'elemento viene tenuto nello schema per continuità con la versione precedente.
Diagramma	
Elementi	**Informazione**
	c:Organizzazione: si veda elemento c:Organizzazione
	c:Persona: riporta i dati della persona fisica (struttura libera)
Elementi sovraordinati	MetadatiIntegrativi (Documento)

elemento c:***Organizzazione***

Descrizione	Descrizione dell'organizzazione mittente dell'unità documentale.
Diagramma	
Elementi	**Informazione**
	c:Denominazione: riporta i dati dell'Organizzazione
	c:UnitaOrganizzativa: riporta i dati dell'Unità organizzativa (struttura libera)
	c:Persona: riporta i dati della persona fisica (struttura libera)
Elementi sovraordinati	MittenteNonAmministrativo

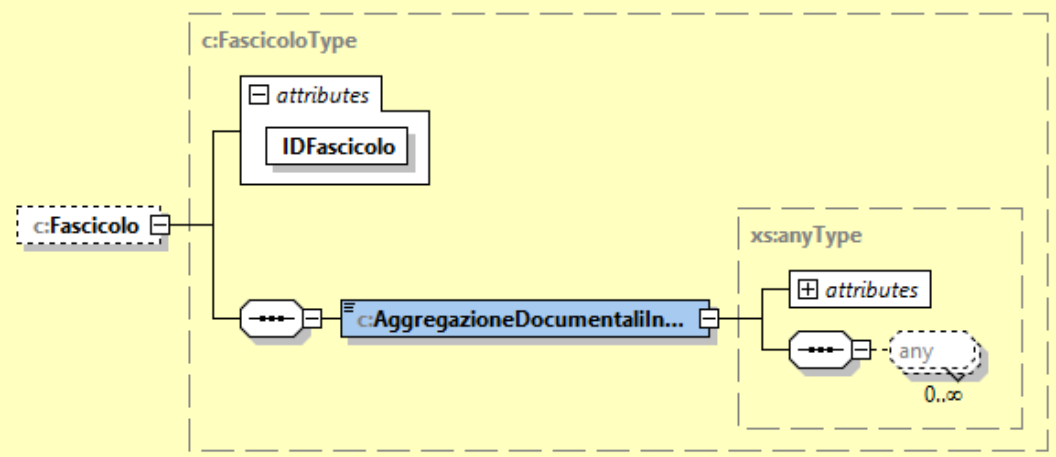
elemento ***c:UnitaArchivistica***

Descrizione	All'interno di un'unità archivistica vengono riportati i metadati descrittivi dei fascicoli da versare nel sistema di conservazione.
Diagramma	

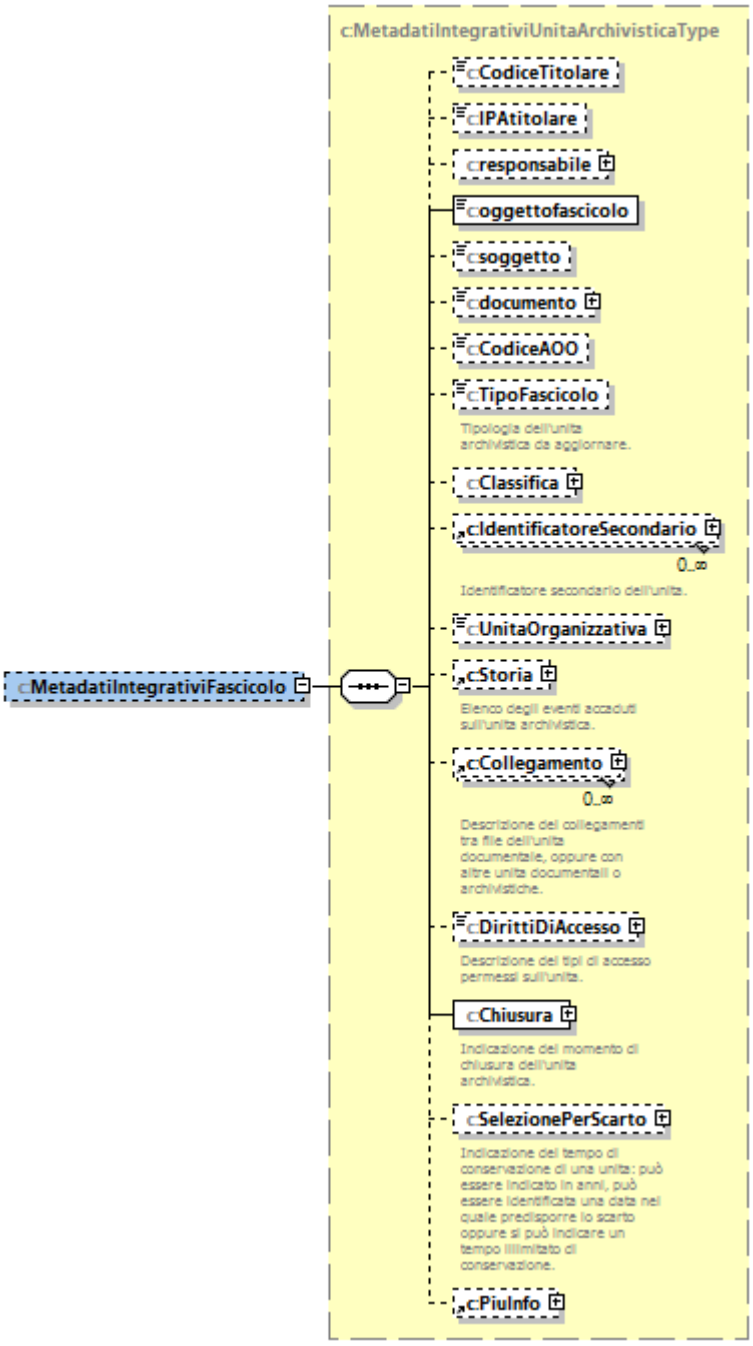
Attributi	Informazione	Valori ammessi	Tipo dato	Default
	Tipologia: Codifica della tipologia di unità archivistica definita dal produttore in accordo con il conservatore	Testo libero	Alfanumerico	-
	VersioneTipologia: Versione della tipologia dell'unità archivistica (se vuoto, si considera la versione definita nell'ultimo accordo di versamento)	Testo libero	Alfanumerico	-

Elementi	Informazione
	c:Fascicolo: si veda l'elemento Fascicolo
	c:MetadatiIntegrativiFascicolo: si veda elemento c:MetadatiIntegrativi
	c:SottoUnita: si veda elemento elemento c:***SottoUnita***

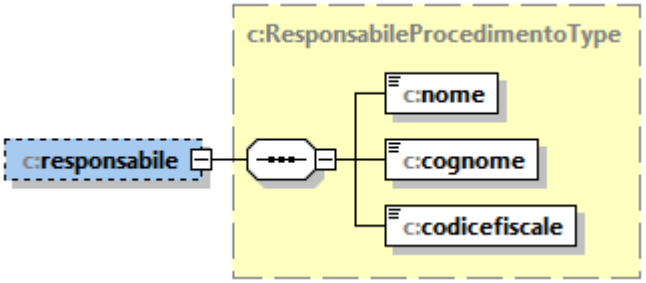
Elementi sovraordinati	
	UnitaDiVersamento

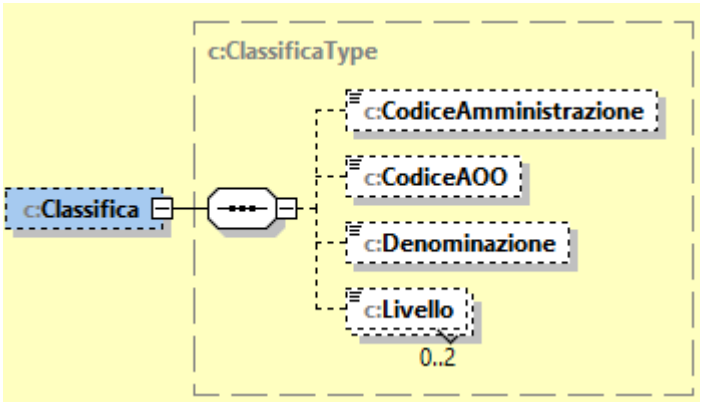
elemento ***Fascicolo***				
Descrizione	Metadati fascicolo informatico.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	IDFascicolo: Identificativo univoco del fascicolo per il sistema produttore.	Testo libero	Alfanumerico	-
Elementi	**Informazione**			
	c: AggregazioneDocumentaliInformatiche: si veda l'elemento Fascicolo			
Elementi sovraordinati	UnitaArchivistica SottoUnitaArchivistica AggiornamentoUnitaArchivistica AggiornamentoSottoUnitaArchivistica			

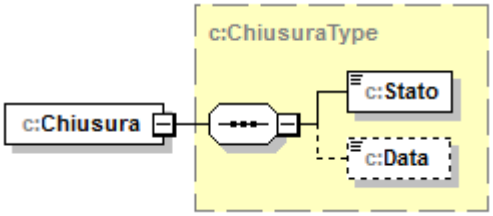
elemento ***c:AggregazioneDocumentaliInformatiche***	
Descrizione	Metadati aggregazioni documentali informatiche (vedi paragrafo '4. METADATI DELLE AGGREGAZIONI DOCUMENTALI INFORMATICHE' dell'Allegato 5 al documento "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici").
Elementi	Informazione
	vedi paragrafo '4. METADATI DELLE AGGREGAZIONI DOCUMENTALI INFORMATICHE' dell'Allegato 5 al documento "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici")
Elementi sovraordinati	Fascicolo SerieDocumentale

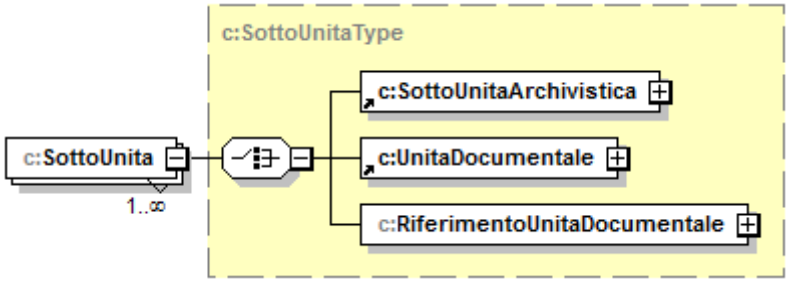
<table>
<tr><td colspan="2">elemento c:MetadatiIntegrativiFascicolo</td></tr>
<tr><td>Descrizione</td><td>Metadati integrativi che consentono di estendere la descrizione del fascicolo informatico</td></tr>
<tr><td>Diagramma</td><td> 
</td></tr>
<tr><td>Elementi</td><td>Informazione</td></tr>
<tr><td></td><td>c:CodiceTitolare: Codice amministrazione + Codice AOO della struttura titolare del fascicolo come riconosciuto dal sistema produttore.</td></tr>
<tr><td></td><td>c:IPAtitolare: Codice amministrazione + Codice AOO della struttura titolare del</td></tr>
</table>

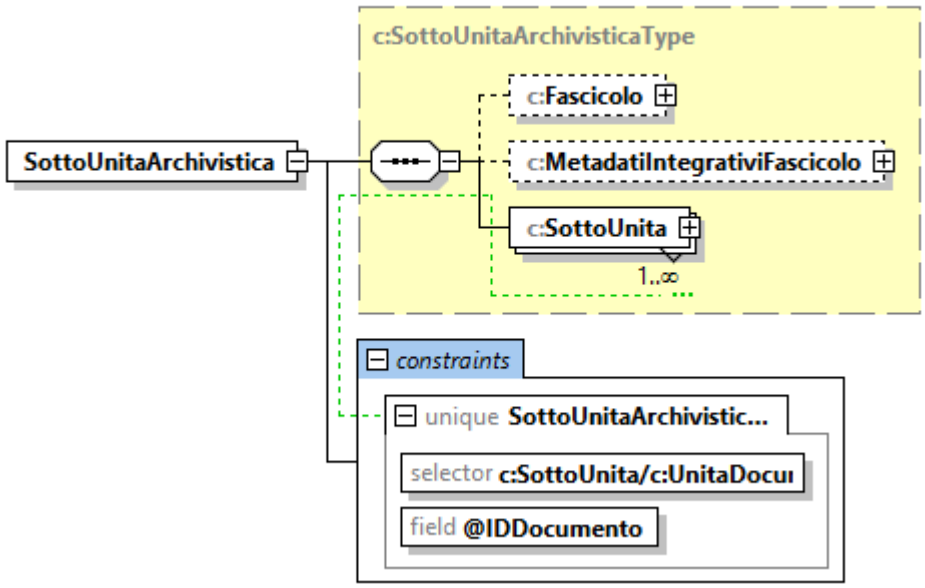
	fascicolo come riconosciuto dal registro delle Pubbliche Amministrazioni.
	c:responsabile: Per dettagli si veda elemento responsabile
	c:oggettofascicolo: Oggetto del fascicolo.
	c:soggetto: Riporta indicazioni sul soggetto cui il fascicolo si riferisce.
	c:documento: Documento inserito nel fascicolo nella fase attuale del versamento (questo campo era tra i metadati minimi nella vecchia versione delle regole tecniche, tenuto per retrocompatibilità)
	c:CodiceAOO: Identificativo univoco dell'AOO per il sistema che ha generato il documento (Stringa).
	c:TipoFascicolo: Tipologia del fascicolo, valori ammessi: Procedimento, Affare, Attivita, Persona fisica, Persona giuridica, Generico.
	c:Classifica*:* riporta i dati di classificazione, per dettagli vedi elemento Classifica
	c:IdentificatoreSecondario*:* si veda elemento IdentificatoreSecondario
	c:UnitaOrganizzativa: riporta i dati dell'Unità Organizzativa, si lascia libera l'organizzazione del campo.
	c:Storia: si veda elemento Storia
	c:Collegamento: si veda elemento Collegamento.
	c:DirittiDiAccesso: si veda elemento c:DirittiDiAccesso
	c:Chiusura: si veda elemento Chiusura
	c:SelezionePerScarto: si veda *elemento* c:SelezionePerScarto
	c:**PiuInfo*:*** riporta informazioni supplementari al documento, si veda elemento PiuInfo
Elementi sovraordinati	UnitaArchivistica SottoUnitaArchivistica AggiornamentoUnitaArchivistica AggiornamentoSottoUnitaArchivistica

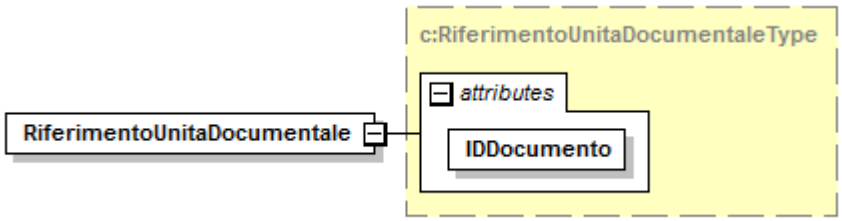
elemento c:responsabile	
Descrizione	Responsabile del procedimento amministrativo
Diagramma	
Elementi	**Informazione**
	c:nome*:* nome del responsabile del procedimento amministrativo.
	c:cognome: cognome del responsabile del procedimento amministrativo.
	c:codicefiscale: codice fiscale del responsabile del procedimento amministrativo.
Elementi sovraordinati	MetadatiIntegrativiFascicolo

elemento c:Classifica	
Descrizione	Riporta i dati di classificazione
Diagramma	
Elementi	**Informazione**
	c:CodiceAmministrazione*:* Identificativo univoco dell'amministrazione per il sistema che ha generato il documento (Stringa).
	c:CodiceAOO: Identificativo univoco dell'AOO per il sistema che ha generato il documento (Stringa).
	c:Denominazione: Descrizione della classificazione
	c:Livello: Codici identificativi del livello di classificazione (elemento ripetibile, massimo 2 volte).
Elementi sovraordinati	MetadatiIntegrativiFascicolo

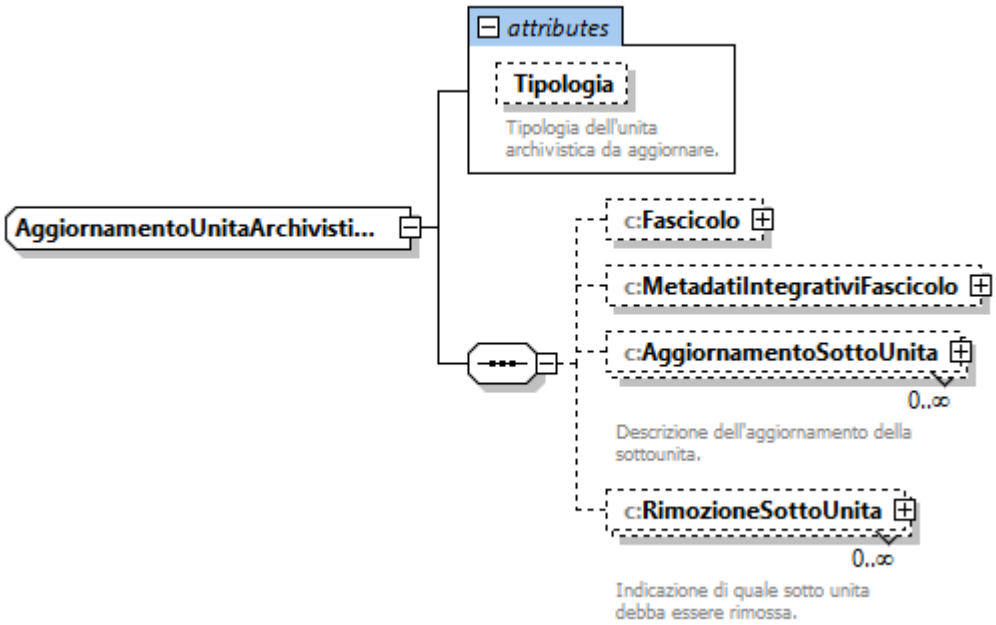
elemento c:Chiusura	
Descrizione	Indicazione del momento di chiusura dell'unità archivistica (fascicolo/serie)
Diagramma	
Elementi	**Informazione**
	c:Stato: stato dell'unità archivistica. Può assumere i valori "*APERTO*" o "*CHIUSO*"
	c:Data: data di chiusura in formato ISO 8601 del fascicolo (se chiuso). Se il fascicolo è aperto, il campo è vuoto.
Elementi sovraordinati	MetadatiIntegrativiFascicolo

elemento c:***SottoUnita***	
Descrizione	Descrizione dei sottofascicoli, dei documenti o ulteriori sottounità che possono essere presenti all'interno dell'unità archivistica.
Diagramma	
Elementi	**Informazione**
	c:SottoUnitaArchivistica: si veda *elemento* SottoUnitaArchivistica
	c:UnitaDocumentale: si veda elemento UnitaDocumentale
	c:RiferimentoUnitaDocumentale: si veda elemento RiferimentoUnitaDocumentale
Elementi sovraordinati	UnitaArchivistica SottoUnitaArchivistica

elemento ***SottoUnitaArchivistica***	
Descrizione	Descrizione dell'unità archivistica figlia dell'attuale (sottofascicolo, inserto, annesso)
Diagramma	
Elementi	**Informazione**
	c:**Fascicolo:** si veda elemento Fascicolo
	c:MetadatiIntegrativiFascicolo: si veda elemento c:***MetadatiIntegrativi***
	c:SottoUnita: si veda elemento SottoUnita
Elementi sovraordinati	SottoUnita AggiornamentoSottoUnita

elemento ***RiferimentoUnitaDocumentale***				
Descrizione	Riporta il riferimento ad un'unità documentale già versata in precedenza. In questo modo è possibile riportare un riferimento ad un documento, senza inserirlo nuovamente all'interno del pacchetto di versamento.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	IDDocumento: identificativo univoco assegnato dal sistema mittente al documento. Deve essere già stato inviato in conservazione.			
Elementi sovraordinati	SottoUnita AggiornamentoSottoUnita			

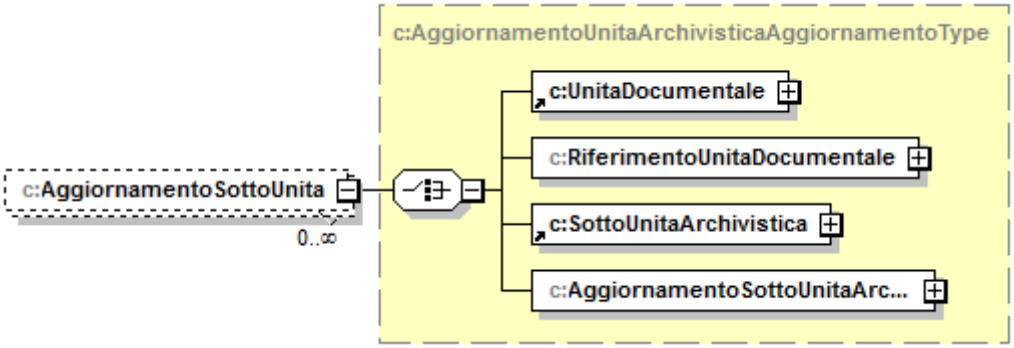
elemento ***c:AggiornamentoUnitaArchivistica***

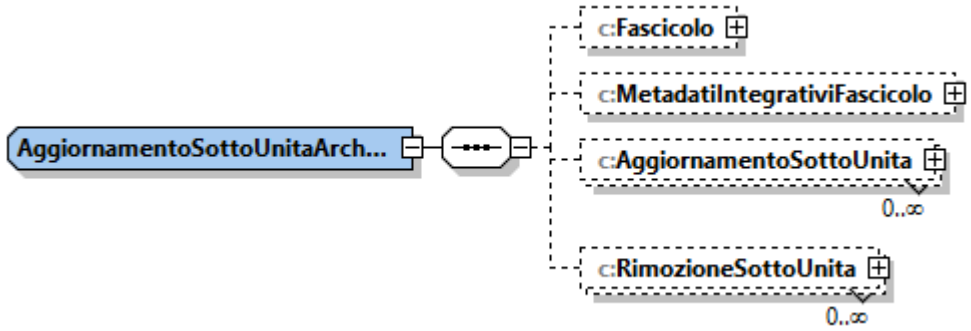
Descrizione	Metadati tramite i quali vengono trasmesse modifiche ed aggiornamenti a documenti o fascicoli già versati in conservazione. Ad esempio, per trasmettere al sistema di conservazione una variazione ad un fascicolo, per l'aggiunta di un documento, sarà sufficiente trasmettere un aggiornamento del fascicolo con il solo documento da aggiungere. In caso di modifica dei metadati del fascicolo, sarà sufficiente trasmettere i metadati, senza re-inviare l'intero contenuto del fascicolo.
Diagramma	

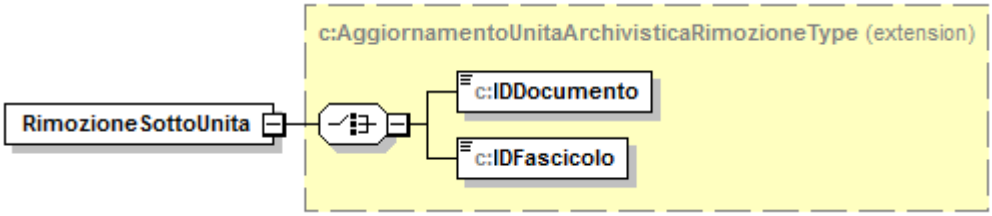
Attributi	Informazione	Valori ammessi	Tipo dato	Default
	Tipologia: Codifica della tipologia di unità archivistica definita dal produttore in accordo con il conservatore	Testo libero	Alfanumerico	-

Elementi	Informazione
	c:**Fascicolo:** si veda elemento Fascicolo
	c:**MetadatiIntegrativiFascicolo**: si veda elemento c:***MetadatiIntegrativi***
	c:**AggiornamentoSottoUnita:** si veda elemento c:***AggiornamentoSottoUnita***
	c:**RimozioneSottoUnita:** si veda elemento RimozioneSottoUnita

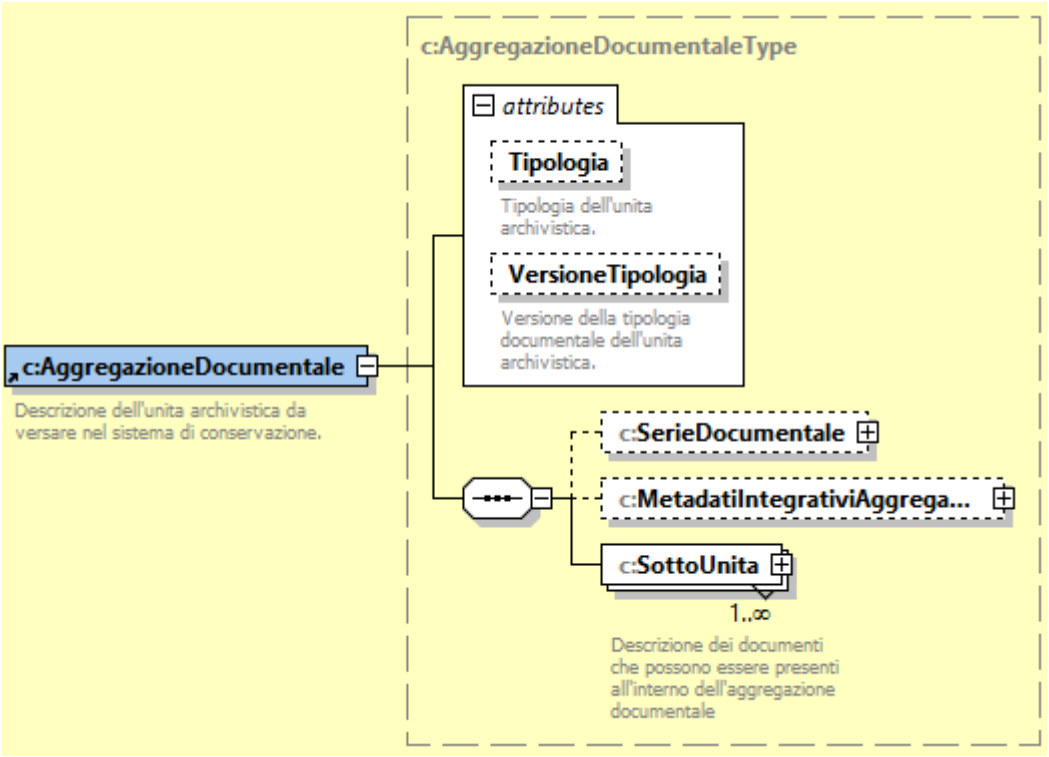
Elementi sovraordinati	
	UnitaDiVersamento

elemento c:***AggiornamentoSottoUnita***	
Descrizione	Descrive l'aggiornamento di un documento, sottofascicolo, inserto o annesso facenti parte a loro volta di un fascicolo, sottofascicolo, inserto.
Diagramma	
Elementi	**Informazione**
	c:UnitaDocumentale: si veda elemento c:***UnitaDocumentale***
	c:RiferimentoUnitaDocumentale: si veda elemento RiferimentoUnitaDocumentale
	c:SottoUnitaArchivistica: si veda *elemento* SottoUnitaArchivistica
	c:AggiornamentoSottoUnitaArchivistica: si veda elemento c:AggiornamentoSottoUnitaArchivistica
Elementi sovraordinati	**AggiornamentoUnitaArchivistica** **AggiornamentoSottoUnitaArchivistica**

elemento c:***AggiornamentoSottoUnitaArchivistica***	
Descrizione	Descrive l'aggiornamento di un sottofascicolo, inserto o annesso contenuto in un fascicolo, sottofascicolo, inserto. L'aggiornamento può riguardare metadati, l'aggiunta di elementi figli o la rimozione di parte dello stesso.
Diagramma	
Elementi	**Informazione**
	c:Fascicolo: si veda elemento Fascicolo
	c:MetadatiIntegrativiFascicolo: si veda elemento c:***MetadatiIntegrativi***
	c:AggiornamentoSottoUnita: si veda elemento c:***AggiornamentoSottoUnita***
	c:RimozioneSottoUnita: si veda elemento RimozioneSottoUnita
Elementi sovraordinati	**AggiornamentoSottoUnita**

elemento ***RimozioneSottoUnita***	
Descrizione	Tramite questo elemento è possibile comunicare a Conserva la rimozione di un sottofascicolo o di un documento figli dell'unità archivistica.
Diagramma	
Elementi	**Informazione**
	c:IDDocumento: identificativo del documento da rimuovere dall'unità archivistica. L'identificativo è quello assegnato dal sistema mittente.
	c:IDFascicolo: identificativo del sottofascicolo, inserto, annesso da rimuovere dall'unità archivistica. L'identificativo è quello assegnato dal sistema mittente.
Elementi sovraordinati	**AggiornamentoUnitaArchivistica** **AggiornamentoSottoUnitaArchivistica**

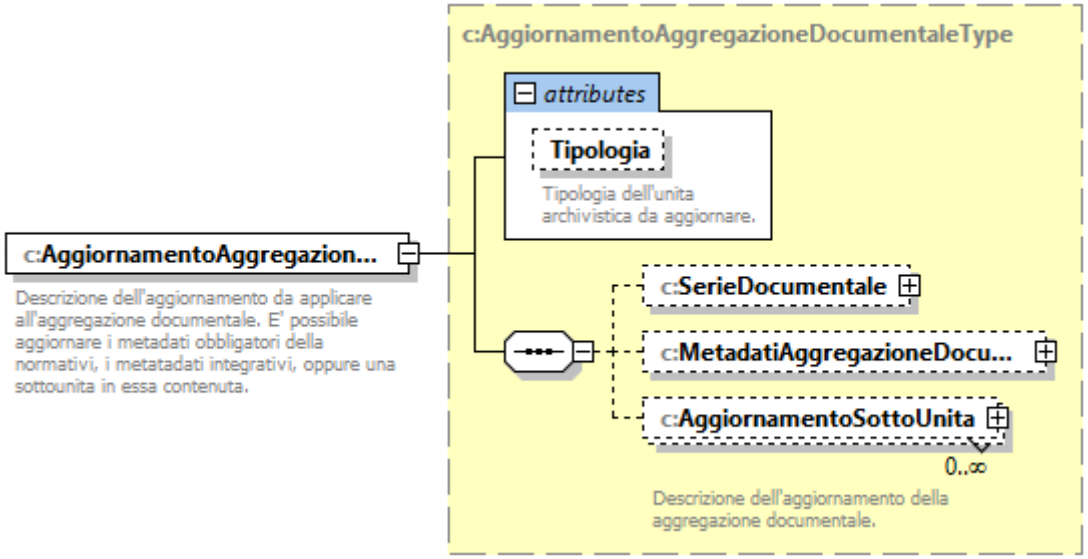
elemento ***c:AggregazioneDocumentale***

Descrizione	All'interno di un'aggregazione documentale vengono riportati i metadati descrittivi delle serie da versare nel sistema di conservazione (queste informazioni vengono portate in conservazione ma la gestione della serie rimane in capo all'applicazione Conserva)
Diagramma	

Attributi	Informazione	Valori ammessi	Tipo dato	Default
	Tipologia: Codifica della tipologia dell'aggregazione documentale definita dal produttore, corrisponde al codice di repertorio.	Testo libero	Alfanumerico	-
	VersioneTipologia: Versione della tipologia dell'aggregazione documentale (se vuoto, si considera la versione definita nell'ultimo accordo di versamento)	Testo libero	Alfanumerico	-

Elementi	Informazione
	c:SerieDocumentale: si veda l'elemento SerieDocumentale
	c:MetadatiIntegrativiAggregazioneDocumentale: si veda elemento MetadatiIntegrativiAggregazioneDocumentale
	c:SottoUnita: si veda elemento elemento c:***SottoUnita***

Elementi sovraordinati	UnitaDiVersamento

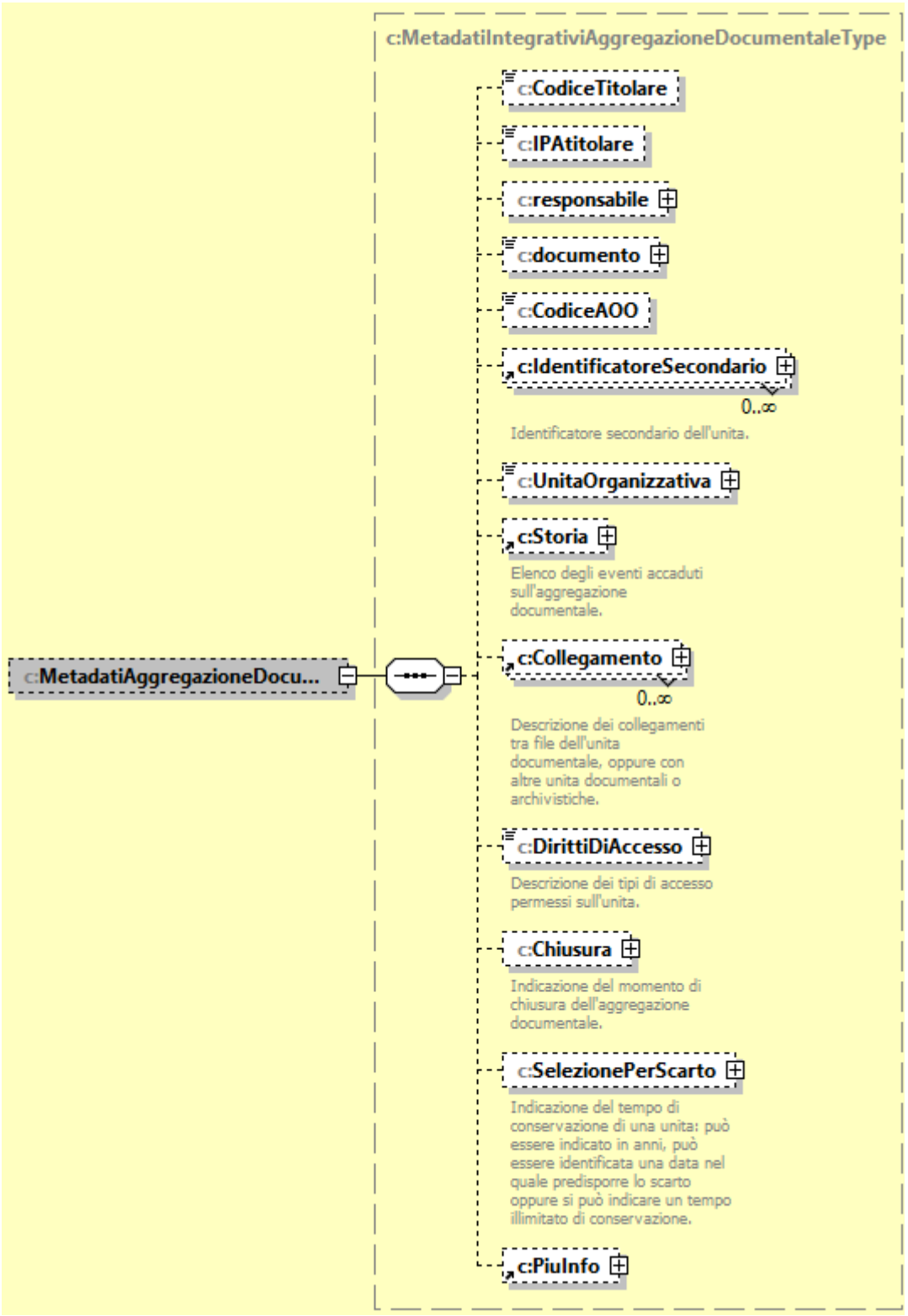
elemento ***c:AggiornamentoAggregazioneDocumentale***	
Descrizione	All'interno di un'aggregazione documentale vengono riportati i metadati descrittivi delle serie da versare nel sistema di conservazione (queste informazioni vengono portate in conservazione ma la gestione della serie rimane in capo all'applicazione Conserva)
Diagramma	

Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	Tipologia: Codifica della tipologia dell'aggregazione documentale definita dal produttore, corrisponde al codice di repertorio.	Testo libero	Alfanumerico	-

Elementi	**Informazione**
	c:SerieDocumentale: si veda l'elemento SerieDocumentale
	c:MetadatiIntegrativiAggregazioneDocumentale: si veda elemento MetadatiIntegrativiAggregazioneDocumentale
	c:AggiornamentoSottoUnita: si veda elemento elemento c:SottoUnita
Elementi sovraordinati	UnitaDiVersamento

elemento c:***MetadatiIntegrativiAggregazioneDocumentale***	
Descrizione	Metadati integrativi che consentono di estendere la descrizione del fascicolo informatico

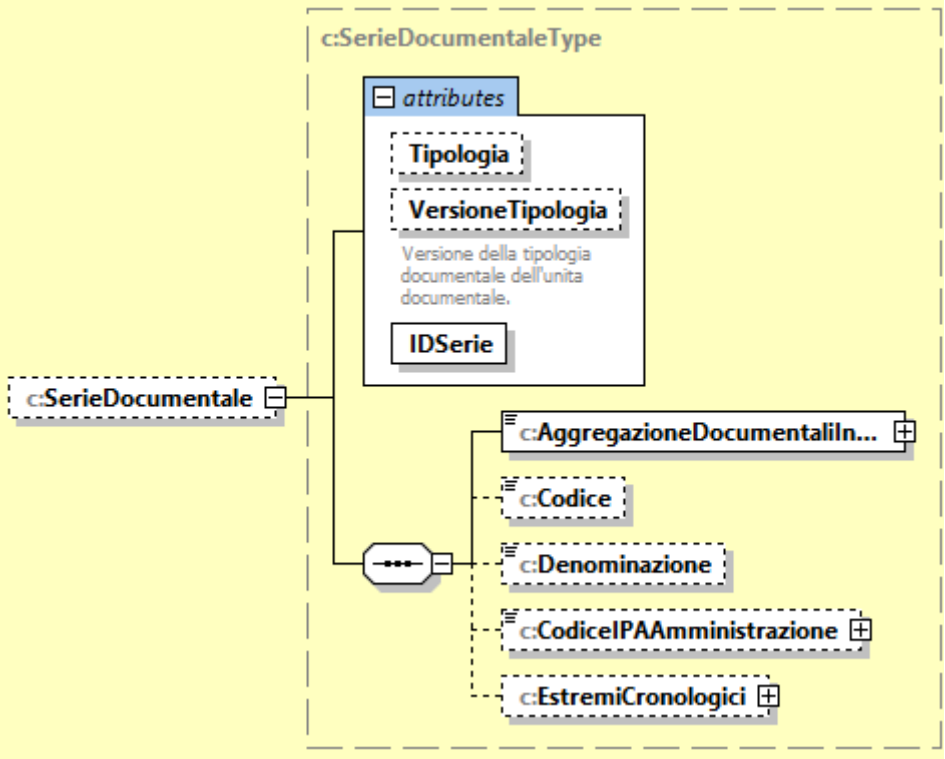
Diagramma



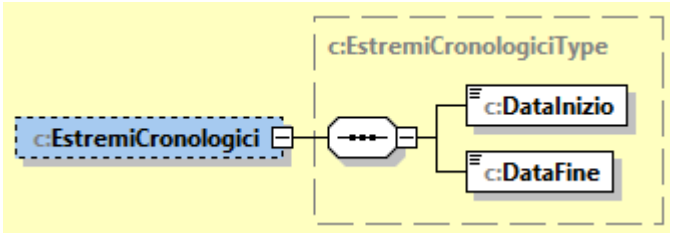
Elementi

Informazione
c:CodiceTitolare*:* Codice amministrazione + Codice AOO della struttura titolare del

	fascicolo come riconosciuto dal sistema produttore.
	c:IPAtitolare*:* Codice amministrazione + Codice AOO della struttura titolare del fascicolo come riconosciuto dal registro delle Pubbliche Amministrazioni.
	c:responsabile: Per dettagli si veda elemento responsabile
	c:documento: Documento inserito nel fascicolo nella fase attuale del versamento (questo campo era tra i metadati minimi nella vecchia versione delle regole tecniche, tenuto per retrocompatibilità)
	c:CodiceAOO: Identificativo univoco dell'AOO per il sistema che ha generato il documento (Stringa).
	c:IdentificatoreSecondario*:* si veda elemento IdentificatoreSecondario
	c:UnitaOrganizzativa: riporta i dati dell'Unità Organizzativa, si lascia libera l'organizzazione del campo.
	c:Storia: si veda elemento Storia
	c:Collegamento: si veda elemento Collegamento.
	c:DirittiDiAccesso: si veda elemento c:DirittiDiAccesso
	c:Chiusura: si veda elemento Chiusura
	c:SelezionePerScarto: si veda *elemento* c:SelezionePerScarto
	c:**PiuInfo*:*** riporta informazioni supplementari al documento, si veda elemento PiuInfo
Elementi sovraordinati	AggregazioneDocumentale AggiornamentoAggregazioneDocumentale

<table>
<tr><td colspan="3">elemento c:SerieDocumentale</td></tr>
<tr><td>Descrizione</td><td colspan="2">Metadati serie documentale.</td></tr>
<tr><td>Diagramma</td><td colspan="2"> 
</td></tr>
<tr><td>Attributi</td><td colspan="2"><table>
<tr><th>Informazione</th><th>Valori ammessi</th><th>Tipo dato</th><th>Default</th></tr>
<tr><td>IDSerie: Identificativo univoco della serie per il sistema produttore.</td><td>Testo libero</td><td>Alfanumerico</td><td>-</td></tr>
<tr><td>Tipologia: Codifica della tipologia della serie documentale definita dal produttore, corrisponde al codice di repertorio.</td><td>Testo libero</td><td>Alfanumerico</td><td>-</td></tr>
<tr><td>VersioneTipologia: Versione della tipologia della serie</td><td>Testo libero</td><td>Alfanumerico</td><td>-</td></tr>
</table></td></tr>
<tr><td>Elementi</td><td colspan="2"><table>
<tr><th>Informazione</th></tr>
<tr><td>c: AggregazioneDocumentaliInformatiche: si veda l’elemento Fascicolo.</td></tr>
<tr><td>c:Codice: Codice della serie documentale (max 100 caratteri).</td></tr>
<tr><td>c:Denominazione: Descrizione della serie documentale.</td></tr>
<tr><td>c:CodiceIPAAmministrazione: Codice IPA amministrazione che produce la serie (struttura libera)</td></tr>
</table></td></tr>
</table>

	c:EstremiCronologici: Per dettagli si veda l'elemento EstremiCronologici
Elementi sovraordinati	AggregazioneDocumentale AggiornamentoAggregazioneDocumentale

elemento ***c:EstremiCronologici***	
Descrizione	Estremi cronologici della serie documentale.
Diagramma	
Elementi	**Informazione**
	c:DataInizio: data inizio serie documentale in formato ISO 8601.
	c:DataFine: data fine serie documentale in formato ISO 8601.
Elementi sovraordinati	SerieDocumentale

Manuale di Conservazione

Allegato 5 – Rapporto di versamento

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**	**01/12/2015**	**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
1.3	26/10/2022	Intestazione	Modificato ente certificatore ed aggiornato il relativo logo	M. Mingrone	-	M. Valente
1.2	29/11/2021	Tutto	Sostituzione "Produttore" con "Titolare" Revisione generale	M. Mingrone N. Carofiglio	A. De Angelis	M. Valente
1.1	22/04/2016		Revisione a seguito delle osservazioni dello Studio Lisi	Laura Nisi		P. Vandelli

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

Introduzione

Il rapporto di versamento è un documento xml generato al termine del processo di ingestion di un pacchetto di versamento e descrive i risultati di versamento e validazione di tutte le unità contenute nel pacchetto.

Qui di seguito la descrizione della struttura del rapporto di versamento.

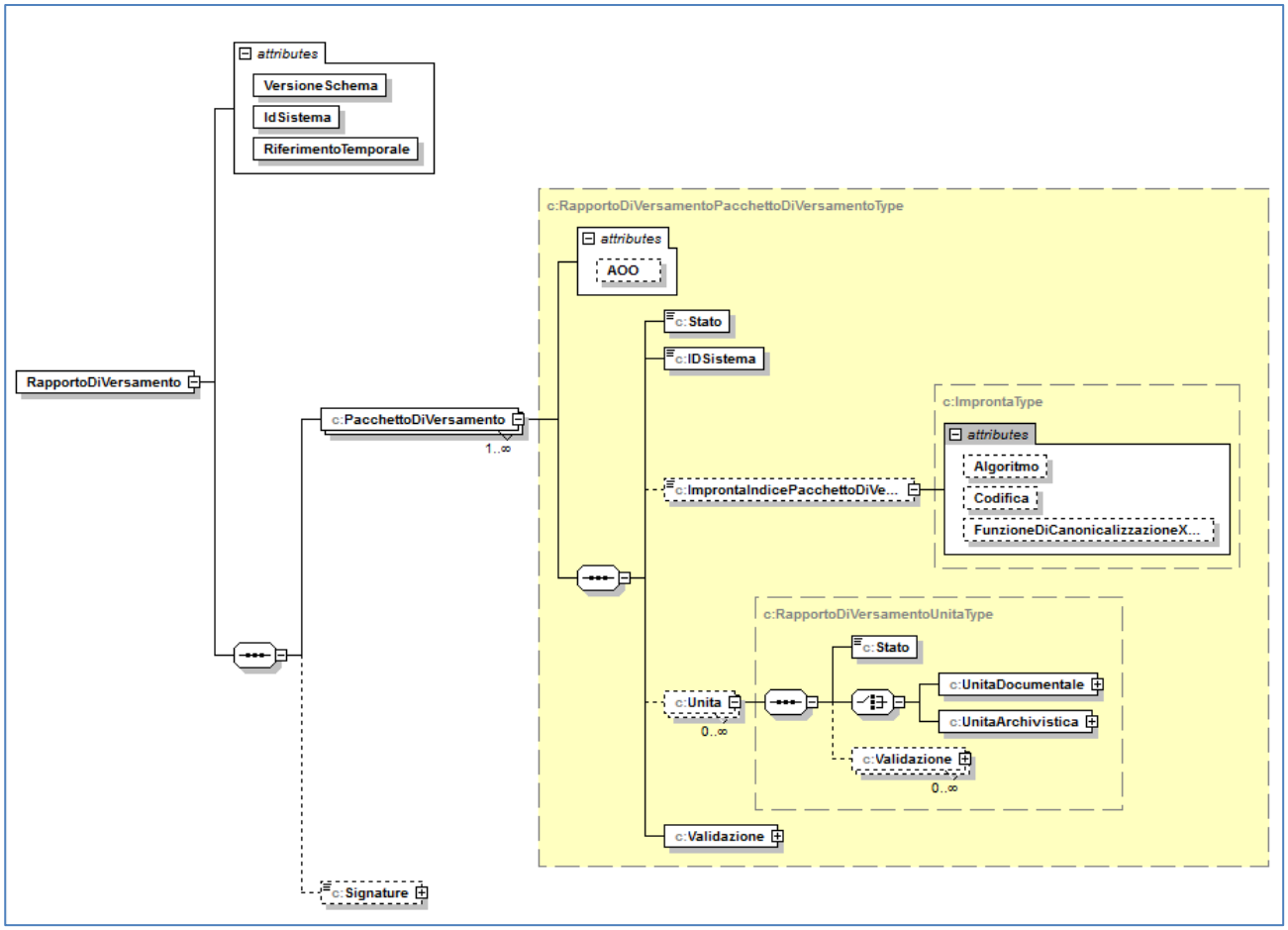


Figura 1 - Rapporto di Versamento

Descrizione elementi e attributi del rapporto di versamento

Elemento: RapportoDiVersamento

L'elemento radice ***RapportoDiVersamento*** ha come attributi:

- ***IdSistema****:* id univoco attribuito da Conserva al RdV;
- ***VersioneSchema***: versione dello schema utilizzato per questo rapporto;
- ***RiferimentoTemporale***: riferimento temporale assegnato al RdV da Conserva.

È inoltre composto dai seguenti elementi:

- ***PacchettoDiVersamento***: elemento ripetibile in cui vengono descritti i pacchetti di versamento gestiti in questo rapporto (nell'uso consueto c'è un solo elemento PacchettoDiVersamento per ogni rapporto di versamento);
- ***Signature***: elemento in cui vengono riportati i dati di firma apposti al termine della generazione del rapporto con formato di busta crittografica XAdES-T in modalità enveloped, in conformità alle attuali regole tecniche sulla firma digitale (standard RFC 3075 e ETSI TS 903 v1.4.1).

Elemento: PacchettoDiVersamento

L'elemento pacchetto di versamento ha come attributi:

- ***AOO***: (opzionale) codice AOO riportato nel pacchetto di versamento dal Titolare dell'oggetto di conservazione.

È composto dai seguenti elementi:

- ***Stato***: esplicita lo stato del pacchetto nel processo di versamento e può assumere i valori di *rifiutato*, *interamente versato* e *parzialmente versato* (vedere Allegato 4 - Mezzi di trasmissione per i dettagli);
- ***IDSistema***: identificativo univoco dato da Conserva al pacchetto di versamento. L'identificativo è lo stesso trasmesso da Conserva al Titolare al completamento del trasferimento del pacchetto;

- ***ImprontaIndicePacchettoDiVersamento***: riporta l'impronta SHA256 dell'indice del pacchetto di versamento;
- ***Unita***: elemento ripetibile contenente le informazioni delle unità archivistiche o documentali contenute nel pacchetto ricevuto dal produttore;
- ***Validazione***: elemento contenente l'esito dei controlli effettuati sul pacchetto di versamento.

Elemento: Unita

Elemento ripetibile che riporta i dettagli delle unità versate tramite il pacchetto di versamento, che a loro volta sono composte dai seguenti elementi:

- ***Stato***: esplicita lo stato dell'unità nel processo di versamento e può assumere i valori di *versata* o *rifiutata da sistema* (per il dettaglio sui controlli che possono generare un rifiuto dell'unità da parte del sistema vedere l'Allegato 6 - Controlli);
- ***RisultatoValidazioneUnita:*** esplicita il risultato dell'attività di controllo per l'unità cui si riferisce;
- ***UnitaDocumentale***: elemento alternativo a *UnitaArchivistica*, viene usato per riportare, per ogni documento contenuto nel pacchetto, l'esito dell'attività di versamento;
- ***UnitaArchivistica***: elemento alternativo a *UnitaDocumentale*, viene usato per riportare, per ogni unità archivistica contenuta nel pacchetto, l'esito dell'attività di versamento;
- ***Validazione***: esplicita l'esito della validazione sulla singola unità, che può assumere i valori: *OK*, *fallito forzabile*, *fallito non forzabile*. Riporta anche il dettaglio di tutti i controlli effettuati, sulla base di quanto stabilito nell'accordo di versamento, fino all'eventuale primo fallimento.

Elemento: RisultatoValidazioneUnita

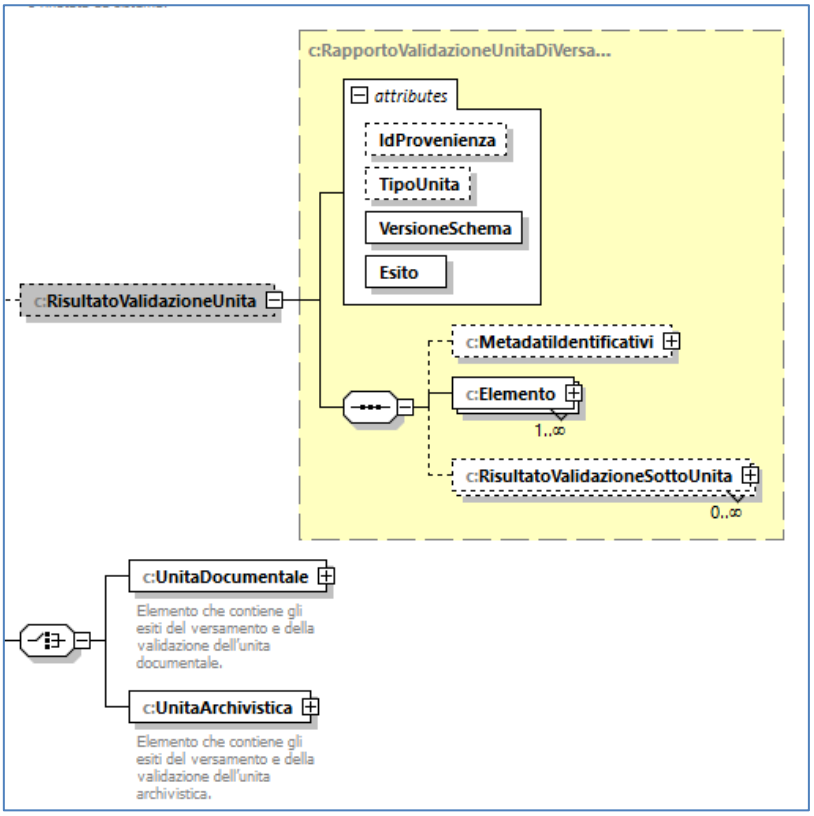


Figura 2 - RisultatoValidazioneUnita

L'elemento RisultatoValidazioneUnita ha come attributi:

- ***Esito***: esito del controllo. Ha come valori possibili: *OK*; *FALLITO_FORZABILE*; *FALLITO_NON_FORZABILE*; *SUPERATO_CON_FORZATURA.*
- ***IdProvenienza:*** identificativo dell'unità documentale o dell'unità archivistica
- ***TipoUnita:*** tipologia dell'unità cui si riferisce il controllo, può assumere solo due valori possibili (UnitaArchivistica; UnitaDocumentale)
- ***VersioneSchema:*** la versione dello schema per la validazione della struttura xml del Rapporto di Versamento

L'elemento RisultatoValidazioneUnita è composto dai seguenti elementi:

- ***Metadati identificativi:*** i metadati identificativi specifici dell'unità
- ***Elemento:*** l'elemento su cui è stato effettuato il controllo
- ***RisultatoValidazioneSottoUnità:*** (ripetibile); esplicita il risultato dell'attività di controllo per tutte le sottounità cui si riferisce e di cui composta l'unità di livello superiore.

Elemento: MetadatiIdentificativi

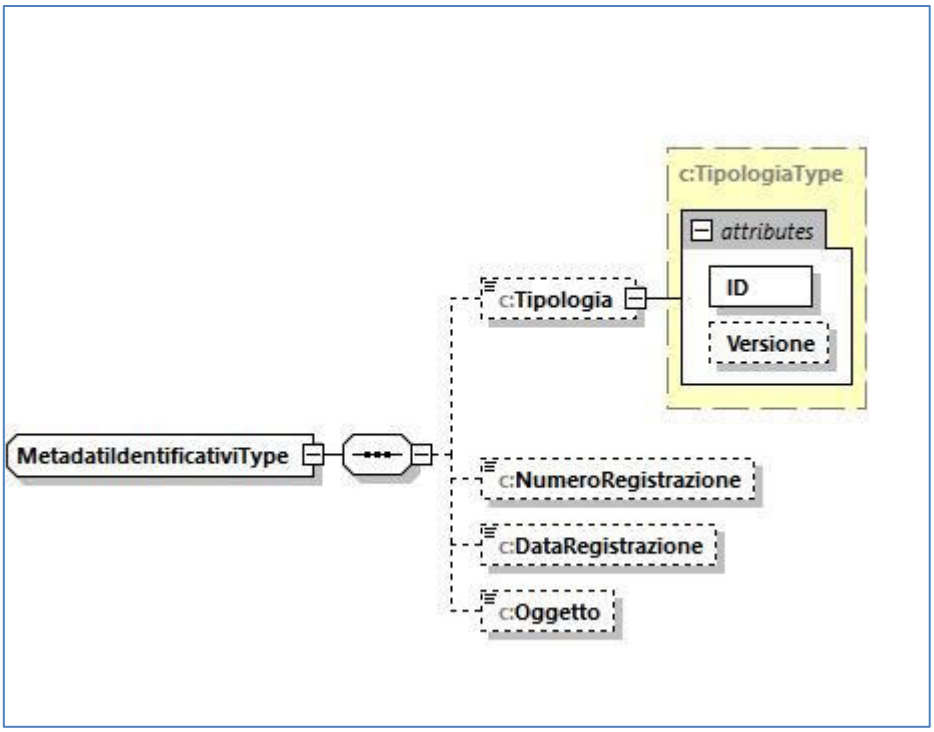


Figura 3 – MetadatiIdentificativi

L'elemento MetadatiIdentificativi contiene una serie di metadati indentificativi specifici propri dell'unità cui si riferisce, ad esempio la tipologia, l'oggetto, le informazioni di registrazione.

Elemento: Elemento

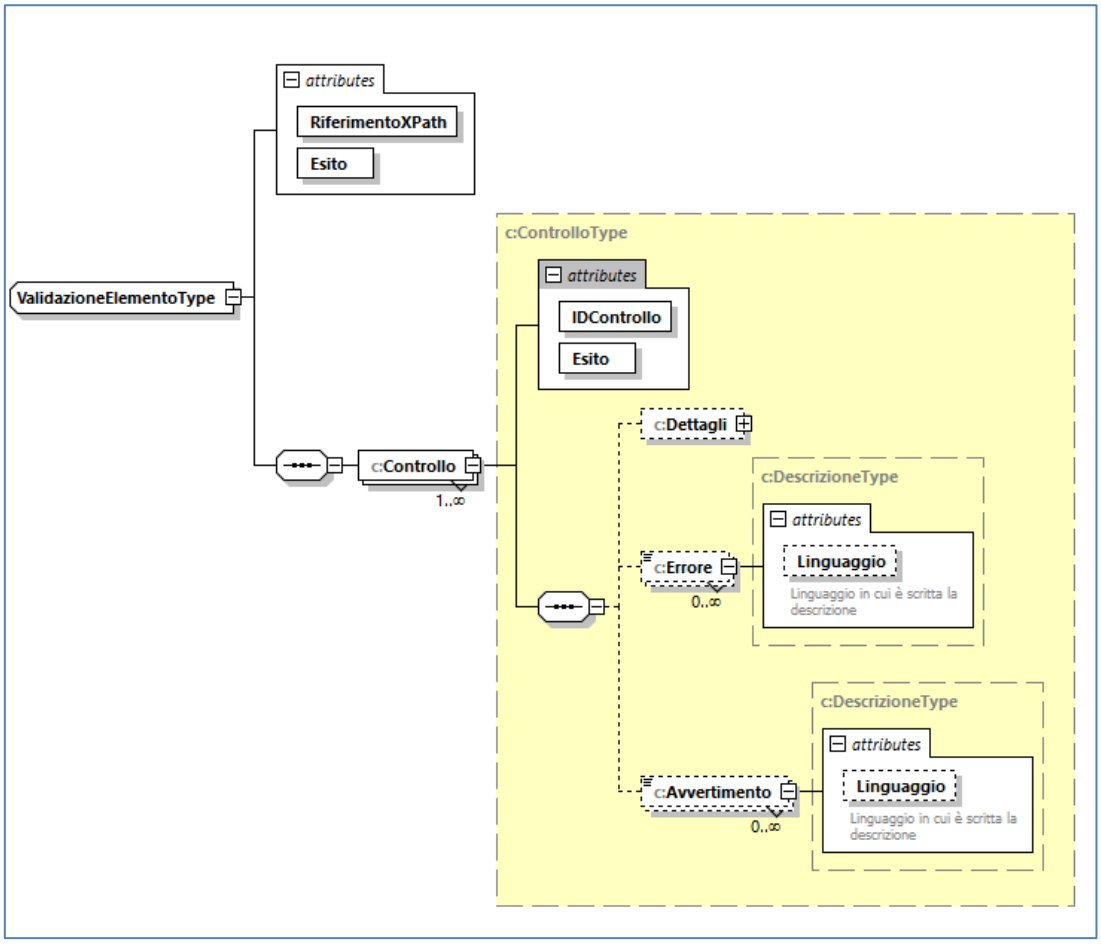


Figura 4 - Elemento

L'elemento Elemento ha come attributi:

- ***RiferimentoXPath***: il riferimento al XPath che è stato sottoposto al controllo.
- ***Esito***: esito del controllo. Ha come valori possibili: *OK*; *FALLITO_FORZABILE*; *FALLITO_NON_FORZABILE*; *SUPERATO_CON_FORZATURA.*

L'elemento Elemento è costituito dai seguenti sotto-elementi:

- **Controlli:** (ripetibile)

Elemento: Controlli

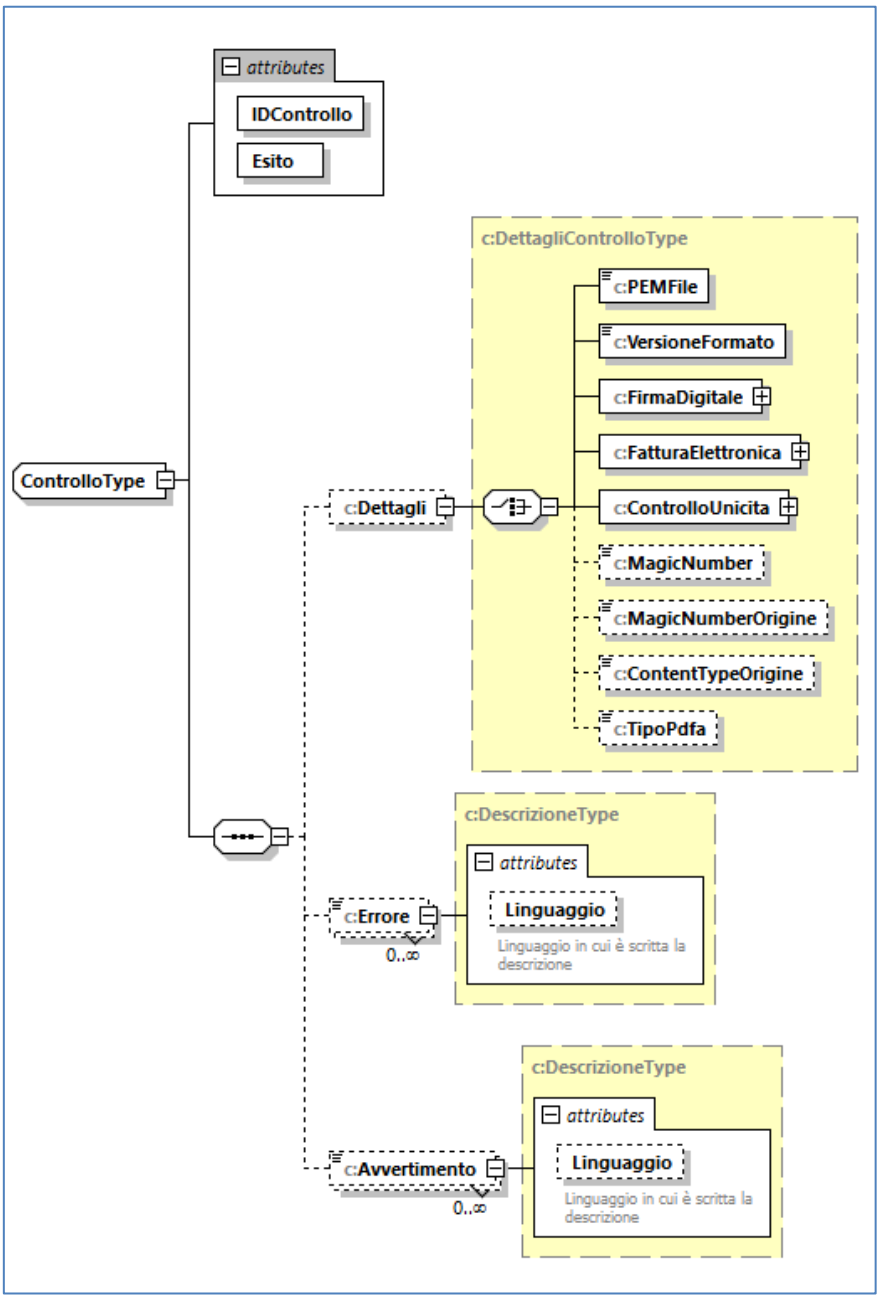


Figura 5 - Controlli

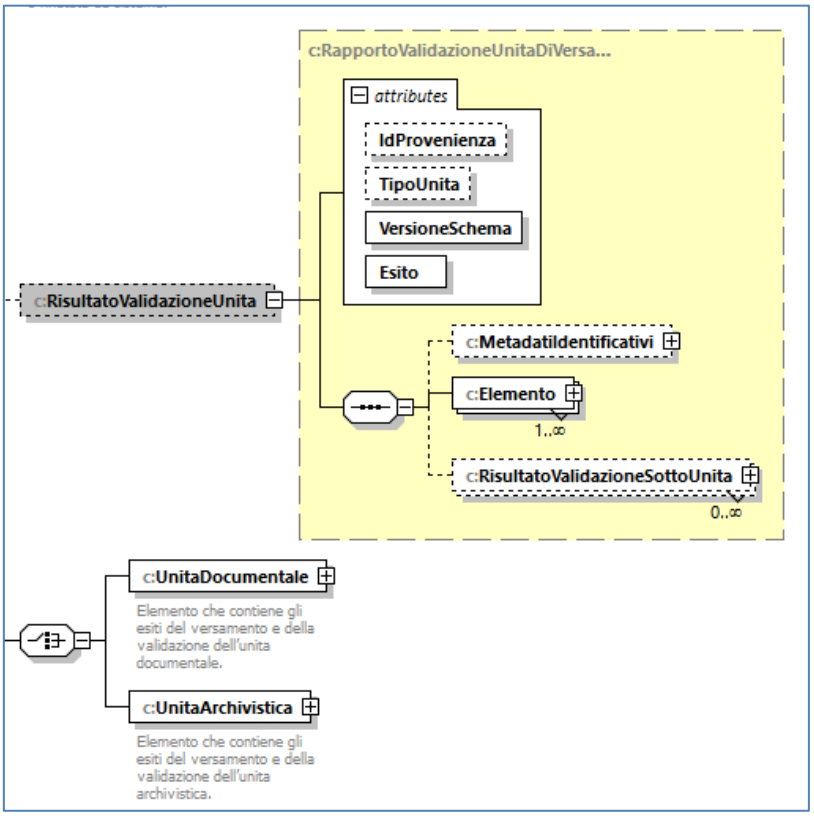
L'elemento Controllo ha come attributi:

- ***Esito***: esito del controllo. Ha come valori possibili: *OK*; *FALLITO_FORZABILE*; *FALLITO_NON_FORZABILE*; *SUPERATO_CON_FORZATURA.*
- ***IDControllo***: identificativo del controllo effettuato. Per una lista completa dei controlli esistenti si rimanda all'Allegato 6 – Controlli sui pacchetti di versamento.

L'elemento Controllo ha come elementi:

- ***Dettagli***: (opzionale); ulteriori dettagli specifici in merito al controllo.
- ***Errore***: (opzionale); eventuali specifiche in merito all'errore.
- ***Avvertimento***: (opzionale); eventuali specifiche in merito agli avvertimenti.

Elemento: RisultatoValidazioneSottoUnita



L'elemento RisultatoValidazioneSottoUnita ha come attributi:

- ***Esito***: esito del controllo. Ha come valori possibili: *OK*; *FALLITO_FORZABILE*; *FALLITO_NON_FORZABILE*; *SUPERATO_CON_FORZATURA.*
- ***IdProvenienza:*** identificativo dell'unità documentale o dell'unità archivistica
- ***TipoUnita:*** tipologia dell'unità cui si riferisce il controllo, può assumere solo due valori possibili (UnitaArchivistica; UnitaDocumentale)
- ***VersioneSchema:*** la versione dello schema per la validazione della struttura xml del Rapporto di Versamento

L'elemento RisultatoValidazioneSottoUnita è composto dai seguenti elementi:

- ***Metadati identificativi:*** i metadati identificativi specifici dell'unità
- ***Elemento:*** l'elemento su cui è stato effettuato il controllo

Elemento: UnitaDocumentale

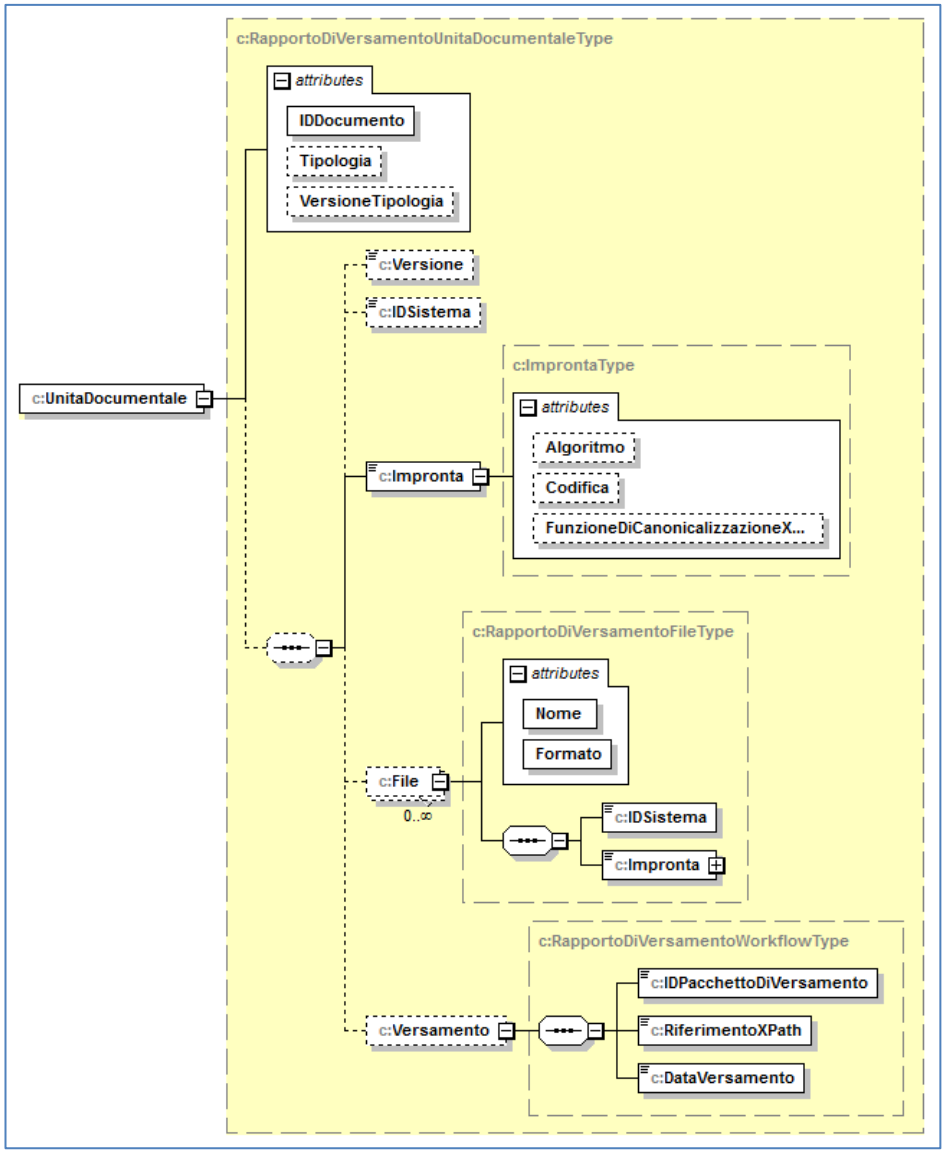


Figura 6 - Unita Documentale

L'unità documentale ha i seguenti attributi:

- ***IDDocumento***: identificativo univoco assegnato dal sistema mittente al documento;
- ***Tipologia***: elemento opzionale; rappresenta la tipologia di documento, come concordato nell'accordo di versamento;

- ***VersioneTipologia***: elemento opzionale; riporta la versione indicata nel pacchetto di versamento.

L'unità documentale ha i seguenti elementi:

- ***Versione***: (opzionale); versione del documento all'interno del sistema di conservazione, nel caso sia stato versato in più momenti lo stesso documento con variazioni al suo contenuto (file, metadati);
- ***IDSistema***: (opzionale); identificativo univoco assegnato da Conserva al documento;
- ***Impronta***: (opzionale); impronta SHA256 del documento conservato. Consente al mittente di accertare che corrisponda all'impronta del documento versato;
- ***File***: (opzionale); elemento ripetibile. Ogni elemento riporta gli estremi di ogni singolo file, facente parte del documento, inviato in conservazione;
- ***Versamento***: (opzionale); riporta gli estremi del pacchetto di versamento cui fa riferimento il rapporto.

Elemento: UnitaArchivistica

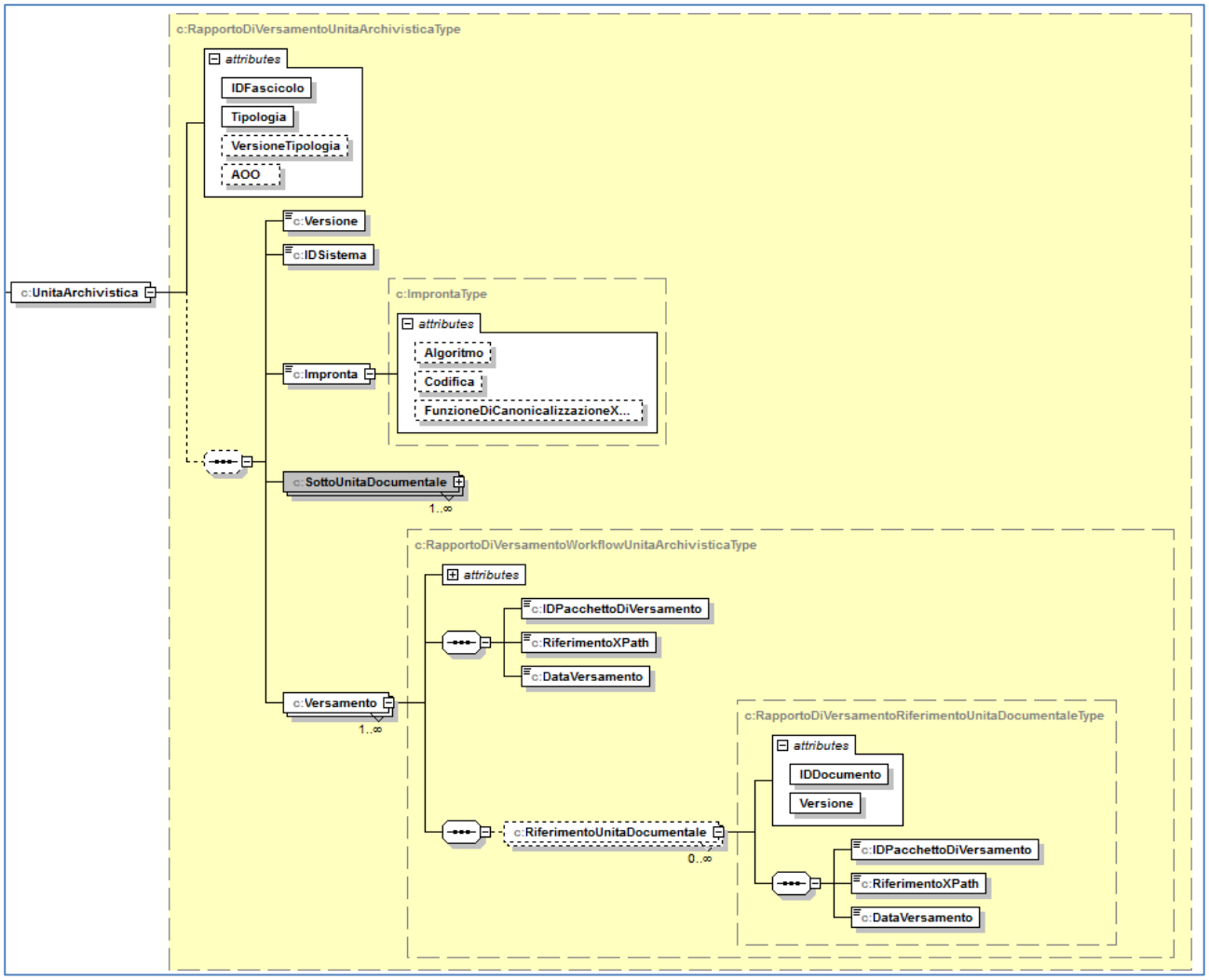


Figura 7 - UnitàArchivistica

L'unità archivistica (composta da fascicoli o serie di documenti omogenei) ha i seguenti attributi:

- ***IDFascicolo***: assume l'identificativo univoco assegnato al fascicolo o alla serie dal sistema mittente. In caso di id non assegnato (tipicamente per le serie), viene assegnato automaticamente dal sistema;
- ***Tipologia***: assume il nome della tipologia di unità archivistica (fascicolo o serie archivistica - es: VERB.ESAMI.UNIV-SERIE), come concordato nell'accordo di versamento;
- ***VersioneTipologia***: (opzionale) riporta la versione indicata nel pacchetto di versamento;
- ***AOO***: (opzionale) l'AOO di riferimento dell'unità archivistica;

L'unità archivistica ha i seguenti elementi:

- ***Versione***: (opzionale); versione dell'unità archivistica all'interno del sistema di conservazione, nel caso sia stato versato in più momenti la stessa unità con variazioni al suo contenuto (metadati, documenti);
- ***IDSistema***: (opzionale); identificativo univoco assegnato da Conserva all'unità archivistica;
- ***Impronta***: (opzionale); impronta SHA256 dell'unità archivistica conservata. Consente al mittente di accertare che corrisponda all'impronta dell'unità versata;
- ***SottoUnitaDocumentale***: (ripetibile). Ogni elemento riporta il contenuto di ogni singola unità documentale o ogni singolo file, facente parte del documento, inviato in conservazione;
- ***Versamento***: (opzionale); riporta gli estremi del pacchetto di versamento cui fa riferimento il rapporto.

Elemento: Validazione

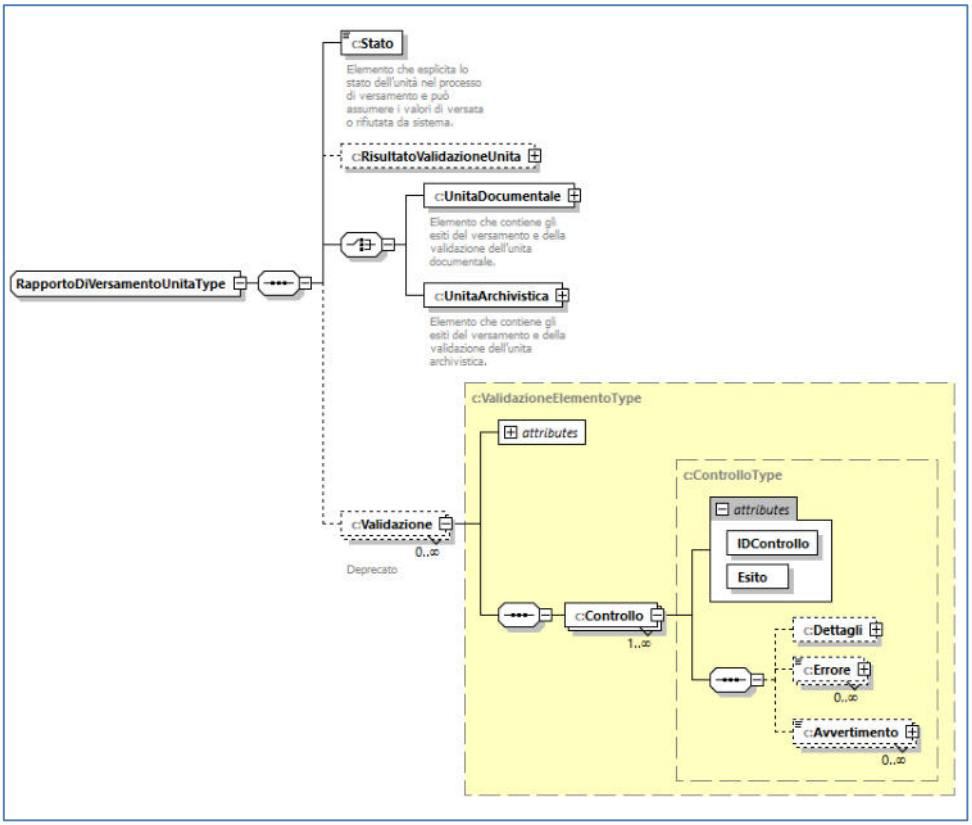


Figura 8 - Validazione

Elemento che riporta l'elencazione di tutti i controlli effettuati sul pacchetto di versamento.

L'elemento Validazione ha come attributi:

- ***Esito***: esito del controllo. Ha come valori possibili: *OK*; *FALLITO_FORZABILE*; *FALLITO_NON_FORZABILE*; *SUPERATO_CON_FORZATURA.*
- ***IDControllo***: identificativo del controllo effettuato. Per una lista completa dei controlli esistenti si rimanda all'Allegato 6 – Controlli sui pacchetti di versamento.

L'elemento Validazione ha come elementi:

- ***Dettagli***: (opzionale); ulteriori dettagli specifici in merito al controllo.
- ***Errore***: (opzionale); eventuali specifiche in merito all'errore.
- ***Avvertimento***: (opzionale); eventuali specifiche in merito agli avvertimenti.

Nota bene: il sistema interrompe l'esecuzione dei controlli degli oggetti digitale contenuti *nel pacchetto nel momento in cui riscontra un singolo risultato FALLITO_NON_FORZABILE.*

Di conseguenza un rapporto di versamento contiene tutti i controlli con esito OK, *FALLITO__FORZABILE, e SUPERATO_CON_FORZATURA* e, al massimo, un singolo risultato *FALLITO_NON_FORZABILE.*

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**	**01/12/2015**	**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
1.5	20/06/2024	Introduzione Controlli sul Pacchetto di Versamento e sull'Indice del Pacchetto di	Differenziato per tipologia di unità il controllo CONSISTENZA_TIPOLOGIA Aggiunto controllo ESISTENZA_SEGNATURA	M. Mingrone	A. De Angelis	A. De Angelis

		Versamento Controlli sull' Unità di Versamento Controlli sull' Unità Documentale Controlli sull' Unità Archivistica e l'aggiornamento dell'Unità Archivistica	Controllo SCHEMA_XML_PIUINFO Non forzabile Specificato che il controllo CONSISTENZA_PROGRESSIVO_SERIE è Non forzabile per fatture attive Reso Forzabile il controllo: UNICITA_IMPRONTE_FILE Eliminato controllo ANNULLAMENTO per le unità archivistiche			
1.4	04/11/2022	Controlli sull' Unità di Versamento	Aggiunto "partitario coge" al controllo TIPO_LIBRO_CONTABILE	M. Mingrone	A. De Angelis	M. Valente
1.3	26/10/2022	Intestazione	Modificato ente certificatore ed aggiornato il relativo logo	M. Mingrone	-	M. Valente

1.2	29/11/2021	Tutto	Sostituito “Produttore” con “Titolare” Rivisti e aggiornati controlli	M. Mingrone N. Carofiglio	A. De Angelis	M. Valente
1.1	22/04/2016		Revisione a seguito delle osservazioni dello Studio Lisi	Laura Nisi		P. Vandelli
1.0	01/12/2015		Emissione	Laura Nisi	F. Merighi, A. De Angelis, P. Vandelli	P. Vandelli

Introduzione

Di seguito sono elencati tutti i controlli che il sistema di conservazione CONSERVA esegue al momento della trasmissione e del versamento dei Pacchetti di Versamento.

Alcuni controlli si ripetono all'interno del documento, in sezioni diverse, poiché uno stesso controllo può essere applicato ad oggetti digitali differenti (ad esempio il controllo CONSISTENZA_TIPOLOGIA è valido sia per le Unita Documentali che per le Unità Archivistiche).

Ciascun controllo riporta i seguenti dati:

- Denominazione: denominazione del controllo così come riportato su CONSERVA
- Descrizione: descrizione del funzionamento del controllo anche rispetto ad eventuali
- Ambito di applicazione: l'oggetto del controllo
- Tipo: la tipologia del controllo (forzabile dal Titolare dell'oggetto di conservazione; non forzabile dal Titolare dell'oggetto di conservazione)

Controlli eseguiti in fase di trasferimento

Denominazione (Codice)	Descrizione	Ambito di applicazione	Tipo
FILE_NOME_NON_AMMESSO	Verifica che i file allegati al pacchetto di versamento (non compresso) non abbiano nomi duplicati.	Pacchetto di versamento non compresso	Non forzabile
	Verifica che i nomi dei file allegati all'indice del pacchetto di versamento siano ammessi, ovvero che non contengano caratteri proibiti.	Pacchetto di versamento non compresso	Non forzabile
FILE_VUOTO	Verifica che il file dell'indice del pacchetto di versamento non sia vuoto.	Pacchetto di versamento non compresso	Non forzabile

	Verifica che il file di archivio del pacchetto di versamento compresso non sia vuoto.	Pacchetto di versamento compresso	
FILE_ECCEDE_DIMENSIONE_MASSIMA	Verifica che la dimensione del file dell'indice del pacchetto di versamento non ecceda la dimensione massima consentita.	Pacchetto di versamento non compresso	Non forzabile
	Verifica che il file di archivio del pacchetto di versamento compresso non ecceda la dimensione massima consentita.	Pacchetto di versamento compresso	Non forzabile
HASH_NON_CORRISPONDENTE	Verifica che l'impronta dell'indice del pacchetto di versamento inviato corrisponda a quella dichiarata nella richiesta di versamento.	Pacchetto di versamento non compresso	Non forzabile
	Verifica che l'impronta del file di archivio del pacchetto di versamento compresso corrisponda a quella dichiarata nella richiesta di versamento.	Pacchetto di versamento compresso	Non forzabile
RICHIESTA_MALFORMATA	Verifica che nella richiesta di versamento di pacchetto compresso la versione dello schema dell'indice sia indicata nella richiesta e che corrisponda ad uno schema di versamento valido.	Pacchetto di versamento compresso	Non forzabile
	Verifica che nella richiesta di versamento la versione dello schema indicato nella richiesta corrisponda ad uno schema di versamento valido.	Pacchetto di versamento non compresso	Non forzabile

PARTI_IN_SEQUENZA_ERRATA	In caso di pacchetto di versamento compresso e inviato in seguito a frazionamento: Verifica che le parti precedenti di un pacchetto di versamento compresso siano state già inviate.	Pacchetto di versamento compresso e frazionato	Non forzabile
ID_PDV_MANCANTE	In caso di pacchetto di versamento compresso e inviato in seguito a frazionamento: Verifica che sia indicato all'interno della prima parte inviata, nella richiesta di versamento, l'identificativo del pacchetto di versamento.	Pacchetto di versamento compresso e frazionato	Non forzabile
PDV_NON_APPARTENENTE_PRODUTTORE	In caso di pacchetto di versamento compresso e inviato in seguito a frazionamento: Verifica all'interno della frazione di pacchetto corrente che l'identificativo del pacchetto di versamento della prima parte, specificato nella richiesta, appartenga al produttore corrente.	Pacchetto di versamento compresso	Non forzabile
PDV_NON_ESISTENTE	In caso di pacchetto di versamento compresso e inviato in seguito a frazionamento: Verifica all'interno della frazione di pacchetto corrente che l'identificativo del pacchetto di versamento della	Pacchetto di versamento compresso	Non forzabile

	prima parte, specificato nella richiesta, corrisponda ad un pacchetto esistente nel sistema.		
PDV_NON_IN_TRASFERIMENTO	In caso di pacchetto di versamento compresso e inviato in seguito a frazionamento: Verifica all'interno della frazione di pacchetto corrente che l'identificativo del pacchetto di versamento della prima parte, specificato nella richiesta, sia in stato IN_TRASFERIMENTO.	Pacchetto di versamento compresso	Non forzabile
FILE_ESISTENTE	In caso di pacchetto di versamento compresso e inviato in seguito a frazionamento: Verifica che la parte non sia già stata inviata.	Pacchetto di versamento compresso	Non forzabile
ERRORE_DI_SISTEMA	Codice di errore generico imputabile ad un malfunzionamento del sistema	Tutti	Non forzabile
PDV_NON_ELIMINABILE	In caso durante l'elaborazione il pacchetto di versamento risulti in stato "non riconosciuto" da Conserva: Viene generata un'eccezione che ne impedisce l'eliminazione.	Pacchetto di versamento	Non forzabile
UTENTE_NON_AUTORIZZATO	Verifica che l'utente che effettua il trasferimento sia tra quelli autorizzati.	Pacchetto di versamento	Non forzabile

Controlli eseguiti in fase di versamento

Controlli sul Pacchetto di Versamento e sull'Indice del Pacchetto di Versamento

Il controllo COMPRESSIONE_PACCHETTO_DI_VERSAMENTO viene eseguito in fase di decompressione.

I controlli STRUTTURA_XML, SCHEMA_XML e INTEGRITA_INDICE_PACCHETTO_DI_VERSAMENTO sono eseguiti in fase di spacchettamento.

Denominazione (Codice)	Descrizione	Ambito di applicazione	Tipo
COMPRESSIONE_PACCHETTO_DI_VERSAMENTO	Verifica l'integrità del pacchetto compresso.	Pacchetto di versamento compresso.	Non forzabile
ESISTENZA_SEGNATURA	Verifica la presenza del tag segnatura in caso di documento protocollato.	Indice del pacchetto di versamento.	Non forzabile
STRUTTURA_XML	Verifica che l'indice del pacchetto di versamento e il file contenente la sua impronta abbiano una struttura XML valida.	Indice del pacchetto di versamento. Impronta dell'indice del pacchetto di versamento in archivio compresso.	Non forzabile
SCHEMA_XML	Valida lo schema XML dell'indice del pacchetto di versamento e il file contenente la	Indice del pacchetto di versamento.	Non forzabile

	sua impronta inclusa in un archivio compresso.	Impronta dell'indice del pacchetto di versamento in archivio compresso.	
INTEGRITA_INDICE_PACCHETTO_DI_VERSAMENTO	Verifica che l'impronta calcolata sull'indice del pacchetto di versamento corrisponda a quella specificata dal soggetto produttore.	Indice del pacchetto di versamento.	Non forzabile

Controlli sull' Unità di Versamento

Tutti i controlli riportati sono eseguiti in fase di validazione.

Denominazione (Codice)	Descrizione	Ambito di applicazione	Tipo
SCHEMA_XML_PIUINFO	Valida lo schema XML dei metadati personalizzati presenti nell'elemento *"PiuInfo"* dell'unità.	Tutte le unità di versamento con metadati personalizzati e valorizzati nell'elemento *"PiuInfo"* dell'unità.	Non Forzabile
ESISTENZA_TIPOLOGIA	Verifica che la tipologia dell'unità di versamento sia presente tra quelle concordate con il soggetto titolare dell'oggetto di conservazione.	Tutte le unità di versamento	Non forzabile
CONSISTENZA_TIPOLOGIA	Verifica che la tipologia della nuova versione dell'unità coincida con quella della versione precedente.	Unità documentale	Non forzabile
		Unità archivistica	Forzabile
CONSISTENZA_AOO	Verifica che l'AOO della nuova versione dell'unità coincida con quella della versione precedente.	Tutte le unità di versamento	Forzabile
TIPO_UNITA_DI_VERSAMENTO	Verifica che il tipo di unità di versamento corrisponda a quello specificato nella sua tipologia	Tutte le unità di versamento	Non forzabile
TIPO_LIBRO_CONTABILE	In caso sia valorizzata la tipologia documentale "Libro contabile" (LIB.CONT): Verifica che il tipo sia valorizzato con uno dei seguenti valori: libro giornale, libro inventari, bilancio, registro beni	Unità versamento di tipologia LIB.CONT	Non forzabile

	ammortizzabili, liquidazioni IVA, elenco intrastat, dichiarazione di intento, partitario coge.		
TIPO_MULTI_SERIE	In caso sia valorizzata una tipologia documentale specifica che presenta delle sotto-tipologie (tipo documento): Verifica che la sotto-tipologia indicata (tipo documento) sia tra quelle previste dalla tipologia documentale.	Unità versamento di tipologia specifica	Non forzabile

Controlli sull' Unità Documentale

Tutti i controlli riportati sono eseguiti in fase di validazione.

Denominazione (Codice)	Descrizione	Ambito di applicazione	Tipo
ANNULLAMENTO	Verifica lo stato di annullamento di un documento, generando errore se viene inviato un oggetto in stato non annullato che in Conserva risulta essere annullato.	Unità documentale	Forzabile
CODICE_AMMINISTRAZIONE	Verifica che l'oggetto abbia il Codice Amministrazione previsto per l'ente che sta effettuando il versamento.	Unità documentale	Non forzabile
ESISTENZA_FILE	Verifica che il file specificato nell'indice sia incluso nel pacchetto di versamento.	Unità documentale	Non forzabile
INTEGRITA_FILE	Verifica che l'impronta calcolata sul file presente nel pacchetto di versamento coincida con quella specificata nell'indice.	Unità documentale	Non forzabile

FORMATO_FILE	Verifica che il formato calcolato sul file presente nel pacchetto di versamento coincida con quello specificato nell'indice.	Unità documentale	Non forzabile
	Verifica che il formato sia conforme a quanto stabilito all'interno dell'Allegato 8 – Formati accettati. Controllo di idoneità dei formati rispetto a quanto dichiarato nell'Allegato 8	Unità documentale	Forzabile / Non forzabile [1]
UNICITA_IMPRONTE_FILE	Verifica che l'unità documentale non contenga file con la stessa impronta.	Unità documentale	Forzabile
DIMENSIONE_FILE	Verifica che l'unità documentale non contenga file vuoti.	Unità documentale	Non forzabile
VALIDAZIONE_FILE_PER_TIPOLOGIA	Verifica la corrispondenza tra il formato accettato dalla tipologia documentale e il formato del file principale ricevuto. Controllo di corrispondenza dei formati rispetto a quanto dichiarato negli Accordi di Versamento.	Unità documentale	Forzabile / Non forzabile [2]

[1] Il controllo è impostato di default in Conserva come Non forzabile. Qualora il Soggetto Produttore (Titolare dell'oggetto di conservazione) intenda procedere con la conservazione di formati non elencati all'interno dell'Allegato 8 al Manuale della Conservazione, può richiedere a Cineca di modificare il controllo rendendolo forzabile.
[2] Stabilito mediante configurazione.

VALIDAZIONE_FIRMA_DIGITALE	Verifica che la firma apposta al file sia valida. La validità della firma è calcolata prendendo come riferimento le seguenti date: • Documenti protocollati: data di protocollo • Documenti repertoriati: data di repertorio • Documenti non protocollati e non repertoriati: data di versamento • Documenti marcati temporalmente: data di apposizione della marca	Unità documentale	Forzabile / Non forzabile [3]

Controlli sull' Unità Documentale in Serie

Tutti i controlli riportati sono eseguiti in fase di validazioni e sono validi esclusivamente per le unità documentali che prevedono raggruppamento in serie.

Denominazione (Codice)	Descrizione	Ambito di applicazione	Tipo
PRESENZA_CODICE_SERIE	Verifica che il codice della serie sia specificato nell'indice oppure configurato all'interno della tipologia.	Unità documentale in serie	Non forzabile
CONSISTENZA_CODICE_SERIE	In caso di versioni successive di unità documentali già versate: Verifica che il codice della serie della nuova versione dell'unità documentale coincida con quello della versione precedente.	Unità documentale in serie	Forzabile

[3] Il controllo è Non forzabile nei seguenti casi: 1) certificato revocato, 2) file modificato dopo apposizione firma, 3) formato della firma non valido.

CONSISTENZA_PROGRESSIVO_SERIE	In caso di versioni successive di unità documentali già versate: Verifica che il codice serie della nuova versione dell'unità documentale coincida con quello della versione precedente.	Unità documentale in serie	Forzabile/ Non forzabile[4]
ESISTENZA_PROGRESSIVO_SERIE	In caso di unità documentali con specificato il codice serie: Verifica che la serie non contenga già un'unità documentale con stesso progressivo.	Unità documentale in serie	Non forzabile
CONSISTENZA_STATO_SERIE	In caso di unità documentali con specificato il codice serie: Verifica che la serie di appartenenza sia in stato aperto.	Unità documentale in serie	Non forzabile
CREAZIONE_SERIE	In caso di unità documentali con specificato il codice serie: Verifica che, se la serie non esiste nel sistema, la tipologia dell'unità documentale permetta la creazione automatica della serie.	Unità documentale in serie	Non forzabile

[4] Il non superamento del controllo CONSISTENZA_PROGRESSIVO_SERIE è di tipo NON_FORZABILE nel caso in cui si tratti del progressivo delle fatture attive

Controlli sull' Unità Archivistica e l'aggiornamento dell'Unità Archivistica

Tutti i controlli riportati sono eseguiti in fase di validazione

Denominazione (Codice)	Descrizione	Ambito di applicazione	Tipo
CODICE_AMMINISTRAZIONE	Verifica che l'oggetto abbia il Codice Amministrazione previsto per l'ente che sta effettuando il versamento.	Unità archivistica	Non forzabile
UNICITA_UNITA_DOCUMENTALI	In caso di unità archivistica che contiene unità documentale con lo stesso id: Verifica che le unità documentali siano identiche.	Unità archivistica	Non forzabile
ESISTENZA_RIFERIMENTI_UNITA_ARCHIVISTICA	Verifica che i riferimenti contenuti nell'unità archivistica corrispondano a unità documentali presenti nel sistema.	Unità archivistica	Non forzabile
CONSISTENZA_AGGIORNAMENTO_UNITA_ARCHIVISTICA	Verifica che il risultato dell'aggiornamento dell'unità archivistica sia un'unità archivistica valida (generata correttamente durante l'elaborazione).	Aggiornamento unità archivistica	Non forzabile
	Verifica che la versione precedente esista	Aggiornamento unità archivistica	

Manuale di Conservazione

Allegato 7 – Organigramma

Consorzio Interuniversitario CINECA

STATO/STORIA DELLE REVISIONI

Versione	Data	Paragrafo rev.	Oggetto dalla revisione	Autore/i principale della revisione	Altri contributi	Validato
1.2	13/06/2023	Organigramma Organigramma Operativo	Figura Organigramma generale Sostituita Area Dematerializzazione con Conservazione e Architettura Dematerializzazione	M. Mingrone	N. Carofiglio	A. De Angelis
1.1	26/10/2022	Intestazione Organigramma Organigramma Operativo	Modificato ente certificatore ed aggiornato il relativo logo Figura Organigramma generale Sostituita Area Dematerializzazione con Conservazione e Architettura Dematerializzazione	M. Mingrone	-	M. Valente
1.0	29/11/2021		Emissione	N. Carofiglio, M. Mingrone		M. Valente

Organigramma

Di seguito si riportano le aree di alto livello dell'organigramma Cineca coinvolte nel processo di conservazione.

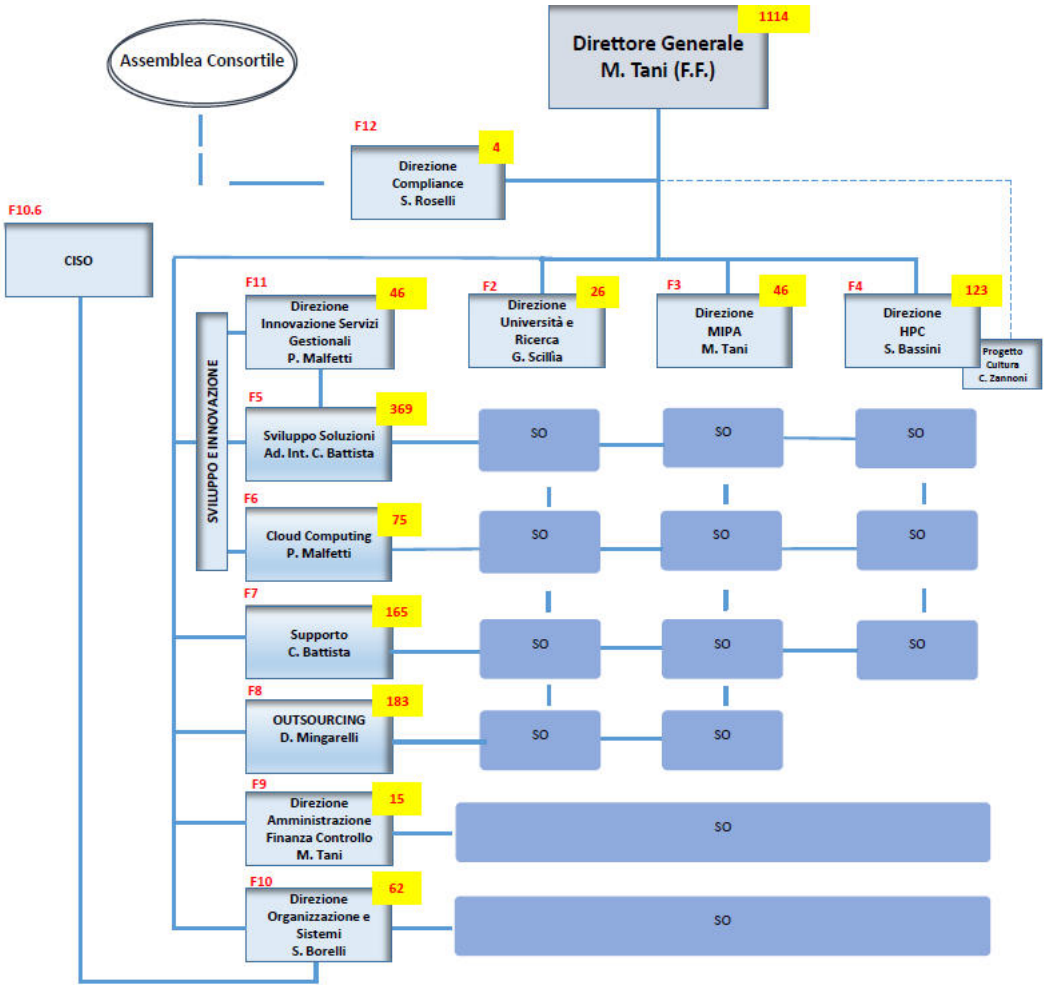


Figura 1 - Organigramma generale

Vengono descritte le unità organizzative e le responsabilità delle principali funzioni CINECA:

- **Direzione generale:** garantisce il raggiungimento degli obiettivi e del piano pluriennale definiti dagli Organi di governo assicurando lo svolgimento di tutte le funzioni necessarie alla direzione, l'organizzazione e l'attuazione degli obiettivi di istituto, secondo criteri di efficacia e di economicità gestionale.

- **Direzione Organizzazione e sistemi:** si occupa di nominare le figure previste dalla normativa in materia di conservazione digitale.
- **Direzione Compliance:** è responsabile della manutenzione delle certificazioni qualità e sicurezza, a tal fine monitora i processi interni.
- **Direzione Università e Ricerca:** produce il piano degli investimenti per i prodotti e per i servizi legati al Servizio di Conservazione. Favorisce logiche di partnership e di condivisione degli orientamenti con il sistema dei consorziati. In particolare, si descrivono le figure di Demand/Client Manager e Project manager:
  - **Demand/Client Manager:** gestisce le relazioni con gli enti produttori e si occupa della parte dell'offerta, del contratto e del rinnovo dei canoni.
  - **Project manager:** gestisce le fasi di progetti di personalizzazione dei produttori, gestisce la fatturazione dei progetti di personalizzazione, gestisce le commesse relative alle attività a pagamento.
- **Struttura Complessa Cloud Computing:** ha il compito di gestire l'infrastruttura ICT per il sistema di conservazione Conserva di CINECA e di garantire qualità ed economicità di servizio:
  - gestendo l'infrastruttura ICT nei suoi componenti (servizi di rete, storage e relativi servizi, server fisici e virtualizzati, data base, middleware, postazioni di lavoro);
  - assicurando l'aggiornamento tecnologico e fornendo servizi ad alto valore (continuità, sicurezza, qualità) e competitivi in termini economici;
  - gestendo gli ambienti di sviluppo applicativi, i sistemi di gestione aziendali, i servizi di rete e fonia;
  - garantendo il rispetto degli SLA in termini di business continuity e disaster recovery;
  - sviluppando consulenze tecnologiche.

Organigramma operativo

Di seguito si riportano le aree specifiche operative coinvolte nel processo di conservazione.

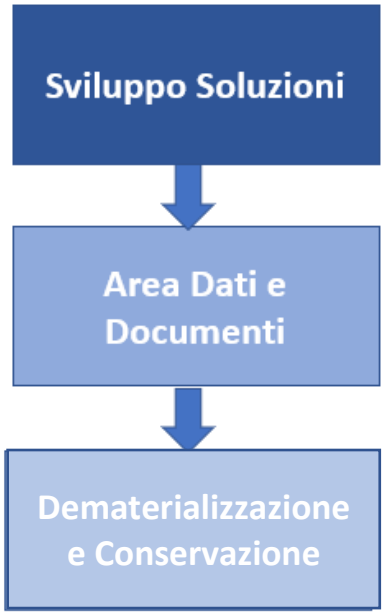


Figura 2- Aree dell'organigramma coinvolte operativamente nel sistema di conservazione

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

- **Struttura Complessa Sviluppo Soluzioni:** verifica il rispetto dei tempi e dei costi dei rilasci del sistema di conservazione Conserva di CINECA. Verifica l'efficienza del supporto fornito al sistema di conservazione Conserva di CINECA.
- **Area Dati e documenti:** non ha compiti diretti nel sistema di Conservazione è la struttura di raccordo tra la struttura semplice "Dematerializzazione" e la Struttura Complessa Sviluppo Soluzioni.

- **Dematerializzazione e Conservazione**: cura sviluppo, manutenzione ed evoluzione del sistema di conservazione Conserva di CINECA. Individua le tecnologie da utilizzare e valuta eventuali cambiamenti tecnologici da mettere in atto. Verifica la qualità del servizio erogato da terze parti ed evidenzia eventuali criticità al Responsabile del servizio di conservazione. Garantisce il raggiungimento della roadmap evolutiva del servizio sulla base dei requisiti normativi e funzionali provenienti dal Responsabile del servizio di conservazione e dal Responsabile della funzione archivistica di conservazione. Cura l'attivazione e la configurazione di nuovi enti produttori. Ha la responsabilità della gestione dei progetti e della raccolta dei requisiti avanzati dall'ente.

Manuale di Conservazione

Allegato 8 – Formati accettati

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**	**01/10/2021**	**Massimiliano Valente**	**Titolari dell'oggetto di conservazione, Personale Cineca**

STATO/STORIA DELLE REVISIONI

Versione	Data	Paragrafo rev.	Oggetto dalla revisione	Autore/i principale della revisione	Altri contributi	Validato
1.2	26/10/2022	Intestazione	Modificato ente certificatore ed aggiornato il relativo logo	M. Mingrone	-	M. Valente
1.1	29/11/2021	3.2	Aggiunti formati fogli di calcolo	M. Mingrone N. Carofiglio	A. De Angelis	M. Valente
1.0	01/10/2021		Emissione	M. Mingrone N. Carofiglio	A. De Angelis	M. Valente

1. Introduzione

Il presente allegato riporta l'elenco completo dei formati accettati dal Sistema di Conservazione Conserva.

I criteri di scelta dei formati seguiti per la stesura dell'elenco e necessari a garantire la leggibilità e la reperibilità del documento informatico sono i seguenti:

- apertura
- sicurezza
- portabilità
- funzionalità
- supporto allo sviluppo
- diffusione

La valutazione dei formati è stata condotta seguendo le disposizioni previste dall'Allegato 2 - Formati di file e riversamento delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici.

L'elenco include tutti i formati ritenuti idonei alla conservazione oppure estremamente diffusi all'interno degli Enti Titolari dell'oggetto di conservazione.

2. Modalità di aggiornamento

L'elenco viene mantenuto aggiornato a seguito di valutazioni periodiche effettuate dal team del Servizio di Conservazione in relazione, ad esempio, a:

- evoluzioni tecnologiche
- disposizioni normative
- richieste specifiche dei Titolari dell'oggetto di conservazione

L'elenco viene reso pubblico e messo a disposizione di tutti i Titolari dell'oggetto della conservazione di Cineca (https://wiki.u-gov.it/confluence/display/Conserva/Conserva+-+Il+servizio+di+conservazione+CINECA)

3. Formati di file accettati

3.1 Legenda

L'elenco è suddiviso in base alla tipologia di formato secondo quanto riportato dall'Allegato 2 - Formati di file e riversamento delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici (ad esempio Archivi compressi, Caratteri tipografici, Documenti impaginati, etc).

Per ciascun formato viene indicato:

- **Nome:** nome completo del formato.
- **Estensione:** estensione del file.
- **Tipo Mime:** codifica MIME del formato. In particolare, un tipo Mime è composto da un identificatore del tipo seguito da un identificatore del sottotipo. Ad esempio application/pdf.
- **Restrizioni:** eventuali vincoli nell'uso del formato, necessari a incrementare il livello qualitativo della conservazione. Ad esempio l'uso del PDF/A.

3.2 Elenco formati

Nome	Estensione	Tipo Mime	Restrizioni
Archivi compressi – 2.13 Allegato 2 LLGG			
GNU Zip	.gzip	application/gzip	All'interno dell'archivio compresso NON devono essere presenti: (1) archivi compressi e (2) formati NON previsti dal seguente allegato.
Java Archive file format	.jar	application/jar-archive	All'interno dell'archivio compresso NON devono essere presenti: (1) archivi compressi e (2) formati NON previsti dal seguente allegato.
Immagine di volume ISO9660	.iso	application/x-iso9660-image	All'interno dell'archivio compresso NON devono essere presenti: (1) archivi compressi e (2) formati NON previsti dal seguente allegato.
UNIX Standard Tape Archive (TAR)	.tar	application/x-tar	All'interno dell'archivio compresso NON devono essere presenti: (1) archivi compressi e (2) formati NON previsti dal seguente allegato.
7-Zip compressed archive format	.7z	application/x-7z-compressed	All'interno dell'archivio compresso NON devono essere presenti: (1) archivi compressi

			e (2) formati NON previsti dal seguente allegato.
Zip	.zip, .zipx	application/zip	All'interno dell'archivio compresso NON devono essere presenti: (1) archivi compressi e (2) formati NON previsti dal seguente allegato.
Audio e Musica – 2.9 Allegato 2 LLGG			
[Broadcast] Waveform File	.wav, .bwf, .rf64	audio/wave	Non deve presentare compressione.
Caratteri tipografici – 2.8 Allegato 2 LLGG			
OpenType®	.otf	application/x-font-otf	Valido solo come file allegato e non come file principale
OpenType®	.otf	font/otf	Valido solo come file allegato e non come file principale
TrueType®	.ttf	application/x-font-ttf	Valido solo come file allegato e non come file principale
TrueType®	.ttf	font/ttf	Valido solo come file allegato e non come file principale
Web Open Font Format	.woff2	font/woff2	Valido solo come file allegato e non come file principale
Web Open Font Format	.woff	application/font-woff	Valido solo come file allegato e non come file principale
Contenitori e pacchetti di file multimediali – 2.12 Allegato 2 LLGG			
MPEG-4, Part 14	.mp4, .m4a, .m4v	audio/mp4	
MPEG-4, Part 14	.mp4, .m4a, .m4v	video/mp4	
Digital Cinema Distribution Master	.tif/.tiff	image/tiff	Non deve presentare compressione.
Dati strutturati – 2-3 Allegato 2 LLGG			
JavaScript Object Notation	.json	application/json	
JavaScript Object Notation for Linked Data	.jsonld	application/ld+json	
Structured Query Language	.sql	application/sql	
Comma-Separated Value	.csv	text/csv	
Documenti impaginati – 2.1 Allegato 2 LLGG			
Portable Document Format	.pdf	application/pdf	Solo PDF/A

WordProcessingML OOXML Extension	.docx	application/vnd.openxmlformats-officedocument.wordprocessingml.document	Solo profilo Strict
WordProcessingML OOXML Extension	.dotx	application/vnd.openxmlformats-officedocument.wordprocessingml.template	Solo profilo Strict
Open Document Text	.odt	application/vnd.oasis.opendocument.text	
Fogli di calcolo e presentazioni multimediali – 2.5 Allegato 2 LLGG			
Open Document Format for Office Spreadsheets	.ods	application/vnd.oasis.opendocument.spreadsheet	
Open Document Format for Presentations	.odp	application/vnd.oasis.opendocument.presentation	
PresentationML OOXML Extension	.pptx, .ppsx, .potx	application/vnd.openxmlformats-officedocument.presentationml.presentation	Solo profilo Strict
SpreadsheetML OOXML Extension	xlsx, .xltx	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	Solo profilo Strict
Immagini raster - 2.6 Allegato 2 LLGG			
JPEG File Interchange Format (JFIF)	.jpeg	image/jpeg	
JPEG File Interchange Format (JFIF)	.jpg	image/jpg	
Portable Network Graphics	.png	image/png	
Immagini vettoriali e modellazione digitale – 2.7 Allegato 2 LLGG			
Autodesk® AutoCAD® Drawing	.dwg, .dwt	application/acad	
Autodesk® AutoCAD® Drawing	.dwg, .dwt	image/vnd.dwg	
Scalable Vector Graphics	.svg	image/svg+xml	
Scalable Vector Graphics	.svgz	image/svg+xml+zip	
Ipertesti – 2.2 Allegato 2 LLGG			

Extensible Hypertext Markup Language	.xhtml, .html	application/xhtml+xml	Solo se presente foglio di stile (CSS)
Extensible Markup Language	.xml	application/xml text/xml	
Extensible Stylesheet Language Transformations	.xslt	application/xslt+xml	
Cascaded Style Sheet	.css	text/css	
Hypertext Markup Language	.html, .htm	text/html	
Extensible Stylesheet Language	.xsl	text/xsl	
Posta elettronica - 2.4 Allegato 2 LLGG			
Electronic Mail Format	.eml	application/email	
"Default" Mbox Database Format	.mbox	application/mbox	
Altri formati individuati da Cineca non indicati nelle Linee Guida			
Plain Text	.txt	text/plain	

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	**X**	**01/01/2014**	**Paolo Vandelli**	**Personale Cineca e Kion, Studio Legale Lisi AGID**
Ad uso interno				
Di dominio pubblico				

STATO/STORIA DELLE REVISIONI

Versione	Data	Paragrafo revisionato	Oggetto dalla revisione	Autore/i principale della revisione	Altri contributi	Validato
1.3	07/11/2023	Intestazione Intero documento	Aggiornato logo Cineca Modificato ente certificatore ed aggiornato il relativo logo Revisione del documento per	Mariagrazia Mingrone	Nicola Carofiglio	Alessandro De Angelis

			introduzione UNISINCRO versione 2020			
1.2	24/09/2019		Revisione globale della forma e dei contenuti	Laura Nisi	Alessandro De Angelis	Riccardo Righi
1.1	22/04/2016		Revisione a seguito delle osservazioni dello Studio Lisi	Laura Nisi		Paolo Vandelli
1.0	01/12/2015		Emissione	Laura Nisi	Francesca Merighi, Alessandro De Angelis, Paolo Vandelli	Paolo Vandelli

Allegato 3 – Implementazione dell'indice UNI SInCRO

Premessa

La struttura dei Pacchetti di Archiviazione e dei Pacchetti di Distribuzione di Conserva segue lo standard UNI SInCRO – Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali – UNI 11386 – Versione 2020.

L'implementazione specifica dell' Indice UNISInCRO all'interno del dominio di riferimento di Cineca è descritta nel presente documento.

Al fine di impostare la seguente descrizione si esplicita che si è ritenuto opportuno far coincidere:

- l'elemento <PVolume> con la serie documentale o l'unità archivistica;
- l'elemento <FileGroup> con la singola unità documentale;
- l'elemento <File> con il singolo file che compone l'unità documentale.

All'interno del servizio di conservazione Conserva ogni pacchetto di archiviazione corrisponde ad una serie documentale o ad una unità archivistica al fine di ricostruire l'archivio dell'ente secondo l'organizzazione archivistica fornita dal Sistema di gestione documentale.

Se una unità documentale è sia all'interno di una serie documentale che all'interno di una o più unità archivistiche, l'unità documentale verrà referenziata tutte le volte necessarie.

Lo schema utilizzato per validare l'istanza di un indice è lo schema UNI SInCRO, integrato per quanto riguarda le informazioni aggiuntive, in particolare le integrazioni sono legate all'aggiunta di dichiarazioni di namespace, di modelli di MoreInfo per la validazione, di valore fissi per alcuni attributi e note descrittive relative agli elementi.

Indicazioni di lettura

La descrizione dell'implementazione dello schema XML dell'indice UNI SInCRO ha una forma tabellare coerente con la gerarchia dello stesso schema XML[1] divisa per i quattro sotto elementi principali del PIndex:

[1] Fanno eccezione alcuni elementi non valorizzati la cui struttura esplicitata renderebbe illeggibile la tabella.

- SelfDescription
- PVolume
- FileGroup
- Process

<table>
<tr><td colspan="5">elemento sin:PIndex</td></tr>
<tr><td>Descrizione</td><td colspan="4">Elemento radice dell’indice di conservazione.</td></tr>
<tr><td>Diagramma</td><td colspan="4"></td></tr>
<tr><td rowspan="4">Attributi</td><td>Informazione</td><td>Valori ammessi</td><td>Tipo dato</td><td>Default</td></tr>
<tr><td>sin:language</td><td>-</td><td>-</td><td>IT</td></tr>
<tr><td>sin:sincroVersion</td><td>-</td><td>-</td><td>2.0</td></tr>
<tr><td>xsi:schemaLocation</td><td>-</td><td>-</td><td>http://www.uni.com/U3011/sincro-v2/ conserva-schema-uni-sincro-v2.0.xsd</td></tr>
<tr><td></td><td>sin:uri</td><td>-</td><td>-</td><td>http://www.uni.com/U3011/sincro-v2/PIndex.xsd</td></tr>
<tr><td rowspan="2">Elementi</td><td colspan="4">Informazione</td></tr>
<tr><td colspan="4">sin:SelfDescription, sin:PVolume, sin:FileGroup, sin:Process</td></tr>
<tr><td>Elementi sovraordinati</td><td colspan="4">-</td></tr>
</table>

<table>
<tr><td colspan="5">elemento sin:SelfDescription</td></tr>
<tr><td>Descrizione</td><td colspan="4">Elemento contenitore che fornisce informazioni generali sull’indice del pacchetto di archiviazione.</td></tr>
<tr><td>Diagramma</td><td colspan="4"></td></tr>
<tr><td rowspan="2">Attributi</td><td>Informazione</td><td>Valori ammessi</td><td>Tipo dato</td><td>Default</td></tr>
<tr><td>-</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td rowspan="2">Elementi</td><td colspan="4">Informazione</td></tr>
<tr><td colspan="4">sin:ID, sin:CreatingApplication, sin: PIndexSource, sin:MoreInfo</td></tr>
<tr><td>Elementi sovraordinati</td><td colspan="4">sin:PIndex</td></tr>
</table>

<table>
<tr><td colspan="5">elemento sin:ID</td></tr>
<tr><td>Descrizione</td><td colspan="4">Elemento relativo all’identificazione univoca dell’indice del pacchetto di archiviazione all’interno del servizio di conservazione. Viene calcolato contestualmente alla generazione dell’indice in fase di chiusura del pacchetto di archiviazione.
L’identificatore viene costruito secondo la seguente regola:

[idproduttore]-IPDA-[anno]-[n]

• con idproduttore: codice IPA o dominio del sito dell’ente inserito in fase di configurazione dell’ente;
• con IPDA: acronimo di Indice del Pacchetto di Archiviazione;
• con anno: anno di apertura del pacchetto di archiviazione;
• con n: numero progressivo della successione idproduttore-IPDA-anno.
L’attributo sin:scheme definisce il dominio e preserva l’univocità dell’identificatore; al momento della redazione di questo documento ha valore fisso: scheme=Conserva</td></tr>
<tr><td>Diagramma</td><td colspan="4"></td></tr>
<tr><td rowspan="2">Attributi</td><td>Informazione</td><td>Valori ammessi</td><td>Tipo dato</td><td>Default</td></tr>
<tr><td>sin:scheme</td><td>-</td><td>-</td><td>scheme=Conserva</td></tr>
<tr><td rowspan="2">Elementi</td><td colspan="4">Informazione</td></tr>
<tr><td colspan="4">-</td></tr>
<tr><td>Elementi sovraordinati</td><td colspan="4">sin:SelfDescription</td></tr>
</table>

elemento ***sin:CreatingApplication***				
Descrizione	Elemento contenitore che identifica l'applicazione che ha generato l'indice del pacchetto di archiviazione.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	-	-	-
Elementi	**Informazione**			
	sin:Name, sin:Version, sin:Producer			
Elementi sovraordinati	***sin:SelfDescription***			

elemento ***sin:Name***				
Descrizione	Elemento relativo al nome dell'applicazione che ha generato l'indice del pacchetto di archiviazione. Al momento della redazione di questo documento ha valore fisso: ***Name=Conserva***			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	-	-	-
Elementi	**Informazione**			
	-			
Elementi sovraordinati	***sin:CreatingApplication***			

elemento ***sin:Version***				
Descrizione	Elemento relativo alla versione dell'applicazione che ha generato l'indice del pacchetto di archiviazione. Il suo valore varia in base all'aggiornamento di versione dell'applicativo Conserva; al momento della redazione di questo documento ha valore fisso: ***Version=2.00***			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	-	-	-
Elementi	**Informazione**			
	-			
Elementi sovraordinati	***sin:CreatingApplication***			

elemento ***sin:Producer***				
Descrizione	Elemento relativo al nome del produttore responsabile dell'applicazione che ha generato l'indice del pacchetto di archiviazione. Al momento della redazione di questo documento ha valore fisso: ***Producer=CINECA Consorzio Interuniversitario***			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	-	-	-
Elementi	**Informazione**			
	-			

Elementi sovraordinati	***sin:CreatingApplication***

elemento ***sin:PIndexSource***				
Descrizione	Elemento contenitore valorizzato nel momento in cui vi è una migrazione di indici di conservazione, oppure una frammentazione o una unione di più indici antecedenti. Ad esempio: quando un pacchetto di archiviazione è chiuso e viene versato un documento dello stesso fascicolo del pacchetto oppure viene ritrasmessa una nuova versione di un documento già archiviato, il servizio migra il pacchetto precedente generando nuovo pacchetto contenente anche l'ultimo documento arrivato.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	sin:derivation	-	-	-
Elementi	**Informazione**			
	sin:ID, sin:Path, sin:Hash			
Elementi sovraordinati	***sin:SelfDescription***			

<table>
<tr><td colspan="5">elemento sin:ID</td></tr>
<tr><td>Descrizione</td><td colspan="4">Elemento relativo all’identificazione univoca dell’indice del pacchetto di archiviazione all’interno del sistema di conservazione. Viene calcolato contestualmente alla generazione dell’indice in fase di chiusura del pacchetto di archiviazione.
L’identificatore viene costruito secondo la seguente regola:

[idproduttore]-IPDA-[anno]-[n]

• con idproduttore: codice IPA o dominio del sito dell’ente inserito in fase di configurazione dell’ente;
• con IPDA: acronimo di Indice di Pacchetto di Archiviazione;
• con anno: anno di apertura del pacchetto di archiviazione;
• con n: numero progressivo della successione idproduttore-IPDA-anno.
L’attributo @scheme definisce il dominio e preserva l’univocità dell’identificatore; al momento della redazione di questo documento ha valore fisso: scheme=Conserva</td></tr>
<tr><td>Diagramma</td><td colspan="4"></td></tr>
<tr><td rowspan="2">Attributi</td><td>Informazione</td><td>Valori ammessi</td><td>Tipo dato</td><td>Default</td></tr>
<tr><td>sin:Scheme</td><td>-</td><td>-</td><td>scheme=Conserva</td></tr>
<tr><td rowspan="2">Elementi</td><td colspan="4">Informazione</td></tr>
<tr><td colspan="4">-</td></tr>
<tr><td>Elementi sovraordinati</td><td colspan="4">sin:PIndexSource</td></tr>
</table>

elemento ***sin:Path***				
Descrizione	Elemento relativo alla localizzazione dell'indice cui l'elemento si riferisce, espressa come indirizzo URI. Il valore dell'elemento coincide con il path *relativo* dell'indice rispetto alla posizione dell'indice di conservazione. Tale elemento può essere valorizzato e assume significato solo nel caso in cui, nei processi di esportazione, i *file* siano memorizzati all'interno di un *file system*: in presenza di un database il valore dell'elemento <ID> è ritenuto sufficiente all'identificazione puntuale del *file* e questo elemento di conseguenza non necessita di essere valorizzato.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	-	-	-
Elementi	**Informazione**			
	-			
Elementi sovraordinati	***sin:PIndexSource***			

elemento ***sin:Hash***				
Descrizione	Elemento relativo all'impronta del file dell'indice del pacchetto di archiviazione antecedente. L'attributo ***sin:canonicalXML*** riporta le informazioni per determinare, in presenza di un *file* XML, se questo sia stato trasformato nella forma canonica prima di essere sottoposto a hash. L'attributo è opzionale. L'attributo ***sin:hashFunction*** è utilizzato per identificare la funzione di hash utilizzata per calcolare l'impronta e al momento della redazione di questo documento ha valore fisso: ***hashFunction =SHA-256***			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	sin:canonicalXML	-	-	-

	sin:hashFunction	-	-	SHA-*256*
Elementi	**Informazione**			
	-			
Elementi sovraordinati	***sin:PIndexSource***			

elemento ***sin:MoreInfo***				
Descrizione	Elemento contenitore di informazioni ulteriori, relative all'elemento padre di <MoreInfo>, che non è possibile associare ad altri elementi. L'attributo *@ xmlSchema* riporta la localizzazione dello Schema XML della struttura di metadati; il valore deve essere espresso nella forma di URL. Al momento della redazione di questo documento ha valore fisso: ***xmlSchema*= conserva-schema-pindex-v2.0.xsd**			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	sin:xmlSchema	-	-	conserva-schema-pindex-v2.0.xsd
Elementi	**Informazione**			
	sin:EmbeddedMetadata, sin:ExternalMetadata			
Elementi sovraordinati	***sin:SelfDescription***			

elemento ***sin:EmbeddedMetadata***				
Descrizione	Elemento contenente le informazioni dell'elemento <MoreInfo> integrate all'interno dell'indice di conservazione e strutturate nel formato XML. Identificatore del pacchetto di archiviazione precedente relativo alla serie.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	-		-
Elementi	**Informazione**			
	sin:InformazioniPIndex, sin:InformazioniFile, sin:InformazioniUnitaDocumentale			
Elementi sovraordinati	***sin:MoreInfo***			

elemento ***c:InformazioniPIndex***				
Descrizione	Contiene metadati relativi a: • funzione di canonicalizzazione; • il codice dell'AOO di riferimento; • ulteriori informazioni in caso di serie documentali *(ad esempio: numero progressivo, data prima e ultima unità…)*			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	xmlns:c	-	-	http://conserva.cineca.it/xsd
Elementi	**Informazione**			
	c:FunzioneDiCanonicalizzazione, c:AOO, c:InformazioniPartizioneSerie			

Elementi sovraordinati	***sin:EmbeddedMetadata***

elemento ***c: FunzioneDiCanonicalizzazione***				
Descrizione	Al momento della redazione del presente allegato ha valore fisso **c:*FunzioneDiCanonicalizzazione*** = http://www.w3.org/2001/10/xml-exc-c14n#			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	-	-	-
Elementi	**Informazione**			
	-			
Elementi sovraordinati	***c:InformazioniPIndex***			

elemento ***c:AOO***				
Descrizione	Codice Area Organizzativa Omogenea del produttore del pacchetto.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	-	-	-

Elementi	Informazione
	c:CodiceAOO
Elementi sovraordinati	***c:InformazioniPIndex***

elemento ***c:CodiceAOO***				
Descrizione	Codice Area Organizzativa Omogenea del produttore del pacchetto.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	-	-	-
Elementi	**Informazione**			
	c:CodiceAOO			
Elementi sovraordinati	***c:AOO***			

<table>
<tr><td colspan="5">elemento c:InformazioniPartizioneSerie</td></tr>
<tr><td>Descrizione</td><td colspan="4">Contenitore che raccoglie le informazioni necessarie nel caso di serie documentali.</td></tr>
<tr><td>Diagramma</td><td colspan="4"></td></tr>
<tr><td rowspan="2">Attributi</td><td>Informazione</td><td>Valori ammessi</td><td>Tipo dato</td><td>Default</td></tr>
<tr><td>-</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td rowspan="2">Elementi</td><td colspan="4">Informazione</td></tr>
<tr><td colspan="4">c:PartizioneCorrente, c:PartizionePrecedente</td></tr>
<tr><td>Elementi sovraordinati</td><td colspan="4">c:InformazioniPIndex</td></tr>
</table>

<table>
<tr><td colspan="5">elemento c:PartizioneCorrente</td></tr>
<tr><td>Descrizione</td><td colspan="4">Contiene informazioni relative a:
i progressivi di serie della prima e dell’ultima unità documentale del pacchetto;
date di versamento della prima e dell’ultima unità documentale della serie;</td></tr>
<tr><td>Diagramma</td><td colspan="4"></td></tr>
<tr><td rowspan="2">Attributi</td><td>Informazione</td><td>Valori ammessi</td><td>Tipo dato</td><td>Default</td></tr>
<tr><td>-</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td rowspan="2">Elementi</td><td colspan="4">Informazione</td></tr>
<tr><td colspan="4">c:Progressivi (suddiviso in c:MinimoProgressivo e c:MassimoProgressivo), c:Date (suddiviso in c:DataPrimaUnita e c:DataUltimaUnita)</td></tr>
</table>

Elementi sovraordinati	***c:InformazioniPartizioneSerie***

elemento ***c: Progressivi***				
Descrizione	Contiene informazioni relative a: • i progressivi di serie della prima e dell'ultima unità documentale del pacchetto.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	-	-	-
Elementi	**Informazione**			
	c:MinimoProgressivo, ***c:MassimoProgressivo***			
Elementi sovraordinati	***c:PartizioneCorrente***			

elemento ***c:Date***				
Descrizione	Contiene informazioni relative a: • date di versamento della prima e dell'ultima unità documentale della serie			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	-	-	-
Elementi	**Informazione**			
	c:DataPrimaUnita, ***c:DataUltimaUnita***			
Elementi sovraordinati	***c:PartizioneCorrente***			

elemento ***c:PartizionePrecedente***				
Descrizione	Contiene l'ID dell'indice del pacchetto di archiviazione nel caso in cui ci sia stata una migrazione.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	-	-	-
Elementi	**Informazione**			
	c:IDIndicePacchettoDiArchiviazione			
Elementi sovraordinati	***c:InformazioniPartizioneSerie***			

elemento ***c:IDIndicePacchettoDiArchiviazione***				
Descrizione	Identificativo dell'indice del pacchetto di archiviazione nel caso in cui ci sia stata una migrazione.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	-	-	-
Elementi	**Informazione**			
	-			
Elementi sovraordinati	***c:PartizionePrecedente***			

elemento ***sin:PVolume***				
Descrizione	Informazioni relative al volume di conservazione. Può coicidere con la serie documentale o l'unità archivistica.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	-	-	-
Elementi	**Informazione**			
	sin:ID, sin:Label, sin:Description, sin:PVolumeGroup			
Elementi sovraordinati	***sin:PIndex***			

<table>
<tr><td colspan="5">elemento sin:ID</td></tr>
<tr><td>Descrizione</td><td colspan="4">Elemento relativo all’identificazione univoca del volume di conservazione.
L’identificatore viene costruito secondo la seguente regola:

PVolume[idproduttore][anno][n]

• PVolume
• idproduttore: codice IPA o dominio del sito dell’ente inserito in fase di configurazione dell’ente;
• anno: anno di riferimento del PVolume;
• n: numero progressivo della successione PVolume[idproduttore][anno].

L’attributo sin:scheme definisce il dominio e preserva l’univocità dell’identificatore; al momento della redazione di questo documento ha valore fisso:
scheme=Conserva</td></tr>
<tr><td>Diagramma</td><td colspan="4"></td></tr>
<tr><td rowspan="2">Attributi</td><td>Informazione</td><td>Valori ammessi</td><td>Tipo dato</td><td>Default</td></tr>
<tr><td>sin:scheme</td><td>-</td><td>-</td><td>Conserva</td></tr>
<tr><td rowspan="2">Elementi</td><td colspan="4">Informazione</td></tr>
<tr><td colspan="4">-</td></tr>
<tr><td>Elementi sovraordinati</td><td colspan="4">sin:PVolume</td></tr>
</table>

<table>
<tr><td colspan="5">elemento sin:Label</td></tr>
<tr><td>Descrizione</td><td colspan="4">L’identificatore viene costruito secondo la seguente regola:

• per le serie documentali viene valorizzato con il codice della serie costruito con i dati del sistema mittente;
• per le unità archivistiche viene valorizzato con l’id del sistema mittente.</td></tr>
<tr><td>Diagramma</td><td colspan="4"></td></tr>
<tr><td rowspan="2">Attributi</td><td>Informazione</td><td>Valori ammessi</td><td>Tipo dato</td><td>Default</td></tr>
<tr><td></td><td>-</td><td>-</td><td>-</td></tr>
<tr><td rowspan="2">Elementi</td><td colspan="4">Informazione</td></tr>
<tr><td colspan="4">-</td></tr>
<tr><td>Elementi sovraordinati</td><td colspan="4">sin:PVolume</td></tr>
</table>

<table>
<tr><td colspan="5">elemento sin:Description</td></tr>
<tr><td>Descrizione</td><td colspan="4">Descrizione della composizione dell’entità cui si riferisce l’elemento.</td></tr>
<tr><td>Diagramma</td><td colspan="4"></td></tr>
<tr><td rowspan="2">Attributi</td><td>Informazione</td><td>Valori ammessi</td><td>Tipo dato</td><td>Default</td></tr>
<tr><td>-</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td rowspan="2">Elementi</td><td colspan="4">Informazione</td></tr>
<tr><td colspan="4">-</td></tr>
</table>

Elementi sovraordinati	***sin:PVolume***

elemento ***sin:PVolumeGroup***				
Descrizione	Informazione relativa ad un’aggregazione (di natura logica o fisica) cui il volume di conservazione appartiene.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	-	-	-
Elementi	**Informazione**			
	sin:ID, sin:Label, sin:Description			
Elementi sovraordinati	***sin:PVolume***			

<table>
<tr><td colspan="5">elemento sin:ID</td></tr>
<tr><td>Descrizione</td><td colspan="4">Elemento relativo all’identificazione univoca del volume di conservazione.
L’identificatore viene costruito secondo la seguente regola:

[idproduttore]-SD-[anno]-[n]

• idproduttore: codice IPA o dominio del sito dell’ente inserito in fase di configurazione dell’ente;
• SD: serie documentale
• anno: anno di riferimento della serie;
• n: numero progressivo della successione [idproduttore]-SD-[anno] .

L’attributo sin:scheme definisce il dominio e preserva l’univocità dell’identificatore; al momento della redazione di questo documento ha valore fisso:
scheme=Conserva</td></tr>
<tr><td>Diagramma</td><td colspan="4"></td></tr>
<tr><td rowspan="2">Attributi</td><td>Informazione</td><td>Valori ammessi</td><td>Tipo dato</td><td>Default</td></tr>
<tr><td>sin:scheme</td><td>-</td><td>-</td><td>Conserva</td></tr>
<tr><td rowspan="2">Elementi</td><td colspan="4">Informazione</td></tr>
<tr><td colspan="4">-</td></tr>
<tr><td>Elementi sovraordinati</td><td colspan="4">sin:PVolumeGroup</td></tr>
</table>

elemento ***sin:Label***				
Descrizione	• per le serie documentali viene valorizzato con il codice della serie costruito con i dati del sistema mittente; • per le unità archivistiche viene valorizzato con l'id del sistema mittente.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
		-	-	-
Elementi	**Informazione**			
	-			
Elementi sovraordinati	***sin:PVolumeGroup***			

elemento ***sin:Description***				
Descrizione	Descrizione della composizione dell'entità cui si riferisce l'elemento.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	-	-	-
Elementi	**Informazione**			
	-			
Elementi sovraordinati	***sin:PVolumeGroup***			

<table>
<tr><td colspan="5">elemento sin:FileGroup</td></tr>
<tr><td>Descrizione</td><td colspan="4">Elemento di aggregazione di più file oggetto di conservazione. In Conserva coincide con la singola unità documentale.</td></tr>
<tr><td>Diagramma</td><td colspan="4"></td></tr>
<tr><td rowspan="2">Attributi</td><td>Informazione</td><td>Valori ammessi</td><td>Tipo dato</td><td>Default</td></tr>
<tr><td>-</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td rowspan="2">Elementi</td><td colspan="4">Informazione</td></tr>
<tr><td colspan="4">sin:ID, sin:Label, sin:Description, sin:File</td></tr>
<tr><td>Elementi sovraordinati</td><td colspan="4">sin:PIndex</td></tr>
</table>

<table>
<tr><td colspan="5">elemento sin:ID</td></tr>
<tr><td>Descrizione</td><td colspan="4">Elemento relativo all’identificazione univoca del volume di conservazione.
L’identificatore viene costruito secondo la seguente regola:

[idproduttore]-UD-[anno]-[n]

• idproduttore: codice IPA o dominio del sito dell’ente inserito in fase di configurazione dell’ente;
• UD: unità documentale;
• anno: anno di riferimento della serie;
• n: numero progressivo della successione [idproduttore]-UD-[anno] .

L’attributo sin:scheme definisce il dominio e preserva l’univocità dell’identificatore; al momento della redazione di questo documento ha valore fisso:
scheme=Conserva</td></tr>
<tr><td>Diagramma</td><td colspan="4"></td></tr>
<tr><td rowspan="2">Attributi</td><td>Informazione</td><td>Valori ammessi</td><td>Tipo dato</td><td>Default</td></tr>
<tr><td>sin:scheme</td><td>-</td><td>-</td><td>Conserva</td></tr>
<tr><td rowspan="2">Elementi</td><td colspan="4">Informazione</td></tr>
<tr><td colspan="4">-</td></tr>
<tr><td>Elementi sovraordinati</td><td colspan="4">sin:FileGroup</td></tr>
</table>

elemento ***sin:Label***				
Descrizione	Identificativo univoco assegnato all'unità documentale dal sistema mittente.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	-	-	-
Elementi	**Informazione**			
	-			
Elementi sovraordinati	***sin:FileGroup***			

elemento ***sin:Description***				
Descrizione	Descrizione della tipologia relativa all'unità documentale.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	-	-	
Elementi	**Informazione**			
	-			
Elementi sovraordinati	***sin:FileGroup***			

<table>
<tr><td colspan="5">elemento sin:File</td></tr>
<tr><td>Descrizione</td><td colspan="4">Informazioni relative al file oggetto di conservazione.</td></tr>
<tr><td>Diagramma</td><td colspan="4"></td></tr>
<tr><td rowspan="4">Attributi</td><td>Informazione</td><td>Valori ammessi</td><td>Tipo dato</td><td>Default</td></tr>
<tr><td>sin:encoding</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td>sin:extension</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td>sin:format</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td rowspan="2">Elementi</td><td colspan="4">Informazione</td></tr>
<tr><td colspan="4">sin:ID, sin:Path, sin:Hash, sin:PreviousHash, sin:MoreInfo</td></tr>
<tr><td>Elementi sovraordinati</td><td colspan="4">sin:FileGroup</td></tr>
</table>

<table>
<tr><td colspan="5">elemento sin:ID</td></tr>
<tr><td>Descrizione</td><td colspan="4">Identificativo univoco del file.</td></tr>
<tr><td>Diagramma</td><td colspan="4"></td></tr>
<tr><td rowspan="3">Attributi</td><td>Informazione</td><td>Valori ammessi</td><td>Tipo dato</td><td>Default</td></tr>
<tr><td>sin:scheme</td><td>-</td><td>-</td><td>Conserva</td></tr>
<tr><td rowspan="2">Elementi</td><td colspan="4">Informazione</td></tr>
<tr><td colspan="4"></td></tr>
</table>

Elementi sovraordinati	***sin:File***

elemento ***sin:Path***				
Descrizione	Elemento relativo alla localizzazione del file.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	**-**	**-**	**-**
Elementi	**Informazione**			
Elementi sovraordinati	***sin:File***			

elemento ***sin:Hash***				
Descrizione	Elemento relativo all'impronta del file.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	sin:hashFunction	-	-	SHA-256

Elementi	Informazione
	-
Elementi sovraordinati	***sin:File***

elemento ***sin:PreviousHash***				
Descrizione	Impronta precedente del file oggetto di conservazione. Al momento della redazione di questo allegato non viene utilizzato.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	sin:canonicalXML	-	-	-
	sin:hashFunction	SHA-256	-	SHA-256
	sin:relatedPIndex	-	stringa	-
Elementi	**Informazione**			
	-			
Elementi sovraordinati	***c:File***			

elemento ***sin:MoreInfo***				
Descrizione	Metadati descrittivi del file e informazioni sulla verifica di firma.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	sin:xmlSchema	-	-	conserva-schema-pindex-v2.0.xsd
Elementi	**Informazione**			
	-			
Elementi sovraordinati	***sin:File***			

elemento ***c:EmbeddedMetadata***				
Descrizione	Elemento relativo alle informazioni dell'elemento <MoreInfo>, integrate all'interno dell'indice del pacchetto di archiviazione e strutturate nel formato XML. Per i file sono aggiunti: • metadati descrittivi del file; • informazioni sulla verifica della firma digitale.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	-	-	-
Elementi	**Informazione**			
	c:InformazioniFile			

Elementi sovraordinati	***c:MoreInfo***

elemento ***c:InformazioniFile***				
Descrizione	Metadati descrittivi del file.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	xmlns:c	-	-	http://conserva.cineca.it/xsd
Elementi	**Informazione**			
	c:NomeFile, c:VersioneFormato, c:Dimensione, c:PEMFile, c:MagicNumber, c:TipoPdfa, c:DettagliFirmaDigitale			
Elementi sovraordinati	***sin:EmbeddedMetadata***			

elemento ***c:NomeFile***				
Descrizione	Denominazione del file.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	-	-	-
Elementi	**Informazione**			

Elementi sovraordinati	***c:InformazioniFile***

elemento ***c:VersioneFormato***				
Descrizione	Versione del formato.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	**-**	**-**	**-**
Elementi	**Informazione**			
Elementi sovraordinati	***c:InformazioniFile***			

elemento ***c:Dimensione***				
Descrizione	Dimensione del file espressa in byte.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	-	-	-

Elementi	**Informazione**
Elementi sovraordinati	***c:InformazioniFile***

elemento ***c:PEMFile***				
Descrizione	Dichiara se il file è firmato in formato PEM (base64) Può assumere valori true o false.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	-	-	-
Elementi	**Informazione**			
Elementi sovraordinati	***c:InformazioniFile***			

elemento ***c:MagicNumber***				
Descrizione	Identificativo del formato del file.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	-	-	-
Elementi	**Informazione**			
Elementi sovraordinati	***c:InformazioniFile***			

elemento ***c:TipoPdfa***				
Descrizione	Dettaglio del file pdf. Elemento presente solo nel caso in cui il formato del sia pdf.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	-	-	-
Elementi	**Informazione**			
Elementi sovraordinati	***c:InformazioniFile***			

<table>
<tr><td colspan="5">elemento c:DettagliFirmaDigitale</td></tr>
<tr><td>Descrizione</td><td colspan="4">Informazioni sulla verifica della firma apposta sul file.</td></tr>
<tr><td>Diagramma</td><td colspan="4"></td></tr>
<tr><td rowspan="2">Attributi</td><td>Informazione</td><td>Valori ammessi</td><td>Tipo dato</td><td>Default</td></tr>
<tr><td>-</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td rowspan="2">Elementi</td><td colspan="4">Informazione</td></tr>
<tr><td colspan="4">-</td></tr>
<tr><td>Elementi sovraordinati</td><td colspan="4">c:InformazioniFile</td></tr>
</table>

elemento ***c:FirmaDigitale***				
Descrizione	Informazioni sulla firma.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	FormatoSottoscrizione	-	-	-
	ModalitaImbustamento	-	-	-
Elementi	**Informazione**			
	c:Validita, c:DataValidazione, c:RisultatoValidazioneElementoDiFirma			
Elementi sovraordinati	***c:DettagliFirmaDigitale***			

elemento ***c:Validita***				
Descrizione	Elemento che indica se la firma è VALIDA o NON VALIDA.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	-	-	-
Elementi	**Informazione**			

Elementi sovraordinati	***c:DettagliFirmaDigitale***

elemento ***c:DataValidazione***				
Descrizione	Riferimento temporale utilizzato per verificare la validità del certificate di firma.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	-	-	-
Elementi	**Informazione**			
Elementi sovraordinati	***c:DettagliFirmaDigitale***			

elemento ***c:RisultatoValidazioneElementoDiFirma***				
Descrizione	Dettagli relative all'esito della validazione			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**

	-	-	-	-
Elementi	**Informazione**			
	c:SignatureId, c:DataValidazione con attributo ***DaMarcaturaTemporale, c:Validita, c:DataFirma, c:RisultatoValidazioneCertificato***			
Elementi sovraordinati	***c:FirmaDigitale***			

elemento ***c:RisultatoValidazioneCertificato***				
Descrizione	Dettagli relative alla validazione del certificate di firma.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	DataValidazione	-	Data	-
Elementi	**Informazione**			
	c:Soggetto con sottoelementi ***c:Country***, ***c:DNQualifier***, ***c:NameAndSurname***, ***c:SerialNumber***, ***c:LastName*** e ***c:FirstName***			
	c:Emittente con sottoelementi ***c:Country***, ***c:Organization***, ***c:OrganizationalUnit***, ***c:CommonName*** e ***c:SerialNumber***			
	c:ValiditaTemporale con sottoelementi ***c:NonPrima*** e ***c:NonDopo***			
	c:Validita			
Elementi sovraordinati	***c:RisultatoValidazioneElementoDiFirma***			

<table>
<tr><td colspan="5">elemento sin:MoreInfo</td></tr>
<tr><td>Descrizione</td><td colspan="4">Elemento contenitore di informazioni ulteriori, relative all’elemento padre di <MoreInfo>, che non è possibile associare ad altri elementi. È strutturato come gli altri elementi <MoreInfo>. Attualmente ne viene valorizzato solo l’<EmbeddedMetadata>.
L’attributo @XMLScheme riporta la localizzazione dello Schema XML della struttura di metadati; il valore deve essere espresso nella forma di URL. Al momento della redazione di questo documento ha valore fisso:
XMLScheme= conserva-schema-pindex-v2.0.xsd</td></tr>
<tr><td>Diagramma</td><td colspan="4"></td></tr>
<tr><td rowspan="2">Attributi</td><td>Informazione</td><td>Valori ammessi</td><td>Tipo dato</td><td>Default</td></tr>
<tr><td>sin:xmlSchema</td><td>-</td><td>-</td><td>conserva-schema-pindex-v2.0.xsd</td></tr>
<tr><td rowspan="2">Elementi</td><td colspan="4">Informazione</td></tr>
<tr><td colspan="4">sin:EmbeddedMetadata</td></tr>
<tr><td>Elementi sovraordinati</td><td colspan="4">c:FileGroup</td></tr>
</table>

<table>
<tr><td colspan="5">elemento sin:Process</td></tr>
<tr><td>Descrizione</td><td colspan="4">Informazioni relative alla modalità di svolgimento del processo di creazione dell’indice di conservazione.</td></tr>
<tr><td>Diagramma</td><td colspan="4"></td></tr>
<tr><td>Attributi</td><td>Informazione</td><td>Valori ammessi</td><td>Tipo dato</td><td>Default</td></tr>
</table>

	-	-	-	-
Elementi	**Informazione**			
	sin:Submitter, sin:Holder con attributo ***sin:holderRole*** obbligatorio, ***sin:AuthorizedSigner*** con attributo ***sin:signerRole, sin:TimeReference, sin:LawsAndRegulations*** fissato sulla normativa vigente, ***sin:MoreInfo***			
Elementi sovraordinati	***sin:PIndex***			

elemento ***sin:Submitter***				
Descrizione	Informazioni relative al soggetto che effettua il trasferimento fisico degli oggetti digitali nel Sistema di conservazione.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	sin:agentType	-	-	Legal person
Elementi	**Informazione**			
	sin:AgentID, sin:AgentName, sin:RelevantDocument			
Elementi sovraordinati	***Sin:Process***			

<table>
<tr><td colspan="5">elemento sin:Agent</td></tr>
<tr><td>Descrizione</td><td colspan="4">Elemento che riporta le informazioni relative ad un soggetto che interviene nel processo di creazione dell’indice di conservazione.
Ha come attributo sin:agentType (indica se il soggetto è una persona fisica o giuridica)</td></tr>
<tr><td>Diagramma</td><td colspan="4"></td></tr>
<tr><td rowspan="2">Attributi</td><td>Informazione</td><td>Valori ammessi</td><td>Tipo dato</td><td>Default</td></tr>
<tr><td>sin:agentType</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td rowspan="2">Elementi</td><td colspan="4">Informazione</td></tr>
<tr><td colspan="4">sin:AgentID, sin:AgentName, sin:RelevantDocument, sin:MoreInfo</td></tr>
<tr><td>Elementi sovraordinati</td><td colspan="4">sin:Submitter</td></tr>
<tr><td></td><td colspan="4">sin:Holder</td></tr>
<tr><td></td><td colspan="4">sin:AuthorizedSigner</td></tr>
</table>

<table>
<tr><td colspan="5">elemento sin:AgentID</td></tr>
<tr><td>Descrizione</td><td colspan="4">Identificatore univoco del soggetto che interviene nel processo di creazione dell’indice di conservazione.</td></tr>
<tr><td>Diagramma</td><td colspan="4"></td></tr>
<tr><td rowspan="2">Attributi</td><td>Informazione</td><td>Valori ammessi</td><td>Tipo dato</td><td>Default</td></tr>
<tr><td>sin:nameRegistrationAuthority</td><td>-</td><td>-</td><td>-</td></tr>
</table>

Elementi	Informazione
	-
Elementi sovraordinati	***sin:Submitter***

elemento ***sin:AgentName***				
Descrizione	Denominazione del soggetto che interviene nel processo di creazione dell'indice di conservazione. Nel caso di persona giuridica ha come elemento ***sin:FormalName*** altrimenti ha come element ***sin:NameAndSurname***			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	**-**	**-**	**-**
Elementi	**Informazione**			
	sin:FormalName, sin:NameAndSurname			
Elementi sovraordinati	***sin:Submitter***			

elemento ***sin:RelevantDocument***				
Descrizione	Riferimento ad un documento rilevante del soggetto che interviene nel processo di conservazione. Secondo questa versione dell'indice, Conserva lo valorizza indicando il manuale di conservazione dell'ente titolare dell'oggetto di conservazione.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	**-**	**-**	**-**
Elementi	**Informazione**			
Elementi sovraordinati	***sin:Submitter***			

elemento ***sin:Holder***				
Descrizione	Informazioni relative al soggetto detentore o proprietario degli oggetti digitali trasferiti nel Sistema di conservazione.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	sin:agentType	-	-	legal person
	sin:signerRole	Soggetto proprietario	-	-

Elementi	Informazione
	sin:AgentID, sin:AgentName, sin:RelevantDocument
Elementi sovraordinati	***Sin:Process***

elemento ***sin:AgentID***				
Descrizione	Identificatore univoco del soggetto detentore o proprietario degli oggetti digitali trasferiti nel Sistema di conservazione..			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	sin:nameRegistrationAuthority	-	-	-
Elementi	**Informazione**			
	-			
Elementi sovraordinati	***sin:Holder***			

elemento ***sin:AgentName***				
Descrizione	Denominazione del soggetto detentore o proprietario degli oggetti digitali trasferiti nel Sistema di conservazione.. Nel caso di persona giuridica ha come elemento ***sin:FormalName*** altrimenti ha come elemento ***sin:NameAndSurname***			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	**-**	**-**	**-**
Elementi	**Informazione**			
	sin:FormalName, sin:NameAndSurname			
Elementi sovraordinati	***sin:Holder***			

elemento ***sin:RelevantDocument***				
Descrizione	Riferimento ad un documento rilevante del soggetto che interviene nel processo di conservazione. Secondo questa versione dell'indice, Conserva lo valorizza indicando: • il Manuale della Conservazione del titolare dell'oggetto di conservazione; • il Manuale della Gestione Documentale del titolare dell'oggetto di conservazione.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	**-**	**-**	**-**

Elementi	Informazione
	-
Elementi sovraordinati	***sin:Holder***

elemento ***sin:AuthorizedSigner***				
Descrizione	Informazioni relative al soggetto autorizzato ad apporre la firma elttronica (avanzata o qualificata) o il sigillo elettronico (avanzato o qualificato) sull'indice di conservazione, a conclusione del processo di creazione dell'indice. Secondo questa versione dell'indice l'elemento viene ripetuto indicando: • il responsabile della conservazione del titolare dell'oggetto di conservazione; • il responsabile del servizio di conservazione.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	sin:agentType	-	-	natural person
	sin:signerRole	PreservationManager Delegate	-	-
Elementi	**Informazione**			
	sin:AgentID, sin:AgentName, sin:RelevantDocument			
Elementi sovraordinati	***Sin:Process***			

elemento ***sin:AgentID***				
Descrizione	Identificatore univoco del soggetto autorizzato ad apporre la firma elettronica o il sigillo elettronico sull'indice di conservazione, a conclusion del processo di creazione dell'indice.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	sin:nameRegistrationAuthority	-	-	-
Elementi	**Informazione**			
	-			
Elementi sovraordinati	***sin:AuthorizedSigner***			

elemento ***sin:AgentName***				
Descrizione	Soggetto autorizzato ad apporre la firma elettronica o il sigillo elettronico sull'indice di conservazione, a conclusion del processo di creazione dell'indice. Ha come elemento ***sin:NameAndSurname*** che a sua volta contiene gli elementi ***sin:FirstName*** e ***sin:LastName*** valorizzati con il nome e il cognome del responsabile della conservazione del titolare dell'oggetto di conservazione e con il nome e cognome del responsabile del servizio di conservazione.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**

	-	-	-	-
Elementi	**Informazione**			
	sin:NameAndSurname *con* elementi ***sin:FirstName*** e ***sin:LastName***			
Elementi sovraordinati	***sin:AuthorizedSigner***			

elemento ***sin:RelevantDocument***				
Descrizione	Riferimento ad un documento rilevante del soggetto autorizzato ad apporre la firma elettronica o il sigillo elettronico sull'indice di conservazione, a conclusione del processo di creazione dell'indice. Secondo questa versione dell'indice, Conserva lo valorizza indicando: • il Manuale della Gestione Documentale del titolare dell'oggetto di conservazione. • il Manuale della Conservazione del conservatore Cineca.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	-	-	-
Elementi	**Informazione**			
	-			
Elementi sovraordinati	***sin:AuthorizedSigner***			

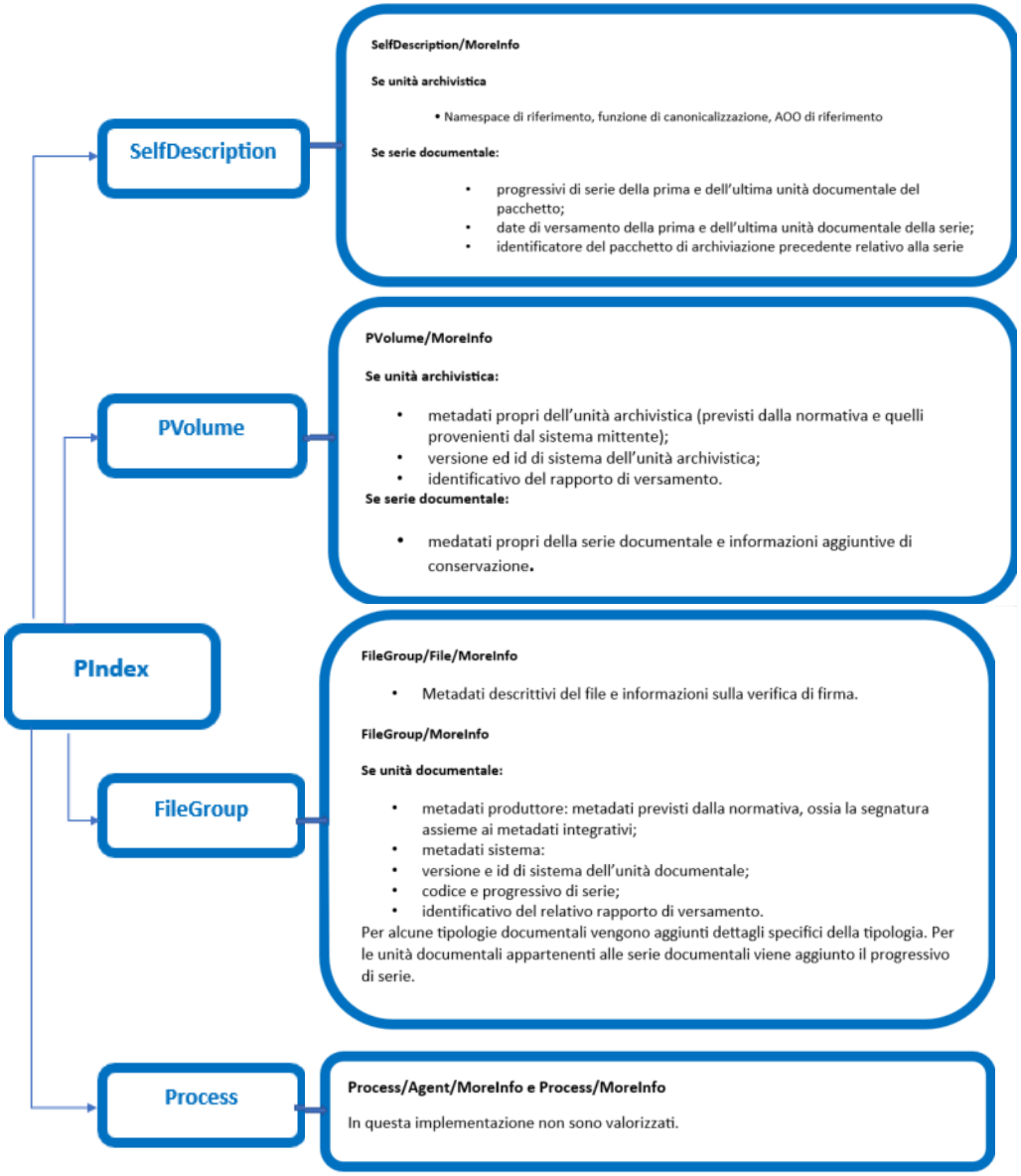
elemento ***sin:TimeReference***				
Descrizione	Informazioni di data e ora relative alla chiusura dell'indice di conservazione.			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	-	-	-
Elementi	**Informazione**			
	sin:TimeInfo			
	sin:TimeStamp			
Elementi sovraordinati	***sin:Process***			

elemento ***sin:TimeInfo***				
Descrizione	Informazioni di data e ora relative alla chiusura dell'indice di conservazione, sottoforma di marca temporale collegata attached. Il formato in cui vengono espressi la data e l'ora secondo la seguente sintassi yyyy-MM-dd 'T' HH:mm:ss			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**

	sin:attachedTimeStamp	-	-	-
Elementi	**Informazione**			
	-			
Elementi sovraordinati	***sin: TimeReference***			

elemento ***sin: LawsAndRegulations***				
Descrizione	Norme, regolamenti e standard che guidano il processo di creazione dell'indice di conservazione. Secondo questa versione dell'indice l'elemento viene valorizzato indicando le "Linee guida per la formazione, gestione e conservazione dei documenti informatici".			
Diagramma				
Attributi	**Informazione**	**Valori ammessi**	**Tipo dato**	**Default**
	-	-	-	-
Elementi	**Informazione**			
Elementi sovraordinati	***sin:Process***			

Sintesi della valorizzazione degli elementi MoreInfo all'interno dell'indice



Esempio Indice Pacchetto di Distribuzione

Di seguito viene riportato un esempio di indice del pacchetto di distribuzione, il quale, viene generato dal sistema di conservazione Conserva, in maniera analoga al pacchetto di archiviazione, ossia sempre rispettando le specifiche dello standard UniSinCRO ai fini di supportare l'interoperabilità con altri sistemi di conservazione.


```
<sin:PIndex xmlns:sin="http://www.uni.com/U3011/sincro-v2/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" sin:language="IT"
sin:sincroVersion="2.0" sin:uri="http://www.uni.com/U3011/sincro-v2/PIndex.xsd" xsi:schemaLocation="http://www.uni.com/U3011/sincro-v2/
conserva-schema-uni-sincro-v2.0.xsd">
        <sin:SelfDescription>
                <sin:ID sin:scheme="Conserva">PIndexDEMOCONSERVA2023DU0000007</sin:ID>
                <sin:CreatingApplication>
                        <sin:Name>Conserva</sin:Name>
                        <sin:Version>2.0</sin:Version>
                        <sin:Producer>CINECA Consorzio Interuniversitario</sin:Producer>
                </sin:CreatingApplication>
                <sin:PIndexSource sin:derivation="onetoone">
                        <sin:ID sin:scheme="Conserva">PIndexDEMOCONSERVA20230000005</sin:ID>
                        <sin:Path>PIndexDEMOCONSERVA20230000005.xml</sin:Path>
                        <sin:Hash sin:canonicalXML="true" sin:hashFunction="SHA-
256">5q0R8/XBQgmKaPYlJSz5jIwc2uLd95ro4xoPon9tpCA=</sin:Hash>
                </sin:PIndexSource>
                <sin:MoreInfo sin:xmlSchema="conserva-schema-pindex-v2.0.xsd">
                        <sin:EmbeddedMetadata>
                                <c:InformazioniPIndex xmlns:c="http://conserva.cineca.it/xsd">
                                        <c:FunzioneDiCanonicalizzazione>http://www.w3.org/2001/10/xml-exc-
c14n#</c:FunzioneDiCanonicalizzazione>
                                        <c:AOO>
                                                <c:CodiceAOO>ADM</c:CodiceAOO>
                                        </c:AOO>
                                        <c:InformazioniPartizioneSerie>
                                                <c:PartizioneCorrente>
                                                        <c:Progressivi>
```

```
                                                <c:MinimoProgressivo>257</c:MinimoProgressivo>
                                                <c:MassimoProgressivo>257</c:MassimoProgressivo>
                                        </c:Progressivi>
                                        <c:Date>
                                                <c:DataPrimaUnita>2023-09-14+02:00</c:DataPrimaUnita>
                                                <c:DataUltimaUnita>2023-09-14+02:00</c:DataUltimaUnita>
                                        </c:Date>
                                </c:PartizioneCorrente>
                                <c:PartizionePrecedente>
                                        <c:IDIndicePacchettoDiArchiviazione>DEMOCONSERVA-IPDA-2023-
0000005</c:IDIndicePacchettoDiArchiviazione>
                                </c:PartizionePrecedente>
                        </c:InformazioniPartizioneSerie>
                </c:InformazioniPIndex>
        </sin:EmbeddedMetadata>
    </sin:MoreInfo>
</sin:SelfDescription>
<sin:PVolume>
    <sin:ID sin:scheme="Conserva">PVolumeDEMOCONSERVA2023DU0000007</sin:ID>
    <sin:Label>RIPG-RIPG^ADMNADM-2023</sin:Label>
    <sin:Description>Unità Documentale di tipologia Registro informatico di protocollo</sin:Description>
    <sin:PVolumeGroup>
        <sin:ID sin:scheme="Conserva">DEMOCONSERVA-SD-2023-0000003</sin:ID>
        <sin:Label>RIPG-RIPG^ADMNADM-2023</sin:Label>
        <sin:Description>RIPG-SERIE</sin:Description>
    </sin:PVolumeGroup>
</sin:PVolume>
<sin:FileGroup>
    <sin:ID sin:scheme="Conserva">DEMOCONSERVA-UD-2023-0010726</sin:ID>
    <sin:Label>000224774-ADMNTTT-5c12e357-f44a-465f-a477-1bca981e64d5</sin:Label>
    <sin:Description>Unità Documentale di tipologia Registro informatico di protocollo</sin:Description>
    <sin:File sin:encoding="binary" sin:extension="xml" sin:format="application/xml">
        <sin:ID sin:scheme="Conserva">65086c4f63ddaf010d09dcab</sin:ID>
        <sin:Path>DEMOCONSERVA-UD-2023-0010726/ADMNTTT_20230913.xml</sin:Path>
        <sin:Hash sin:hashFunction="SHA-256">foab+d+JdcgnmDnB/mlAAHSHdI1iNEpuht3b3BC6/7Q=</sin:Hash>
        <sin:MoreInfo sin:xmlSchema="conserva-schema-pindex-v2.0.xsd">
            <sin:EmbeddedMetadata>
```

<c:InformazioniFile xmlns:c="http://conserva.cineca.it/xsd">
<c:NomeFile>ADMNTTT_20230913.xml</c:NomeFile>
<c:VersioneFormato>1.0</c:VersioneFormato>
<c:Dimensione>420</c:Dimensione>
<c:PEMFile>false</c:PEMFile>
<c:MagicNumber>3C3F786D6C</c:MagicNumber>
</c:InformazioniFile>
</sin:EmbeddedMetadata>
</sin:MoreInfo>
</sin:File>
<sin:MoreInfo sin:xmlSchema="conserva-schema-pindex-v2.0.xsd">
<sin:EmbeddedMetadata>
<c:InformazioniUnitaDocumentale xmlns:c="http://conserva.cineca.it/xsd">
<c:MetadatiProduttore>
<c:MetadatiInterni XMLSchema="conserva-schema-unita-versamento-v1.1.xsd">
<UnitaDocumentale xmlns="http://conserva.cineca.it/xsd" Tipologia="RIPG">
<DocumentoAmministrativoInformatico IDDocumento="000224774-ADMNTTT-5c12e357-
f44a-465f-a477-1bca981e64d5">
<Segnatura xmlns="http://www.digitPa.gov.it/protocollo/">
<Intestazione>
<Identificatore>
<CodiceAmministrazione>ADMN</CodiceAmministrazione>
<CodiceAOO>ADM</CodiceAOO>
<CodiceRegistro>RIPG^ADMNADM</CodiceRegistro>
<NumeroRegistrazione>257</NumeroRegistrazione>
<DataRegistrazione>2023-09-14</DataRegistrazione>
</Identificatore>
<Origine>
<IndirizzoTelematico
tipo="smtp">n.d.</IndirizzoTelematico>
<Mittente>
<Amministrazione>
<Denominazione>PRODUTTORE DI
TEST</Denominazione>
<UnitaOrganizzativa>

<Denominazione>Amministra</Denominazione>

<Ruolo>
<Denominazione>Responsabile del procedimento amministrativo</Denominazione>
<Persona>
<Denominazione>Amministratore Amministratore</Denominazione>
</Persona>
</Ruolo>
<IndirizzoPostale>
<Denominazione>n.d.</Denominazione>
</IndirizzoPostale>
<IndirizzoTelematico>cineca@cineca.it</IndirizzoTelematico>
</UnitaOrganizzativa>
</Amministrazione>
<AOO>
<Denominazione>Amministrazione</Denominazione>
</AOO>
</Mittente>
</Origine>
<Destinazione confermaRicezione="no">
<IndirizzoTelematico>n.d.</IndirizzoTelematico>
</Destinazione>
<Oggetto>Registro informatico di protocollo del giorno 13/09/2023 dell'AOO 'TEST'</Oggetto>
<Classifica>
<Denominazione>01/07 - Archivio</Denominazione>
<Livello>01</Livello>
<Livello>07</Livello>
</Classifica>
<Note/>
</Intestazione>
<Descrizione>
<Documento id="ID-000141102-FS_FILES-c2925a3c-40d0-420c-8473-0d7cd80a9990.xml" nome="ADMNTTT_20230913.xml" tipoMIME="application/xml" tipoRiferimento="telematico">

<CollocazioneTelematica>000141102-FS_FILES-c2925a3c-
40d0-420c-8473-0d7cd80a9990[1].xml</CollocazioneTelematica>
<Impronta algoritmo="SHA-
256">foab+d+JdcgnmDnB/mlAAHSHdI1iNEpuht3b3BC6/7Q=</Impronta>
<TitoloDocumento>ADMNTTT_20230913.xml</TitoloDocumento>
<PiuInfo XMLSchema="conserva-titulus-schema-v1.xsd">
<MetadatiInterni>
<t:doc
xmlns:t="http://www.kion.it/ns/titulus">
<t:Firmato>no</t:Firmato>
<t:Clonato>no</t:Clonato>
</t:doc>
</MetadatiInterni>
</PiuInfo>
</Documento>
</Descrizione>
<segnatura:PiuInfo
xmlns:segnatura="http://www.digitPa.gov.it/protocollo/" XMLSchema="titulus-documento-generico_v1.xsd">
<segnatura:MetadatiInterni>
<UlterioriInformazioni
xmlns="http://www.kion.it/ns/titulus">
<Voce_indice>RIPg (Registro Informatico giornaliero
di protocollo) - TTT</Voce_indice>
<registro periodicita="giornaliero" tipo="Registro
informatico di protocollo" versione="1.0">
<codice_aoo>TTT</codice_aoo>
<data_prima_registrazione>2023-09-
13</data_prima_registrazione>
<data_ultima_registrazione>2023-09-
13</data_ultima_registrazione>
<registrazioni anno="2023"
cod_reg="ADMNTTT" numero_annullamenti="0" numero_registrazioni="0"/>
</registro>
<destinatario>Amministra (SI000005) -
Amministratore Amministratore (1)</destinatario>
</UlterioriInformazioni>

```
                                                                    </segnatura:MetadatiInterni>
                                                                </segnatura:PiuInfo>
                                                            </Segnatura>
                                                            <MetadatiIntegrativi>
                                                                <DatiRegistrazione>
                                                                    <TipoRegistrazione>Non protocollato</TipoRegistrazione>

        <RiferimentoTemporaleDaProtocollo>false</RiferimentoTemporaleDaProtocollo>
                                                                    <IdentificatoreSecondario>
                                                                        <TipoRegistro>Registro informatico giornaliero di
protocollo</TipoRegistro>
                                                                        <segnatura:CodiceRegistro
xmlns:segnatura="http://www.digitPa.gov.it/protocollo/">RIPG</segnatura:CodiceRegistro>
                                                                        <segnatura:NumeroRegistrazione
xmlns:segnatura="http://www.digitPa.gov.it/protocollo/">RIPG^ADMNTTT-20230000257</segnatura:NumeroRegistrazione>
                                                                        <segnatura:DataRegistrazione
xmlns:segnatura="http://www.digitPa.gov.it/protocollo/">2023-09-14</segnatura:DataRegistrazione>
                                                                    </IdentificatoreSecondario>
                                                                </DatiRegistrazione>
                                                                <Storia>
                                                                    <Evento>
                                                                        <segnatura:Denominazione
xmlns:segnatura="http://www.digitPa.gov.it/protocollo/">creazione</segnatura:Denominazione>
                                                                        <Agente>
                                                                            <segnatura:Denominazione
xmlns:segnatura="http://www.digitPa.gov.it/protocollo/"> Applicazione Titulus</segnatura:Denominazione>
                                                                        </Agente>
                                                                        <Data>2023-09-14T00:10:14</Data>
                                                                        <segnatura:Note
xmlns:segnatura="http://www.digitPa.gov.it/protocollo/"> Versione Titulus: 04.06.15.00 Applicativo Produttore: Applicazione
RIP_G</segnatura:Note>
                                                                    </Evento>
                                                                    <Evento>
                                                                        <segnatura:Denominazione
xmlns:segnatura="http://www.digitPa.gov.it/protocollo/">assegnazione per competenza</segnatura:Denominazione>
                                                                        <Agente>
```

<segnatura:Denominazione xmlns:segnatura="http://www.digitPa.gov.it/protocollo/">1 Amministratore Amministratore</segnatura:Denominazione>
</Agente>
<Data>2023-09-14T00:10:14</Data>
<segnatura:Note xmlns:segnatura="http://www.digitPa.gov.it/protocollo/">1 Amministratore Amministratore (Amministra) è responsabile del procedimento amministrativo Versione Titulus: 04.06.15.00</segnatura:Note>
</Evento>
</Storia>
<DescrizioneAllegati>0 - nessun allegato,
</DescrizioneAllegati>
<SelezionePerScarto ConservazioneIllimitata="true">
<Anni>9999</Anni>
</SelezionePerScarto>
</MetadatiIntegrativi>
</DocumentoAmministrativoInformatico>
</UnitaDocumentale>
</c:MetadatiInterni>
</c:MetadatiProduttore>
<c:MetadatiDiSistema>
<c:IDSistema>DEMOCONSERVA-UD-2023-0010726</c:IDSistema>
<c:Versione>1</c:Versione>
<c:Tipologia ID="RIPG" Versione="1.0">Registro informatico di protocollo</c:Tipologia>
<c:AOO>
<c:CodiceAOO>ADM</c:CodiceAOO>
</c:AOO>
<c:SelezionePerScarto ConservazioneIllimitata="true"/>
<c:IDRapportoDiVersamento>DEMOCONSERVA-RDV-2023-0001970</c:IDRapportoDiVersamento>
<c:Serie>
<c:IDSerie>RIPG-RIPG^ADMNADM-2023</c:IDSerie>
<c:Progressivo>257</c:Progressivo>
</c:Serie>
</c:MetadatiDiSistema>
</c:InformazioniUnitaDocumentale>
</sin:EmbeddedMetadata>
</sin:MoreInfo>
</sin:FileGroup>

```
<sin:Process>
	<sin:Submitter sin:agentType="legal person">
		<sin:AgentID sin:nameRegistrationAuthority="Agenzia delle Entrate">TINIT-12345678901</sin:AgentID>
		<sin:AgentName>
			<sin:FormalName>Conserva Ambiente Demo</sin:FormalName>
		</sin:AgentName>
		<sin:RelevantDocument>Manuale della Conservazione dell'ente: Conserva Ambiente Demo</sin:RelevantDocument>
	</sin:Submitter>
	<sin:Holder sin:agentType="legal person" sin:holderRole="soggetto proprietario">
		<sin:AgentID sin:nameRegistrationAuthority="Agenzia delle Entrate">TINIT-12345678901</sin:AgentID>
		<sin:AgentName>
			<sin:FormalName>Conserva Ambiente Demo</sin:FormalName>
		</sin:AgentName>
		<sin:RelevantDocument>Manuale della Conservazione dell'ente: Conserva Ambiente Demo</sin:RelevantDocument>
		<sin:RelevantDocument>Manuale della Gestione Documentale dell'ente: Conserva Ambiente Demo</sin:RelevantDocument>
	</sin:Holder>
	<sin:AuthorizedSigner sin:agentType="natural person" sin:signerRole="PreservationManager">
		<sin:AgentID sin:nameRegistrationAuthority="Agenzia delle Entrate">TINIT-RSPDLC80M48B880X</sin:AgentID>
		<sin:AgentName>
			<sin:NameAndSurname>
				<sin:FirstName>Responsabile</sin:FirstName>
				<sin:LastName>della Conservazione</sin:LastName>
			</sin:NameAndSurname>
		</sin:AgentName>
		<sin:RelevantDocument>Manuale della Gestione Documentale dell'ente: Conserva Ambiente Demo</sin:RelevantDocument>
	</sin:AuthorizedSigner>
	<sin:AuthorizedSigner sin:agentType="natural person" sin:signerRole="Delegate">
		<sin:AgentID sin:nameRegistrationAuthority="Agenzia delle Entrate">TINIT-XXXYYY76M21F205H</sin:AgentID>
		<sin:AgentName>
			<sin:NameAndSurname>
				<sin:FirstName>Responsabile del</sin:FirstName>
				<sin:LastName>Servizio di Conservazione</sin:LastName>
			</sin:NameAndSurname>
		</sin:AgentName>
		<sin:RelevantDocument>Manuale della Conservazione del conservatore CINECA Consorzio
Interuniversitario</sin:RelevantDocument>
	</sin:AuthorizedSigner>
```

```
            <sin:TimeReference>
                  <sin:TimeInfo sin:attachedTimeStamp="false">2023-11-03T00:07:19.603+01:00</sin:TimeInfo>
            </sin:TimeReference>
            <sin:LawsAndRegulations>Linee guida per la formazione, gestione e conservazione dei documenti
informatici</sin:LawsAndRegulations>
      </sin:Process>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="IpddSignature">
            <ds:SignedInfo>
                  <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2006/12/xml-c14n11"/>
                  <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
                  <ds:Reference Id="r-id-IpddSignature-0" URI="">
                        <ds:Transforms>
                              <ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
                                    <dsig-xpath:XPath xmlns:dsig-xpath="http://www.w3.org/2002/06/xmldsig-filter2"
Filter="subtract">/descendant::ds:Signature</dsig-xpath:XPath>
                              </ds:Transform>
                              <ds:Transform Algorithm="http://www.w3.org/2006/12/xml-c14n11"/>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                        <ds:DigestValue>5sDqOY3YHSfgfHSVxpk1dgLMLKRjwjWn4BESyulom64=</ds:DigestValue>
                  </ds:Reference>
                  <ds:Reference Type="http://uri.etsi.org/01903#SignedProperties" URI="#IpddSignatureSignedProperties">
                        <ds:Transforms>
                              <ds:Transform Algorithm="http://www.w3.org/2006/12/xml-c14n11"/>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                        <ds:DigestValue>pY7dPSTPFf9BV/fyOCj4KrcmLqH8myCkqOdtI0N1UdE=</ds:DigestValue>
                  </ds:Reference>
                  <ds:Reference Id="r-id-IpddSignature-KeyInfo" URI="#IpddSignatureKeyInfo">
                        <ds:Transforms>
                              <ds:Transform Algorithm="http://www.w3.org/2006/12/xml-c14n11"/>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                        <ds:DigestValue>iHUUVHn5buTslJFDU/30tdplMDi9/aEB7/xoP3NX2bs=</ds:DigestValue>
                  </ds:Reference>
            </ds:SignedInfo>
```

```
<ds:SignatureValue Id="IpddSignatureValue">
  ……..
</ds:SignatureValue>
<ds:KeyInfo Id="IpddSignatureKeyInfo">
    <ds:X509Data>
        <ds:X509Certificate>
            ……
        </ds:X509Certificate>
    </ds:X509Data>
</ds:KeyInfo>
<ds:Object>
    <xades:QualifyingProperties xmlns:xades="http://uri.etsi.org/01903/v1.3.2#" Target="#IpddSignature">
        <xades:SignedProperties Id="IpddSignatureSignedProperties">
            <xades:SignedSignatureProperties>
                <xades:SigningTime>2023-11-02T23:07:19Z</xades:SigningTime>
                <xades:SigningCertificate>
                    <xades:Cert>
                        <xades:CertDigest>
                            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<ds:DigestValue>3iVv7QwG2HxyjdqCSGbqOJXNOEwPskOVJAnHoICVskA=</ds:DigestValue>
                        </xades:CertDigest>
                        <xades:IssuerSerial>
                            <ds:X509IssuerName>CN=Namirial CA Firma Qualificata,OU=Certification
Authority,O=Namirial S.p.A./02046570426,C=IT</ds:X509IssuerName>
                            <ds:X509SerialNumber>5851693192785762014</ds:X509SerialNumber>
                        </xades:IssuerSerial>
                    </xades:Cert>
                </xades:SigningCertificate>
            </xades:SignedSignatureProperties>
            <xades:SignedDataObjectProperties>
                <xades:DataObjectFormat ObjectReference="#r-id-IpddSignature-0">
                    <xades:MimeType>application/xml</xades:MimeType>
                </xades:DataObjectFormat>
                <xades:DataObjectFormat ObjectReference="#r-id-IpddSignature-KeyInfo">
                    <xades:MimeType>application/xml</xades:MimeType>
                </xades:DataObjectFormat>
```

```
                                        </xades:SignedDataObjectProperties>
                                    </xades:SignedProperties>
                                    <xades:UnsignedProperties>
                                        <xades:UnsignedSignatureProperties>
                                            <xades:SignatureTimeStamp>
                                                <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2006/12/xml-c14n11"/>
                                                <xades:EncapsulatedTimeStamp
Encoding="http://uri.etsi.org/01903/v1.2.2#DER">MIAGCSqGSIb3DQEHAqCAMII……
                                            </xades:SignatureTimeStamp>
                                        </xades:UnsignedSignatureProperties>
                                    </xades:UnsignedProperties>
                                </xades:QualifyingProperties>
                            </ds:Object>
                        </ds:Signature>
</sin:PIndex>
```

Manuale di Conservazione

Allegato 4 – Mezzi di trasmissione

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**	**01/12/2015**	**P. Vandelli**	**Titolari dell'oggetto di conservazione, Personale Cineca, AGID**

STATO/STORIA DELLE REVISIONI

Versione	Data	Paragrafo revisionato	Oggetto dalla revisione	Autore/i principale della revisione	Altri contributi	Validato
1.3	26/10/2022	Intestazione	Modificato ente certificatore ed aggiornato il relativo logo	M. Mingrone	-	M. Valente
1.2	29/11/2021	2.	Aggiornamento delle modalità di invio del pacchetto e ricezione dello stato	M. Mingrone N. Carofiglio	A. De Angelis	M. Valente
1.1	22/04/2016		Revisione a seguito delle	Laura Nisi		P. Vandelli

			osservazioni dello Studio Lisi			
1.0	01/12/2015		Emissione	Laura Nisi	F. Merighi	P. Vandelli

Sommario

1. Modalità di invio dei documenti in conservazione

L'invio al sistema di conservazione Conserva può avvenire tramite due modalità:

- Tramite l'uso di web service;
- Tramite interfaccia web in Conserva

Qui di seguito la descrizione dettagliata delle due possibilità di invio dei documenti.

1.1 Invio del pacchetto di versamento tramite l'uso di web service

Conserva mette a disposizione un web service che espone dei metodi finalizzati al trasferimento dei pacchetti di versamento e all'interrogazione del loro stato all'interno del sistema di conservazione.
Il web service utilizza il meccanismo di ottimizzazione della trasmissione dei messaggi *MTOM* (Message Transmission Optimization Mechanism) che consente di trasmettere allegati binari di grandi dimensioni.
Il web service accetta il trasferimento del pacchetto di versamento in due modalità:

- modalità non compressa (*PacchettoDiVersamentoCompresso*);
- modalità compressa (*PacchettoDiVersamento*).

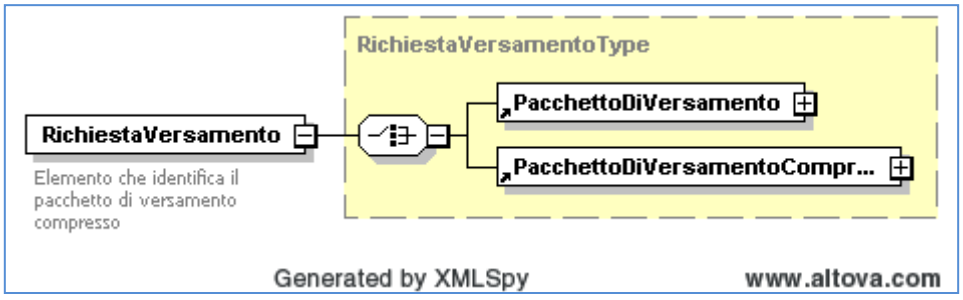


Figura A4.1 – Tipo di richiesta di versamento

La modalità di invio in conservazione di pacchetti non compressi è adatta a pacchetti di versamento composti da un numero limitato di file, di dimensione inferiore ai 20 MB.

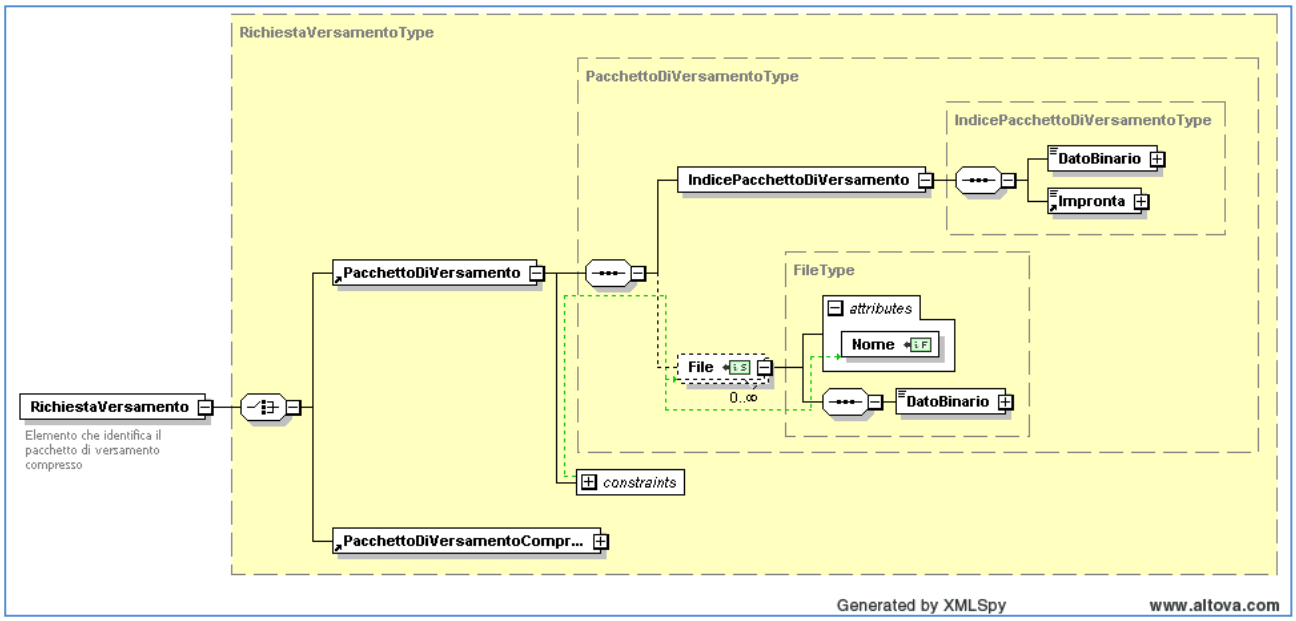


Figura A4.2 – Richiesta di versamento di un pacchetto di versamento non compresso

In questa modalità, il metodo del web service richiede come parametri in ingresso:

- l'indice del pacchetto di versamento (*IndicePacchettoDiVersamento*) rappresentato dal formato binario (*DatoBinario*) e dalla sua impronta (*Impronta*);
- i file (*File*) che compongono le unità documentali contenute nel pacchetto di versamento.

La modalità di invio in conservazione di pacchetti compressi è adatta a pacchetti di versamento composti da un numero elevato di file e/o da file di dimensione superiore ai 20 MB.

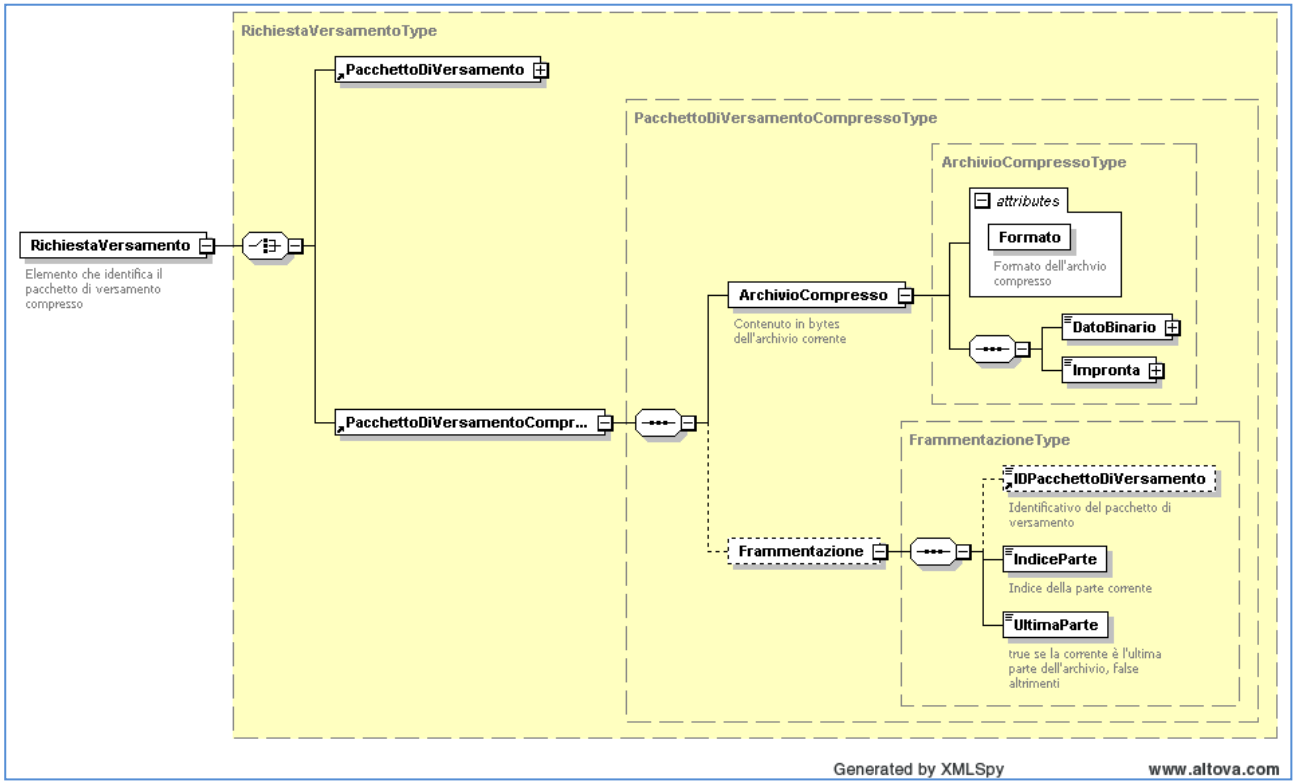


Figura A4.3 - Richiesta di versamento di un pacchetto di versamento compresso

In questa modalità, il metodo del web service richiede come parametri in ingresso:

- le cartelle compresse (*ArchivioCompresso*) rappresentato dal formato binario (*DatoBinario*) e dalla sua impronta (*Impronta*).

Qualora le cartelle compresse superassero i 20 MB è possibile suddividerle in più parti (*Frammentazione*) e inviarle al sistema di conservazione separatamente.

In questo caso nella richiesta di versamento andrà specificato:

- la parte corrente delle cartelle compresse (*ArchivioCompresso*) rappresentata in formato binario e la sua impronta;
- le informazioni di frammentazione (*Frammentazione*) ovvero:
  - l'identificativo assegnato al pacchetto di versamento (*IDPacchettoDiVersamento*), se la parte da mandare in conservazione non è la prima inviata (in quanto al primo invio non si ha ancora l'id che ti viene restituito in risposta); per le partizioni successive

l'identificativo corrisponde a quello ottenuto in risposta all'invio della prima porzione;

- l'indice del progressivo numerico (*IndiceParte*) della parte inviata;
- l'indicazione, nel caso lo fosse, che la partizione inviata sia l'ultima delle cartelle compresse (*UltimaParte*).

Al termine dell'invio il servizio fornisce l'identificativo assegnato al pacchetto di versamento (*IDPacchettoDiVersamento*) e le relative informazioni presenti all'interno del sistema di conservazione come:

- la posizione (*Stato*) del pacchetto all'interno del processo di versamento;
- la data e l'ora in cui è iniziato (*InizioTrasferimento*) il trasferimento del pacchetto di versamento dal sistema del titolare dell'oggetto di conservazione al sistema di conservazione;
- la data e l'ora in cui è terminato (*FineTrasferimento)* il trasferimento del pacchetto di versamento dal sistema del titolare dell'oggetto di conservazione al sistema di conservazione;
- il numero di cartelle compresse (*ArchiviCompressiRicevuti)* componenti il pacchetto di versamento ricevute dal sistema.

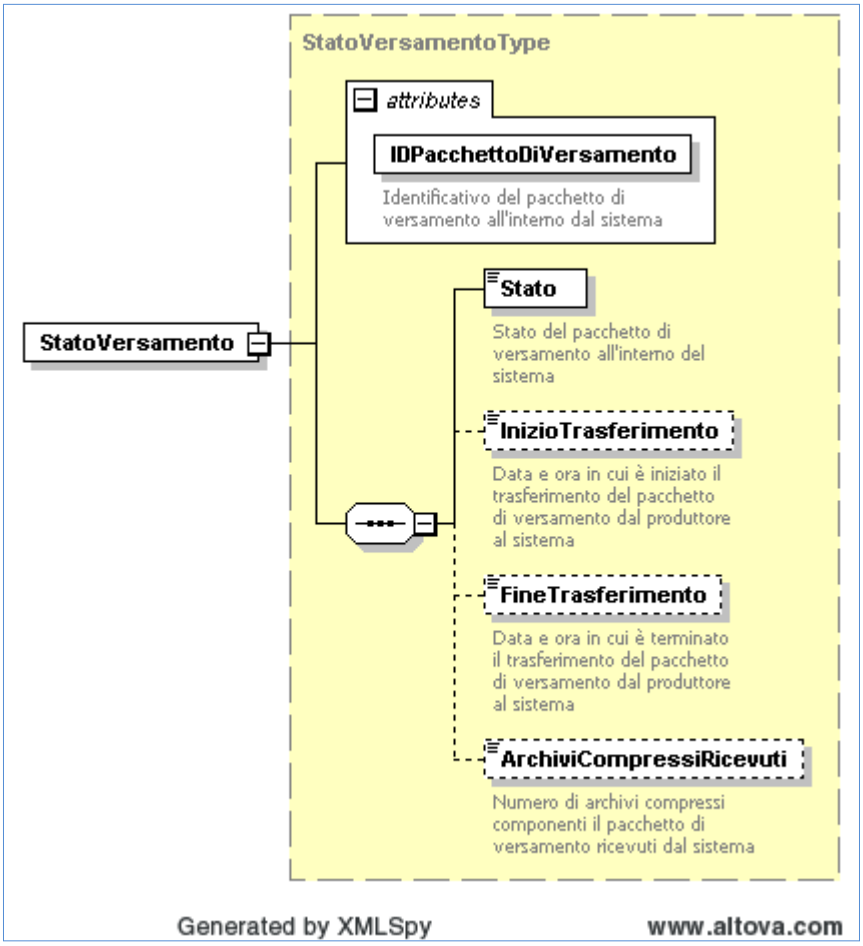


Figura A4.4 Stato del versamento

In caso di fallimento del trasferimento il servizio invia un codice e un messaggio di errore descritto nell'Allegato 6 Controlli sul pacchetto di versamento (in particolare Controlli eseguiti in fase di trasferimento).

1.2 Invio del pacchetto di versamento tramite interfaccia web in Conserva

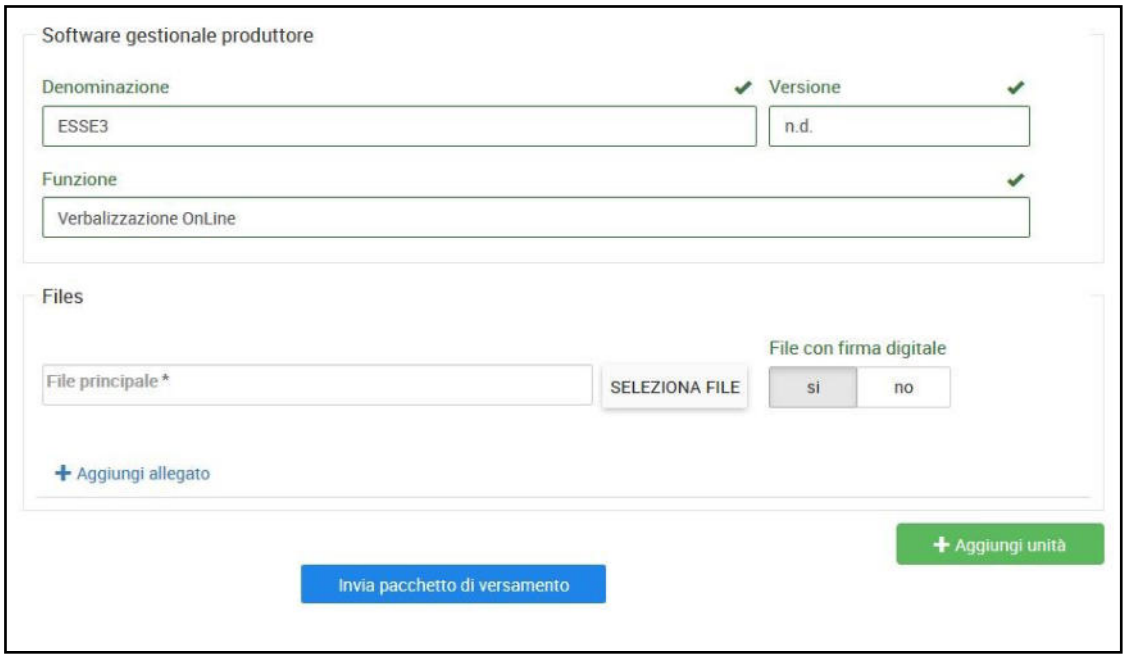
L'invio del pacchetto può essere effettuato caricando manualmente i documenti tramite interfaccia Conserva.

Selezionando dal cruscotto il pannello *"Gestione Versamento"* tramite la funzione *"Invia pacchetti"* è possibile generare pacchetti di versamento tramite upload dei documenti da interfaccia.

La funzione è resa disponibile solo previa richiesta di attivazione da parte dell'ente.

Per caricare i singoli documenti è necessario eseguire i seguenti passaggi:

- selezionare la tipologia di documento di interesse
- compilare i campi che contengono i metadati che confluiranno all'interno dell'indice del pacchetto di versamento
- aggiungere nella sezione inferiore della maschera il file principale del documento che si vuole inviare in conservazione e, se presenti, anche eventuali allegati



2. Interrogazione dello stato del pacchetto di versamento

Una volta che il pacchetto di versamento è stato versato è possibile reperire informazioni sullo stato di avanzamento e sull'esito del processo di conservazione. Esistono due modalità di richiesta di tali informazioni, qui di seguito descritte.

2.1 Polling – Richiesta periodica dell'esito dell'ingestion

Il web service che espone i metodi di trasferimento del pacchetto di versamento mette a disposizione anche due metodi per interrogare il sistema sullo stato del pacchetto trasferito. Una volta completato il trasferimento del pacchetto, il web service fornisce al chiamante l'identificativo assegnato al pacchetto all'interno del sistema. Fornendo nuovamente in input questo identificativo è possibile richiedere al sistema:

- lo **stato del pacchetto di versamento** in cui valori e relative descrizioni sono riportati in *Tabella 1*;
- il **resoconto del pacchetto di versamento** descritto in *Tabella 2*.

STATO DEL PACCHETTO DI VERSAMENTO	**VALORE**	**DESCRIZIONE**
Il web service fornisce al chiamante informazioni sul pacchetto di versamento senza entrare nel merito delle unità che compongono il pacchetto stesso. In particolare le risposte che possono esser date al chiamante sono i valori presenti nella seconda colonna.	*NON ESISTENTE*	tipicamente in caso di invio errato dell'input;
	IN TRASFERIMENTO	quando ancora non è terminato il trasferimento del pacchetto di versamento;
	DA DECOMPRIMERE	quando il pacchetto inviato è compresso ed è in attesa di essere decompresso all'interno del sistema;
	IN DECOMPRESSIONE	quando il pacchetto inviato è compresso ed è in fase di decompressione;
	DA SPACCHETTARE	quando il pacchetto inviato era compresso, è stato decompresso ed è in attesa di essere spacchettato;

		oppure quando il pacchetto inviato non compresso è in attesa di essere spacchettato;
	IN SPACCHETTAMENTO	quando il pacchetto inviato è in fase di spacchettamento;
	DA VALIDARE	quando il pacchetto inviato è in attesa di essere validato;
	IN VALIDAZIONE	quando il pacchetto inviato è in fase di validazione;
	RIFIUTATO	quando tutte le unità di versamento del pacchetto inviato sono state rifiutate;
	PARZIALMENTE VERSATO	quando parte delle unità di versamento del pacchetto inviato sono state versate e parte sono state rifiutate;
	INTERAMENTE VERSATO	quando tutte le unità di versamento del pacchetto inviato sono state versate.

Figura A4.5 – Tabella 1

IL RESOCONTO DI VERSAMENTO	**STATO-VALORE**	**DESCRIZIONE**
Il web service fornisce al chiamante, oltre allo stato del pacchetto, anche le informazioni relative alle singole unità che lo compongono. Tutte le unità hanno: • l'*id di provenienza* che è l'identificativo dato dal soggetto produttore/titolare dell'oggetto di conservazione alla risorsa; • l'*id di sistema* che è l'identificativo dato dal sistema di conservazione;	*DA VALIDARE*	l'unità di versamento del pacchetto inviato è in attesa di essere validato;
	DA REVISIONARE	l'unità di versamento del pacchetto inviato non ha superato dei controlli forzabili;
	RIFIUTATA	l'unità di versamento del pacchetto inviato è stata rifiutata;
	RIFIUTATA DAL RDC	l'unità di versamento del pacchetto inviato viene ritirata dal Responsabile della Conservazione prima della mezzanotte;
	VERSATA	l'unità di versamento del pacchetto inviato è correttamente versata;
	CONSERVATA	l'unità di versamento del pacchetto inviato è conservata in un pacchetto di archiviazione chiuso.

• la *data* del versamento; • il *risultato della* validazione per ogni unità; • lo *stato* che può assumere i valori presenti nella seconda colonna.		

Figura A4.6 – Tabella 2

Poiché la richiesta del resoconto di versamento è dal punto di vista computazionale più onerosa, al fine di non sovraccaricare il sistema si consiglia di richiedere lo stato del pacchetto e solo successivamente, nel caso in cui il pacchetto sia stato parzialmente o completamente rifiutato, richiedere il resoconto di versamento.

2.2 Pushing – Conserva notifica al sistema mittente l'esito delle varie fasi dell'ingestion

La seconda modalità disponibile per avere informazioni sul pacchetto di versamento prevede che il sistema mittente esponga un web service che rispetti precise specifiche imposte da Conserva e che consenta al sistema mittente di prendere in carico le notifiche provenienti dal sistema di conservazione. Quando l'attività di ingestion cambia di stato, Conserva notifica al titolare dell'oggetto di conservazione uno degli eventi elencati in *Tabella 3*:

STATO DEL PACCHETTO DI VERSAMENTO	VALORE	DESCRIZIONE
Il web service fornisce al chiamante informazioni sul pacchetto di versamento senza entrare nel merito delle unità che compongono il pacchetto stesso. In particolare le	*RIFIUTATO*	quando tutte le unità di versamento del pacchetto inviato sono state rifiutate
	PARZIALMENTE VERSATO	quando parte delle unità di versamento del pacchetto inviato sono state versate e parte sono state rifiutate;

risposte che possono esser date al chiamante sono i valori presenti nella seconda colonna.	*INTERAMENTE VERSATO*	quando tutte le unità di versamento del pacchetto inviato sono state versate.

Figura A4.7 – Tabella 3