



Manuale del Servizio di Conservazione di **ZUCCHETTI S.p.a.**

Zucchetti spa
via Solferino, 1 | 26900 Lodi
Tel 0371 594 1

www.zucchetti.it

R.I. / C.F. e P.IVA n. 05006900962
R.E.A. n. LO-1458208
Capitale Sociale € 6.300.000,00 i.v.
Società ad azionista unico

Coordinate Bancarie:
BANCO BPM S.p.A. | Sede di Lodi
IBAN: IT 41 N 05034 20301 000000398566
Intesa Sanpaolo spa | Sede di Lodi
IBAN: IT 92 B 03069 20310 100000011898



EMISSIONE DEL DOCUMENTO

| Azione | Data | Nominativo | Funzione |
|---------------------|------------|------------------|---|
| Redazione | 1/07/2015 | Maurizio Bonetta | <i>Responsabile sviluppo e manutenzione</i> |
| Verifica | 15/07/2015 | Angelo Cian | <i>Responsabile sistemi informativi conservazione</i> |
| Approvazione | 28/07/2015 | Paolo Camia | <i>Responsabile servizio conservazione</i> |

REGISTRO DELLE VERSIONI

| N°Ver/Rev/Bozza | Data emissione | Codice interno documento |
|-----------------|----------------|--|
| 1.0 | 28/07/2015 | MSC.ver.1.0_manuale_servizio_conservazione |

| N°Ver/Rev/Bozza | Data emissione | Codice interno documento |
|----------------------------|--|--|
| 1.1 | 15/01/2016 | MSC.ver.1.1_manuale_servizio_conservazione |
| Modifiche apportate | a) Adeguamento alle linee guida per l'accessibilità dettate dallo "Schema di manuale di conservazione v.2"; b) Revisione grafica. c) Inserimento della definizione di titolare | |
| Osservazioni | Le variazioni sono state apportate secondo quanto previsto dal punto 1.2 del presente manuale. | |

| N°Ver/Rev/Bozza | Data emissione | Codice interno documento |
|----------------------------|---|--|
| 1.2 | 12/07/2018 | MSC.ver.1.2_manuale_servizio_conservazione |
| Modifiche apportate | a) Adeguamento riferimenti normativi, privacy e standard di riferimento; b) Aggiornamento dei riferimenti alle certificazioni; c) Revisione grafica e correzione refusi; d) Aggiornamento scheda classi documentali non standard; e) Aggiornamento procedura di gestione incidenti. | |
| Osservazioni | Le variazioni sono state apportate secondo quanto previsto dal punto 1.2 del presente manuale. | |

Sommario

| | |
|---|-----------|
| Emissione del documento..... | 2 |
| Registro delle versioni..... | 3 |
| 1. SCOPO E AMBITO DEL DOCUMENTO..... | 6 |
| 1.1 Trattamento dei dati personali e degli oggetti digitali conservati | 7 |
| 1.2 Versione del Manuale | 8 |
| 2. TERMINOLOGIA (GLOSSARIO, ACRONIMI)..... | 9 |
| 3. NORMATIVA E STANDARD DI RIFERIMENTO..... | 21 |
| 3.1 Normativa di riferimento | 21 |
| 3.2 Certificazioni del conservatore | 22 |
| 4. RUOLI E RESPONSABILITÀ | 24 |
| 5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE | 28 |
| 5.1 Organigramma | 28 |
| 5.2 Dati di riferimento del Conservatore, della CA e della TSA..... | 30 |
| 5.2.1 Dati identificativi del Conservatore..... | 30 |
| 5.2.2 Presentazione del Conservatore | 30 |
| 5.2.3 Dati identificativi della CA e TSA | 31 |
| 5.3 Ruoli del sistema di conservazione | 31 |
| 5.4 Fasi del sistema di conservazione..... | 34 |
| 5.4.1 Processo di avviamento del sistema di conservazione..... | 35 |
| 5.4.2 Pre-Vendita / Commerciale | 36 |
| 5.4.3 Contrattuale | 37 |
| 5.4.4 Attivazione | 37 |
| 6. OGGETTI SOTTOPOSTI A CONSERVAZIONE | 38 |
| 6.1 Oggetti conservati..... | 40 |
| 6.2 Metadati da associare alle diverse tipologie di documenti | 42 |
| 6.3 Formati gestiti..... | 42 |
| 6.4 Caratteristiche generali dei formati | 43 |
| 6.5 Formati per la conservazione | 44 |
| 6.6 Controlli sui formati..... | 46 |
| 6.7 Migrazione dei formati | 47 |
| 6.8 Utilizzo di formati di compressione..... | 47 |
| 6.9 Pacchetti informativi | 48 |
| 6.10 Pacchetto di versamento..... | 48 |
| 6.11 Pacchetto di archiviazione | 58 |
| 6.12 Pacchetto di distribuzione | 68 |
| 7. IL PROCESSO DI CONSERVAZIONE..... | 77 |
| 7.1 Modalità di acquisizione dei pacchetti di versamento | 78 |
| 7.2 Verifiche effettuate sui pacchetti di versamento | 79 |
| 7.3 Accettazione dei pacchetti di versamento e generazione del rapporto di versamento | 80 |

| | | |
|------------|---|------------|
| 7.4 | Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie | 81 |
| 7.5 | Preparazione e gestione del pacchetto di archiviazione | 82 |
| 7.6 | Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione | 84 |
| 7.7 | Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti | 85 |
| 7.8 | Scarto dei pacchetti di archiviazione..... | 86 |
| 7.9 | Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori..... | 87 |
| 8. | IL SISTEMA DI CONSERVAZIONE | 88 |
| 8.1 | Componenti Logiche e tecnologiche | 89 |
| 8.2 | Componenti fisiche | 91 |
| 8.3 | Procedure di gestione e di evoluzione | 92 |
| 8.3.1 | Conduzione e manutenzione del sistema di conservazione..... | 93 |
| 8.3.2 | Gestione e conservazione dei log..... | 94 |
| 8.3.3 | Change mangement | 95 |
| 8.3.4 | Verifica periodica di conformità a normativa e standard di riferimento | 97 |
| 9. | MONITORAGGIO E CONTROLLI | 98 |
| 9.1 | Procedure di monitoraggio | 98 |
| 9.2 | Verifica dell'integrità degli archivi..... | 99 |
| 9.3 | Soluzioni adottate in caso di anomalie | 100 |
| 10. | CANCELLAZIONE DEI DOCUMENTI | 101 |
| 10.1 | Richiesta del Titolare di cancellazione dei documenti | 102 |
| 10.2 | Richiesta di conferma via pec della cancellazione..... | 102 |
| 10.3 | Conferma del Produttore/Titolare alla cancellazione..... | 102 |
| 10.4 | Eliminazione dei documenti | 102 |

1. SCOPO E AMBITO DEL DOCUMENTO

Il presente documento è il **Manuale di conservazione** di Zucchetti S.p.a. e descrive il servizio di conservazione di archivi digitali prodotti da soggetti terzi, illustrando dettagliatamente l'organizzazione, i ruoli, le funzioni e le responsabilità dei soggetti coinvolti, il modello di funzionamento, la descrizione del processo di conservazione, la descrizione dell'architettura e dell'infrastruttura utilizzata, le misure di sicurezza adottate e ogni altra informazione utile alla gestione ed alla verifica del funzionamento, nel tempo, del sistema di conservazione digitale di documenti informatici realizzato da Zucchetti S.p.a..

Il presente Manuale di conservazione, (d'ora in poi "Manuale"), viene pubblicato a garanzia dell'affidabilità del servizio di conservazione digitale di dati e documenti informatici erogato da Zucchetti S.p.a. nei confronti dei Produttori che lo utilizzano.

Il sistema di conservazione di Zucchetti S.p.a. assicura, tramite l'adozione delle regole, delle procedure e delle tecnologie di seguito descritte, la conservazione dei dati e degli oggetti informatici in esso conservati, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità.

Costituiscono oggetti della conservazione:

- i documenti informatici e i documenti amministrativi informatici con i metadati ad essi associati;
- i fascicoli informatici ovvero le aggregazioni documentali informatiche con i metadati ad essi associati, contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che appartengono al fascicolo o all'aggregazione documentale.

Le componenti funzionali del sistema di conservazione di Zucchetti S.p.a. sono in grado di assicurare il trattamento dell'intero ciclo di gestione degli oggetti conservati nell'ambito del processo di conservazione, garantendo, al contempo, l'accesso al Cliente (come di seguito definito) agli oggetti conservati per il periodo prescritto dalla norma o concordato con quest'ultimo nel contratto di servizio e ciò, indipendentemente dall'evolversi del contesto tecnologico.

Nel presente documento vengono inoltre illustrate le caratteristiche degli applicativi e delle strutture informatico-sistemistiche che implementano, presidiano e gestiscono i processi di conservazione.

Le attività di sviluppo, di governo e di presidio del sistema di conservazione sono state assegnate a figure professionali altamente qualificate, dotate delle necessarie competenze in tema di formazione, gestione e conservazione di documenti informatici, della necessaria conoscenza della normativa domestica e delle relative regole tecniche in tema di gestione e conservazione di documenti informatici, con particolare riferimento alle regole contenute nel DPCM 3.12.2013 (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).

Il presente Manuale recepisce altresì 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 "**Normativa di riferimento**" nonché i provvedimenti di natura tecnica richiamati nel capitolo "**Standard di riferimento**".

Il presente Manuale è depositato presso l'Agenzia per l'Italia Digitale, è un documento informatico prodotto nel formato PDF/A, su cui è apposta la firma digitale del Responsabile del Servizio di Conservazione ed è conservato presso la Zucchetti S.p.a. secondo le disposizioni di cui al DPCM 3.12.2013.

Una copia del presente Manuale è raggiungibile previa autenticazione anche al seguente link <https://conservazionedigitale.zucchetti.it/infinitycodi>.

Relativamente ad alcune fasi del processo di conservazione si rimanda alle condizioni generali per il servizio di conservazione e all'ordine per la fornitura del servizio di conservazione, quest'ultimo redatto dal Conservatore sulla base delle informazioni condivise con il Produttore dei documenti, contenente i requisiti essenziali del Servizio, le relative specifiche tecnico-funzionali e procedurali per le varie fasi del servizio (attivazione, versamento, conservazione, post-produzione, distribuzione, cessazione) oltre ai livelli di Servizio (SLA); tale documento è redatto in fase di pre-analisi, prima dell'avvio del processo di conservazione. Ogni variazione delle modalità di erogazione del Servizio di conservazione, dovuta a specifiche richieste del Produttore e/o a evoluzioni del sistema di conservazione, può comportare la necessità di aggiornare l'Allegato B – Scheda servizio - Specificità del contratto. L'allegato in questione viene redatto con riferimento alle caratteristiche contenute nel contratto stipulato con il cliente; per tale motivo, essendo un documento fortemente personalizzato e particolarmente riservato non viene allegato al presente manuale ma fa parte degli accordi contrattuali.

[Torna al sommario](#)

1.1 Trattamento dei dati personali e degli oggetti digitali conservati

Ai sensi e per gli effetti dell'articolo 28 del Regolamento UE 2016/679, relativamente e limitatamente ai trattamenti riguardanti la conservazione degli oggetti digitali affidati in conservazione a Zucchetti S.p.a., a partire dalla data di sottoscrizione del contratto di affidamento del servizio, il produttore/titolare dei suddetti oggetti digitali, a norma di quanto disposto dall'art. 6, co. 8, del DPCM 3.12.2013, nomina Zucchetti S.p.a. quale Responsabile esterno del trattamento dei dati.

Tale nomina viene formalizzata con un apposito documento che contiene anche le politiche di Zucchetti S.p.a. in tema di privacy

La nomina a Responsabile esterno del trattamento dei dati avrà la medesima validità ed efficacia della durata del Contratto di servizio

[Torna al sommario](#)

1.2 Versione del Manuale

Eventuali modifiche e aggiornamenti al presente Manuale saranno effettuate dal Responsabile del servizio di Conservazione, previa condivisione con il:

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

Come versione corrente del Manuale si intenderà esclusivamente la versione in formato elettronico disponibile sul sito dell'Agenzia per l'Italia Digitale. Il **codice interno** di questo documento è riportato sul frontespizio.

Il Produttore è tenuto a leggere con la massima attenzione il presente Manuale predisposto da Zucchetti S.p.a..

Il produttore dei dati e degli oggetti informatici conservati presso Zucchetti S.p.a., e per lui il Responsabile della conservazione, approvano e fanno propri i contenuti del presente Manuale.

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, 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 di servizio, da intendersi, pertanto, qui interamente riportate e trascritte, nonché le seguenti:

| Glossario dei Termini | |
|---|--|
| 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 |
| Affidabilità | Caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico |
| Agente di Alterazione | Sono agenti di alterazione le macro, i codici eseguibili nascosti, le formule di foglio di lavoro nascoste o difficili da individuare, sequenze di caratteri nascoste all'interno dei dati le quali sono ignorate dall'applicazione originalmente prevista per la presentazione, che però possono essere riconosciute quando i dati vengano elaborati con altre applicazioni |
| 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 |
| Applicativo | E' il software utilizzato nel sistema di conservazione |
| Archivio | Complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un Produttore durante lo svolgimento dell'attività |

| | |
|--|--|
| Archivio informatico | Archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico |
| Area organizzativa omogenea | Un insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445 e s.m.i. |
| Area documentale o pre-ingest | Area che non fa parte del sistema di conservazione. Si tratta di un insieme di funzionalità che consente al Produttore di predisporre i propri documenti informatici da inviare al sistema di conservazione |
| 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 |
| Audit | È una valutazione volta a ottenere prove, relativamente ad un determinato oggetto, e valutarle con obiettività, al fine di stabilire in quale misura i criteri prefissati siano stati soddisfatti o meno |
| Audit dei documenti | È una valutazione volta a ottenere prove, relativamente ad un determinato documento informatico, e valutarle con obiettività, al fine di stabilire in quale misura i criteri prefissati siano stati soddisfatti o meno. Si tratta di un'attività che riguarda i documenti informatici presenti nel sistema di conservazione |
| Audit periodico dei documenti | È una valutazione volta a ottenere prove, relativamente ad un determinato documento informatico, e valutarle con obiettività, al fine di stabilire in quale misura i criteri prefissati siano stati soddisfatti o meno. Si tratta di un'attività che riguarda i documenti informatici presenti nel sistema di conservazione effettuata con una periodicità minima stabilita dalla normativa in materia di conservazione digitale |
| 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 |

| | |
|---|---|
| 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 o Chiusura della conservazione | Operazione consistente nella sottoscrizione del pacchetto di archiviazione con firma digitale apposta da un Firmatario Delegato di Zucchetti S.p.a. e apposizione di una validazione temporale con marca temporale alla relativa impronta |
| Classe documentale | Un insieme di oggetti e/o documenti informatici che condividono una o più proprietà quali ad esempio la tipologia, i metadati, ecc. |
| Classificazione | Attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati |
| Cliente | È il soggetto che sottoscrive il contratto di affidamento del servizio di conservazione erogato da Zucchetti S.p.a.. Può coincidere con il Produttore e/o con il Titolare. |
| 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 di dati e documenti informatici al quale sia stato riconosciuto dall'Agenzia per l'Italia Digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza |
| 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 |
| Contratto di servizio | E' il Contratto per l'affidamento del servizio di conservazione digitale di documenti informatici perfezionato tra Zucchetti S.p.a. ed il Cliente che regola gli aspetti generali dell'erogazione del Servizio di conservazione digitale dei documenti informatici del Titolare |

| | |
|---|---|
| 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 analogica del documento informatico | Documento analogico avente contenuto identico a quello del documento informatico 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 |
| Dati personali | Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale |
| Dati sensibili | Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale |
| Destinatario | Identifica il soggetto/sistema al quale il documento informatico è indirizzato |
| 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 | È 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 elettronico | Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva |
| Documento informatico | Il documento elettronico che contiene 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 |
| Esibizione | Operazione che consente di visualizzare un documento conservato e di ottenerne copia |
| 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 di firma elettronica tramite la chiave privata e a un soggetto terzo 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 |
| Firma elettronica | Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare |
| Firma elettronica avanzata | Una firma elettronica che soddisfi i requisiti di cui all'articolo 26 del Regolamento n. 910/2014 (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 |
| Firmatario delegato | Responsabile del servizio di conservazione o Persona formalmente delegata ad apporre la propria firma digitale sul Pacchetto di archiviazione per conto di Zucchetti S.p.a.; questa persona può essere interna o esterna a Zucchetti S.p.a., laddove giuridicamente possibile |
| Formato | Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file |

| | |
|---|--|
| Fornitore esterno | Organizzazione che fornisce a Zucchetti S.p.a. servizi relativi al suo sistema di conservazione dei documenti |
| Fruibilità di un dato | La possibilità di utilizzare il dato anche trasferendolo nei sistemi informativi automatizzati di un'altra amministrazione |
| 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 |
| 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 |
| Immagine Iso | File immagine contenente l'intero contenuto o parte di un archivio, può essere usato direttamente (tramite software di emulazione) oppure scritto su un supporto ottico tramite il processo di masterizzazione. L'estensione del file immagine è .iso (deriva dallo standard ISO 9660) |
| 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 |
| Linee Guida | Le regole tecniche e di indirizzo adottate secondo il procedimento di cui all'art. 71 del CAD |
| 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 |
| 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 |
| Memorizzazione | Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici |
| Metadati | Insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione |
| Normativa regolante la conservazione digitale di documenti informatici | 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 ed aggiungendo, per il documento informatico a rilevanza tributaria, le disposizioni di cui al DMEF 17 giugno 2014 e s.m.i., il DPR 633/1972 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 presente Manuale di conservazione |
| Pacchetto di distribuzione | Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta |
| Pacchetto di versamento | Pacchetto informativo inviato dal Produttore al sistema di conservazione, secondo un formato predefinito e concordato, descritto nel Manuale di conservazione |

| | |
|--|--|
| Pacchetto informativo | Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, 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. |
| Piano generale della sicurezza | Documento per la pianificazione delle attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza |
| Posta elettronica certificata o PEC | Sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici, ove previsto |
| 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 |
| Prestatore di servizi fiduciari | Una persona fisica o giuridica che presta uno o più servizi fiduciari, o come prestatore di servizi fiduciari qualificato o come prestatore di servizi fiduciari non qualificato |
| Prestatore di servizi fiduciari qualificato | Un prestatore di servizi fiduciari che presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato |
| Processo di conservazione | Insieme delle attività finalizzate alla conservazione dei documenti informatici |
| Processo/servizio di marcatura temporale | È 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 |

| | |
|--|--|
| Processo schedulato | Esecuzione di un processo informatico programmato che non necessita di intervento umano. Si tratta di processi ripetitivi che iniziano in relazione a determinate modalità. |
| Produttore | Persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con il responsabile della gestione documentale |
| Rapporto di versamento | Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal Produttore |
| Rapporto di rifiuto | Documento informatico che attesta il rifiuto da parte del sistema di conservazione dei documenti contenuti nel Pacchetto di versamento |
| 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 |
| 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, ai sensi dell'art. 61 del Testo Unico, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione |

| | |
|--|---|
| Responsabile della conservazione | È la persona fisica, presente all'interno dell'organizzazione del titolare dei documenti informatici, responsabile dell'insieme delle attività elencate nell'articolo 8 comma 1 delle regole tecniche del sistema di conservazione (DPCM 3.12.2013). Nella fattispecie, è il responsabile dell'insieme delle attività finalizzate alla conservazione a norma dei documenti informatici versati in conservazione nell'ambito della fornitura del servizio conservazione digitale fornito da Zucchetti S.p.a. |
| Responsabile del Servizio di conservazione | È Zucchetti S.p.a. che opera attraverso uno o più persone fisiche formalmente incaricate all'esecuzione dell'insieme delle attività finalizzate alla conservazione a norma dei documenti informatici nell'ambito della fornitura del servizio di conservazione erogato ai propri clienti |
| Responsabile del trattamento dei dati | La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali |
| Responsabile della sicurezza | Soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza |
| Riferimento temporale | Informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione 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 |
| Scadenario di lavorazione | Successione nei tempi di una determinata attività. |
| Servizio di conservazione dei documenti informatici | È il Servizio di conservazione digitale dei documenti informatici fornito da Zucchetti S.p.a. che risponde all'esigenza dell'ente Produttore di avere i documenti informatici conservati nel rispetto della normativa vigente per il periodo di tempo specificato nel Contratto di servizio |
| Sistema di classificazione | Strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata |
| Sistema di conservazione: | Sistema di conservazione dei documenti informatici di cui all'art. 44 del Codice |
| Sistema di gestione informatica dei documenti | Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445 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 |
| Supporto ottico | Mezzo fisico che consente la memorizzazione di documenti informatici mediante l'impiego della tecnologia laser; sono supporti ottici, ad esempio, i CD, i dischi magneto-ottici, i DVD |
| Time stamping Authority (TSA) | Enti certificatori abilitati a prestare il servizio di marca temporale |
| Transazione informatica | Particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche della base di dati |
| Testo unico o TUDA | Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni |
| Titolare | È il soggetto Produttore, ossia la Persona fisica o giuridica, la Pubblica Amministrazione o l'Ente titolare dei documenti informatici da conservare. |
| Titolare del trattamento | La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza |
| 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 |

Di seguito si riporta la forma estesa degli acronimi e delle abbreviazioni utilizzati nel presente documento.

| Acronimi | |
|-----------------|---|
| AgID | Agenzia per l'Italia Digitale |
| CA | Certification Authority |
| CAD | Decreto legislativo 7 marzo 2005, n. 82, e s.m.i. - "Codice dell'amministrazione digitale"; |
| CD | Compact disc |
| D.Lgs. | Decreto Legislativo |
| DM | Decreto Ministeriale |
| DPCM | Decreto del Presidente del Consiglio dei Ministri |
| DPR | Decreto del Presidente della Repubblica |
| DPS | Documento programmatico della Sicurezza informatica |
| DVD | Digital versatile disc |
| ETSI | European Telecommunications Standards Institute; |
| FTP | File transfer protocol |
| HSM | Hardware security module |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext transfert protocol over secure socket layer |
| IDC | Indice Di Conservazione |
| IP | Internet protocol address |
| ISO | International standard organization |
| JPEG | Joint photographic experts group |
| MEF | Ministero dell'Economia e delle Finanze |
| NAS | Network attached storage |
| PA | Pubblica amministrazione |
| PdA | Pacchetto di archiviazione |
| PdD | Pacchetto di distribuzione |
| PDF | Portable document format |
| PdV | Pacchetto di versamento |
| PEC | Posta elettronica certificata |
| SinCRO | Supporto all'interoperabilità nella conservazione e nel recupero degli oggetti digitali |
| SLA | Service Level Agreement |
| TSA | Time Stamping Authority |
| TUDA | DPR 28 dicembre 2000, n. 445, e successive modificazioni - "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa" da lasciare |
| UNI | Ente nazionale italiano di unificazione |
| URL | Uniform resource locator |
| 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

Di seguito si riporta la normativa di carattere generale, nonché gli standard e i principali documenti della prassi di riferimento. Queste informazioni sono riportate nell'allegato 1 – Descrizione del servizio per la conservazione dei documenti informatici delle Condizioni generali del servizio e sono periodicamente aggiornate in base alle eventuali modifiche della normativa.

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 generale sulla protezione dei dati), applicabile in tutti gli Stati membri a partire dal 25 maggio 2018;
- **Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i.** – Codice dei Beni Culturali e del Paesaggio;
- **Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i.** – Codice dell'amministrazione digitale (CAD);
- **Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013** – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;
- **Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013** - Regole tecniche 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 3 dicembre 2013** - Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- **Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014**, Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

- **Decreto MEF del 17 giugno 2014** - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto – articolo 21, comma 5, del decreto legislativo n. 82/2005. (Ministero dell'economia e delle finanze);
- **Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014** - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- **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 **Regolamento (UE) n. 910/2014 eIDAS** (electronic IDentification Authentication and Signature), costituisce una base normativa comune per i Paesi membri dell'U.E. per quanto riguarda i servizi fiduciari, i mezzi di identificazione elettronica e le modalità di interazioni elettroniche sicure fra cittadini, imprese e pubbliche amministrazioni.

Standard di riferimento:

- **UNI EN ISO 9001:2015** Sistemi di gestione per la Qualità;
- **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.

[Torna al sommario](#)

3.2 Certificazioni del conservatore

La Zucchetti S.p.a. per l'erogazione del servizio di conservazione digitale si è dotata delle seguenti certificazioni:

| Tipo certificazione | data prima certificazione | data emissione corrente | data scadenza | Descrizione |
|---------------------------------------|---------------------------|-------------------------|---------------|---|
| Certificazione ISO 9001:2015 | 13/12/2000 | 17/05/2018 | 27/05/2021 | Progettazione, sviluppo, installazione e relativa formazione e manutenzione di prodotti software e relativi servizi di assistenza post vendita per professionisti e aziende. Realizzazione, erogazione e gestione di servizi di Data Center in modalità IaaS, PaaS, Server Cloud, Hosting, Colocation per professionisti in genere del settore contabile amministrativo, aziende ed enti pubblici. Certification Authority CA Firma Digitale e Time Stamping Authority (Trust Services). Progettazione ed erogazione di eventi formativi in ambito fiscale, giuslavoristico, contabile, amministrativo e manageriale. |
| Certificazione ISO 27001: 2013 | 17/08/2011 | 30/06/2017 | 16/08/2020 | Servizio di conservazione digitale a norma di documenti informatici e servizi di assistenza. Servizi di Datacenter. IaaS, PaaS, Server Cloud, Hosting, Housing, Colocation, Servizi fiduciari. |
| Certificazione BS 10012:2017 | 10/07/2018 | 10/07/2018 | 09/07/2021 | Zucchetti ha adottato un Sistema di Gestione delle Informazioni Personali conforme alla norma BS 10012:2017 nell'ambito dei processi e attività di fornitura di servizi fiduciari, della conservazione digitale a norma, dei servizi erogati dal Data center e dello sviluppo e commercializzazione software, al fine di garantire la tutela dei dati personali conformemente ai requisiti del Regolamento Generale sulla Protezione dei Dati (GDPR – General Data Protection Regulation - Reg UE 2016/679) in vigore dal 25 maggio 2018 in tutti i Paesi membri dell'Unione Europea. |

[Torna al sommario](#)

4. RUOLI E RESPONSABILITÀ

Il sistema di conservazione gestito dal conservatore Zucchetti S.p.a. si basa su un modello organizzativo formalmente definito nei ruoli e nelle responsabilità dei vari attori coinvolti nel processo di conservazione, come riportato nella tabella che segue, in conformità ai ruoli e alle attività ad essi associati indicati nel documento "Profili professionali" pubblicato da AgID sul proprio sito istituzionale.

In questo contesto, il modello organizzativo della Zucchetti S.p.a. prevede l'assegnazione di specifici ruoli distribuiti tra il Titolare, che produce e gestisce i documenti informatici da versare in conservazione e Zucchetti S.p.a. che svolge il ruolo di Responsabile del Servizio di conservazione di detti documenti informatici.

Si precisa che il nominativo ed i riferimenti del Responsabile della conservazione dell'organizzazione del titolare dei documenti informatici sono indicati nell'allegato "Specificità del contratto" nel quale sono anche riportate le attività affidate al Responsabile del Servizio di conservazione.

Al fine di garantire la corretta esecuzione del servizio, qui di seguito si elencano le figure professionali che compongono il gruppo di lavoro del servizio di conservazione.



Figura 1
Figure professionali del gruppo di lavoro del servizio di conservazione

| | | | |
|---|---|------------------------------|--|
| Ruolo | Responsabile del servizio di conservazione | | |
| Nominativo | Paolo Camia | | |
| Perimetro attività di competenza | <p>Definizione ed attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione.</p> <p>Definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente.</p> <p>Corretta erogazione del servizio di conservazione all'ente produttore.</p> <p>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.</p> | | |
| Data assunzione ruolo | Luglio 2015 | Data cessazione ruolo | |
| Deleghe | | | |

| | | | |
|---|---|------------------------------|--|
| Ruolo | Responsabile della sicurezza dei sistemi per la conservazione | | |
| Nominativo | Mario Brocca | | |
| Perimetro attività di competenza | <p>Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza.</p> <p>Segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.</p> | | |
| Data assunzione ruolo | Luglio 2015 | Data cessazione ruolo | |
| Deleghe | | | |

| | | | |
|---|--|------------------------------|--|
| Ruolo | Responsabile della funzione archivistica di conservazione | | |
| Nominativo | Daniela Mondoni | | |
| Perimetro attività di competenza | <p>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.</p> <p>Definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici.</p> <p>Monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione.</p> <p>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.</p> | | |
| Data assunzione ruolo | Luglio 2015 | Data cessazione ruolo | |
| Deleghe | | | |

| | | |
|---|--|------------------------------|
| Ruolo | Responsabile del trattamento dati personali | |
| Nominativo | Mario Brocca | |
| Perimetro attività di competenza | <p>Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali.</p> <p>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.</p> | |
| Data assunzione ruolo | Luglio 2015 | Data cessazione ruolo |
| Deleghe | | |

| | | |
|---|--|------------------------------|
| Ruolo | Responsabile dei sistemi informativi per la conservazione | |
| Nominativo | Angelo Cian | |
| Perimetro attività di competenza | <p>Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione.</p> <p>Monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore.</p> <p>Segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.</p> <p>Pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione.</p> <p>Controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.</p> | |
| Data assunzione ruolo | Luglio 2015 | Data cessazione ruolo |
| Deleghe | | |

| | | |
|---|--|------------------------------|
| Ruolo | Responsabile dello sviluppo e manutenzione del sistema di conservazione | |
| Nominativo | Maurizio Bonetta | |
| Perimetro attività di competenza | <p>Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione.</p> <p>Pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione.</p> <p>Monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione.</p> <p>Interfaccia con l'ente 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.</p> <p>Gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.</p> | |
| Data assunzione ruolo | Luglio 2015 | Data cessazione ruolo |
| Deleghe | | |

Tutti i Responsabili hanno ricevuto e sottoscritto un documento di nomina nel quale sono esplicitati i rispettivi incarichi e la durata degli stessi.
Al momento l'attività è espletata dai responsabili sopra individuati. Non sono state formalizzate deleghe di funzione.

[Torna al sommario](#)

5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Organigramma

Il modello organizzativo utilizzato dalla Zucchetti S.p.a. per l'erogazione del servizio di conservazione si basa sullo standard ISO 14721:2012 OAI (Open Archival Information System).

Il suddetto modello si basa su un sistema informativo aperto e cioè un archivio, inteso come struttura organizzata di persone e sistemi, che accetti la responsabilità di conservare l'informazione e renderla disponibile ad una determinata comunità di riferimento.

Concettualmente, nel sistema di conservazione di Zucchetti S.p.a. operano tre soggetti aventi diversi ruoli e competenze:

- **l'ente produttore detto anche Titolare** (è il ruolo svolto dalle persone fisiche o giuridiche o dai sistemi che forniscono le informazioni da conservare);
- **il responsabile della conservazione** (è la persona fisica interna all'organizzazione del titolare dei documenti informatici che definisce e attua le politiche complessive del sistema e ne governa la gestione con piena responsabilità e autonomia);
- **l'utente** (è il ruolo svolto da persone o sistemi che interagiscono con il sistema di conservazione al fine di accedere e ricercare le informazioni di interesse).

In pratica, il Titolare, attraverso il proprio Responsabile della Conservazione, affida a **Zucchetti S.p.a.** il servizio di conservazione dei propri dati e oggetti informatici, la quale, in veste di **conservatore accreditato, assume le responsabilità del servizio di conservazione** in accordo con quanto previsto dal Contratto di servizio, dai relativi allegati contrattuali e dal DPCM 3 dicembre 2013 e sue s.m.i..

Zucchetti S.p.a. provvede ad affidare il ruolo di **Responsabile del servizio di conservazione** ad una persona fisica interna alla propria organizzazione che, per competenza ed esperienza, garantisca la corretta esecuzione dei processi di conservazione definiti dalle norme, dal presente Manuale, dal Contratto di servizio e dagli allegati contrattuali.

Il Responsabile del Servizio di conservazione di Zucchetti S.p.a. può delegare lo svolgimento di parte del processo a una o più persone con adeguata competenza ed esperienza, secondo quanto previsto nella documentazione interna di organizzazione e gestione del sistema di conservazione.

Le attività eventualmente affidate ai singoli soggetti interni all'organizzazione del conservatore sono definite nell'ordine di servizio che regola il rapporto tra Zucchetti S.p.a. ed i propri collaboratori.

In ogni caso, il conservatore garantisce che tutte le persone coinvolte, a qualsiasi livello, nei processi di conservazione hanno raggiunto un comprovato livello di competenza e/o esperienza tali da consentire un adeguato livello di autonomia, pur sotto la costante supervisione del diretto superiore gerarchico e/o del Responsabile del servizio di conservazione.

Di seguito si rappresenta l'organigramma adottato da Zucchetti S.p.a. per la gestione del servizio di conservazione digitale di dati e documenti informatici:

Il Cliente che sceglie il Sistema di Conservazione Digitale di Zucchetti S.p.a. (Conservatore) mantiene all'interno della propria struttura organizzativa il ruolo di Responsabile della Conservazione mentre affida al Conservatore la responsabilità del relativo servizio e le funzioni a ciò correlate.

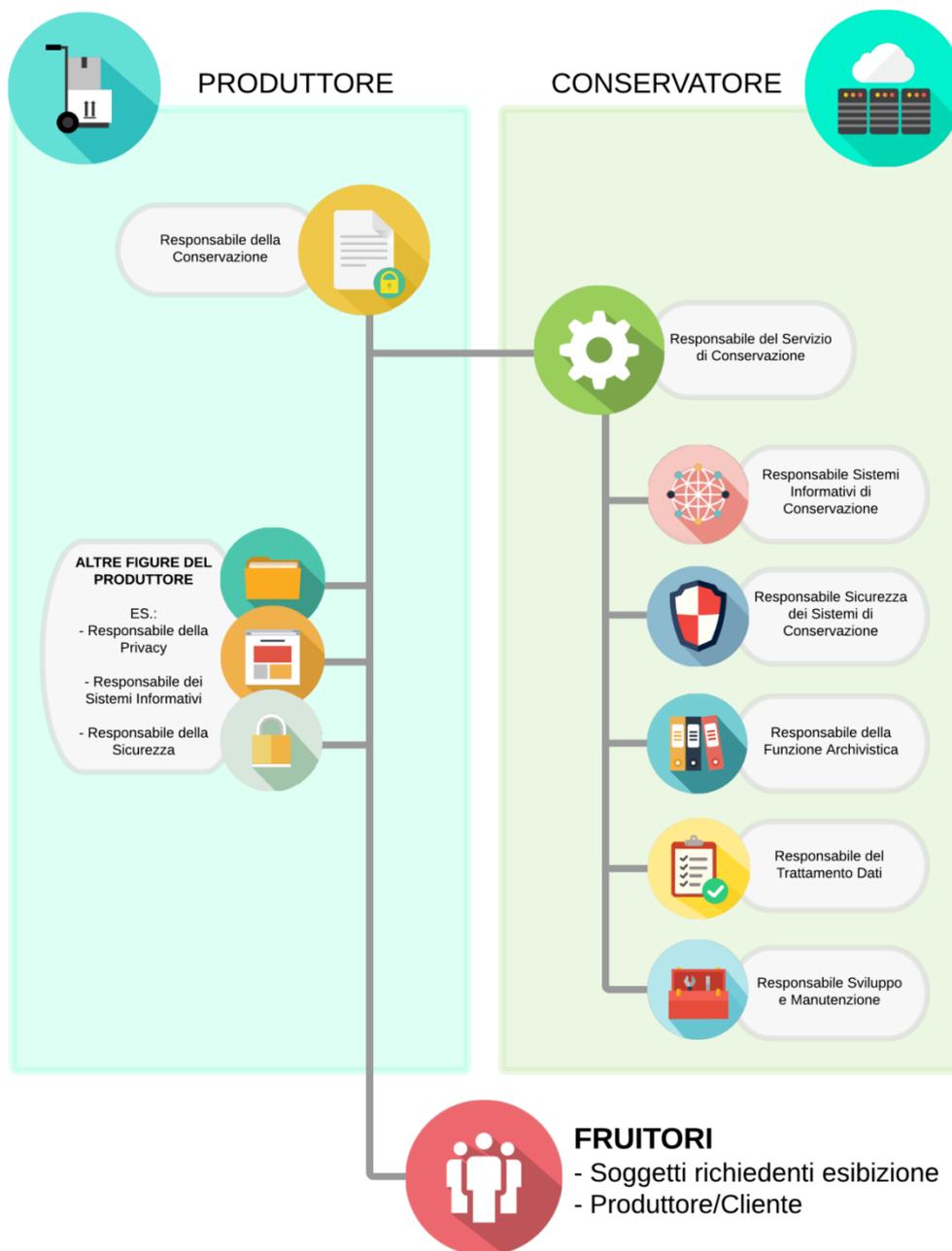


Figura 2
Distinzione tra le figure professionali dell'ente Produttore e quelle del Conservatore

[Torna al sommario](#)

5.2 Dati di riferimento del Conservatore, della CA e della TSA

Nel presente paragrafo vengono riportati i dati di riferimento e una presentazione del Conservatore, nonché i dati della Certification Authority.

[Torna al sommario](#)

5.2.1 Dati identificativi del Conservatore

Denominazione sociale : **Zucchetti S.p.a.**
Sede legale in : Lodi
Via e n. civico. : Via Solferino 1
Numero Iscrizione R.I. di Lodi, Codice fiscale .. : 05006900962
Partita IVA : 05006900962
C.C.I.A.A. di Lodi N° R.E.A..... : 1458208
PEC..... : zucchettispa@gruppozucchetti.it
Sito web generale (informativo)..... : www.zucchetti.it
Sito web del servizio di conservazione : <https://conservazionedigitale.zucchetti.it/codi>

[Torna al sommario](#)

5.2.2 Presentazione del Conservatore

Con oltre 3.800 addetti, una rete distributiva che supera i 900 Partner sull'intero territorio nazionale e 200 all'estero, oltre 150.000 clienti, il gruppo Zucchetti è uno dei più importanti protagonisti italiani del settore dell'IT.

L'offerta del gruppo Zucchetti consente al cliente di acquisire importanti vantaggi competitivi e di avvalersi di un unico partner informatico in grado di soddisfare le più svariate esigenze di carattere informatico.

Soluzioni software, hardware e servizi innovativi realizzati e studiati per soddisfare le specifiche esigenze di ogni natura e dimensione.

La completezza multidisciplinare, un approccio che valorizza i bisogni dei clienti e la capacità di coordinare, di gestire e di realizzare progetti, permettono da sempre al gruppo Zucchetti di sviluppare prodotti e servizi di altissima qualità che garantiscono all'utente di disporre della miglior soluzione del mercato.

Zucchetti S.p.a. è da sempre attenta ad offrire servizi efficienti e professionali, oltre che soluzioni di qualità. Attraverso personale altamente qualificato e preparato, il gruppo Zucchetti garantisce:

- un competente supporto pre-vendita (analisi delle esigenze, studio della soluzione ecc.);
- un tempestivo e valido servizio post-vendita (installazione, assistenza ecc.);
- una puntuale formazione per sfruttare al meglio tutte le potenzialità delle proprie soluzioni;
- un costante aggiornamento su tematiche civilistiche, contabili, fiscali, giuslavoristiche, previdenziali ecc.

Zucchetti è anche sinonimo di sicurezza. Attraverso un datacenter di proprietà, infatti, assicura elevati standard di sicurezza informatica, logica (sistemi antintrusione),

applicativa e fisica (sistemi antincendio, controllo accessi ecc.), nonché la continuità dei servizi di outsourcing in tutte le condizioni.

I principali settori in cui opera la Società, sia in modo diretto che attraverso partecipazioni di controllo, sono i seguenti:

- a) Settore professionisti;
- b) Settore gestione personale;
- c) Settore gestionali ERP;
- d) Settore sicurezza e automazione.

[Torna al sommario](#)

5.2.3 Dati identificativi della CA e TSA

I certificati di firma digitale sono rilasciati da Zucchetti S.p.a. (<https://www.zucchetti.it/>)

Le marche temporali sono rilasciate da Zucchetti S.p.a.

Nel corso dell'erogazione del Servizio potranno essere utilizzate firme digitali e marche temporali di altre CA/TSA, comunque accreditate ai sensi dell'art. 29 del CAD.

[Torna al sommario](#)

5.3 Ruoli del sistema di conservazione

In premessa, è opportuno precisare che la Zucchetti S.p.a. possiede tutte le caratteristiche strutturali, giuridiche, economiche e tecniche indispensabili al corretto svolgimento del proprio ruolo di conservatore cioè, per utilizzare i termini di OAIS, è titolare di una struttura organizzata di persone e sistemi che accetta la responsabilità di conservare documenti informatici e renderli disponibili ad una Comunità di riferimento.

Come già accennato in precedenza, le logiche operative ed organizzative di Zucchetti S.p.a. nel suo ruolo di conservatore accreditato e i suoi rapporti con i diversi Produttori fanno riferimento, come modello concettuale, al modello Open Archival Information System (OAIS), certificato standard ISO 14721 nel 2003 e recentemente aggiornato (ISO 14721:2012).

Il Sistema di conservazione di Zucchetti S.p.a. opera secondo modelli organizzativi esplicitamente definiti che garantiscono ed assicurano la sua distinzione logica dal sistema di gestione documentale dell'organizzazione del titolare dei documenti informatici ove esistente.

Oltre alle figure concettualmente individuate dal modello OAIS e alla luce di quanto indicato dalle Regole tecniche vigenti, nel sistema di conservazione di Zucchetti S.p.a. si possono identificare i seguenti ruoli fondamentali:

- Ente produttore,
- Utente,
- Responsabile della conservazione,
- Responsabile del Servizio di conservazione,
- Organismi di vigilanza e controllo.

Produttore

Il Produttore è la persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con il responsabile della gestione documentale. Nel Contratto di servizio vengono formalizzati e regolati i rapporti di servizio, le responsabilità delle parti, le condizioni economiche e gli eventuali ulteriori servizi offerti da Zucchetti S.p.a..

Il Responsabile della funzione archivistica del conservatore avrà cura di definire con il Responsabile della conservazione le tipologie degli oggetti informatici da sottoporre al processo di conservazione. Le modalità di versamento saranno specificate nell'allegato "Specificità del contratto", allegato al Contratto di servizio.

Il Produttore, secondo quanto previsto nel Contratto di servizio e nei suoi allegati, si impegna a depositare i documenti informatici e le loro aggregazioni documentali informatiche nei modi e nelle forme definite e concordate, garantendone l'autenticità e l'integrità nelle fasi di produzione, effettuata nel rispetto delle norme sulla formazione e sui sistemi di gestione dei documenti informatici. In particolare, garantisce che il trasferimento dei documenti informatici venga realizzato utilizzando formati compatibili con la funzione di conservazione e rispondenti a quanto previsto dalla normativa vigente.

Le tipologie documentarie da trasferire, le modalità di versamento ed i metadati sono concordati e specificati nell'allegato "Specificità del contratto".

Il Titolare mantiene la titolarità degli oggetti informatici, completi dei relativi metadati, versati in conservazione.

Il Titolare è responsabile del contenuto degli oggetti informatici versati in conservazione e del contenuto del Pacchetto di versamento ed è obbligato a trasmetterlo al Conservatore secondo le modalità e nei termini stabiliti nel presente Manuale e in dettaglio nell'allegato Specificità del contratto".

Sono a carico del Produttore le seguenti attività:

- la produzione, in forma stabile e non modificabile, degli oggetti informatici da versare in conservazione;
- la produzione degli oggetti informatici da versare in conservazione nel rispetto della normativa, delle regole tecniche in materia e di quanto stabilito dal Contratto di servizio;
- l'associazione agli oggetti informatici dei metadati previsti dalla legge e/o da regolamento, dal presente manuale e dal Contratto di servizio, comprensivi dei metadati di protocollazione, classificazione e fascicolazione, ove previsti;
- l'eventuale sottoscrizione digitale degli oggetti informatici da versare in conservazione;
- l'estrazione degli oggetti informatici destinati alla conservazione dai propri sistemi documentali e/o di gestione documentale;
- attraverso il Produttore che li forma, il versamento, mediante appositi pacchetti di versamento, degli oggetti informatici da conservare nel sistema di conservazione.

Utente

Si identifica come Utente una persona, ente o sistema che interagisce con i servizi del sistema di conservazione di Zucchetti S.p.a. al fine di fruire delle informazioni di interesse.

Più in generale, gli Utenti costituiscono la comunità di riferimento che interagisce con il Conservatore per avere accesso ai documenti informatici e alle informazioni di interesse

nei limiti previsti dalla legge.

Le informazioni richieste vengono fornite dal sistema di conservazione secondo le modalità previste all'art. 10 del DPCM 3 dicembre 2013 e secondo le procedure illustrate nel presente Manuale.

Il ruolo dell'Utente si può identificare in relazione a specifici soggetti abilitati, indicati dal Titolare stesso, che possono accedere ai documenti conservati secondo le politiche di accesso concordate.

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

Responsabile della conservazione

Il Responsabile della conservazione è la persona fisica presente all'interno dell'organizzazione del titolare dei documenti informatici, che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia, in relazione al modello organizzativo adottato ed esplicitato nel presente Manuale e nel Contratto per l'affidamento del servizio di conservazione.

Il Responsabile della conservazione, sotto la propria responsabilità, affida a Zucchetti S.p.a., quale prestatore del servizio di conservazione, il servizio di conservazione digitale dei documenti informatici, affidando le attività previste dal relativo Contratto di servizio.

Nello specifico, Zucchetti S.p.a., ai fini dell'erogazione del servizio oggetto del Contratto, svolge le attività ad essa affidate dal Responsabile della Conservazione come in dettaglio riportate nel documento "Incarico per il servizio di conservazione digitale", allegato al suddetto Contratto di servizio.

Contestualmente al perfezionamento del suddetto Contratto di servizio, il Responsabile della conservazione nomina Zucchetti S.p.a. quale Responsabile esterno del trattamento dei dati come previsto in materia di protezione dei dati personali.

Responsabile del servizio di conservazione

Il Responsabile del servizio di conservazione è la Zucchetti S.p.a. che opera attraverso uno o più persone fisiche formalmente incaricate all'esecuzione dell'insieme delle attività finalizzate alla conservazione dei documenti informatici del Titolare nell'ambito della fornitura del servizio di conservazione ad essa affidato dal Responsabile della conservazione.

In particolare, Zucchetti S.p.a., attraverso il proprio Responsabile del Servizio di Conservazione pro tempore o attraverso altri soggetti da questi formalmente delegati, indicati nel loro complesso come Firmatari delegati, appositamente dotati di certificati qualificati emessi secondo la normativa vigente in tema di firma digitale, provvederà ad apporre la firma digitale e la marca temporale laddove previsto dalla legge, dai regolamenti tecnici e/o dal presente Manuale.

Si precisa che, nel contesto del presente documento, i certificati qualificati di firma utilizzati dal Conservatore o dai suoi Firmatari delegati, sono utilizzati come uno strumento per dimostrare l'integrità di un insieme di dati o documenti informatici, a prescindere che il documento informatico sia firmato dal titolare al momento della sua accettazione nel sistema di conservazione.

Le firme utilizzate nei processi di conservazione, anche in base alla legislazione vigente, non integrano in alcun caso la sottoscrizione del contenuto dei documenti conservati, del cui contenuto la Zucchetti S.p.a. non è mai e in nessun modo responsabile.

Zucchetti S.p.a., per le attività finalizzate alla conservazione digitale degli oggetti

informatici ad essa delegate, si avvale di personale appartenente alla propria struttura, dotato di idonea conoscenza, esperienza, capacità e affidabilità, formalmente incaricato a svolgere ciascuna specifica funzione. Zucchetti S.p.a. si riserva, a proprio insindacabile giudizio, di sostituire, in qualunque momento, i suddetti incaricati.

Organismi di vigilanza e controllo

Gli organismi di vigilanza e controllo rappresentano i soggetti deputati, con diversi gradi di intervento, alla vigilanza ed al controllo dell'attività del Titolare e, di conseguenza, anche della loro documentazione, nonché della tutela della stessa come, ad esempio:

- Il Ministero per i beni e le attività culturali e del turismo (MiBACT);
- Le Soprintendenze archivistiche;
- L'Istituto per la Vigilanza sulle Assicurazioni (IVASS) che ha compiti di vigilanza nei settori finanziario e assicurativo;
- L'Agenzia delle Entrate;
- L'AgID;
- ed altri ancora.

Sempre ai fini della vigilanza e del controllo si ricorda che il Ministero per i beni e le attività culturali e del turismo (MiBACT) esercita funzioni di tutela e vigilanza dei sistemi di conservazione degli archivi di enti pubblici o di enti privati dichiarati di interesse storico particolarmente importante e autorizza le operazioni di scarto e trasferimento della documentazione conservata ai sensi del D.lgs 42/200412.

La tutela e la vigilanza sugli Archivi di enti pubblici non statali è esercitata dal MiBACT, tramite le Soprintendenze archivistiche competenti per territorio. Pertanto, "lo spostamento, anche temporaneo dei beni culturali mobili" compresi gli Archivi storici e di deposito è soggetto ad autorizzazione della Soprintendenza archivistica (D.lgs 22 gen. 2004, n. 42, art. 21, c. 1, lettera b). Così, anche "il trasferimento ad altre persone giuridiche di complessi organici di documentazione di Archivi pubblici, nonché di Archivi di privati per i quali sia intervenuta la dichiarazione ai sensi dell'articolo 13", sia che comporti o non comporti uno spostamento, rientra tra gli interventi soggetti ad **autorizzazione della Soprintendenza archivistica** (D.lgs 22 gen. 2004, n. 42, art.21, c. 1, lettera e).

L'AgID ha il compito di garantire la realizzazione degli obiettivi dell'Agenda digitale italiana in coerenza con l'Agenda digitale europea. In particolare, ad AgID è assegnata la funzione di emanazione di indirizzi, regole tecniche, linee guida e metodologie progettuali in materia di tecnologie informatiche.

Si dà altresì conto che in base alle Regole tecniche il sistema di conservazione del conservatore, in quanto accreditato, è soggetto alla vigilanza dell'AgID, e per tale fine il Sistema di conservazione di Zucchetti S.p.a. prevede la materiale conservazione dei dati e delle copie di sicurezza sul territorio nazionale e l'accesso ai dati presso la sede del Titolare.

[Torna al sommario](#)

5.4 Fasi del sistema di conservazione

Il Sistema di Conservazione attraversa diverse fasi durante il suo ciclo di vita che sono state individuate in:

- avviamento del Sistema di Conservazione;

- processo di Conservazione;
- manutenzione e Continuità del Sistema di Conservazione;
- chiusura del Sistema di Conservazione.

Di seguito sono descritti nel dettaglio l'avviamento del Sistema di Conservazione e le strutture organizzative di Zucchetti S.p.a. in esso coinvolte, mentre le altre fasi saranno trattate in appositi paragrafi successivi.

[Torna al sommario](#)

5.4.1 Processo di avviamento del sistema di conservazione

Le attività che determinano l'attivazione del Sistema di Conservazione coinvolgono il Titolare e Zucchetti S.p.a. in alcune delle sue principali aree organizzative: Commerciale, Tecnica, Legale/Amministrativa.

Il processo, descritto nell'immagine seguente, si struttura in tre momenti: Pre-Vendita/Commerciale, Contrattuale, Attivazione.

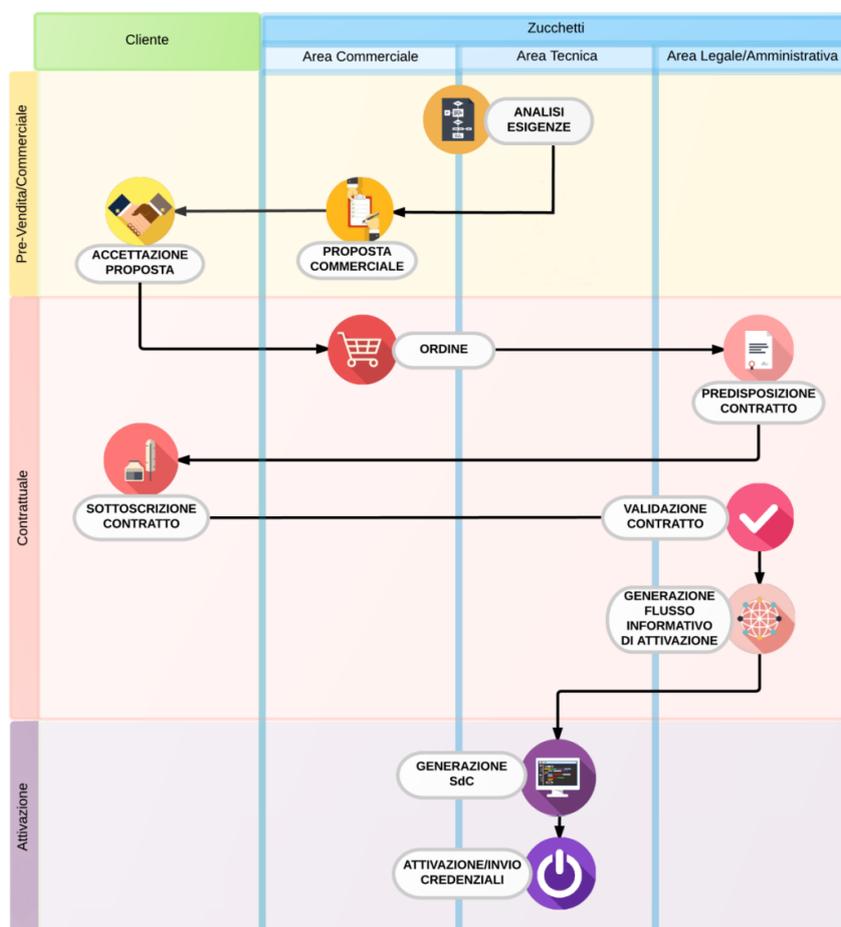


Figura 3
Processo di avviamento del sistema di conservazione

[Torna al sommario](#)

5.4.2 Pre-Vendita / Commerciale

Rappresenta lo stadio iniziale del processo di avviamento che inizia dal contatto con il cliente, volto alla definizione delle sue esigenze, e termina con l'eventuale accettazione della proposta commerciale avanzata dall'area commerciale di Zucchetti S.p.a..



Figura 4

Elementi della fase pre-vendita dell'avviamento del sistema di conservazione

Analisi delle esigenze e gestione progetti

Qualora la natura del potenziale cliente lo richieda, il commerciale di riferimento, in questa fase, può essere affiancato da membri dall'area tecnica al fine di svolgere un'analisi delle esigenze del cliente riguardo la conservazione dei documenti. Tale processo è volto alla definizione delle caratteristiche che dovrà assumere il servizio erogato, in particolar modo, in riferimento alla struttura delle possibili classi documentali non standard e dell'eventuale personalizzazione del Pacchetto di Versamento, nonché degli ulteriori aspetti salienti difforni dalle condizioni standard di erogazione del servizio che, in tal caso, verranno registrati nell'allegato B- Scheda di Servizio - "**Specificità del Contratto**".

I tecnici impegnati nell'analisi delle esigenze restano a disposizione del cliente e del commerciale per tutta la fase di pre-vendita, durante la quale si mantengono in stretto contatto con l'area di produzione (che dovrà presidiare la configurazione del servizio) e con il settore Help Desk (che dovrà fornire i servizi post-vendita); ciò affinché tutte le informazioni rilevanti in merito al rapporto con il cliente siano diffuse e condivise tra tutti i soggetti coinvolti nel processo.

Proposta commerciale

La conferma della possibilità di soddisfare le esigenze del cliente è seguita dalla predisposizione della proposta commerciale più adeguata da sottoporre all'approvazione del cliente.

[Torna al sommario](#)

5.4.3 Contrattuale

Con l'accettazione della proposta commerciale il processo entra nella fase contrattuale che prevede la gestione dell'ordine e la predisposizione del contratto.



Figura 5

Elementi della fase contrattuale del processo di avviamento del sistema di conservazione

Inserimento dell'ordine nel sistema informativo

Il contenuto dell'ordine di fornitura del servizio di conservazione viene definito in base alle analisi operate in precedenza ed è preso in carico dall'area Legale/Amministrativa che si fa carico di predisporre il contratto.

Contratto

Nel contratto, oltre ad essere riportate le informazioni dell'ordine, è presente l'allegato B - "Scheda servizio" - Specificità del contratto che contiene le eventuali specificità emerse durante l'analisi.

Il documento è sottoscritto dal cliente e trasmesso all'area amministrativa. La validazione formale svolta quest'ultima area determina la definitiva registrazione del contratto all'interno del sistema informativo aziendale, dal quale vengono automaticamente trasmesse al reparto tecnico le informazioni necessarie per la configurazione del Sistema di Conservazione e le relative specifiche.

[Torna al sommario](#)

5.4.4 Attivazione

La fase di attivazione inizia con la ricezione del flusso informativo di ordine e contratto da parte dell'area tecnica e termina con l'invio al cliente delle credenziali di accesso al Sistema di Conservazione.



Figura 6

Elementi della fase di attivazione tecnica del sistema di conservazione

Configurazione del servizio

Il sistema di conservazione del cliente viene configurato automaticamente secondo il flusso informativo, presidiato dall'area tecnica, derivante dall'ordine di erogazione del servizio, prendendo le mosse da quanto indicato nella Scheda di Servizio e, in generale, nel contratto. Sono così definite, tra le altre caratteristiche: le anagrafiche, le utenze e le relative profilazioni, le classi documentali, i metadati e le extrainfo, oltre ai parametri che determinano la/e modalità di trasmissione dei documenti al sistema.

In caso di sistemi di conservazione che prevedono personalizzazioni, al completamento della configurazione dell'ambiente viene eseguito un collaudo interno che in caso di esito positivo rende operativo il sistema.

Invio credenziali e completamento attivazione

La fase di avviamento si conclude con l'invio di due distinte PEC/e-mail ai recapiti del Responsabile della Conservazione (definiti contrattualmente); queste contengono rispettivamente lo username e la password di accesso al sistema (alla prima login verrà richiesta la personalizzazione della password notificata).

Dal momento in cui sono inviate le credenziali, si ritiene che il cliente sia nelle condizioni di poter fruire a pieno del servizio e, da questo momento in avanti, per ogni evenienza attinente la formazione riguardo al servizio, all'eventuale ulteriore collaudo del sistema e a tutti gli altri aspetti tecnico/funzionali, potrà fare riferimento all'Help Desk dedicato.

[Torna al sommario](#)

6. OGGETTI SOTTOPOSTI A CONSERVAZIONE

In questo paragrafo si descrivono le tipologie di documenti informatici sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie documentali e le eventuali eccezioni.

Sono **oggetti informatici** del sistema di conservazione:

- a) i documenti informatici;
- b) i documenti informatici rilevanti ai fini delle disposizioni tributarie (di cui al DMef 17.06.2014 e s.m.i.)
- c) i documenti amministrativi informatici;
- d) i fascicoli informatici ovvero le aggregazioni documentali informatiche.

A tutti i documenti informatici versati in conservazione il Titolare associa i metadati di cui all'allegato 5 delle Regole Tecniche contenenti i riferimenti che univocamente identificano i singoli oggetti che appartengono al singolo documento informatico, al fascicolo o all'aggregazione documentale.

Il documento informatico rappresenta l'unità minima di elaborazione, nel senso che viene memorizzato ed esibito come un tutt'uno; pertanto non è possibile estrarre dal sistema parti di un documento informatico.

Un documento informatico conservato nel sistema di conservazione, quindi, ha le seguenti caratteristiche:

- è costituito da un file;
- è memorizzato sui supporti previsti dalla procedura di conservazione;
- è identificato in maniera univoca;
- è conservato unitamente ai suoi metadati e agli altri parametri di conservazione.

Come stabilito dai provvedimenti citati al capitolo 3 “Normativa e standard di riferimento”, i documenti informatici sono statici e non modificabili, ovvero sono redatti in modo tale per cui il contenuto non è alterabile durante le fasi di conservazione ed accesso, e sono immutabili nel tempo. In pratica, il documento non deve contenere macroistruzioni né codici eseguibili.

Le caratteristiche di staticità ed immodificabilità dei documenti versati nel sistema di conservazione sono assicurate dal Produttore che ne verifica, al contempo, l'effettiva compatibilità con il visualizzatore definito.

I documenti informatici che il Cliente intende conservare presso il Conservatore sono puntualmente descritti nelle condizioni generali del servizio, oltre ad eventuali peculiarità dettagliate nell'allegato B dell'ordine (“Specificità del contratto”).

Nelle condizioni generali di contratto nonché nell'allegato B in caso di personalizzazioni per ogni formato definito viene individuato anche il software necessario per la visualizzazione del documento informatico.

Zucchetti S.p.a. configura il servizio di conservazione in ragione del profilo assegnato per ogni tipologia/classe di documenti su indicazione del Produttore, classificato come omogeneo in base ai dati da utilizzare per l'indicizzazione e i termini di conservazione.

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 il Conservatore e configurato sul servizio.

[Torna al sommario](#)

6.1 Oggetti conservati

Il Sistema di conservazione del conservatore è stato progettato e sviluppato integralmente dalla Zucchetti S.p.a. ed è in grado di gestire diverse tipologie di oggetti informatici.

Il sistema di conservazione gestisce gli oggetti informatici sottoposti a conservazione distinti per ogni singolo Titolare, consentendo di definire configurazioni e parametri per ogni Produttore, in base agli accordi stipulati all'atto della sottoscrizione del Contratto di servizio.

Per mantenere anche nel sistema le informazioni relative alla struttura dell'archivio e dei relativi vincoli archivistici, le unità documentarie possono essere versate corredate di un set di metadati di profilo archivistico che include gli elementi identificativi e descrittivi del fascicolo, con riferimento alla voce di classificazione e l'eventuale articolazione in sotto fascicoli. Inoltre è gestita la presenza di classificazioni, fascicoli e sotto fascicoli secondari e collegamenti tra le diverse unità archivistiche e documentarie presenti nel sistema.

Nelle condizioni generali del servizio sono elencate e descritte le tipologie di documenti informatici sottoposte a conservazione e le relative politiche di conservazione.

Le politiche di conservazione da adottare in relazione ai singoli oggetti informatici sono definite attraverso le attività di analisi documentale che precedono la fase di attivazione del servizio.

In particolare, le predette politiche di conservazione relative agli oggetti da conservare riguardano:

- la classe/tipo documentale;
- la natura documentale;
- la descrizione dei formati (comprensivi della relativa versione) utilizzati;
- l'indicazione dei visualizzatori relativi ai formati gestiti, necessari per garantire la leggibilità nel tempo dei documenti conservati;
- l'elenco e la descrizione dei metadati associati ai documenti;
- le peculiarità delle eventuali sottoscrizioni digitali;
- il periodo di conservazione;
- i livelli di servizio (SLA) concordati con l'ente produttore;
- altre politiche (regole) che caratterizzano il processo di conservazione.

La descrizione delle tipologie documentali e le politiche di conservazione sono riportate in dettaglio nell'allegato 2 delle condizioni generali di contratto; eventuali personalizzazioni sono dettagliate nell'allegato B all'ordine.

Di seguito si riporta un esempio della tabella da compilare nell'Allegato B dell'ordine del Servizio di conservazione Zucchetti S.p.a. relativamente alla definizione di eventuali classi documentali non standard.

| SCHEDA CLASSE DOCUMENTALE – _____ | |
|--|--|
| Tipologie di documenti da associare alla classe | - _____ - _____ - _____ - _____ - _____ |
| Firma digitale obbligatoria | <input checked="" type="checkbox"/> Sì |
| Valenza tributaria | <input type="checkbox"/> Sì, <input type="checkbox"/> No |
| Formato del documento da versare in conservazione | <input type="checkbox"/> PDF/A, <input type="checkbox"/> PDF, <input type="checkbox"/> XML, <input type="checkbox"/> EML <input type="checkbox"/> Altro _____ |
| Visualizzatore | _____ _____ _____ |
| Natura di documento informatico amministrativo | <input type="checkbox"/> Sì, <input type="checkbox"/> No |
| Presenza di fascicolo informatico o aggregazione documentale informatica | <input type="checkbox"/> Sì, <input type="checkbox"/> No |
| Metadati extrainfo | <input type="checkbox"/> Sì, <input type="checkbox"/> No - In caso di risposta positiva compilare apposita scheda |
| Frequenza di versamento dei documenti nel sistema | <input type="checkbox"/> Giorno, <input type="checkbox"/> Settimana, <input type="checkbox"/> Mese, <input type="checkbox"/> Bimestre, <input type="checkbox"/> Trimestre, <input type="checkbox"/> Quadrimestre, <input type="checkbox"/> Semestre, <input type="checkbox"/> Annuale, <input type="checkbox"/> Non applicabile |
| Frequenza di chiusura | <input type="checkbox"/> Giorno, <input type="checkbox"/> Settimana, <input type="checkbox"/> Mese, <input type="checkbox"/> Bimestre, <input type="checkbox"/> Trimestre, <input type="checkbox"/> Quadrimestre, <input type="checkbox"/> Semestre, <input type="checkbox"/> Annuale. |
| Note | _____ _____ _____ |

| METADATI EXTRAINFO | |
|---|--|
| Classe documentale ai quali sono associati i metadati extrainfo | <input type="checkbox"/> Fatture attive (non PA) e documenti ciclo attivo <input type="checkbox"/> Fatture passive e documenti ciclo passivo <input type="checkbox"/> Libri contabili <input type="checkbox"/> Dichiarazioni fiscali <input type="checkbox"/> Fattura PA <input type="checkbox"/> Ricevute e notifiche PA <input type="checkbox"/> Libro Unico del Lavoro <input type="checkbox"/> PEC <input type="checkbox"/> Altro _____ |
| Elenco metadati extrainfo | - _____ - _____ - _____ - _____ - _____ |
| Associazione metadati al documento | <input checked="" type="checkbox"/> Cliente |
| Scarto pacchetto di versamento se metadati extrainfo assenti | <input checked="" type="checkbox"/> Sì |
| Note | _____ _____ _____ |

[Torna al sommario](#)

6.2 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.

I metadati devono essere necessariamente associati agli oggetti informatici dal Titolare nella fase di formazione del documento e comunque prima del versamento in conservazione.

I metadati forniti restano di proprietà del Titolare medesimo.

I metadati, seppur chiaramente associati al documento informatico, possono essere gestiti indipendentemente dallo stesso.

In relazione alle diverse tipologie di oggetti informatici posti in conservazione (documenti informatici, documenti amministrativi informatici, fascicoli informatici o aggregazioni documentali informatiche), è previsto un “set minimo” di metadati come specificato nella Specificità del contratto”.

In ogni caso, ad ogni oggetto informatico versato in conservazione, devono, essere associati i metadati di cui all'allegato 5 al DPCM 3.12.2013.

[Torna al sommario](#)

6.3 Formati gestiti

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.

Nel presente capitolo vengono fornite le indicazioni sui formati dei documenti informatici che per le loro caratteristiche sono, al momento attuale, da ritenersi coerenti con la conservazione digitale a lungo termine. Infatti, una possibile soluzione al problema dell'obsolescenza, che porta all'impossibilità di interpretare correttamente formati non più supportati al fine di renderli visualizzabili, è quella di selezionare formati standard.

E' comunque opportuno premettere che per la natura stessa dell'argomento di cui trattasi, questa parte del *Manuale* potrà subire periodici aggiornamenti sulla base dell'evoluzione tecnologica e dell'obsolescenza dei formati.

[Torna al sommario](#)

6.4 Caratteristiche generali dei formati

I formati scelti devono essere, puntualmente richiamati nell'allegato "Specificità del contratto".

Zucchetti S.p.a. raccomanda un insieme di formati che sono stati dalla stessa valutati in funzione di alcune caratteristiche quali:

| | caratteristica | descrizione della caratteristica |
|---|------------------------|--|
| 1 | APERTURA | <p>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.</p> <p>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.</p> <p>In relazione a questo aspetto, Zucchetti S.p.a ha privilegiato formati già approvati dagli Organismi di standardizzazione internazionali quali ISO e OASIS.</p> |
| 2 | SICUREZZA | <p>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.</p> |
| 3 | PORTABILITÀ | <p>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.</p> |
| 4 | FUNZIONALITÀ | <p>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 soggetto produttore per la formazione e gestione del documento informatico.</p> |
| 5 | SUPPORTO ALLO SVILUPPO | <p>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.).</p> |

| | | |
|---|------------|--|
| 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](#)

6.5 Formati per la conservazione

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

Pertanto, alla luce delle suddette considerazioni, **i formati adottati e consigliati dal Conservatore** per la conservazione delle diverse tipologie di documenti informatici sono le seguenti:

| Formato | Descrizione | | |
|--|--|---|--|
| PDF/A o PDF | 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 19005-1:2005 (vers. PDF 1.4) | |
| | 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 | |
|---|--|--|
| 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 |
| | Estensione | .xml |
| | Tipo MIME | Application/xml Text/xml |
| | Formato aperto | SI |
| | Specifiche tecniche | Pubbligate da W3C – http://www.w3.org/XML |
| | Altre caratteristiche | è un formato di testo flessibile derivato da SGML (ISO 8879). |
| Software necessario alla visualizzazione | Microsoft Internet Explorer / Firefox / Google Chrome | |

| 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) |
| | Estensione | .eml |
| | Tipo MIME | Message/rfc2822 |
| | Formato aperto | SI |
| | Specifiche tecniche | Pubbligate 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.

Il formato EML è accettato solamente per le classi documentali di tipo "PEC".

Pertanto, alla luce di quanto sopra esposto, **i formati accettati in conservazione**, salvo quanto diversamente richiesto dal Produttore nell'allegato "Specificità del contratto", **sono esclusivamente quelli richiamati nel presente capitolo.**

Le diverse tipologie di documenti sono prodotti/formati/emessi a cura e sotto l'esclusiva responsabilità del Titolare 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 e dovranno essere identificati in modo univoco e persistente.

Ai sensi della normativa vigente sono conservati solo i formati idonei ad essere conservati a lungo termine, individuati dall'allegato 2 alle Regole Tecniche, a cui integralmente si rinvia, rispettando i requisiti ivi previsti di "standard aperti", in modo da garantire a chiunque in futuro la possibilità tecnica di avere accesso ai documenti conservati, corredati da una struttura di dati per la memorizzazione nel sistema di conservazione in grado di assicurare l'interoperabilità tra sistemi.

Tutti i documenti versati nel sistema di conservazione devono essere contraddistinti da un set di metadati obbligatori per il sistema, che li identificano univocamente.

[Torna al sommario](#)

6.6 Controlli sui formati

Il sistema di conservazione verifica che i file inviati siano corrispondenti ai formati ammessi. In caso di oggetti informatici prodotti con formati non ammessi viene prodotto un Rapporto di Rifiuto.

Le relazioni tra Titolare, tipo/classe documentale e formati ammessi viene configurata in relazione a quanto definito nelle condizioni generali del servizio oltre ad eventuali personalizzazioni dettagliate nell'allegato B dell'ordine di fornitura dello stesso ("Specificità del contratto").

La verifica dell'associazione dell'oggetto informatico ad uno specifico formato ammesso avviene eseguendo i seguenti controlli:

| Tipo di controllo | Descrizione del controllo |
|---------------------------|---|
| Verifica dell'estensione | Una serie di lettere, unita al nome del file attraverso un punto, ad esempio [nome del file].pdf identifica un formato sviluppato dalla Adobe |
| Verifica del magic number | I primi byte presenti nella sequenza binaria del file, ad esempio %PDF identifica i file di tipo PDF |
| Verifica Mime Type | Verifica della corrispondenza tra il Mime Type ricavato dall'estensione del file ed il Mime Type ricavato dal magic number. |

Per identificare il formato dei file oggetto di conservazione viene analizzato ogni singolo oggetto informatico inviato al sistema di conservazione attraverso i pacchetti di versamento

[Torna al sommario](#)

6.7 Migrazione dei formati

L'operazione di migrazione dei formati è una procedura particolarmente complessa che può essere necessaria nei casi di obsolescenza dei formati. Il problema che si pone è quello di comprendere se il contenuto del file di partenza e di arrivo è rimasto inalterato. In altre parole è necessario capire se le *significant properties* si sono conservate.

È necessario quindi impostare dei test di controllo che, inevitabilmente dovranno essere automatici. Sulla base dello specifico formato divenuto obsoleto e sulla base del nuovo formato di destinazione scelto per l'operazione di migrazione verranno scelti quanti e quali controlli sul buon esito della conversione inserire.

Le specifiche dei formati di partenza e di destinazione saranno decisive e determinanti per l'individuazione dei controlli da attuare.

[Torna al sommario](#)

6.8 Utilizzo di formati di compressione

Trattando di formati, tra gli aspetti da considerare si devono includere i metodi di compressione degli oggetti informatici, metodi, questi, utili per tenere sotto controllo la dimensione dei file, ma anche rischiosi perché potrebbero implicare la perdita di informazioni.

Qualora sia inevitabile, e solo dopo aver condiviso con il Titolare, che deve approvare ed autorizzare espressamente le procedure di compressione, si utilizzeranno metodi di compressione dati che garantiscano l'assenza di perdite d'informazione (o compressione dati lossless), ossia algoritmi di compressione che non portino alla perdita di alcuna parte dell'informazione originale durante la fase di compressione/decompressione degli oggetti informatici sottoposti a compressioni.

[Torna al sommario](#)

6.9 Pacchetti informativi

Gli oggetti informatici conservati nel sistema di conservazione sono organizzati in pacchetti informativi, intesi come contenitori che racchiudono uno o più oggetti da trattare (documenti informatici, documenti amministrativi informatici, fascicoli informatici, aggregazioni informatiche oppure anche i soli metadati riferiti agli oggetti informatici da conservare o conservati) comprensivi delle informazioni per la loro interpretazione e rappresentazione.

I pacchetti informativi quindi contengono non solo l'oggetto informatico da conservare, ma anche i metadati necessari a garantirne la conservazione e l'accesso nel lungo periodo.

Si tratta di una rappresentazione concettuale dei diversi momenti in cui si vengono a trovare gli oggetti informatici:

- immissione in archivio;
- archiviazione e conservazione;
- distribuzione ed esibizione all'utenza.

I Pacchetti informativi che identificano le diverse fasi del processo di conservazione sono tre:

1. Il pacchetto di versamento,
2. Il pacchetto di archiviazione,
3. Il pacchetto di distribuzione.

I suddetti pacchetti sono concettualmente differenti tra loro ma possono, per scelta applicativa, coincidere.

Il formato del pacchetto di archiviazione (e del pacchetto di distribuzione) è definito nell'allegato 4 del DPCM 03.12.2013, dove viene descritto l'indice di conservazione; il formato del pacchetto di versamento non è indicato nelle regole tecniche e quindi assolutamente libero. La Zucchetti S.p.a. ha scelto di conformare il Pacchetto di versamento in modo identico al formato dei pacchetti di archiviazione e di distribuzione, garantendo per tutti i pacchetti informativi (versamento, archiviazione e distribuzione) la perfetta conformità allo standard SInCRO UNI 11386:2010.

[Torna al sommario](#)

6.10 Pacchetto di versamento

Il pacchetto di versamento è confezionato dal Produttore che deve produrlo e trasmetterlo al sistema di conservazione secondo le modalità operative di versamento descritte nella sezione "Specifiche tecnico-funzionali e SLA e KPI" delle condizioni generale del servizio.

Eventuali personalizzazioni sul Pacchetto di Versamento devono essere concordate tra le parti.

Il pacchetto di versamento può essere acquisito tramite:

- upload manuale di un file zip
- l'invio via web service di un file zip
- acquisizione da area FTP
- acquisizione dall'area di pre-ingest

Il pacchetto di versamento è composto da un file in formato compresso (.zip) contenente:

- I documenti informatici da conservare, eventualmente firmati digitalmente nello standard di firma Cades (.p7m) oppure nello standard di firma PadES (PDF Advanced Electronic Signature).
- Un file XML come da Norma UNI 11386 (SInCRO) contenente l'indice dei documenti informatici da conservare.

Il file indice del pacchetto di versamento è un file in formato XML conforme allo standard UNI SInCRO 11386:2010: questa scelta progettuale garantisce che le informazioni necessarie alla produzione del pacchetto di archiviazione siano provenienti dal pacchetto di versamento.

In particolare nel pacchetto di versamento sono identificate le seguenti informazioni:

- il Produttore del pacchetto
- l'applicativo che ha prodotto il pacchetto
- il gruppo cui appartiene il pacchetto
- i gruppi cui appartengono i documenti inclusi nel pacchetto
- i documenti inclusi nel pacchetto con i metadati relativi
- la classe documentale cui associare il singolo documento
- i soggetti coinvolti nel processo di produzione del pacchetto e di conservazione
- informazioni relative a data e ora di realizzazione del pacchetto
- riferimenti normativi

Di seguito vengono illustrate le informazioni contenute nel file XML del pacchetto di versamento:

Le definizioni che seguono sono riprese dalla norma Norma UNI 11386 (SInCRO).

Rappresentazione grafica del file XSD dell'indice del pacchetto di versamento.

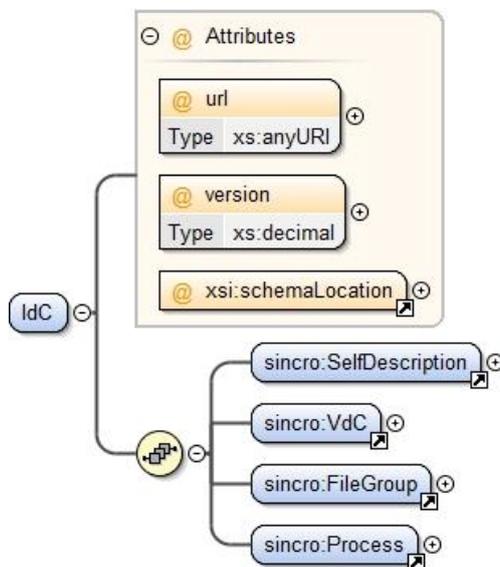


Figura 7

Rappresentazione grafica del file XSD dell'indice del pacchetto di versamento.

IdC: Indice di Conservazione: sono le informazioni relative ai file oggetto di conservazione e al processo di conservazione.

Elementi sovraordinati: nessuno.

Elementi subordinati: SelfDescription, FileGroup, Process, Volume di Conservazione.

SelfDescription: rappresentazione grafica del file XSD

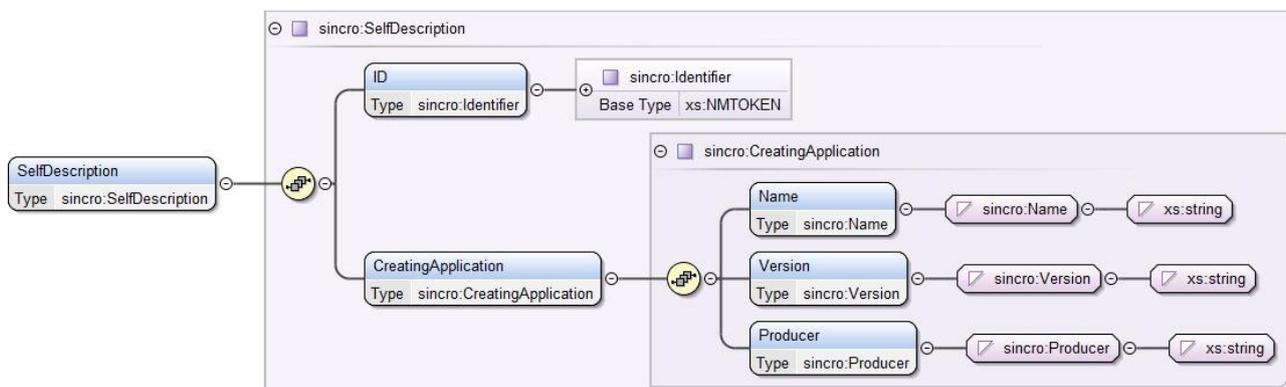


Figura 8

SelfDescription: rappresentazione grafica del file XSD

| Nome elemento | Descrizione |
|---------------------|--|
| SelfDescription | Informazioni relative all'indice di conservazione stesso. |
| ID | Identificatore univoco dell'entità descritta. |
| CreatingApplication | Informazioni sull'applicazione che ha generato l'IdC. |
| Name | Nome dell'applicazione che ha generato l'IdC. |
| Version | Versione dell'applicazione che ha generato l'IdC. |
| Producer | Nome del produttore dell'applicazione che ha generato l'IdC. |

Volume di conservazione, di seguito VdC: rappresentazione grafica del file XSD

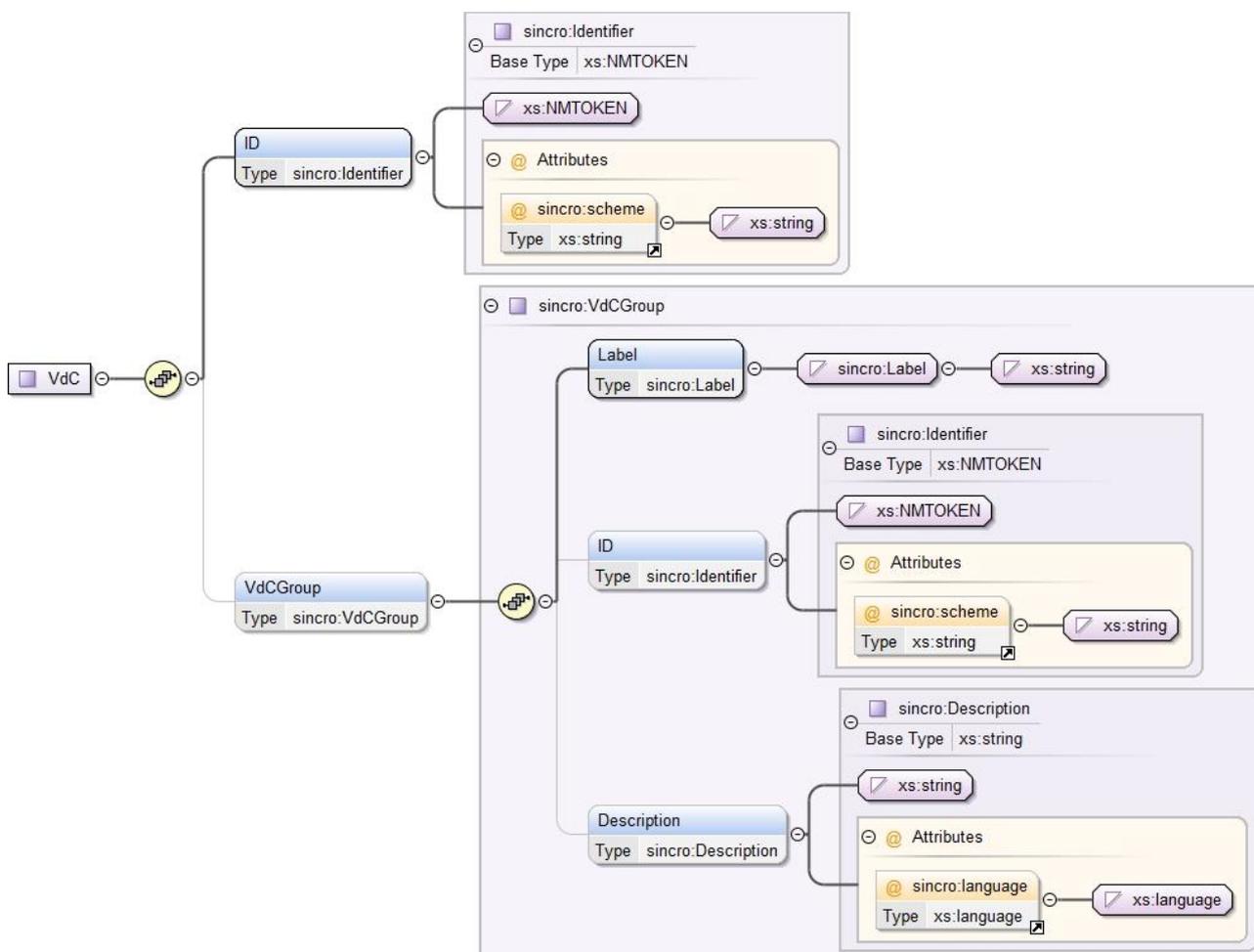


Figura 9
Volume di conservazione, di seguito VdC: rappresentazione grafica del file XSD

| Nome elemento | Descrizione |
|---------------|---|
| ID | Identificatore univoco dell'entità descritta. |
| Description | Descrizione del volume di conservazione. |

FileGroup: rappresentazione grafica del file XSD

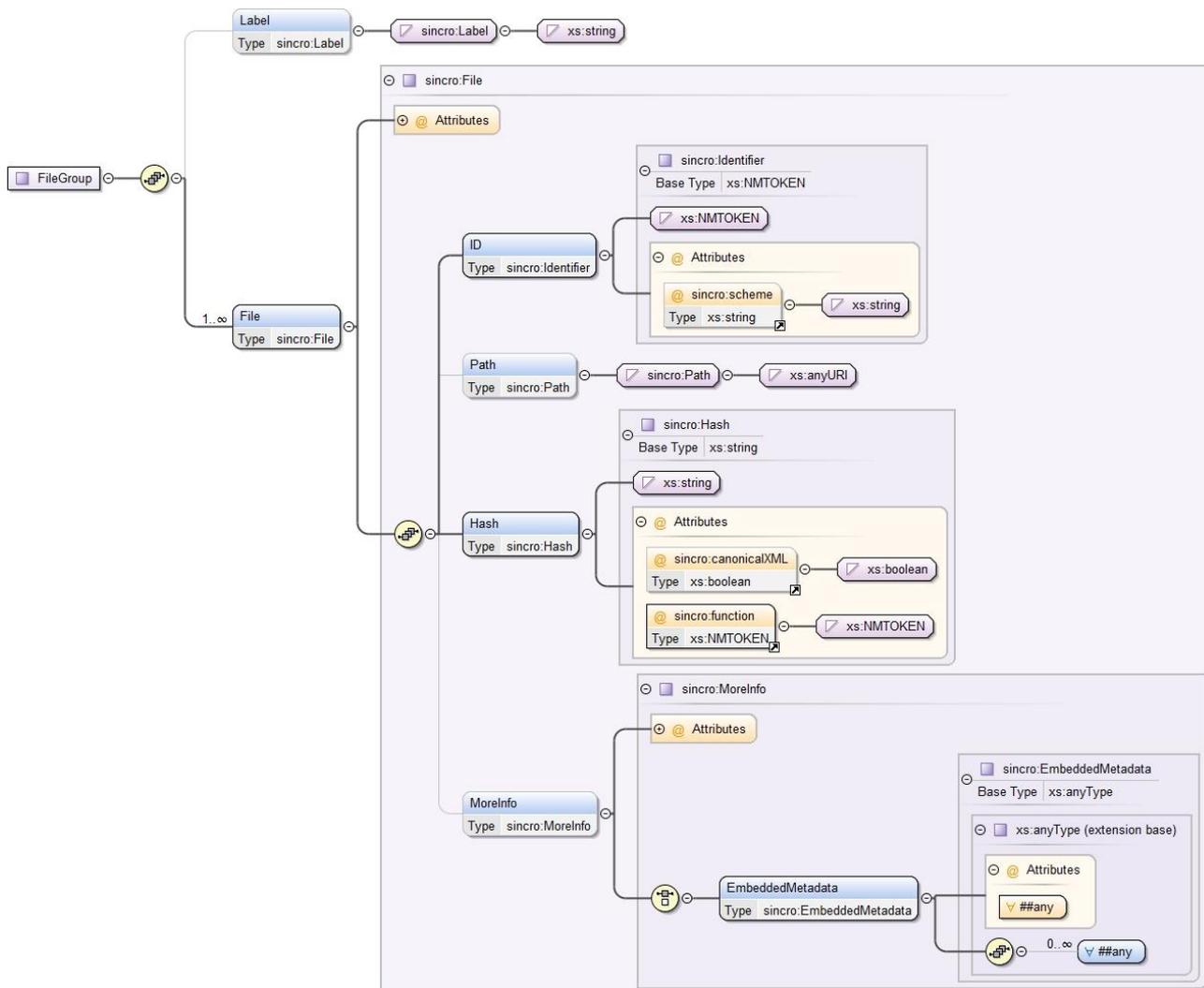


Figura 10
FileGroup: rappresentazione grafica del file XSD

| Nome elemento | Descrizione |
|---------------|---|
| File | Informazioni relative al file oggetto di conservazione. |
| ID | Identificatore univoco del file. |
| Path | Nome del file comprensivo di estensione. |
| Hash | Informazioni sull'impronta in formato SHA-256 del file cui l'elemento si riferisce. |
| MoreInfo | Metadati da associare al file. Tali informazioni devono essere strutturate nel formato XML, utilizzando lo Schema XML che è illustrato di seguito. |

Moreinfo di file: rappresentazione grafica del file XSD

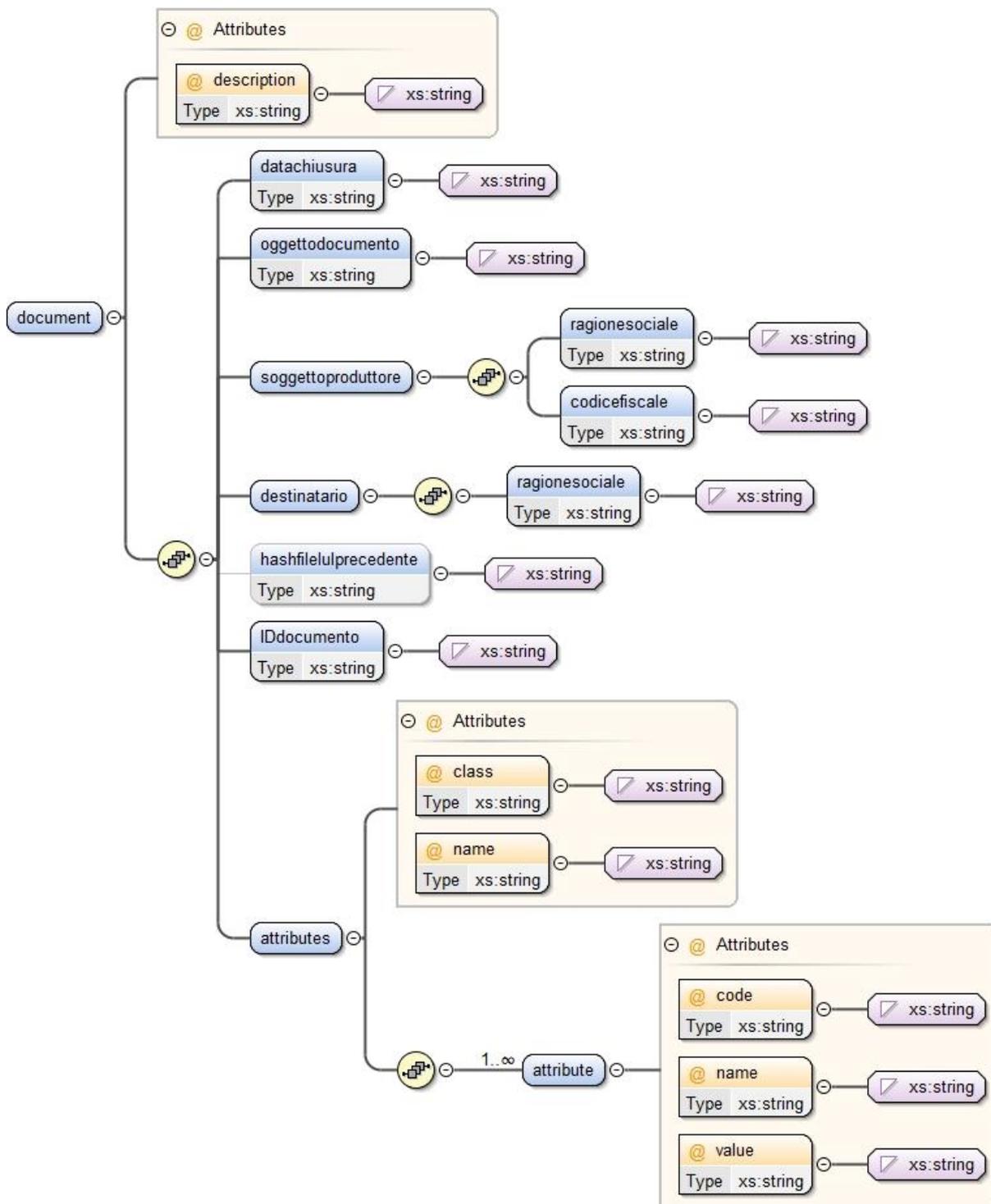


Figura 11
 Moreinfo di file: rappresentazione grafica del file XSD

| Nome elemento | Descrizione |
|-----------------------|--|
| Description | Nome del file comprensivo di estensione. |
| datachiusura | Data di formazione del documento. |
| oggettodocumento | Oggetto del documento. Per convenzione, se non diversamente indicato, può coincidere con la descrizione della classe documentale cui appartiene il documento. |
| Produttore | Dati del soggetto che ha formato il documento. |
| ragionesociale | Ragione sociale o cognome e nome del soggetto che ha formato il documento. |
| codicefiscale | Codice fiscale del soggetto che ha formato il documento. |
| destinatario | Dati del destinatario del documento. |
| ragionesociale | Ragione sociale del destinatario del documento. Per convenzione, se non diversamente indicato, può essere impostato uguale a 'Sistema di conservazione'. |
| hashfilelulprecedente | Se il file è di tipo Libro Unico del Lavoro (LUL) va indicato l'eventuale hash, in formato SHA-256, del file LUL precedente a quello indicato. |
| IDdocumento | Identificativo univoco del documento. |
| Attributes | |
| class | Codice della classe documentale così come riconosciuta dal sistema di conservazione. |
| name | Descrizione della classe documentale. |
| Attribute | |
| code | Codice del metadato così come riconosciuto dal sistema di conservazione. |
| name | Descrizione del metadato. |
| value | Valore da assegnare al metadato. |

Process: rappresentazione grafica del file XSD

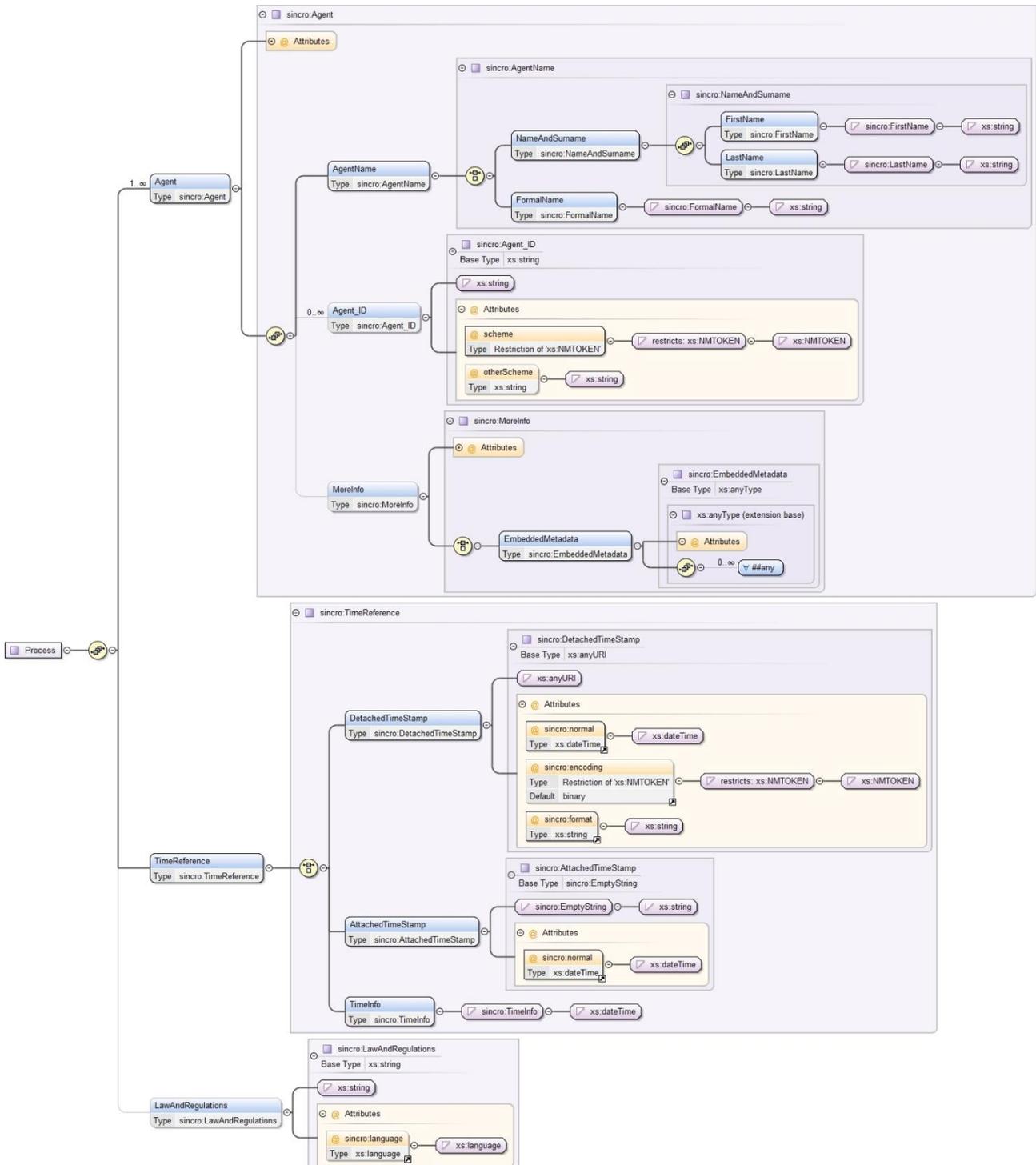


Figura 12
 Process: rappresentazione grafica del file XSD

| Nome elemento | Descrizione |
|----------------------|--|
| Agent | |
| Agent | Informazioni relative ai soggetti che intervengono nel processo di conservazione. |
| AgentName | Nome o denominazione dell'agente che interviene nel processo di conservazione. |
| NameAndSurname | Nome e cognome dell'agente che interviene nel processo di conservazione. Tale elemento deve essere valorizzato nel caso in cui l'Agente sia una persona; in caso contrario, occorre valorizzare l'elemento <FormalName>. |
| FirstName | Nome dell'agente che interviene nel processo di conservazione. |
| LastName | Cognome dell'agente che interviene nel processo di conservazione. |
| FormalName | Denominazione dell'agente che interviene nel processo di conservazione. Tale elemento deve assumere un valore nel caso in cui l'agente sia un ente. |
| Agent_ID | Identificatore univoco dell'agente che interviene nel processo di conservazione. Se l'identificatore è un codice valido in un ambito nazionale (per esempio un codice fiscale), a tale codice deve essere premesso il codice di paese individuato da ISO 3166, seguito dal carattere ":" (due punti). |
| MoreInfo | Metadati da associare al processo. Tali informazioni devono essere strutturate nel formato XML, utilizzando lo Schema XML che è illustrato di seguito. |
| TimeReference | |
| TimeReference | Informazioni relative a data e ora di realizzazione dell'indice di conservazione. Tale elemento funge da mero contenitore di elementi subordinati, per distinguere i seguenti casi: - generico riferimento temporale (usato per valorizzare l'elemento <TimeInfo>); - marca temporale detached (il cui indirizzo URI valorizza l'elemento <DetachedTimeStamp>); - marca temporale attached (all'elemento vuoto <AttachedTimeStamp> è associata la data in forma normale). |
| DetachedTimeStamp | Informazioni sulla localizzazione della marca temporale detached relativa a data e ora di realizzazione dell'indice di conservazione. Il valore dell'elemento deve essere espresso nel nome del file .tsr che contiene la marca temporale. |
| AttachedTimeStamp | Data e ora di realizzazione dell'indice di conservazione, in forma normalizzata. |
| TimeInfo | Informazioni relative a data e ora di realizzazione dell'indice di conservazione, nel caso in cui queste non assumano la forma di una marca temporale. Il valore dell'elemento deve essere nel formato UNI ISO 8601:2010, nella forma |

| | |
|--------------------------|---|
| | YYYY-MM-DDT00:00:00□00 (per l'Italia è di default +01). |
| LawAndRegulations | |
| LawAndRegulations | Informazioni su norme, regolamenti e standard che guidano il processo di conservazione. |

Moreinfo di Agent: rappresentazione grafica del file XSD

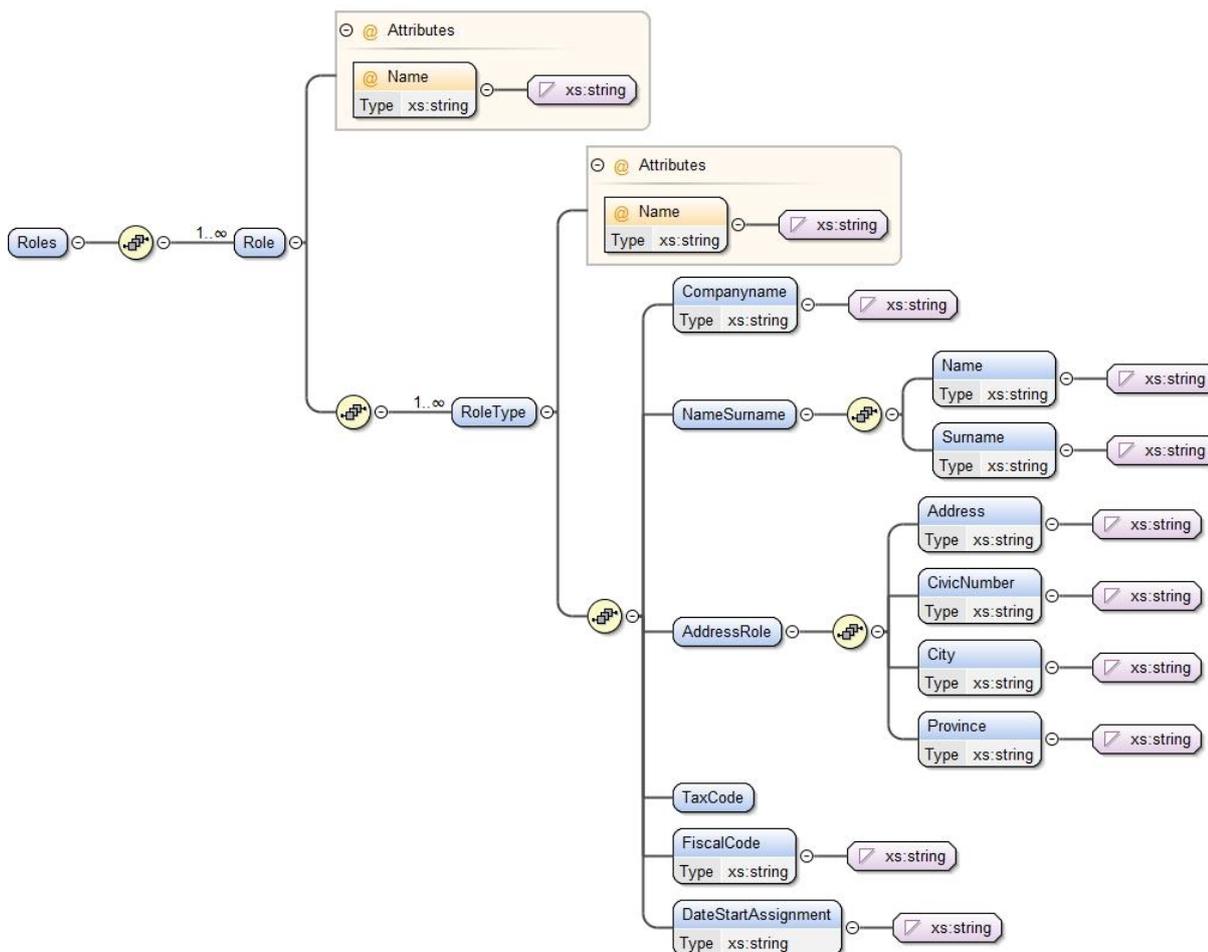


Figura 13
Moreinfo di Agent: rappresentazione grafica del file XSD

| Nome elemento | Descrizione |
|-----------------|---|
| Role | |
| Name | Descrizione del ruolo |
| RoleType | |
| Name | Descrizione della tipologia di ruolo. |
| Companyname | Ragione sociale se il ruolo è assunto da un ente. |
| NameSurname | Dati della persona se il ruolo è assunto da una persona fisica. |
| Name | Nome della persona |
| Surname | Cognome della persona |

| | |
|---------------------|-----------------------------|
| AddressRole | Dati relativo all'indirizzo |
| Address | Indirizzo |
| CivicNumber | Numero civico |
| City | Comune |
| Province | Sigla della provincia |
| TaxCode | Eventuale partita IVA |
| FiscalCode | Codice fiscale |
| DateStartAssignment | Data di inizio incarico |

Eventuali personalizzazioni sul Pacchetto di Versamento devono essere concordate tra le parti e descritte nell'allegato "Scheda servizio – Specificità del contratto".

[Torna al sommario](#)

6.11 Pacchetto di archiviazione

Il pacchetto di archiviazione contiene i file accettati nel sistema di conservazione in seguito a generazione di rapporto di versamento.

In un pacchetto di archiviazione possono confluire i file di uno o più pacchetti di versamento.

Periodicamente, in funzione dello scadenziario di lavorazione definito nel contratto, sono preparati i pacchetti di archiviazione.

La generazione avviene aggregando documenti che appartengono allo stesso cliente ed alla stessa classe documentale; questo non è un vincolo tecnico ma una configurazione ritenuta congruente con le esigenze di una ordinata conservazione.

La preparazione avviene automaticamente; può essere anche eseguita manualmente ma il default è che venga eseguita automaticamente.

Il pacchetto di archiviazione è un contenitore informativo contenente:

- I documenti informatici individuati per la conservazione, eventualmente firmati digitalmente nello standard di firma Cades (.p7m) oppure nello standard di firma PadES (PDF Advanced Electronic Signature).
- Un file XML come da Norma UNI 11386 (SInCRO) contenente l'indice dei documenti informatici da conservare.
- Un file in formato.tsr che contiene l'impronta del file XML SInCRO sottoposto a marca temporale e l'evidenza informatica dell'apposizione della marca temporale.

Il file indice del pacchetto di archiviazione è un file in formato XML conforme allo standard UNI SInCRO 11386:2010 che ha titolo "Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (SInCRO)".

La norma UNI individua gli elementi informativi necessari alla creazione dell'indice di conservazione descrivendone sia la semantica sia l'articolazione per mezzo del linguaggio formale XML.

Il file SInCRO viene firmato digitalmente dal Responsabile del servizio di Conservazione e marcato temporalmente.

In particolare nel pacchetto di archiviazione sono identificate le seguenti informazioni:

- il Produttore del pacchetto
- l'applicativo che ha prodotto il pacchetto
- il gruppo cui appartiene il pacchetto
- i gruppi cui appartengono i documenti inclusi nel pacchetto
- i documenti inclusi nel pacchetto con i metadati relativi
- la classe documentale
- i soggetti coinvolti nel processo di conservazione
- informazioni relative a data e ora di realizzazione del pacchetto
- i riferimenti normativi

Di seguito vengono illustrate le informazioni contenute nel file XML del pacchetto di archiviazione:

Le definizioni che seguono sono riprese dalla norma Norma UNI 11386 (SInCRO)

Rappresentazione grafica del file XSD dell'indice del pacchetto di archiviazione.

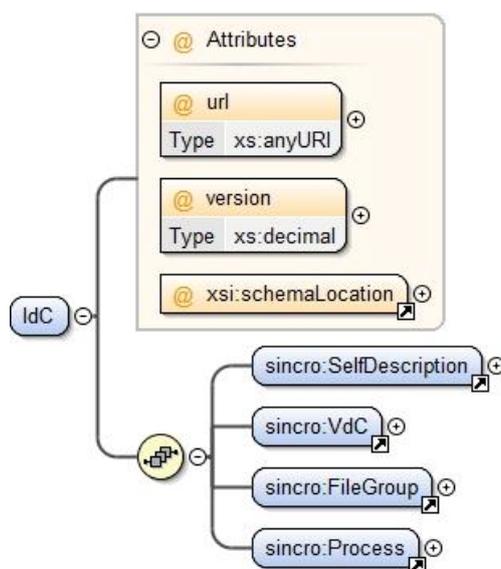


Figura 14

Rappresentazione grafica del file XSD dell'indice del pacchetto di archiviazione.

IdC: Indice di Conservazione: sono le informazioni relative ai file oggetto di conservazione e al processo di conservazione.

Elementi sovraordinati: nessuno.

Elementi subordinati: SelfDescription, FileGroup, Process, VdC.

SelfDescription: rappresentazione grafica del file XSD

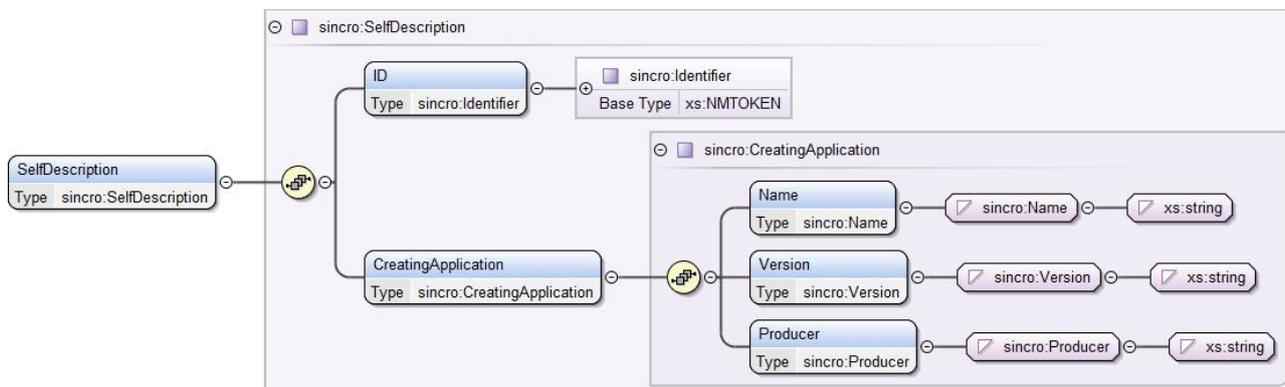


Figura 15
SelfDescription: rappresentazione grafica del file XSD

| Nome elemento | Descrizione |
|---------------------|--|
| SelfDescription | Informazioni relative all'indice di conservazione stesso. |
| ID | Identificatore univoco dell'entità descritta. |
| CreatingApplication | Informazioni sull'applicazione che ha generato l'IdC. |
| Name | Nome dell'applicazione che ha generato l'IdC. |
| Version | Versione dell'applicazione che ha generato l'IdC. |
| Producer | Nome del produttore dell'applicazione che ha generato l'IdC. |

VdC: rappresentazione grafica del file XSD

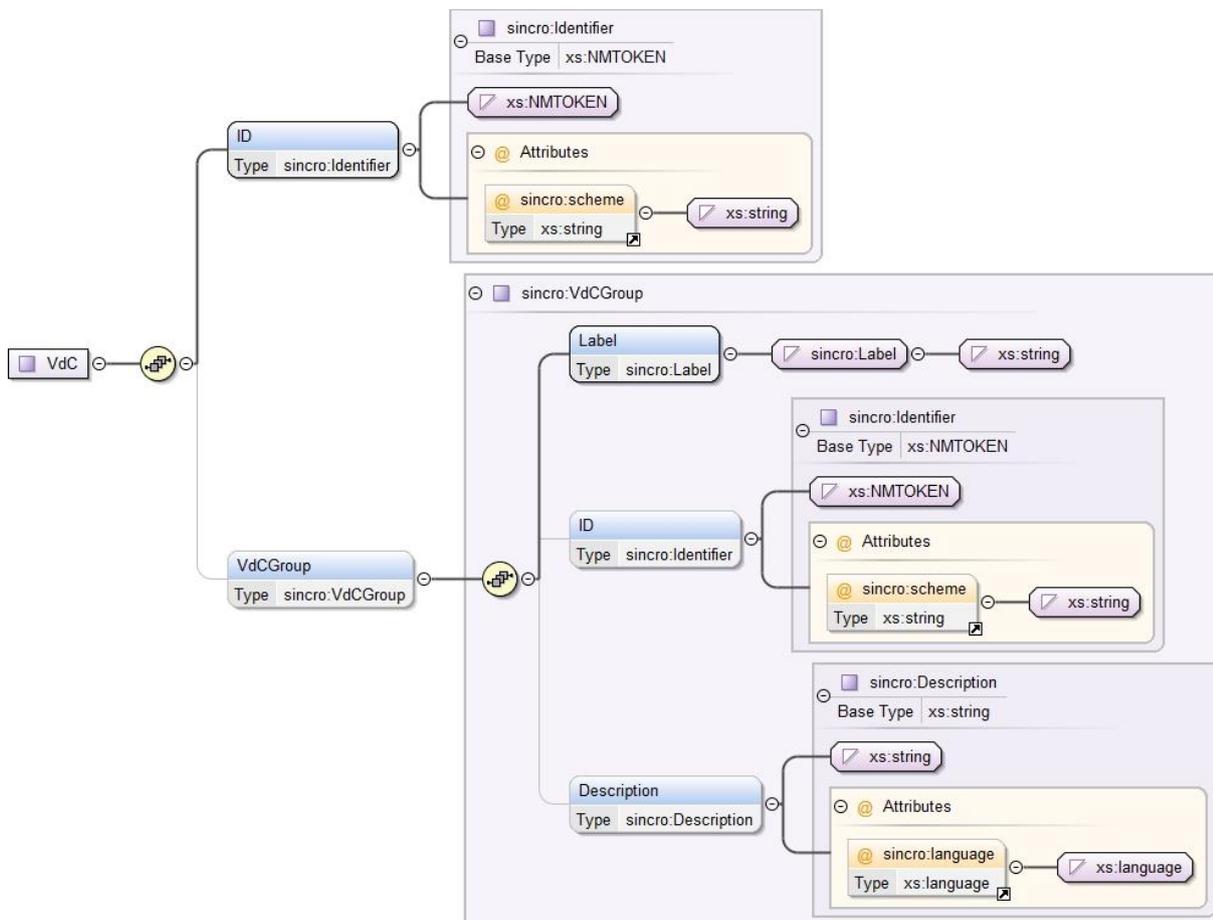


Figura 16
VdC: rappresentazione grafica del file XSD

| Nome elemento | Descrizione |
|---------------|---|
| ID | Identificatore univoco dell'entità descritta. |
| Description | Descrizione del volume di conservazione. |

FileGroup: rappresentazione grafica del file XSD

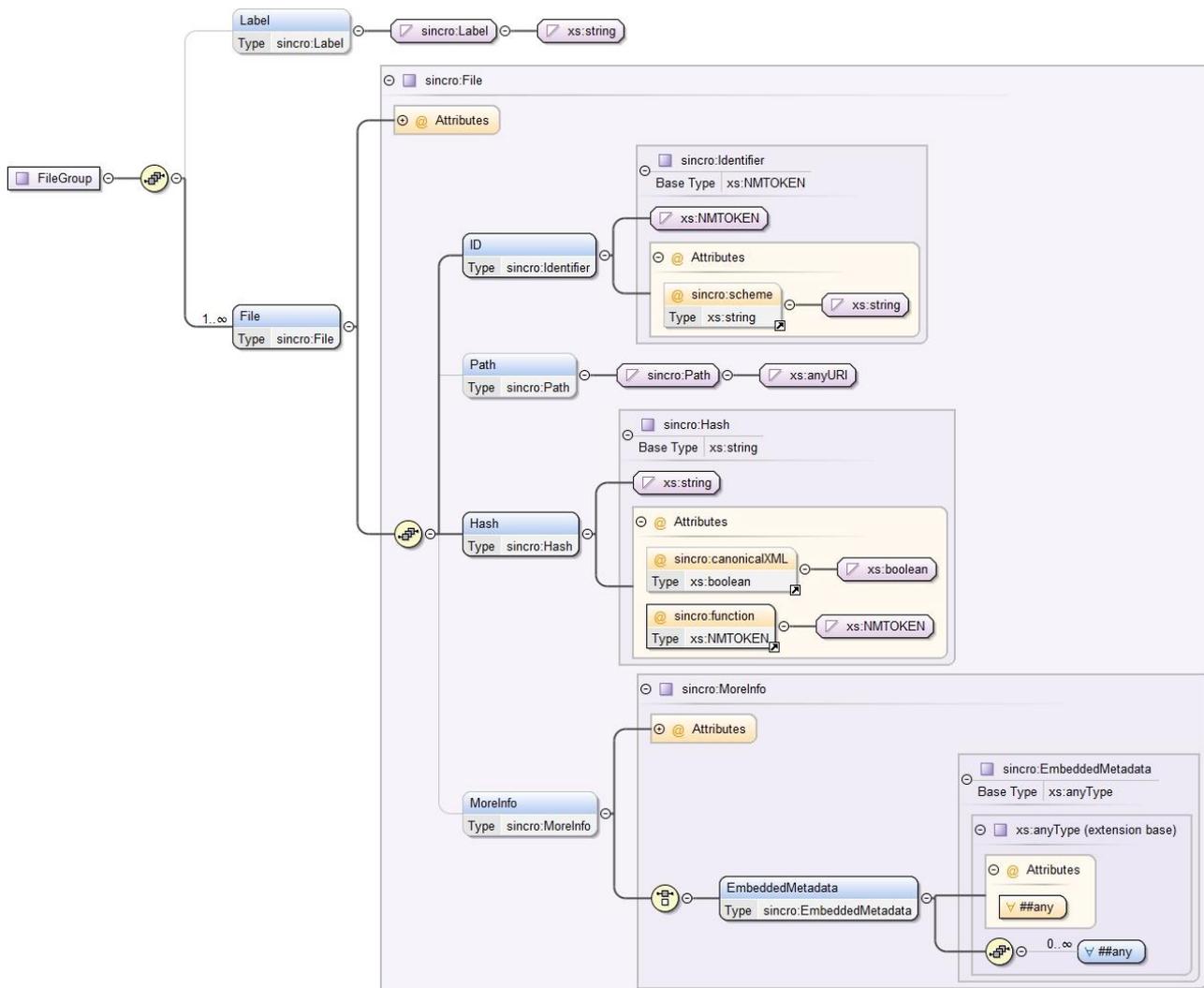


Figura 17
FileGroup: rappresentazione grafica del file XSD

| Nome elemento | Descrizione |
|---------------|---|
| File | Informazioni relative al file oggetto di conservazione. |
| ID | Identificatore univoco del file. |
| Path | Nome del file comprensivo di estensione. |
| Hash | Informazioni sull'impronta in formato SHA-256 del file cui l'elemento si riferisce. |
| MoreInfo | Metadati da associare al file. Tali informazioni devono essere strutturate nel formato XML, utilizzando lo Schema XML che è illustrato di seguito. |

Moreinfo di file: rappresentazione grafica del file XSD

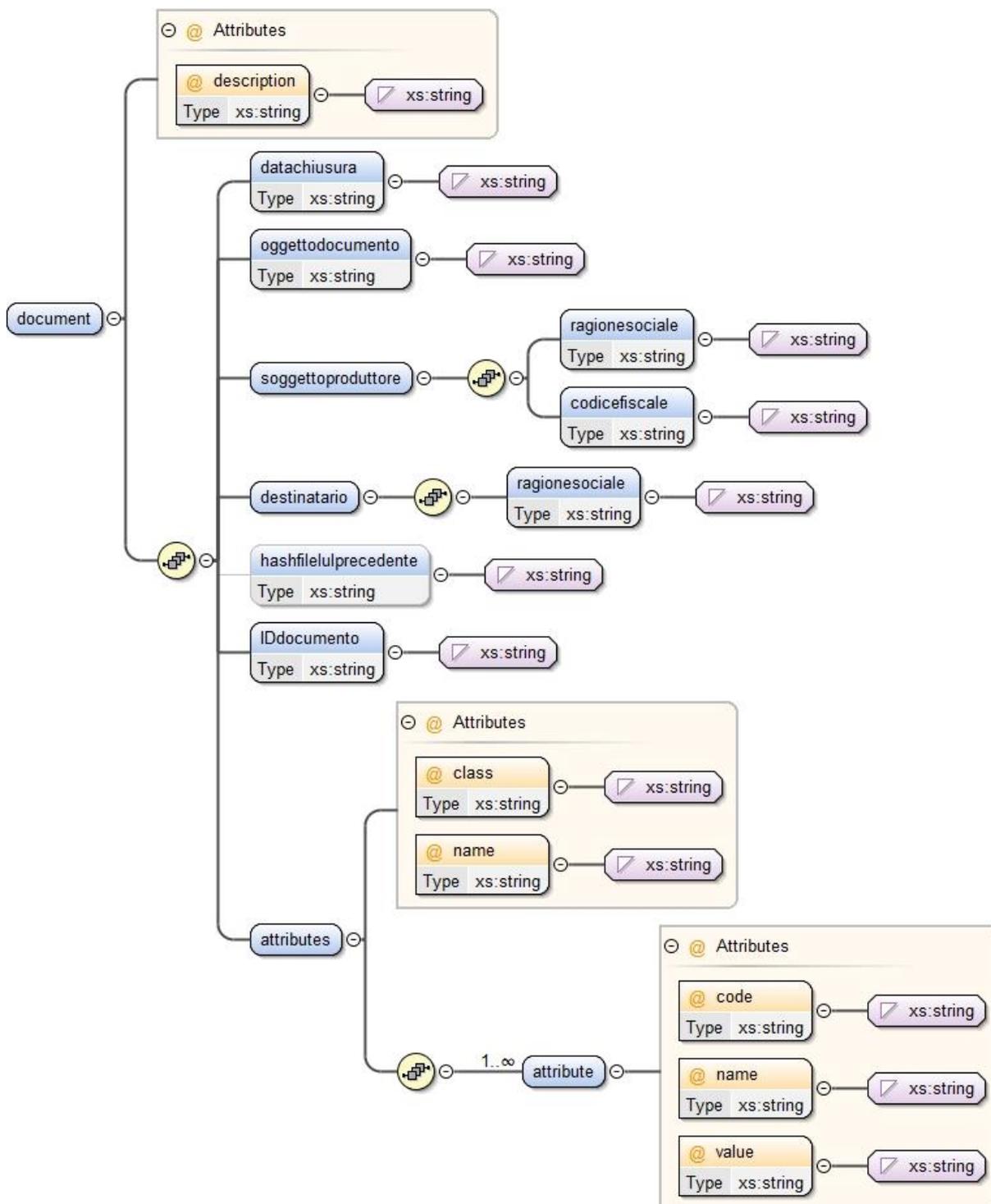


Figura 18
 Moreinfo di file: rappresentazione grafica del file XSD

| Nome elemento | Descrizione |
|-----------------------|--|
| Description | Nome del file comprensivo di estensione. |
| datachiusura | Data di formazione del documento. |
| oggettodocumento | Oggetto del documento. Per convenzione, se non diversamente indicato, può coincidere con la descrizione della classe documentale cui appartiene il documento. |
| Produttore | Dati del soggetto che ha formato il documento. |
| ragionesociale | Ragione sociale o cognome e nome del soggetto che ha formato il documento. |
| codicefiscale | Codice fiscale del soggetto che ha formato il documento. |
| destinatario | Dati del destinatario del documento. |
| ragionesociale | Ragione sociale del destinatario del documento. Per convenzione, se non diversamente indicato, può essere impostato uguale a 'Sistema di conservazione'. |
| hashfilelulprecedente | Se il file è di tipo Libro Unico del Lavoro (LUL) va indicato l'eventuale hash, in formato SHA-256, del file LUL precedente a quello indicato. |
| IDdocumento | Identificativo univoco del documento. |
| Attributes | |
| class | Codice della classe documentale così come riconosciuta dal sistema di conservazione. |
| name | Descrizione della classe documentale. |
| Attribute | |
| code | Codice del metadato così come riconosciuto dal sistema di conservazione. |
| name | Descrizione del metadato. |
| value | Valore da assegnare al metadato. |

Process: rappresentazione grafica del file XSD

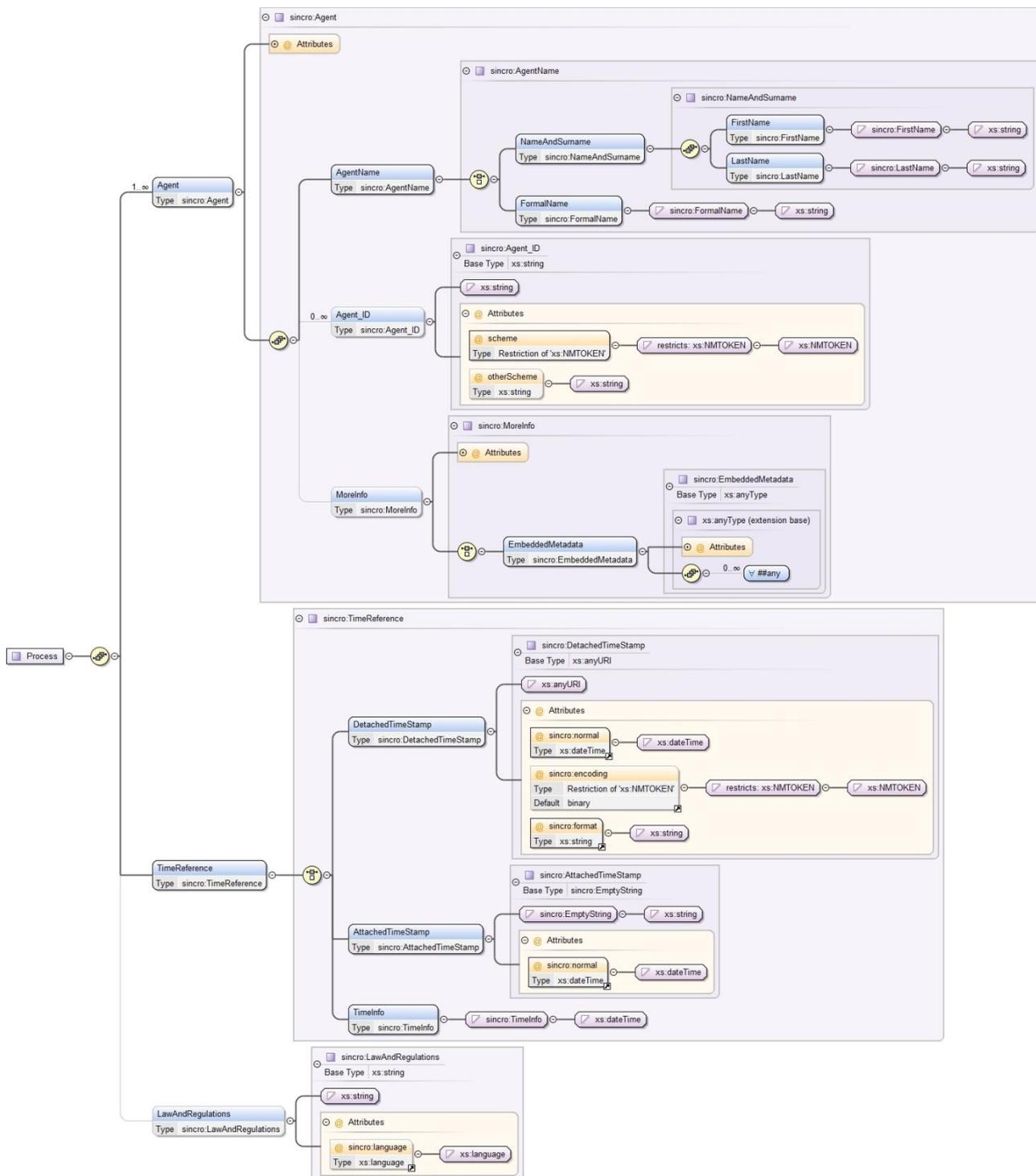


Figura 19
Process: rappresentazione grafica del file XSD

| Nome elemento | Descrizione |
|----------------------|--|
| Agent | |
| Agent | Informazioni relative ai soggetti che intervengono nel processo di conservazione. |
| AgentName | Nome o denominazione dell'agente che interviene nel processo di conservazione. |
| NameAndSurname | Nome e cognome dell'agente che interviene nel processo di conservazione. Tale elemento deve essere valorizzato nel caso in cui l'Agente sia una persona; in caso contrario, occorre valorizzare l'elemento <FormalName>. |
| FirstName | Nome dell'agente che interviene nel processo di conservazione. |
| LastName | Cognome dell'agente che interviene nel processo di conservazione. |
| FormalName | Denominazione dell'agente che interviene nel processo di conservazione. Tale elemento deve assumere un valore nel caso in cui l'agente sia un ente. |
| Agent_ID | Identificatore univoco dell'agente che interviene nel processo di conservazione. Se l'identificatore è un codice valido in un ambito nazionale (per esempio un codice fiscale), a tale codice deve essere premesso il codice di paese individuato da ISO 3166, seguito dal carattere ":" (due punti). |
| MoreInfo | Metadati da associare al processo. Tali informazioni devono essere strutturate nel formato XML, utilizzando lo Schema XML che è illustrato di seguito. |
| TimeReference | |
| TimeReference | Informazioni relative a data e ora di realizzazione dell'indice di conservazione. Tale elemento funge da mero contenitore di elementi subordinati, per distinguere i seguenti casi: - generico riferimento temporale (usato per valorizzare l'elemento <TimeInfo>); - marca temporale detached (il cui indirizzo URI valorizza l'elemento <DetachedTimeStamp>); - marca temporale attached (all'elemento vuoto <AttachedTimeStamp> è associata la data in forma normale). |
| DetachedTimeStamp | Informazioni sulla localizzazione della marca temporale detached relativa a data e ora di realizzazione dell'indice di conservazione. Il valore dell'elemento deve essere espresso nel nome del file .tsr che contiene la marca temporale. |
| AttachedTimeStamp | Data e ora di realizzazione dell'indice di conservazione, in forma normalizzata. |
| TimeInfo | Informazioni relative a data e ora di realizzazione dell'indice di conservazione, nel caso in cui queste non assumano la forma di una marca temporale. Il valore dell'elemento deve essere nel |

| | |
|--------------------------|---|
| | formato UNI ISO 8601:2010, nella forma YYYY-MM-DDT00:00:00□00 (per l'Italia è di default +01). |
| LawAndRegulations | |
| LawAndRegulations | Informazioni su norme, regolamenti e standard che guidano il processo di conservazione. |

Moreinfo di Agent: rappresentazione grafica del file XSD

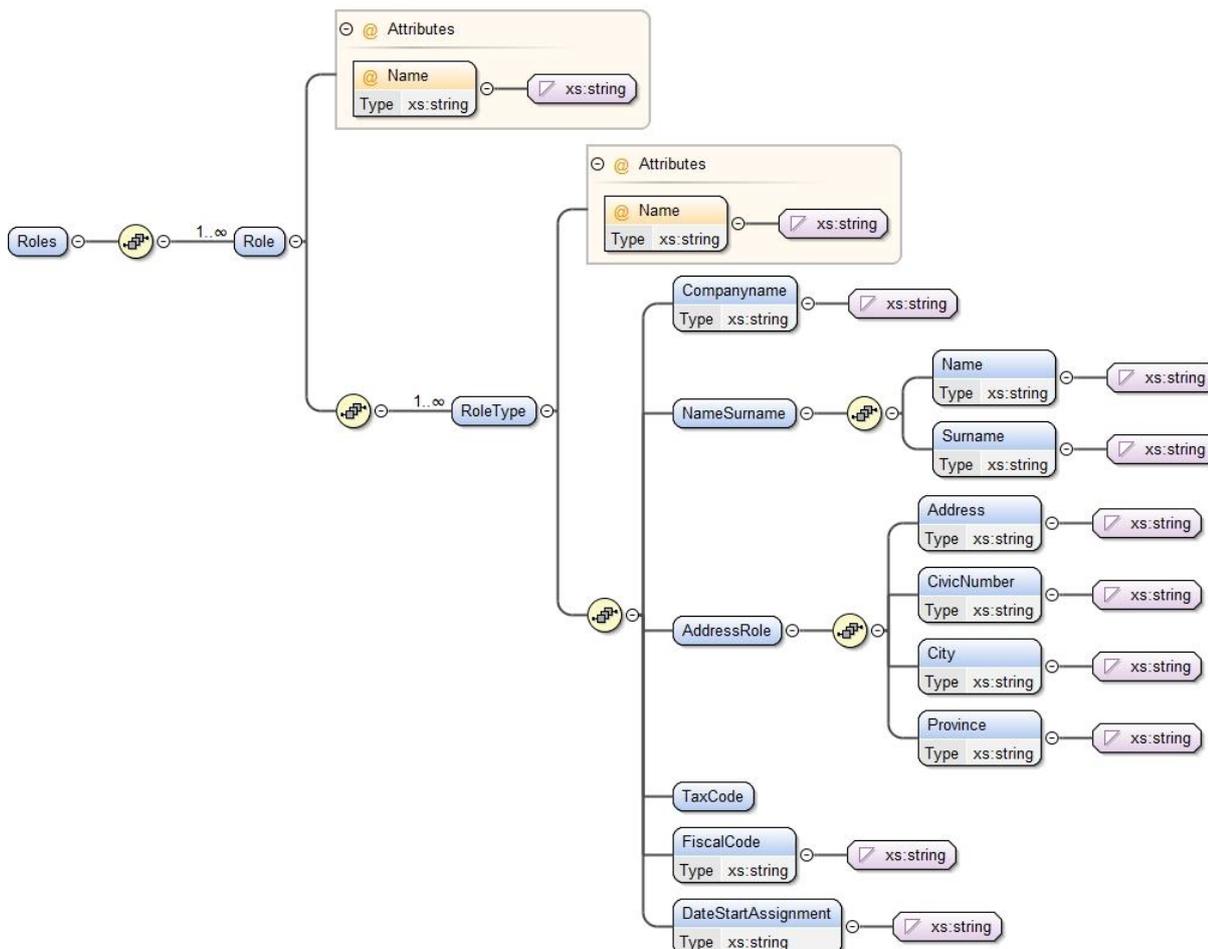


Figura 20
Moreinfo di Agent: rappresentazione grafica del file XSD

| Nome elemento | Descrizione |
|-----------------|---|
| Role | |
| Name | Descrizione del ruolo |
| RoleType | |
| Name | Descrizione della tipologia di ruolo. |
| Companyname | Ragione sociale se il ruolo è assunto da un ente. |
| NameSurname | Dati della persona se il ruolo è assunto da una persona fisica. |

| | |
|---------------------|-----------------------------|
| Name | Nome della persona |
| Surname | Cognome della persona |
| AddressRole | Dati relativo all'indirizzo |
| Address | Indirizzo |
| CivicNumber | Numero civico |
| City | Comune |
| Province | Sigla della provincia |
| TaxCode | Eventuale partita IVA |
| FiscalCode | Codice fiscale |
| DateStartAssignment | Data di inizio incarico |

[Torna al sommario](#)

6.12 Pacchetto di distribuzione

Il pacchetto di distribuzione viene lavorato in seguito a richiesta eseguita dall'utente tramite apposita funzionalità presente nell'applicazione.

Il pacchetto di distribuzione è composto da un file in formato compresso (.zip) contenente:

i documenti informatici richiesti dall'utente, eventualmente firmati digitalmente nello standard di firma Cades (.p7m) oppure nello standard di firma PadES (PDF Advanced Electronic Signature).

Un file XML come da Norma UNI 11386 (SInCRO) contenente l'indice dei documenti informatici oggetto di distribuzione.

Se è stata richiesta la marca temporale viene distribuito anche il file in formato .tsr che contiene l'impronta del file XML SInCRO del PDD sottoposto a marca temporale e l'evidenza informatica dell'apposizione della marca temporale.

Il file XML SInCRO dell'indice del pacchetto di archiviazione con cui sono stati conservati i documenti richiesti.

Il file in formato .tsr che contiene l'impronta del file XML SInCRO dell'indice del pacchetto di archiviazione sottoposto a marca temporale e l'evidenza informatica dell'apposizione della marca temporale.

Se i documenti richiesti sono in numero superiore ad uno e risultano associati a pacchetti di archiviazione diversi sono prodotti tanti zip quanti sono i pacchetti di archiviazione.

In particolare nel pacchetto di archiviazione sono identificate le seguenti informazioni:

- il Produttore del pacchetto
- l'applicativo che ha prodotto il pacchetto
- il gruppo cui appartiene il pacchetto
- i gruppi cui appartengono i documenti inclusi nel pacchetto
- i documenti inclusi nel pacchetto con i metadati relativi
- la classe documentale
- i soggetti coinvolti nel processo di conservazione
- informazioni relative a data e ora di realizzazione del pacchetto
- i riferimenti normativi

Di seguito vengono illustrate le informazioni contenute nel file XML del pacchetto di distribuzione.

Le definizioni che seguono sono riprese dalla norma Norma UNI 11386 (SInCRO)

Rappresentazione grafica del file XSD dell'indice del pacchetto di archiviazione.

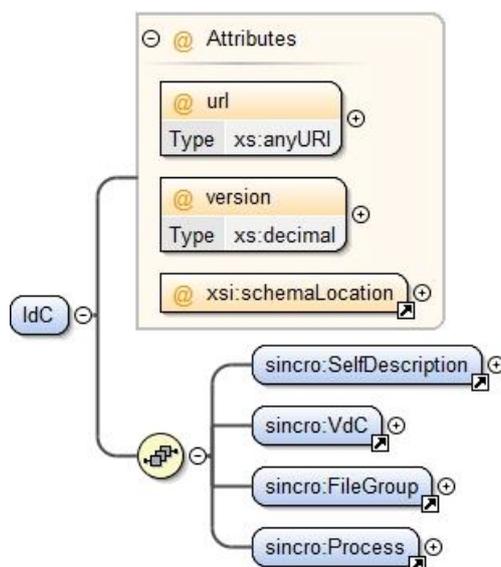


Figura 21

Rappresentazione grafica del file XSD dell'indice del pacchetto di archiviazione.

IdC: Indice di Conservazione: sono le informazioni relative ai file oggetto di conservazione e al processo di conservazione.

Elementi sovraordinati: nessuno.

Elementi subordinati: SelfDescription, FileGroup, Process, VdC.

SelfDescription: rappresentazione grafica del file XSD

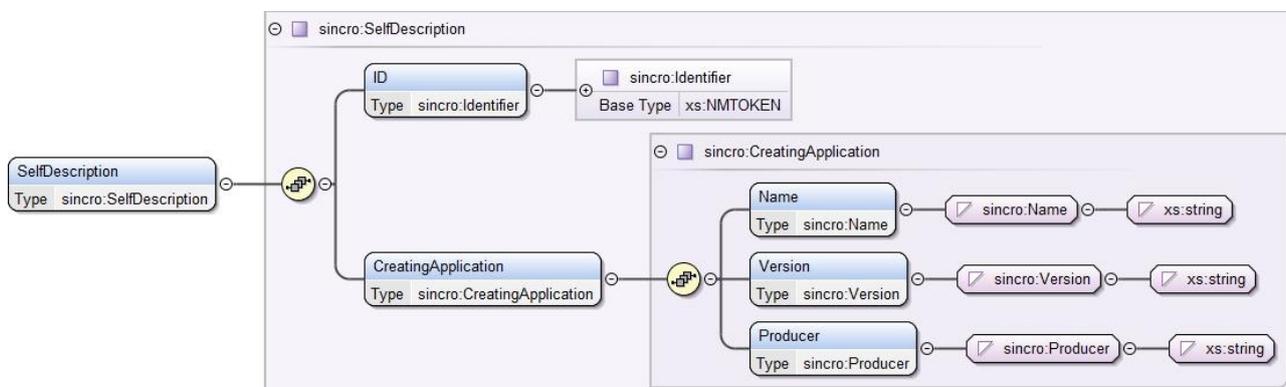


Figura 22

SelfDescription: rappresentazione grafica del file XSD

| Nome elemento | Descrizione |
|---------------------|---|
| SelfDescription | Informazioni relative all'indice di conservazione stesso. |
| ID | Identificatore univoco dell'entità descritta, generato automaticamente dal sistema. |
| CreatingApplication | Applicazione che ha generato l'IdC. |
| Name | Nome dell'applicazione che ha generato l'IdC. |
| Version | Versione dell'applicazione che ha generato l'IdC. |
| Producer | Nome del produttore dell'applicazione che ha generato l'IdC. |

VdC: rappresentazione grafica del file XSD

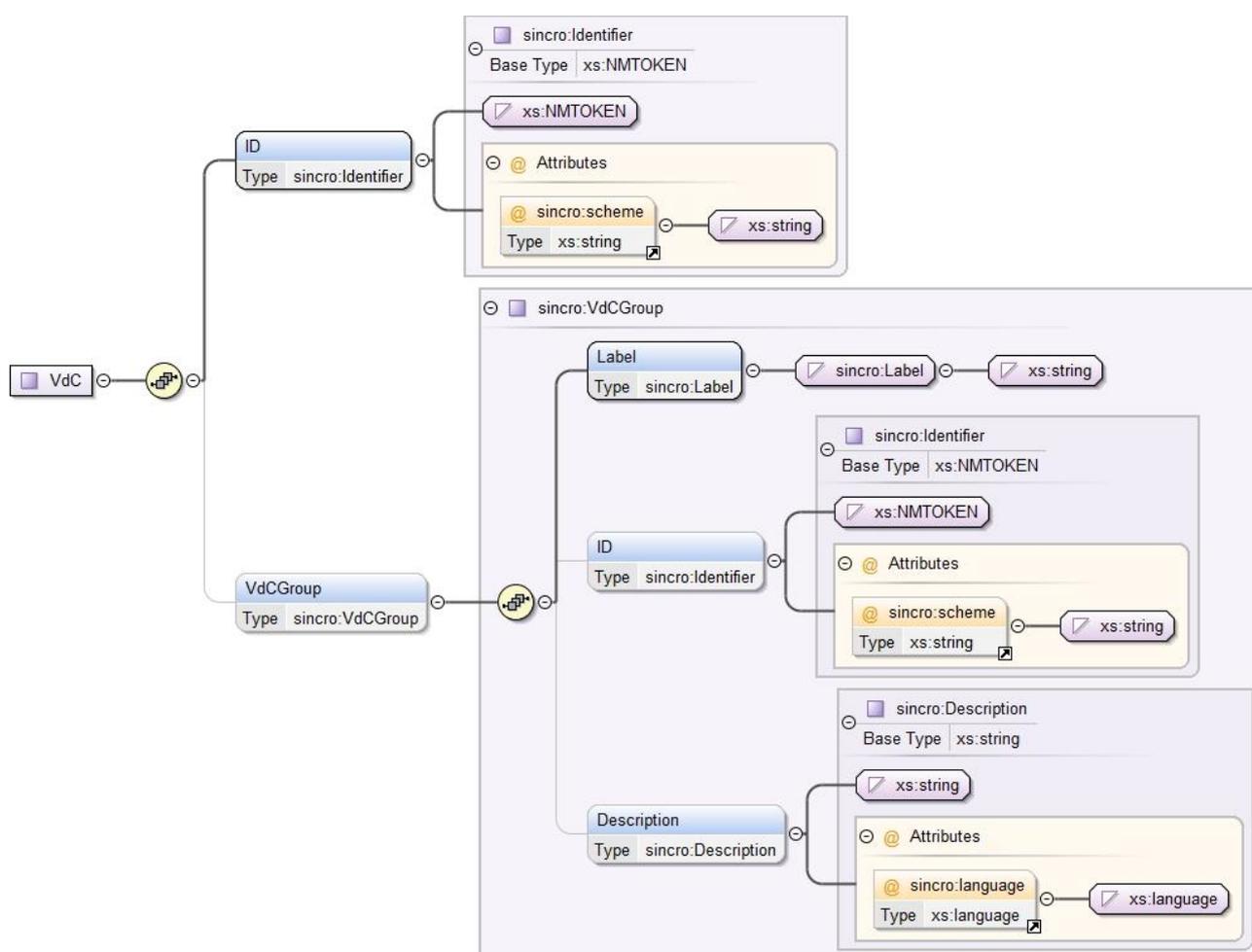


Figura 23
VdC: rappresentazione grafica del file XSD

| Nome elemento | Descrizione |
|---------------|---|
| ID | Identificatore univoco dell'entità descritta, generato automaticamente dal sistema. |
| Description | Descrizione del volume di conservazione. |

FileGroup: rappresentazione grafica del file XSD

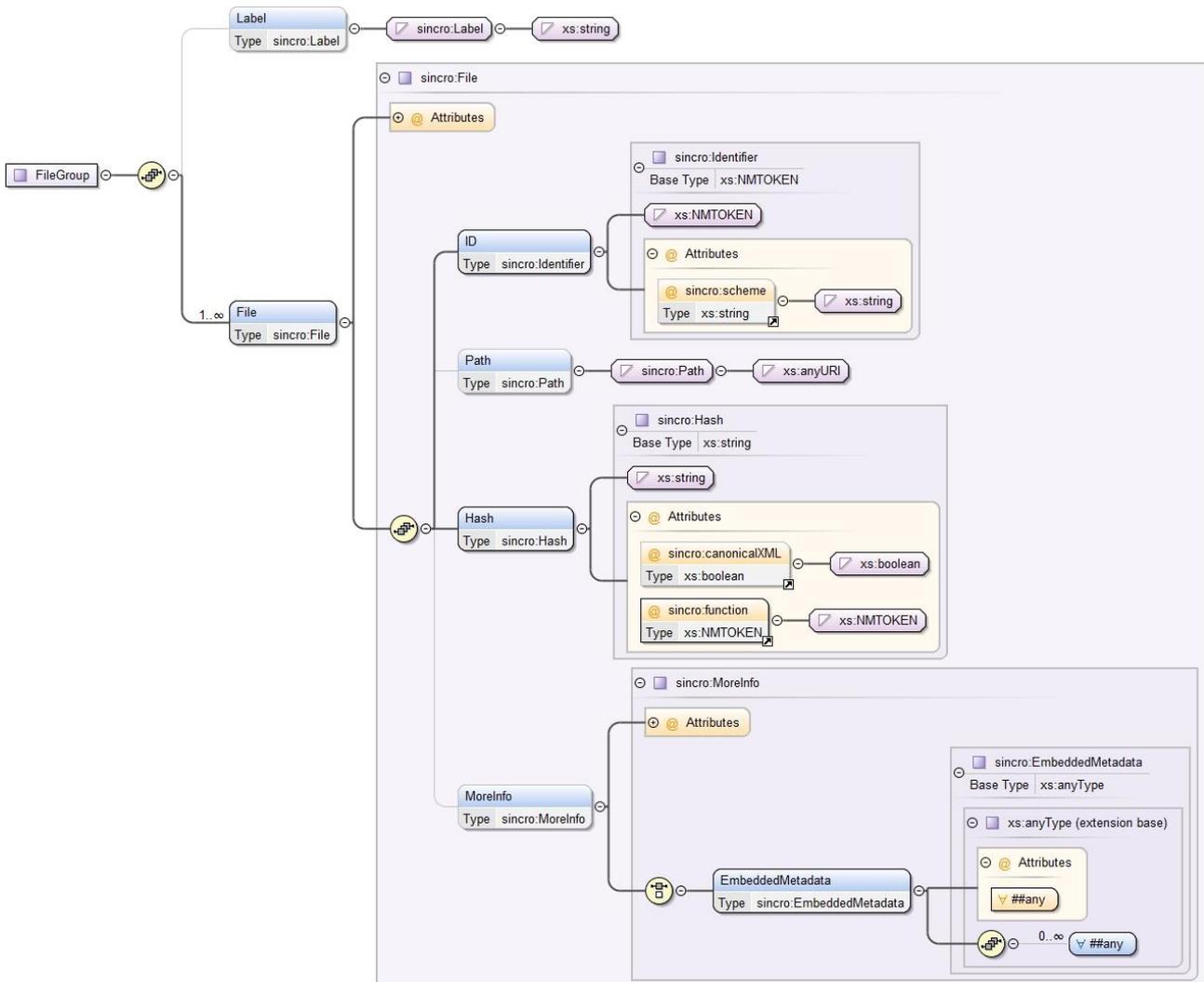


Figura 24
FileGroup: rappresentazione grafica del file XSD

| Nome elemento | Descrizione |
|---------------|---|
| File | Informazioni relative al file oggetto di conservazione. |
| ID | Identificatore univoco del file. |
| Path | Nome del file comprensivo di estensione. |
| Hash | Informazioni sull'impronta in formato SHA-256 del file cui l'elemento si riferisce. |
| MoreInfo | Metadati associati al file. Tali informazioni sono strutturate nel formato XML, utilizzando lo Schema XML che è illustrato di seguito. |

Moreinfo di file: rappresentazione grafica del file XSD

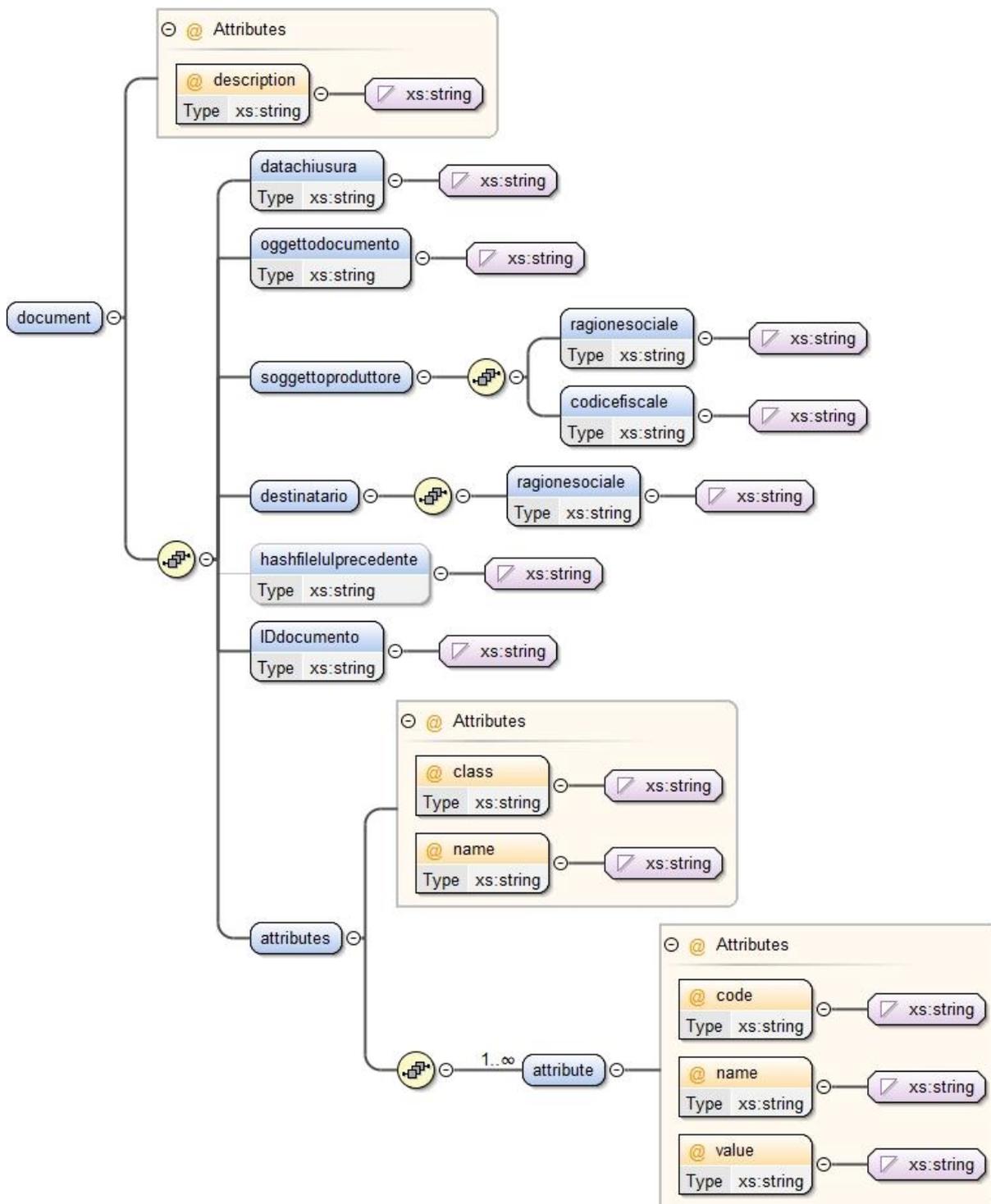


Figura 25
 Moreinfo di file: rappresentazione grafica del file XSD

| Nome elemento | Descrizione |
|-----------------------|---|
| Description | Nome del file comprensivo di estensione. |
| datachiusura | Data di formazione del documento. |
| oggettodocumento | Oggetto del documento. |
| Produttore | Dati del soggetto che ha formato il documento. |
| ragionesociale | Ragione sociale o cognome e nome del soggetto che ha formato il documento. |
| codicefiscale | Codice fiscale del soggetto che ha formato il documento. |
| destinatario | Dati del destinatario del documento. |
| ragionesociale | Ragione sociale del destinatario del documento. |
| hashfilelulprecedente | Se il file è di tipo Libro Unico del Lavoro (LUL) viene indicato l'eventuale hash, in formato SHA-256, del file LUL precedente a quello indicato. |
| IDdocumento | Identificativo univoco del documento. |
| Attributes | |
| class | Codice della classe documentale così come riconosciuta dal sistema di conservazione. |
| name | Descrizione della classe documentale. |
| Attribute | |
| code | Codice del metadato così come riconosciuto dal sistema di conservazione. |
| name | Descrizione del metadato. |
| value | Valore assegnato al metadato. |

Process: rappresentazione grafica del file XSD

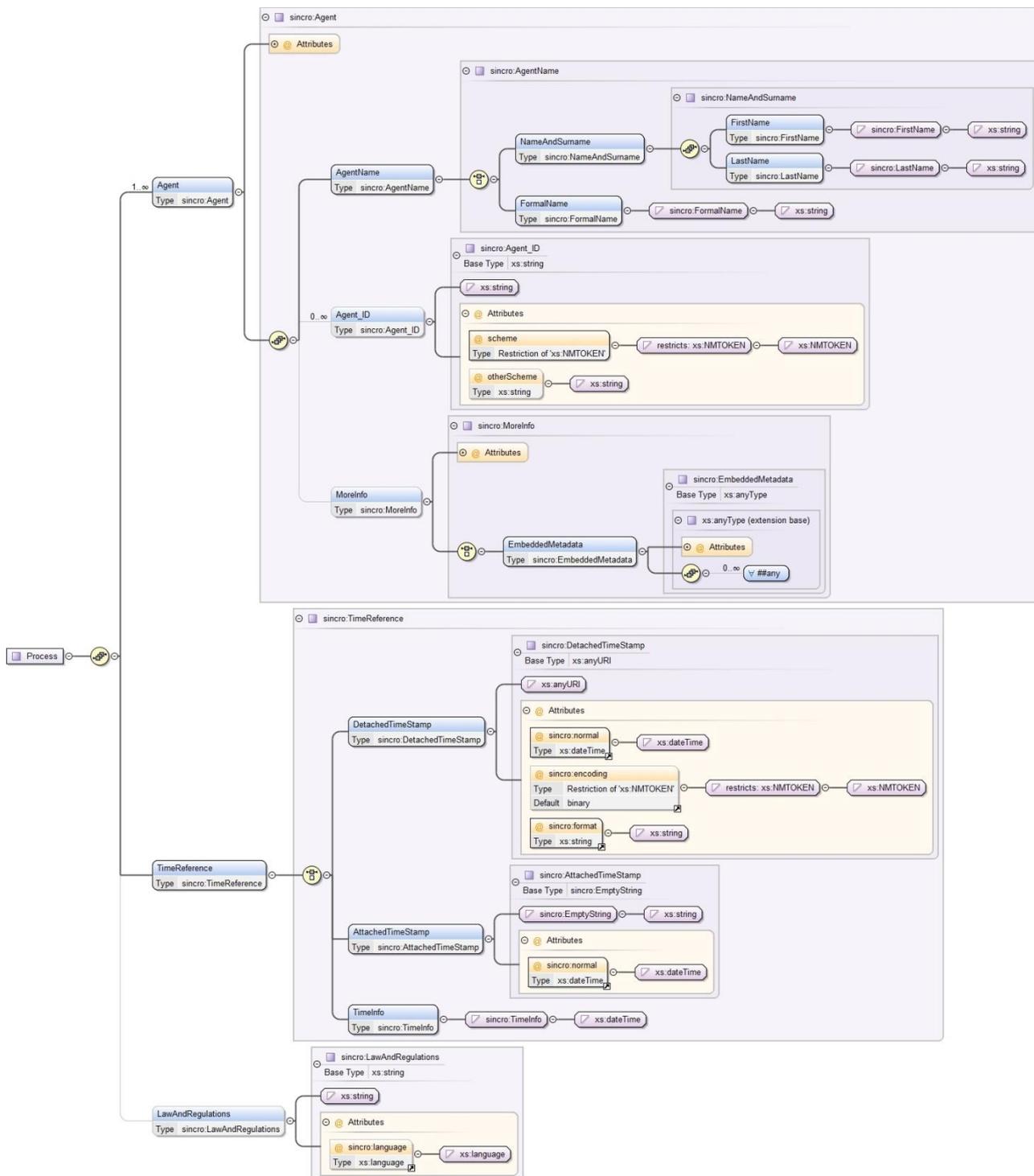


Figura 26
Process: rappresentazione grafica del file XSD

| Nome elemento | Descrizione |
|--------------------------|---|
| Agent | |
| Agent | Informazioni relative ai soggetti che intervengono nel processo di conservazione. |
| AgentName | Nome o denominazione dell'agente che interviene nel processo di conservazione. |
| NameAndSurname | Nome e cognome dell'agente che interviene nel processo di conservazione. Tale elemento deve essere valorizzato nel caso in cui l'Agente sia una persona; in caso contrario, occorre valorizzare l'elemento <FormalName>. |
| FirstName | Nome dell'agente che interviene nel processo di conservazione. |
| LastName | Cognome dell'agente che interviene nel processo di conservazione. |
| FormalName | Denominazione dell'agente che interviene nel processo di conservazione. Tale elemento deve assumere un valore nel caso in cui l'agente sia un ente. |
| Agent_ID | Identificatore univoco dell'agente che interviene nel processo di conservazione. Se l'identificatore è un codice valido in un ambito nazionale (per esempio un codice fiscale), a tale codice viene premesso il codice di paese individuato da ISO 3166, seguito dal carattere ":" (due punti). |
| MoreInfo | Metadati associati al processo. Tali informazioni sono strutturate nel formato XML, secondo lo Schema XML che è illustrato di seguito. |
| TimeReference | |
| TimeReference | Informazioni relative alla marca temporale detached (il cui indirizzo URI valorizza l'elemento <DetachedTimeStamp>). |
| DetachedTimeStamp | Informazioni sulla localizzazione della marca temporale detached relativa a data e ora di realizzazione dell'indice di conservazione. Il valore dell'elemento viene espresso nel nome del file .tsr che contiene la marca temporale. |
| AttachedTimeStamp | Data e ora di realizzazione dell'indice di conservazione, in forma normalizzata. |
| LawAndRegulations | |
| LawAndRegulations | Informazioni su norme, regolamenti e standard che guidano il processo di conservazione. |

Moreinfo di Agent: rappresentazione grafica del file XSD

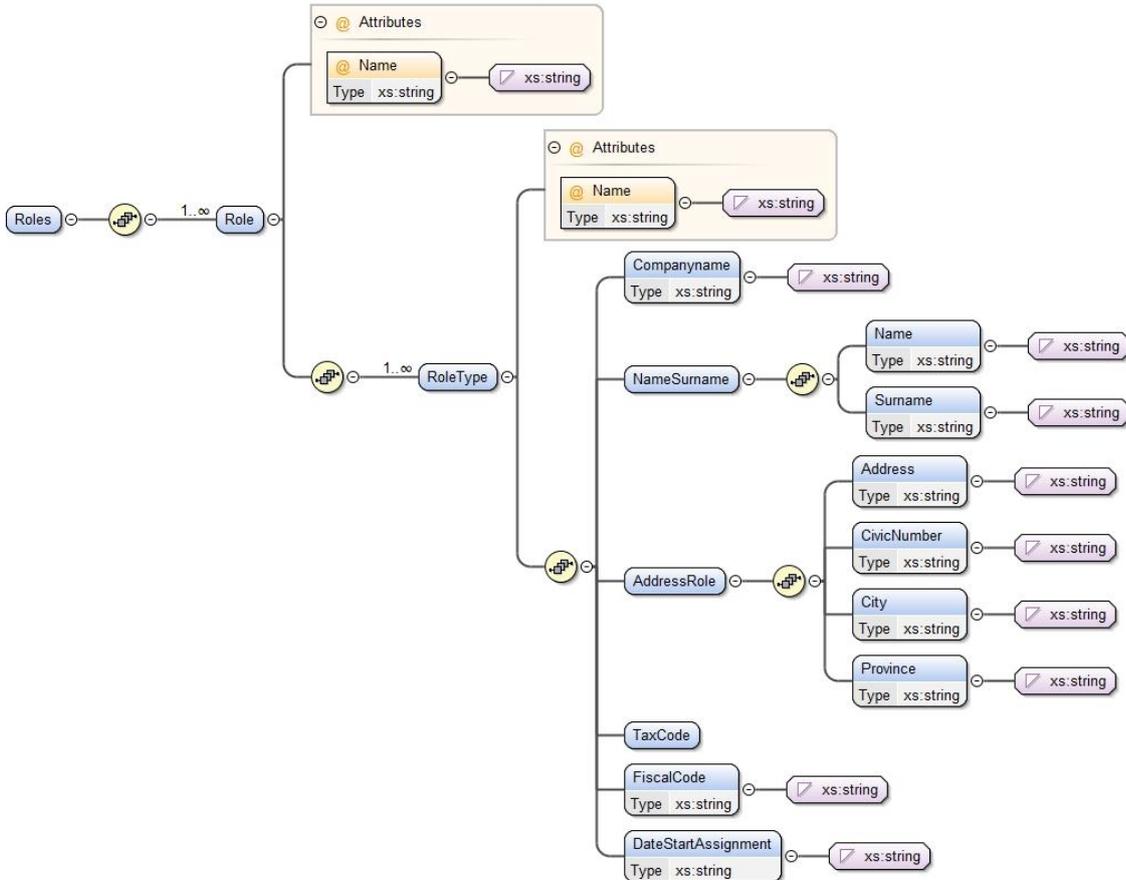


Figura 27
Moreinfo di Agent: rappresentazione grafica del file XSD

| Nome elemento | Descrizione |
|---------------------|---|
| Role | |
| Name | Descrizione del ruolo |
| RoleType | |
| Name | Descrizione della tipologia di ruolo. |
| Companyname | Ragione sociale se il ruolo è assunto da un ente. |
| NameSurname | Dati della persona se il ruolo è assunto da una persona fisica. |
| Name | Nome della persona |
| Surname | Cognome della persona |
| AddressRole | Dati relativo all'indirizzo |
| Address | Indirizzo |
| CivicNumber | Numero civico |
| City | Comune |
| Province | Sigla della provincia |
| TaxCode | Eventuale partita IVA |
| FiscalCode | Codice fiscale |
| DateStartAssignment | Data di inizio incarico |

[Torna al sommario](#)

7. IL PROCESSO DI CONSERVAZIONE

È possibile sintetizzare il processo di conservazione nei passaggi elencati di seguito che saranno approfonditi nei paragrafi successivi:

- Ricezione dei Pacchetti di Versamento;
- Audit dei documenti;
- Accettazione dei PdV e generazione dei relativi Rapporti (Versamento e/o Rifiuto);
- Audit dei documenti accettati;
- Predisposizione dei Pacchetti di Archiviazione;
- Firma digitale e marcatura temporale dei PdA;
- Produzione su richiesta dei Pacchetti di Distribuzione e audit dei relativi documenti.

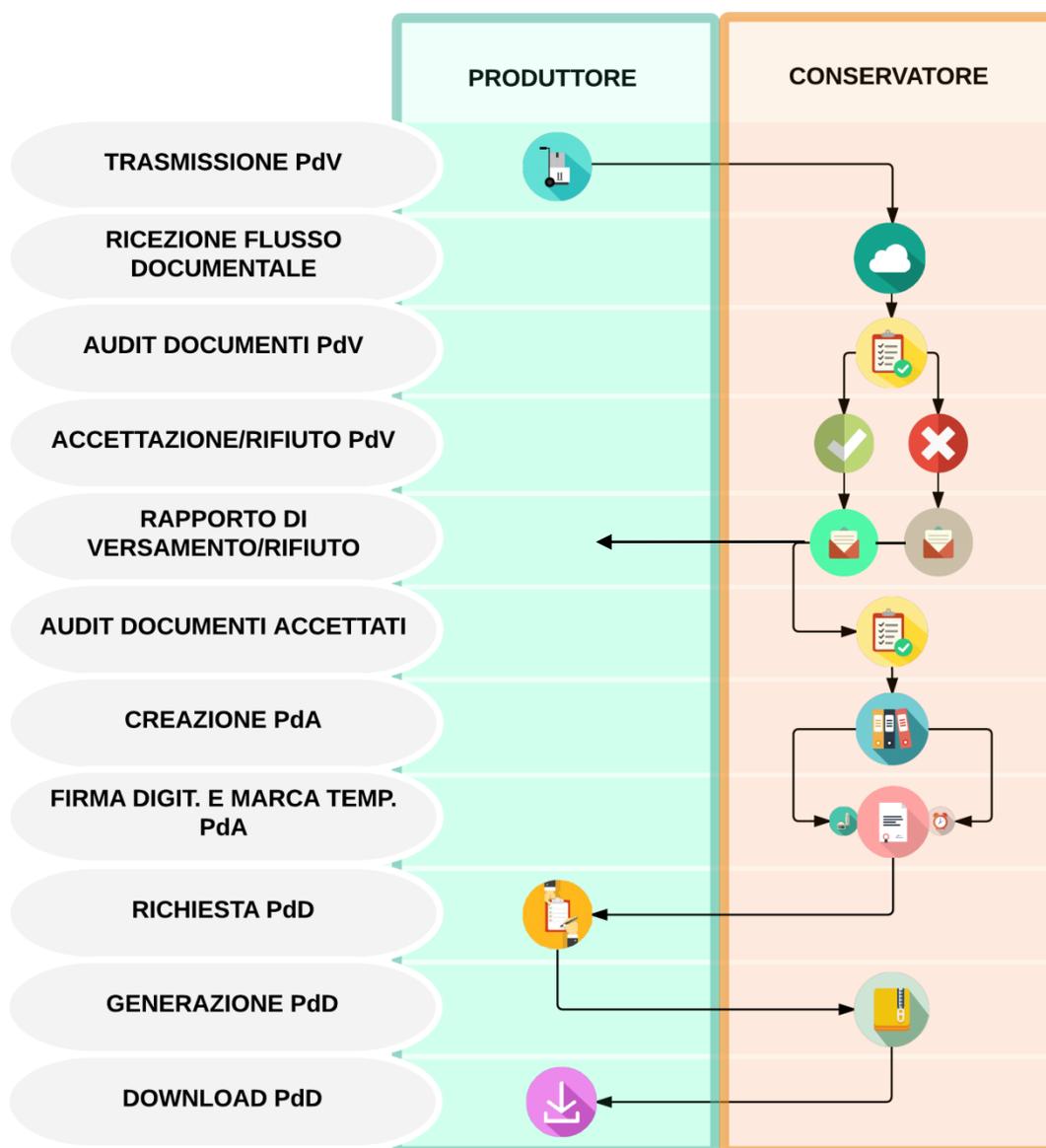


Figura 28
Struttura grafica del processo di conservazione

[Torna al sommario](#)

7.1 Modalità di acquisizione dei pacchetti di versamento

Tutti gli oggetti da versare nel sistema di conservazione sono necessariamente incapsulati in Pacchetti di Versamento (PdV) che Zucchetti S.p.a. ha strutturato secondo la norma UNI 11386 (SInCRO).

Le modalità di versamento nel sistema di conservazione sono stabilite nel contratto con il cliente.

In linea generale, il Pacchetto di Versamento può essere acquisito tramite le seguenti modalità:

- upload manuale di un file zip;
- invio tramite web service di un file zip;
- acquisizione da area FTP;
- acquisizione dall'area di pre-ingest.

Le modalità di versamento indicate garantiscono la sicurezza e riservatezza dei dati trasmessi grazie alla crittografia del canale adottato con tecnologia HTTPS.

Il file zip contiene:

- i documenti informatici da conservare;
- i metadati riferibili a detti documenti;
- un file XML come da Norma UNI 11386 (SInCRO).

A seguito del superamento dei controlli e della sua accettazione il file XML in formato SInCRO, che rappresenta il PdV, viene marcato temporalmente per certificare la data di deposito nel Sistema di Conservazione e per estendere la data di validità della firma apposta sui singoli documenti informatici in esso contenuti.

Il sistema tecnologico che presiede alla ricezione dei pacchetti di versamento è in alta affidabilità e garantisce la completa ridondanza dei dati.

Il servizio di conservazione prevede che i PdV siano sottoposti a procedure di back up secondo le procedure previste dalla ISO 27001. Le copie di sicurezza sono mantenute coerentemente con la politica di conservazione dei back up che tiene conto delle esigenze del servizio di conservazione. Eventuali accordi con il Produttore per un mantenimento personalizzato sono contenute nella "Scheda contratto".

Le operazioni di backup si basano su due processi definiti come segue:

- processo di archiviazione su disco, presso il sito primario ed il sito secondario;
- processo di storicizzazione su nastro. I nastri e le library che si occupano di questo processo sono posti in un sito delocalizzato rispetto al sito primario e secondario.

Il processo di restore dei PdV avviene secondo le seguenti modalità:

1. richiesta telefonica/via email al supporto di Helpdesk, con il dettaglio del dato da recuperare;
2. registrazione della richiesta nell'apposito software di trouble ticketing;
3. assegnazione della richiesta;
4. presa in carico ed avvio del processo di rintracciabilità del dato;

5. attività di restore del dato indicato;
6. ripristino del dato in una cartella di appoggio;
7. comunicazione all'utente (telefonica o tramite email) per ulteriore verifica da parte dell'interessato e feedback di esito positivo;
8. chiusura del ticket.

[Torna al sommario](#)

7.2 Verifiche effettuate sui pacchetti di versamento

Affinché i documenti trasmessi siano ritenuti conformi è necessario che rispettino una serie di requisiti tecnici definiti dalla normativa di riferimento nonché quanto stabilito nelle condizioni generali del servizio; eventuali personalizzazioni sono oggetto di separato accordo tra le parti.

Il sistema di conservazione riceve i Pacchetti di Versamento e avvia i controlli previsti, in particolare, i seguenti:

- verifica che il servizio di conservazione sia attivo ed in corso di validità;
- al fine di controllare l'identificazione certa del soggetto che ha formato il documento e del relativo ente produttore, si verificano le autorizzazioni/credenziali del produttore versante e dei suoi eventuali incaricati/delegati ad effettuare il versamento;
- verifica l'eventuale presenza del PdV nel sistema di conservazione;
- verifica l'integrità dei documenti trasmessi (mediante confronto tra l'hash di ogni documento calcolata dal Produttore con l'HASH ricalcolata su ogni documento dal conservatore dopo la ricezione del pacchetto di versamento);
- verifica l'eventuale presenza del/i documento/i nel sistema di conservazione. Questa verifica implica:
 - la verifica che il documento non sia già stato in precedenza versato in conservazione;
 - il reperimento del documento già versato nel caso di versamento di un allegato a un documento già versato in precedenza o di metadati ad esso relativi;
- controlli sulla firma (in caso di documenti firmati (in caso di firma prossima alla scadenza su uno dei file versati, il sistema evidenzia un warning):
 - controllo di conformità;
 - controllo crittografico;
 - controllo catena trusted;
 - controllo certificato;
 - controllo CRL;
- controllo sulla completezza dei metadati stabiliti:
 - viene verificata l'esistenza dei metadati minimi obbligatori del singolo documento;
 - viene verificata l'esistenza dei metadati aggiuntivi obbligatori del singolo documento. I metadati aggiuntivi obbligatori sono definiti da accordi;
- controllo sulla struttura formale del documento, per verificare se tutte le parti previste sono state inviate;
- controllo sui formati dei file;
- verifica del "Magic Number": Il sistema verifica che i primi byte presenti nella

sequenza binaria del file corrispondano ai formati previsti dagli accordi tra Produttore e il Conservatore;

- verifica del Mime Type: Il sistema verifica la corrispondenza tra il Mime Type ricavato dall'estensione del file ed il Mime Type ricavato dal magic number;
- Verifica dell'esistenza dei documenti dichiarati nell'indice del pacchetto;
- Verifica che il file Zip del pacchetto sia formato correttamente;
- Il file XML dell'indice del pacchetto di versamento viene sottoposto a validazione XSD.

La verifica del Pacchetto di Versamento può produrre l'accettazione totale del pacchetto stesso o il suo totale rifiuto.

Come detto precedentemente, a seguito del superamento dei controlli e della sua accettazione, il file XML in formato SInCRO, che rappresenta il PdV, viene marcato temporalmente per certificare la data di deposito nel Sistema di Conservazione e per estendere la data di validità della firma apposta sui singoli documenti informatici in esso contenuti.

[Torna al sommario](#)

7.3 Accettazione dei pacchetti di versamento e generazione del rapporto di versamento

I PdV per i quali i controlli effettuati (di cui al paragrafo precedente) hanno dato esito positivo sono acquisiti dal Sistema di Conservazione. A tal riguardo, il sistema genera un apposito Rapporto di Versamento in formato SInCRO.

Il Rapporto di Versamento previsto dall'articolo 9 del DPCM 3 Dicembre 2013 è un documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal Produttore.

La generazione del Rapporto di versamento avviene in modo automatico via processo schedato e contiene un riferimento temporale, specificato con riferimento al Tempo universale coordinato (UTC).

Il rapporto di versamento è composto da un file XML in formato UNI 11386 (SInCRO) contenente l'indice dei documenti informatici accettati dal sistema di conservazione con riferimento ad un pacchetto di versamento.

In particolare nel rapporto di versamento sono identificate le seguenti informazioni:

- l'identificativo univoco del pacchetto di versamento cui si riferisce il rapporto
- il Produttore del pacchetto di versamento
- l'applicativo che ha prodotto il pacchetto di versamento
- il gruppo cui appartiene il pacchetto di versamento
- i gruppi cui appartengono i documenti inclusi nel pacchetto di versamento
- i documenti accettati con i metadati relativi e l'audit eseguito sugli stessi
- la classe documentale cui è stato associato il singolo documento
- i soggetti coinvolti nel processo di produzione del pacchetto di versamento
- informazioni relative a data e ora di realizzazione del rapporto di versamento
- riferimenti normativi.

Tale Rapporto è firmato digitalmente dal Responsabile del Servizio di Conservazione, marcato temporalmente (con marca detached) ed inviato tramite PEC al Produttore e/o reso disponibile nell'apposita sezione dell'interfaccia dell'applicativo.

Il Sistema di Conservazione, per gli oggetti in esso contenuti, garantisce, tramite l'adozione di regole, procedure e tecnologie, che dalla presa in carico dal produttore fino all'eventuale scarto siano rispettati i criteri di autenticità, integrità, affidabilità, leggibilità e reperibilità.

[Torna al sommario](#)

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

Per i PdV che non hanno superato i controlli di cui al punto 7.2 il Sistema di Conservazione genera un apposito Rapporto di Rifiuto, in formato XML, contenente le informazioni relative ai files coinvolti e alle anomalie riscontrate. Il Rapporto di Rifiuto è quindi firmato dal Responsabile del Servizio di Conservazione, marcato temporalmente ed inviato tramite PEC al Produttore e/o reso disponibile nell'apposita sezione dell'interfaccia dell'applicativo.

Le anomalie che determinano il rifiuto del pacchetto di versamento sono le seguenti

| Controllo | Errore | Tipo errore |
|---|--|------------------------|
| Verifica che il servizio di conservazione sia attivo ed in corso di validità | Servizio non attivo | Bloccante, rifiuto PdV |
| Verifica l'eventuale presenza del PdV nel sistema di conservazione | PdV già presente | Bloccante, rifiuto PdV |
| Verifica dell'esistenza del responsabile della conservazione | Responsabile della conservazione non censito | Bloccante, rifiuto PdV |
| Verifica l'eventuale presenza dell'identificativo univoco del documento nel sistema di conservazione | Documento già presente | Bloccante, rifiuto PdV |
| Controllo sulla struttura formale del documento | Struttura non congruente o incompleta | Bloccante, rifiuto PdV |
| Verifica dell'HASH Il sistema verifica che l'HASH, calcolato in formato SHA-256, sia identico all'HASH dichiarato nel file XML SInCRO. | Hash non congruente | Bloccante, rifiuto PdV |
| Verifica univocità HASH Viene verificata l'esistenza di un HASH identico | Hash già presente | Bloccante, rifiuto PdV |
| Verifica dell'estensione. Una serie di lettere, unita al nome del file attraverso un punto, identifica l'estensione del file. Il sistema verifica se l'estensione del file rientra tra quelle previste dagli accordi tra produttore e Zucchetti S.p.a.. | Estensione non valida | Bloccante, rifiuto PdV |

| | | |
|---|--|------------------------|
| Verifica del magic number Il sistema verifica che i primi byte presenti nella sequenza binaria del file corrispondano ai formati previsti dagli accordi tra Produttore e Zucchetti S.p.a.. | Formato non ammesso | Bloccante, rifiuto PdV |
| Verifica Mime Type Il sistema verifica la corrispondenza tra il Mime Type ricavato dall'estensione del file ed il Mime Type ricavato dal magic number. | Mime Type non valido | Bloccante, rifiuto PdV |
| Verifica dell'esistenza della firma Se il file deve essere firmato il sistema verifica che nel file sia presente una firma. | File non firmato | Bloccante, rifiuto PdV |
| Verifiche della firma - controllo di conformità; - controllo crittografico; - controllo catena Trusted; - controllo certificato; - controllo CRL; | Firma non valida | Bloccante, rifiuto PdV |
| Verifica dell'esistenza della classe documentale Viene verificata l'esistenza nel sistema della classe documentale dichiarata sul singolo documento. | Classe documentale non valida | Bloccante, rifiuto PdV |
| Verifica dei metadati minimi Viene verificata l'esistenza dei metadati minimi obbligatori nelle Extra Info del singolo documento. | Metadati minimi non presenti | Bloccante, rifiuto PdV |
| Verifica dei metadati aggiuntivi obbligatori. Viene verificata l'esistenza dei metadati aggiuntivi obbligatori nelle Extra Info del singolo documento. I metadati aggiuntivi obbligatori sono definiti da accordi tra Produttore e Zucchetti S.p.a.. | Metadati aggiuntivi obbligatori non presenti | Bloccante, rifiuto PdV |
| Verifica esistenza documenti dichiarati nel pacchetto di versamento | Documento non trovato | Bloccante, rifiuto PdV |
| File Zip del pacchetto di versamento non formato correttamente | Zip non valido | Bloccante, rifiuto PdV |
| Validazione XSD del file XML dell'indice del pacchetto di versamento | File XML non formato correttamente | Bloccante, rifiuto PdV |

[Torna al sommario](#)

7.5 Preparazione e gestione del pacchetto di archiviazione

Il pacchetto di Archiviazione viene formato secondo quanto stabilito nell'Allegato 4 del DPCM 3 Dicembre 2013 e secondo lo standard SInCRO.

Il processo di conservazione dei documenti versati avviene mediante la apposizione della firma digitale da parte del Responsabile del servizio di conservazione e la marcatura temporale dei Pacchetti di Archiviazione ottenuti sulla scorta dei Pacchetti di Versamento precedentemente accettati.

Il processo di preparazione e conservazione dei Pacchetti di Archiviazione si articola nelle seguenti fasi:

- audit dei documenti accettati;
- gestione delle eventuali anomalie riscontrate;
- produzione dei Pacchetti di Archiviazione;
- firma dei PdA;
- marcatura temporale dei PdA;
- inserimento dei PdA nel database;
- copia dei file nell'area di storage;
- invio al Produttore, tramite PEC, della notifica di avvenuta produzione dei PdA.

Periodicamente, in funzione dello scadenziario di lavorazione dei Pacchetti di Versamento e degli eventuali accordi con il produttore, sono preparati i Pacchetti di Archiviazione. Questa fase è preceduta da un nuovo audit di documenti accettati la cui utilità è dettata dai possibili accadimenti verificatisi nell'eventuale arco temporale intercorrente tra l'accettazione dei Pacchetti di Versamento e l'avvio della procedura di produzione dei Pacchetti di Archiviazione. I Pacchetti di Archiviazione sono quindi generati aggregando documenti accettati tramite rapporto di versamento, appartenenti allo stesso produttore ed alla stessa classe documentale (ciò al fine di soddisfare esigenze di una ordinata conservazione); in essi possono confluire i files di uno o più Pacchetti di Versamento.

Schematizzando:

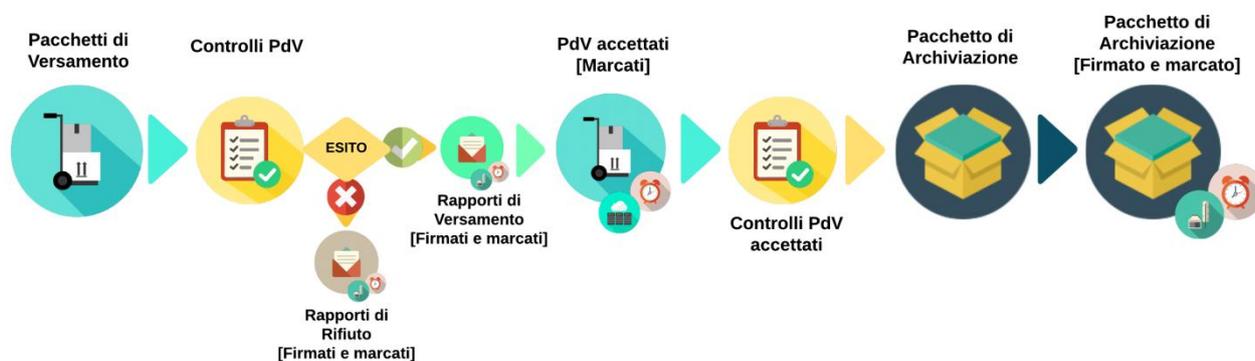


Figura 29
Fasi di creazione del Pacchetto di Archiviazione

Tutte le operazioni legate alla formazione del Pacchetto di Archiviazione sono sottoposte a log.

Il sistema tecnologico che presiede la gestione dei Pacchetti di Archiviazione è in alta affidabilità e garantisce la completa ridondanza dei dati.

Il servizio di conservazione prevede che i PdA siano sottoposti a procedure di backup secondo le procedure previste dalla ISO 27001. Le copie di sicurezza sono mantenute

coerentemente con la politica di conservazione dei backup che tiene conto delle esigenze del servizio di conservazione specificate nelle condizioni generali del servizio. Eventuali accordi con il Titolare per un mantenimento personalizzato sono oggetto di separato accordo tra le parti.

Le operazioni di backup si basano su due processi definiti come segue:

- processo di archiviazione su disco, presso il sito primario ed il sito secondario;
- processo di storicizzazione su nastro. I nastri e le library che si occupano di questo processo sono posti in un sito delocalizzato rispetto al sito primario e secondario.

Il processo di restore dei PdA avviene secondo le seguenti modalità:

1. richiesta telefonica/via email al supporto di Helpdesk, con il dettaglio del dato da recuperare;
2. registrazione della richiesta nell'apposito software di trouble ticketing;
3. assegnazione della richiesta;
4. presa in carico ed avvio del processo di rintracciabilità del dato;
5. attività di restore del dato indicato;
6. ripristino del dato in una cartella di appoggio;
7. comunicazione all'utente (telefonica o tramite email) per ulteriore verifica da parte dell'interessato e feedback di esito positivo;
8. chiusura del ticket.

[Torna al sommario](#)

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

La gestione dei Pacchetti di Distribuzione si articola in tre fasi:

- Richiesta dell'Utente d'invio dei documenti sotto forma di Pacchetti di Distribuzione;
- Produzione dei PdD;
- Prelievo dei PdD.

Richiesta dell'Utente d'invio dei documenti sotto forma di Pacchetti di Distribuzione

L'utente, tramite apposita funzionalità presente nell'applicazione, richiede la produzione di un Pacchetto di Distribuzione, selezionando i documenti che intende prelevare.

L'utente può chiedere, se è necessaria, l'apposizione della marca temporale sul Pacchetto di Distribuzione.

Produzione dei Pacchetti di Distribuzione

In seguito alla richiesta dell'utente, viene prodotto un Pacchetto di Distribuzione, in formato zip, che contiene i documenti richiesti dal l'utente, i files dei Pacchetti di Archiviazione e Versamento di riferimento e i relativi files di marca temporale.

Le fasi della produzione del pacchetto di distribuzione sono le seguenti:

- I documenti richiesti sono estratti dal sistema di conservazione.
- I documenti sono soggetti ad audit.

- Il responsabile della conservazione viene informato via PEC di eventuali problemi riscontrati dall'audit ed esegue le azioni correttive del caso.
- Viene prodotto il file SInCRO del pacchetto di distribuzione.
- Il pacchetto di distribuzione viene firmato dal responsabile del servizio di conservazione.
- Viene eseguita la marcatura temporale del pacchetto di distribuzione se richiesta.
- Viene prodotto un file .zip contenente tutti i file inerenti il pacchetto di distribuzione.
- Viene inviata al richiedente la PEC di conferma della produzione del pacchetto di distribuzione.
- Tutte le informazioni del file SInCRO ed eventuale.tsr della marca temporale sono inserite nel database del sistema documentale.
- I file SInCRO e.tsr sono copiati nell'area di storage del sistema di conservazione.

Prelievo dei Pacchetti di Distribuzione

Al fine di ottenere il Pacchetto di Distribuzione il richiedente si collega al Sistema di Conservazione ed esegue il download dello zip generato contenente i files del Pacchetto di Distribuzione.

[Torna al sommario](#)

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

In questo capitolo vengono descritte le procedure adottate per la produzione di duplicati o copie.

Produzione di duplicati

La produzione di duplicati informatici dei documenti conservati può avvenire a seguito di una richiesta dell'Utente.

La procedura inizia con la 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 inviato all'utente che ne ha fatto richiesta.

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

Richiesta della presenza del pubblico ufficiale

Il Responsabile del servizio di conservazione è obbligato, qualora fosse necessario, a

contattare un Pubblico ufficiale.

Per i documenti informatici di proprietà delle Pubbliche amministrazioni, la funzione di Pubblico ufficiale è svolta da un soggetto interno alla stessa amministrazione.

La Zucchetti S.p.a. 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 Titolare; pertanto, qualora il Titolare non se ne sia fatto carico direttamente, la Zucchetti S.p.a. è sin da ora autorizzata ad addebitare al Titolare 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

Lo scarto è l'operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti informatici ritenuti privi di valore amministrativo e di interesse storico culturale.

Alla scadenza dei termini di conservazione previsti dalla normativa e definiti comunque nel Contratto di servizio, il sistema di conservazione individua i pacchetti di archiviazione ed i relativi metadati che devono essere scartati dal sistema di conservazione, dandone informativa al Titolare.

Il processo di conservazione prevede che nel caso di archivi pubblici (o privati che rivestono interesse storico particolarmente importante), lo scarto del pacchetto di archiviazione avviene previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo rilasciata al Titolare secondo quanto previsto dalla normativa vigente in materia.

Il processo di scarto è articolato nelle seguenti fasi:

1. Sono individuati i documenti informatici oggetto di scarto per scadenza dei termini di conservazione mediante apposita funzione preimpostata;
2. Sono inviate al Titolare via PEC le richieste di conferma dello scarto dei documenti;
3. Il Titolare conferma o rifiuta lo scarto dei documenti in toto o in parte.
4. I documenti informatici per cui il Titolare ha approvato lo scarto sono eliminati dal sistema di conservazione; allo stesso modo sono eliminati i relativi metadati ad essi associati in fase di versamento;
5. La comunicazione di avvenuto scarto dei documenti viene inviata via PEC dal Conservatore al Titolare.

Il Responsabile del servizio di conservazione d'accordo con il responsabile della funzione archivistica mantiene traccia delle operazioni di scarto conservando le ricevute della PEC e le comunicazioni di avvenuto scarto per ogni Titolare; tali rapporti costituiscono una specifica tipologia documentale e pertanto sono sottoposti al processo di conservazione.

Tutto il processo di scarto è sottoposto a log che viene inviato in conservazione a cura del Conservatore.

Eventuali procedure specifiche sono concordate con il Produttore ed oggetto di un separato accordo tra le parti.

[Torna al sommario](#)

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

Alla luce del fatto che interoperabilità e trasferibilità si ritengono garantite dall'adozione dei comuni standard dettati dal DPCM 03.12.2013 in relazione alla struttura dell'Indice di Conservazione e dei relativi Pacchetti Informativi, Zucchetti S.p.a. ha optato di aderire totalmente allo standard UNI 11386 gestendo il formato SInCRO sia per i Pacchetti di Archiviazione e Distribuzione che per il Pacchetto di Versamento.

Zucchetti S.p.a. ha inoltre optato per gestire in formato UNI 11386 anche tutti gli audit eseguiti:

- audit eseguiti sul Pacchetto di Versamento;
- audit propedeutici alla produzione del Pacchetto di Archiviazione o di Distribuzione;
- audit eseguiti periodicamente per garantire la leggibilità e la consistenza dei file nel tempo.

[Torna al sommario](#)

8. IL SISTEMA DI CONSERVAZIONE

La soluzione infrastrutturale prevista per il servizio di Conservazione prevede di creare un ambiente totalmente replicato e disponibile sui 2 siti, dedicando capacità computazionale, reti e replicando i dati tra le diverse tecnologie disponibili in datacenter. Con lo scopo di offrire una soluzione efficiente e funzionale, Zucchetti S.p.a. ha previsto un impianto dedicato al sistema di Conservazione digitale. L'impianto di produzione è ridondato su siti fisici differenti con logiche di alta affidabilità.

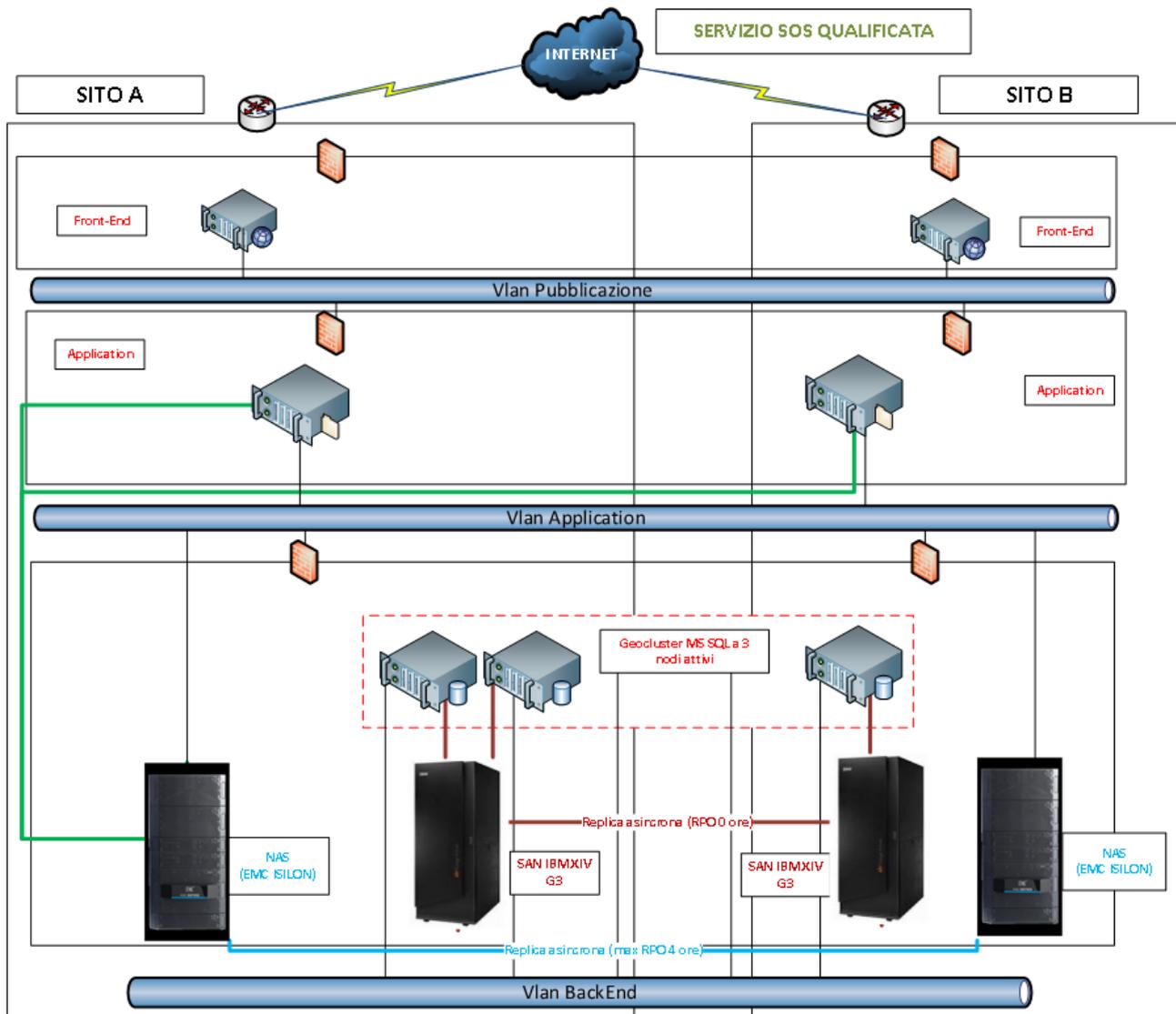


Figura 30
Struttura grafica dell'impianto di produzione del sistema di conservazione

[Torna al sommario](#)

8.1 Componenti Logiche e tecnologiche

I servizi di datacenter Zucchetti ospitanti i sistemi per l'erogazione del servizio di conservazione digitale, si caratterizzano per la presenza di due poli tecnologici in logica di continuità operativa garantita da una soluzione di Disaster Recovery, con soluzioni ingegneristiche in grado di offrire la massima sicurezza, sintesi di innovazione tecnologica e attrezzature sofisticate.

Si identificano i seguenti centri:

- Il sito primario o "Caveau" ove sono localizzati gli elementi principali di erogazione dei servizi.
- Il polo secondario delocalizzato, ove sono concentrati in una logica di disaster recovery le piattaforme di erogazione.
- Il polo "Backup", ove sono ospitate le infrastrutture di backup e conservati i nastri.
- La control room per i sistemisti che presidiano le attività e i servizi del data center.

Le quattro tonnellate di porta d'acciaio che consentono il primo accesso al datacenter Zucchetti e il caveau blindato che lo ospita, sono solo i primi elementi di una architettura atta a proteggere i dati e i servizi applicativi erogati. Analoga attenzione è stata dedicata alle altre infrastrutture fisiche e logiche in modo da garantire piena sicurezza e continuità di servizio, privilegiando logiche di massima qualità del servizio erogato.

Per garantire un ulteriore livello di sicurezza per le applicazioni è stata anche predisposta una apposita struttura esterna che funge da Centro Backup, collegata al datacenter Zucchetti tramite fibra ottica dedicata e collocata in un edificio distante alcune centinaia di metri sia dal complesso primario sia da quello secondario.

Al fine di assicurare funzionalità piena anche in caso di malfunzionamenti delle linee Internet di un Provider, il datacenter è inoltre collegato in fibra ottica con diversi fornitori di connettività. Questo multiplo instradamento fisico corrisponde però ad una singola unità logica essendo Zucchetti sia LIR (Local Internet Registry), in grado di gestire propri lotti di indirizzi IP indipendentemente da provider esterni, che AS (Autonomous System), il che consente di gestire una propria "politica di routing", ossia decidere autonomamente come effettuare l'instradamento del traffico sfruttando più provider esterni e gestendo le linee in modo fault-tolerant.

Per poter intervenire nei tempi necessari a garantire il funzionamento delle apparecchiature è stato installato un sistema di gestione degli allarmi dell'impianto elettrico, di condizionamento, di rilevazione fumo, degli UPS e generici, come potrebbe essere la presenza acqua all'interno dei locali.

Il sistema consente la gestione degli allarmi come segnali on-off con la registrazione degli eventi su console remota e la trasmissione del segnale a distanza (via rete e via telefono) al personale della manutenzione. Il sistema provvede all'acquisizione e alla trasmissione a distanza, di segnali analogici come le temperature dei locali, i parametri di funzionamento delle macchine del condizionamento, i livelli di assorbimento di potenza ed energia (KW, KWh etc.) con la rappresentazione degli stessi su grafici e la possibilità di raccogliere lo storico per rivedere situazioni precedenti al momento di un particolare inconveniente.

Ciascun rack è dotato di alimentazione ridondata ed è raffreddato da un sistema di condizionamento anch'esso ridonato. Sia l'impianto elettrico che il sistema di condizionamento del piano sono in grado di garantire la piena operatività di tutti i rack ed i server/le apparecchiature anche in caso di interruzione di servizio di una delle sezioni elettriche o di condizionamento.

Le caratteristiche del datacenter secondario sono del tutto assimilabili a quelle del datacenter primario, essendo stato progettato con i medesimi criteri di sicurezza e continuità operativa. Cambiano alcuni parametri dimensionali degli impianti, in relazione ai fabbisogni calcolati.

L'area BACKUP è l'ambiente in cui viene ospitata l'infrastruttura di backup con l'archiviazione dei nastri oggetto del servizio.

I locali si trovano in edificio separato sia dal sito primario che secondario ed è composto da:

- ufficio addetti alla gestione fisica e logistica del datacenter;
- area CED per infrastruttura backup e nastri;

Tale area è collegata con fibra proprietaria ad entrambi i siti di erogazione, permettendo di estendere sia la LAN di datacenter che la SAN/TAN, al fine di garantire un trasferimento dei dati sui supporti esterni con la massima affidabilità e sicurezza.

L'accesso all'edificio è disponibile ai soli autorizzati, tramite varco dotato di controllo accessi e badge personale.

Relativamente all'impianto di rete locale, per garantire la massima sicurezza logica, l'affidabilità e le performance della trasmissione dati, ciascun rack è dotato di un proprio Switch con connessioni ottiche ridondate da 10 Gigabit al centro stella di "distribution" del piano e con connessione in rame a 1 Gbit per le apparecchiature presenti nello stesso.

Ciascun rack è pertanto ridonato in termini di connettività al centro stella di "distribution" e, al fine della sicurezza logica, può essere configurato come un'entità indipendente con un segmento di rete isolato.

I controlli relativi alla sicurezza logica sono stati concepiti a tutto tondo, partendo da quelli relativi ai sistemi del datacenter per arrivare a quelli applicativi propri della soluzione di conservazione digitale.

Sono previsti:

- controlli manuali
- scansioni di vulnerability assessment
- controllo degli access log sospetti ai sistemi informatici
- monitoring del consumo di banda internet infrastruttura IT
- controllo navigazione e accessi internet da proxy infrastruttura IT
- controllo accessi negati firewall internet infrastruttura IT
- raccolta e pubblicazione bollettini di sicurezza
- verifica compliance postazioni di lavoro

- controllo accessi falliti superata la soglia di verifica di sicurezza
- controlli automatici
- controlli eventi sospetti da Intrusion Detection System (IPS) presente nell'infrastruttura IT

Per il servizio di conservazione digitale Zucchetti ha predisposto un completo piano di continuità operativa, che considera tutti gli aspetti ritenuti critici a seguito di una specifica analisi dei rischi.

Si sono identificate quindi le strategie necessarie per garantire la continuità del servizio di conservazione, da mettere in atto a fronte di eventi eccezionali e non prevedibili che potrebbero destabilizzare l'erogazione, con l'obiettivo di riprendere nel più breve tempo possibile i servizi.

Il piano è conforme alle modifiche dell'ambiente e tutte le modifiche su tale ambiente sono prese in considerazione, aggiornando il piano ogni volta che se ne verifichi la necessità.

Il piano di continuità relativo al servizio di conservazione digitale è approvato dalla Direzione Aziendale e da questa riesaminato almeno su base annua, in occasione del riesame della Direzione previsto dalla norma ISO27001:2013, cui partecipano il Responsabile del servizio di conservazione e il Responsabile per la sicurezza dei sistemi di conservazione.

La Direzione rivaluta anche i parametri di ripristino: tempi di ripartenza (massimo ritardo accettabile), il grado di perdita delle informazioni e i servizi minimi indispensabili per garantire continuità operativa. Nella valutazione di questi indicatori si tengono in considerazione sia gli aspetti relativi al business sia elementi derivanti da norme e cogenze.

Per poter determinare al meglio come organizzare il piano di continuità e stabilire valutazioni realistiche dei parametri di ripristino, annualmente si conduce un'analisi dei rischi per individuare minacce e vulnerabilità che potrebbero compromettere l'erogazione del servizio di conservazione e avere conseguenze sulla sicurezza delle informazioni.

L'analisi viene condotta secondo la metodologia prevista dal sistema SGSI del sistema di certificazione ISO 27001.

[Torna al sommario](#)

8.2 Componenti fisiche

L'infrastruttura del sistema di conservazione si basa su:

- server di frontend virtuali ridondati con logica di distribuzione geografica del carico (per mezzo di bilanciatori HW che inoltrano le richieste), con possibilità di scalare numericamente
- application server ridondati (all'interno dell'impianto virtuale di hosting) con logica di distribuzione geografica del carico e con possibilità di scalare numericamente. Gli application accedono in NFS alle porzioni di disco rese disponibili sugli storage.
- Per garantire una potenza di calcolo pari al 100% anche in caso di malfunzionamento di uno dei siti, si è deciso di mettere in regime di SRM (Site Recovery Manager) le Virtual Machine sia di frontend sia application, in modo da ripristinare il 100% dell'operatività in caso di fail di un sito. Essendo con SRM la

- replica totale delle Virtual Machine in logica sincrona, l'RPO di queste è da considerarsi zero e in ogni caso su queste Virtual Machine non sono previsti dati.
- file system in modalità NAS replicato su sito secondario in modalità asincrona: la componente NAS (filesystem NFS) viene erogata nel sito A replicata con RPO entro le quattro ore (in modalità asincrona) sul sito B.
 - motore DataBase di produzione su cluster con area storage su SAN e dischi SSD locali per operazioni ad alta velocità. La parte database è in configurazione di alta affidabilità e replicata sui due siti mediante geocluster che sfrutta la tecnologia di replica degli storage. Si tratta di un cluster a tre nodi. Nel caso di fail di uno dei due siti non è necessario alcun intervento manuale perché lo switch delle istanze SQL avviene in automatico.
 - SAN a servizio del cluster database con replica delle LUN su sito secondario.

Per la parte di network, attivata un'infrastruttura dedicata all' ambiente di produzione e definita da tre livelli di vlan:

- Frontend (pubblicazione)
- Application (livello applicativo)
- Backend (area del cluster database) con servizi di firewall "dedicato" (Virtual context su tecnologia Cisco)

Tutti gli apparati facenti parte del servizio di conservazione sono sotto contratto di manutenzione con primarie società valutate ai massimi livelli.

Nei contratti sono previsti i piani di manutenzione e le condizioni di intervento. Tutte le terze parti, come previsto dalle nostre procedure relative ai servizi di fornitura, sono sottoposte ad audit periodici, a rivalutazione annuale e gli esiti derivanti considerati nell'analisi dei rischi.

[Torna al sommario](#)

8.3 Procedure di gestione e di evoluzione

Il sistema di conservazione assicura la conservazione, tramite l'adozione di regole, procedure e tecnologie dei seguenti oggetti in esso conservati, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità:

- a) i documenti informatici e i documenti amministrativi informatici con i metadati ad essi associati di cui all'allegato 5 del DPCM 03.12.2013;
- b) i fascicoli informatici ovvero le aggregazioni documentali informatiche con i metadati ad essi associati di cui all'allegato 5 del DPCM 03.12.2013, contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che appartengono al fascicolo o all' aggregazione documentale.

Le componenti funzionali del sistema di conservazione assicurano il trattamento dell'intero ciclo di gestione dell'oggetto conservato nell'ambito del processo di conservazione.

Il sistema di conservazione garantisce l'accesso all'oggetto conservato, per il periodo prescritto dalla norma o concordato con apposito contratto, indipendentemente dall'evolversi del contesto tecnologico.

Le attività di sviluppo e di presidio sono state assegnate a figure professionali dotate delle

necessarie competenze e di una approfondita conoscenza degli standard in materia di conservazione di documenti informatici, dalle regole tecniche in particolare di quelli indicati negli allegati al DPCM 3.12.2013 al cui contenuto si rimanda direttamente.

[Torna al sommario](#)

8.3.1 Conduzione e manutenzione del sistema di conservazione

L'evoluzione del sistema di conservazione relativamente a modifiche organizzative di processi e tecnologici viene documentata nei verbali che compongono la ISO/IEC 27001:2013 relativa al sistema stesso.

Tutte le figure indicate nel documento "Profili professionali" di AgID verificano l'andamento del servizio di conservazione digitale; di detta verifica viene dato conto nel corso del riesame del Sistema di Gestione della Sicurezza delle Informazioni previsto dalla ISO/IEC 27001:2013.

In questa occasione si verifica la corretta applicazione delle procedure e istruzioni di lavoro, in particolare:

- si consultano le rilevazioni scaturite da audit condotti da parte di personale interno incaricato sui principali processi relativi alla Conservazione. Ogni audit viene registrato e mantenuto nel sistema documentale aziendale, a disposizione degli aventi diritto alla consultazione.
- si esamina l'andamento di azioni preventive e correttive al sistema di conservazione.
- si controllano gli indicatori di prestazione definiti per misurare l'andamento del servizio.

Per quanto riguarda la componente software l'integrità del sistema di conservazione e delle sue evoluzioni parte dall'uso di rigorosi strumenti di analisi e sviluppo, che documentano ogni passaggio.

La documentazione in relazione all'accettazione dei sistemi (nuovi sistemi, upgrade, nuove versioni, ecc.), è mantenuta con modalità che assicurino la sua sicurezza e l'aggiornamento periodico, in particolare per la configurazione dei sistemi e per i processi di test e valutazione degli effetti di tale cambiamento sui processi critici del sistema di conservazione.

I test sono condotti sulla base dei seguenti criteri:

- conformità ai criteri generali emessi dalla direzione
- conformità ai controlli sui requisiti di sicurezza, emessi di concerto dal Responsabile del servizio di conservazione e dal Responsabile della sicurezza
- conformità a requisiti funzionali e comportamenti attesi, definiti di volta in volta da coordinatore analisi prodotto, Responsabile del servizio di conservazione.

I requisiti funzionali, definiti di volta in volta, sono riportati nella documentazione tecnica di analisi e sviluppo, conservata nei sistemi documentali in uso ai gruppi interessati.

Il personale che effettua i test è diverso dal personale che sviluppa ed è diverso dal personale che cura la erogazione del servizio di conservazione.

Relativamente ai test, che devono essere obbligatoriamente effettuati prima di ogni variazione del sistema di conservazione, il personale incaricato deve:

- usare la massima diligenza,
- curare la registrazione degli esiti,
- osservare scrupolosamente l'adesione ai criteri generali di accettazione, ai requisiti di sicurezza e ai comportamenti attesi.

Le attività di test sono sottoposte a log.

Relativamente ai test si precisa che ogni attività deve essere registrata e riportare:

- oggetto del test
- data del test
- approvazione dei Responsabili indicati se si usano dati presi da ambiente di produzione
- cancellazione post test dei dati se si usano dati presi da ambiente di produzione
- criteri specifici di accettazione test (extra criteri generali e requisiti sicurezza)
- esito del test su criteri generali
- esito del test su requisiti sicurezza
- esito del test su comportamenti attesi
- approvazione esito test da parte del Responsabile dello sviluppo e della manutenzione del sistema di conservazione
- data approvazione.

[Torna al sommario](#)

8.3.2 Gestione e conservazione dei log

Sono elencati gli eventi per cui il sistema di conservazione genera dei log e la modalità di conservazione e consultazione degli stessi.

| Tipologia di log | Evento tracciato |
|-------------------------------------|--|
| Accesso al sistema di conservazione | Login al sistema |
| | Logout dal sistema |
| | Login fallito |
| Credenziali d'accesso | Nascita della credenziale |
| | Disattivazione della credenziale |
| | Modifica della password |
| Anagrafe aziende | Nascita anagrafica dell'azienda |
| | Modifica dell'anagrafica dell'azienda |
| | Associazione classe documentale ad azienda |
| Responsabili della conservazione | Definizione del responsabile |
| | Disattivazione del responsabile |
| Pacchetti di versamento | Deposito nel sistema del PDV |
| | Generazione del rapporto di versamento |
| | Generazione del rapporto di rifiuto |
| Pacchetti di archiviazione | Generazione PDA |
| | Audit eseguito sul PDA |
| Pacchetti di distribuzione | Richiesta PDD |
| | Generazione PDD |

| | |
|---|--|
| | Audit eseguito sul PDD |
| | Download del PDD |
| Richieste di cancellazione di sistema | Nascita richiesta di cancellazione |
| | Conferma dell'utente della richiesta di cancellazione |
| | Rifiuto dell'utente della richiesta di cancellazione |
| Richieste di cancellazione eseguite dall'utente | Nascita richiesta di cancellazione |
| | Conferma della richiesta di cancellazione |
| | Rifiuto della richiesta di cancellazione |
| Audit periodici | Nascita audit periodico |
| | Generazione del rapporto di audit ok |
| | Generazione del rapporto di audit ko |
| Invio comunicazioni | Invio email produzione rapporto di versamento |
| | Invio email produzione rifiuto del versamento |
| | Invio email produzione PDA |
| | Invio email produzione PDD |
| | Invio email richiesta conferma cancellazione documenti |

Relativamente alla tipologia di log e all'evento tracciato, la modalità di conservazione e di consultazione è la seguente:

- produzione giornaliera e automatica di report degli eventi in formato PDF/A;
- firma automatica via HSM dei file PDF/A con credenziali del responsabile del servizio di conservazione;
- produzione giornaliera e automatica del pacchetto di archiviazione, in ambiente di conservazione dedicato, dei report di log;
- i pacchetti di archiviazione e relativi documenti sono conservati per 10 anni;
- i log sono consultabili in tempo reale tramite apposite funzionalità rese disponibili agli utenti autorizzati.

[Torna al sommario](#)

8.3.3 Change mangement

Il sistema di conservazione ha un processo di change management formalizzato sulla base del quale:

- identificare, analizzare e valutare i cambiamenti ritenuti utili o necessari per i processi critici, che potrebbero potenzialmente impattare il sistema di conservazione. Tali cambiamenti possono essere, ad esempio, relativi ai processi di versamento, archiviazione e distribuzione dei pacchetti, ai processi, alle modalità di gestione degli accessi, alla architettura infrastrutturale ed applicativa del processo, alla sicurezza, ecc.
- identificare ruoli, responsabilità ed i necessari processi autorizzativi necessari per implementare i cambiamenti nel processo e nel sistema - assegnare personale adeguato alle necessità sul processo di cambiamento (hard skill e soft skills)

- definire adeguati programmi di formazione e sviluppo professionale per il personale coinvolto è presente adeguata documentazione a supporto dei cambiamenti applicati al sistema di conservazione ed in particolare per verificare che ogni cambiamento significativo sia stato:
 - analizzato e valutato dal personale coinvolto
 - autorizzato dal responsabile del servizio, comunque almeno informato in caso di emergenza ed applicazione dei cambiamenti con modalità immediate.

Nel processo di change si identificano i seguenti ruoli:

- sviluppatori software, che implementano i cambiamenti
- personale del gruppo test che esegue i test di conformità (funzionale, dei requisiti di sicurezza ...)
- personale del gruppo installazione/produzione che operativamente esegue l'aggiornamento dell'ambiente di produzione.

La fase di change inizia solamente dopo che siano rispettati e superati i controlli di accettazione formale della fase di test.

Le attività in carico al personale assegnato alla fase di change si possono così riassumere:

- messa in produzione dell'aggiornamento secondo le modalità stabilite dal Responsabile dello sviluppo e della manutenzione del sistema di conservazione
- contenimento degli impatti sul servizio
- rispetto dei tempi concordati
- attuazione di strategie di recovery a fronte di comportamenti inattesi.

Detta attività è nell'area del Responsabile dello sviluppo e della manutenzione del sistema di conservazione che sovrintende le operazioni dei gruppi sopra menzionati.

Le attività di sviluppo relative al software utilizzato nel sistema di conservazione sono tracciate dai gruppi di analisi, sviluppo, test e gestione applicativa mediante un apposito strumento aziendale.

L'autorizzazione ad attuare i cambiamenti è data nel momento in cui il Responsabile dello sviluppo e della manutenzione del sistema di conservazione ha approvato la fase di validazione.

Per ogni attività di change (step installazione/produzione) registrata sono disponibili le seguenti informazioni:

- oggetto del change,
- data di applicazione,
- approvazione,
- esito del change, registrato nella fase di chiusura
- data conferma del change corrispondente a quella della fase di chiusura.

L'operazione di change può schematicamente dare luogo a tre situazioni:

- fallimento immediato (il change non va a buon fine)
- successo
- segnalazioni post-change

Nel caso di fallimento immediato si registra il fallimento e si attua la strategia di rollback.

Nel caso di successo si attua un periodo di osservazione: trascorsi 30 giorni dal change, in assenza di segnalazioni (da strumenti di monitoraggio anche automatici, da parte dei

clienti, da parte di autorità) si considera definitivamente confermato il change, registrando la conferma.

In caso contrario si chiuderà lo step con esito negativo e, sulla base di quanto emerso e della gravità, il Responsabile dello sviluppo e della manutenzione valuterà la strategia migliore.

[Torna al sommario](#)

8.3.4 Verifica periodica di conformità a normativa e standard di riferimento

Il Responsabile del servizio di conservazione, il Responsabile della funzione archivistica di conservazione ed il Responsabile della privacy e sicurezza controllano costantemente l'evoluzione normativa e il quadro regolamentare per tenere il sistema e la corrispondente gestione al passo con le specifiche e i vincoli derivanti da leggi dello stato e regolamenti europei.

[Torna al sommario](#)

9. MONITORAGGIO E CONTROLLI

L'insieme delle evidenze derivanti dai meccanismi di monitoraggio sono considerate annualmente, sia in termini di potenziali elementi di rischio, sia come spunti per la revisione dei piani di conservazione.

In particolare, al verificarsi di problematiche riguardanti i supporti, i formati ed i metadati il Responsabile del Servizio di Conservazione individua le azioni correttive di concerto con le altre figure indicate nei curriculum presentati ad AgID in sede di accreditamento.

E' definito ed attuato un processo di monitoraggio e di valutazione dell'uso delle risorse (capacity management), per analizzare e valutare le attuali prestazioni del sistema ed alla base delle proiezioni e definizione di future esigenze relative alle prestazioni od a nuove ed emergenti tecnologie tali da assicurare che le prestazioni del sistema di conservazione siano adeguate e conformi alle necessità, ai livelli di servizi concordati contrattualmente e nelle convenzioni e prevenivano l'obsolescenza tecnologica.

Il monitoraggio e la valutazione considera tutte le diverse componenti del servizio, per assicurare una visione complessiva in ottica end to end. Il processo di monitoraggio e di valutazione dell'uso delle risorse (capacity management) è eseguito non solo tramite analisi ad hoc, ma anche con strumenti automatizzati in grado di segnalare eventuali alert e messaggi in grado di indirizzare le valutazioni e gli opportuni cambiamenti da valutare sia per l'hardware, che per il software ad esempio per minimizzare i rischi ed i costi, limitare i guasti e migliorare le performance.

[Torna al sommario](#)

9.1 Procedure di monitoraggio

Il Conservatore effettua le seguenti attività:

- verifica periodicamente la continua conformità del sistema di conservazione alle norme e agli standard di riferimento;
- gestisce il cambiamento, ossia tutte le attività che possono portare ad un cambiamento del sistema di conservazione, mantenendo l'aderenza a normativa e standard di riferimento. Esempi di tipologie cambiamenti possono essere:
- infrastrutturali, al fine di garantire l'operatività e fruibilità del servizio;
- tecnologici, al fine di garantire l'adeguamento tecnologico della soluzione realizzata;
- adeguamento al processo di business dettato da un cambiamento della norma e/o degli standard previsti;
- di aggiornamento e reingegnerizzazione delle procedure, qualora gli eventi di cui sopra impattino sui processi definiti e descritti nel presente manuale.

Per quanto riguarda la valutazione delle prestazioni essa viene testata mediante un apposito strumento software.

La rilevazione dei tempi di elaborazione permette di ottenere l'andamento delle prestazioni e di effettuare, qualora sia il caso, opportuni interventi per garantire prestazioni soddisfacenti.

Le prestazioni sono registrate direttamente nel sistema di rilevamento e consultabili dai tecnici. Inoltre il sistema permette di produrre report e grafici di sintesi.

Almeno una volta all'anno si eseguono test di capacity per pronosticare le esigenze in

termini di risorse di calcolo necessarie per garantire nel tempo il buon funzionamento del sistema, in linea con il piano di Conservazione.

Gli esiti dei test sono registrati e sottoposti al Responsabile del servizio di conservazione durante il riesame della Direzione.

[Torna al sommario](#)

9.2 Verifica dell'integrità degli archivi

Per tutti i file conservati viene eseguito un audit che consiste nelle seguenti verifiche:

| Tipo di verifica | Descrizione della verifica |
|--|---|
| Verifica dell'HASH dei file SInCRO | Il sistema verifica che l'HASH, calcolato in formato SHA-256, sia identico all'HASH calcolato all'atto dello storage nel database del pacchetto di archiviazione. |
| Verifica dell'HASH dei file di marca temporale | Il sistema verifica che l'HASH, calcolato in formato SHA-256, sia identico all'HASH calcolato all'atto dello storage nel database del file .tsr che contiene la marca temporale del pacchetto di archiviazione. |
| Verifica dell'HASH dei documenti conservati | Il sistema verifica che l'HASH del file conservato, calcolato in formato SHA-256, sia identico all'HASH dichiarato nel file XML SInCRO del pacchetto di archiviazione. |
| Verifica dei metadati obbligatori dei documenti conservati | Viene verificata l'esistenza nel database dei metadati indicati sul singolo documento. |

Per certificare l'avvenuta verifica viene:

- prodotto un file in formato XML SInCRO;
- il file viene firmato dal Responsabile del servizio di conservazione;
- il file viene marcato temporalmente;
- tutte le informazioni del file SInCRO e del file .tsr della marca temporale sono inserite nel database del sistema di conservazione;
- i file sono versati nel sistema di conservazione.

Come detto, il processo di verifica riguarda tutti i dati contenuti negli archivi, ed è condotto in modo tale da assicurare la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;

Giova ricordare quanto già detto a proposito dei Pacchetti di Versamento e dei Pacchetti di Archiviazione, e cioè che Il sistema tecnologico che presiede il sistema di conservazione è in alta affidabilità e garantisce la completa ridondanza dei dati.

Il servizio di conservazione prevede che gli archivi siano sottoposti a procedure di backup secondo le procedure previste dalla ISO 27001. Le copie di sicurezza sono mantenute coerentemente con la politica di conservazione dei backup che tiene conto delle esigenze del servizio di conservazione. Le politiche di mantenimento dei backup sono dettagliate nelle condizioni generali del servizio di conservazione.

Eventuali accordi con il Titolare per un mantenimento personalizzato sono oggetto di un

separato accordo tra le parti.

Le operazioni di backup si basano su due processi definiti come segue:

- processo di archiviazione su disco, presso il sito primario ed il sito secondario
- processo di storicizzazione su nastro. I nastri e le library che si occupano di questo processo sono posti in un sito delocalizzato rispetto al sito primario e secondario

[Torna al sommario](#)

9.3 Soluzioni adottate in caso di anomalie

Si definisce “incidente di sicurezza” qualsiasi evento che comprometta o minacci di compromettere il corretto funzionamento dei sistemi e/o delle reti dell'organizzazione o l'integrità e/o la riservatezza delle informazioni in esse memorizzate od in transito, o che violi le politiche di sicurezza definite o le leggi in vigore.

Zucchetti classifica gli incidenti definendo preventivamente la codifica e la gestione degli stessi.

In merito al piano di risposta ai security incident per il servizio di conservazione erogato dai sistemi dislocati presso il datacenter Zucchetti, le procedure adottate in ottica IEC/ISO 27001 facenti parte del SGSI aziendale, stabiliscono che il processo nasce dalla pianificazione anticipata e si conclude con la revisione della gestione del security incident.

L'obiettivo è quello di assicurare che i disservizi siano gestiti in modo rapido, efficiente e con il minimo disagio, registrando:

- nel trouble ticketing, tutte le comunicazioni intercorse con il cliente, sino alla chiusura del security incident
- nella relazione del security incident la gestione del caso
- nel CMDB (asset) l'evento ed i dati necessari.

Il suddetto piano di gestione è applicato in coincidenza della rilevazione del security incident, anche se non intenzionali, o nei casi in cui i dati o il servizio stesso non rispettano, anche se pur parzialmente, i requisiti di:

- disponibilità
- integrità
- riservatezza

Come previsto dal SGSI aziendale, è presente un processo di registrazione degli incidenti informatici volto a raccogliere le prove interessanti nel caso si debbano intraprendere azioni legali.

Per quanto riguarda i fornitori, gli stessi, nel prestare il servizio, accettano ed applicano le regole di gestione degli incidenti, recepite in un apposito contratto, in particolare devono essere sempre seguite le seguenti indicazioni:

- informazione agli interessati
- interventi nel rispetto degli SLA e della continuità

- registrazione dell'incidente

Il processo di gestione degli incidenti è articolato nelle seguenti di seguito descritte.

Gestione incidenti

Rilevazione e classificazione

Zucchetti S.p.a. si è dotata di una procedura di gestione degli Incidenti certificata secondo lo standard ISO 27001 che prevede il coinvolgimento di un apposito Team di risposta il quale comprende, oltre al Responsabile del servizio di conservazione, tutte le altre figure eventualmente coinvolte e/o competenti. L'iter di gestione dell'Incidente definito dalla procedura prevede il tracciamento, l'analisi e il monitoraggio fino alla risoluzione dello stesso tramite il sistema di ticketing e un'apposita gestione delle comunicazioni da inviare agli interessati contenenti, in linea generale, tempi e modi di risoluzione stimati.

Ripristino

Vengono pianificate e attuate le operazioni individuate come correzione definitiva, in modo da ripristinare i livelli di servizio alla piena operatività.

Follow-up

Nella fase post incidente si controlla la bontà della soluzione adottata, si valutano eventuali ulteriori migliorie, se è il caso si fa formazione/informazione al personale interessato.

Tutto il personale è informato della procedura sopra citata.

Gestione debolezze

Il personale è reso responsabile circa la continua attenzione a rilevare situazioni di debolezza, di qualsivoglia genere (da quelle tecniche a quelle organizzative), e a comunicarle al Responsabile del servizio di conservazione.

A fronte di una segnalazione di debolezza, il Responsabile del servizio di conservazione, con il supporto del Responsabile della sicurezza e dei reparti interessati, valuta i rischi e le contromisure.

Le contromisure si possono riassumere in:

- Contenimento effetti - si tratta di attuare azioni di tipo preventivo e contenitivo con effetto immediato, volte a limitare i possibili rischi.
- Correzione - sono le azioni risolutive che permettono di superare la debolezza rilevata.

[Torna al sommario](#)

10. CANCELLAZIONE DEI DOCUMENTI

La cancellazione dei documenti dal sistema di conservazione è una problematica

estremamente delicata alla quale il Conservatore presta estrema attenzione. Prima di esaminare la procedura, si evidenzia come la cancellazione di un documento sia in tutto e per tutto una attività simile allo Scarto visto precedentemente.

Lo scarto è l'operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale.

Si ribadisce che il sistema di conservazione prevede che nel caso degli archivi pubblici o privati, che rivestono interesse storico particolarmente importante, lo scarto del pacchetto di archiviazione avviene previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo rilasciata al Titolare secondo quanto previsto dalla normativa vigente in materia.

[Torna al sommario](#)

10.1 Richiesta del Titolare di cancellazione dei documenti

Il Produttore, il Titolare o altro soggetto autorizzato dal cliente nel contratto sottoscritto può inoltrare una richiesta di cancellazione di uno o più documenti inseriti nel sistema di conservazione.

La richiesta avviene tramite apposita funzionalità presente nell'applicazione.

[Torna al sommario](#)

10.2 Richiesta di conferma via pec della cancellazione

In seguito alla richiesta di cancellazione inserita, il sistema di conservazione invia al richiedente autorizzato una PEC contenente l'indicazione di tutti i documenti per cui è stata richiesta la cancellazione.

[Torna al sommario](#)

10.3 Conferma del Produttore/Titolare alla cancellazione

Il soggetto richiedente deve confermare, tramite apposita funzionalità presente nell'applicazione, la richiesta di cancellazione.

Il soggetto richiedente può eliminare la richiesta di cancellazione.

[Torna al sommario](#)

10.4 Eliminazione dei documenti

I documenti ed i relativi metadati per cui esiste una richiesta di cancellazione approvata dal soggetto richiedente sono eliminati del sistema di conservazione tramite una apposita procedura.

Si ribadisce che il sistema di conservazione prevede che nel caso degli archivi pubblici o privati, che rivestono interesse storico particolarmente importante, lo scarto del pacchetto di archiviazione avviene previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo rilasciata al Titolare secondo quanto previsto dalla normativa vigente in materia.

[Torna al sommario](#)