Manuale di Conservazione - Omniadoc Spa

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	15/12/2015	Marcello Avolio	RSC
Verifica	18/12/2015	Marco Dallaturca	RSSC
Approvazione	18/12/2015	Marcello Avolio	RSC

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
Ver 1	18/12/2015	----------	----------
Ver 2	25/04/2016	Introduzione architettura su Cloud Italia	
Ver 3	20/07/2016	Aggiunto Testo alternativo su immagini e aggiornato organigramma	
Ver 4	14/09/2016	Attivazione nuova configurazione su Cloud	
Ver 5	25/01/2018	Recepimento prime raccomandazioni da visita di certificazione	
Ver 6	10/01/2020	Piano cessazione attività di conservazione Aggiornamento riferimenti certificazione 27001:2013 Aggiornamento Siti Data Center	
Ver 7	24/08/2020	Modifiche infrastruttura Hardware, Sistema S3 e database.	

INDICE DEL DOCUMENTO

1. SCOPO E AMBITO DEL DOCUMENTO

Il presente Manuale descrive, dal punto di vista organizzativo, tecnico ed operativo, il *sistema di conservazione* dei documenti informatici che la società OmniaDoc SpA ha realizzato, gestisce e controlla al fine di fornire un servizio di Conservazione a norma in favore dei propri clienti.
Il presente Manuale, in particolare:

- individua il modello organizzativo definito da Omniadoc per il *sistema di conservazione*;
- definisce le competenze, i ruoli e le responsabilità degli attori coinvolti nel processo di conservazione dei documenti;
- elenca le tipologie degli oggetti sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di documenti e delle eventuali eccezioni;
- illustra le procedure atte ad assicurare la conservazione dei documenti informatici prodotti e ricevuti dai singoli clienti, nonché dei fascicoli informatici, garantendone le caratteristiche di **autenticità, integrità, affidabilità, leggibilità e reperibilità**;
- descrive il trattamento dell'intero ciclo di gestione dell'oggetto conservato nell'ambito del processo di conservazione;
- descrive le modalità di accesso ai documenti e ai fascicoli conservati, per il periodo prescritto dalla norma, indipendentemente dall'evolversi del contesto tecnologico e la modalità di svolgimento del processo di esibizione e di esportazione dal *sistema di conservazione* con la produzione del **pacchetto di distribuzione**;
- definisce le procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie;
- precisa le procedure per la produzione di *duplicati* o *copie* ai sensi del C.A.D.;
- indica i tempi entro i quali le diverse tipologie di documenti devono essere scartate ovvero trasferite in conservazione, ove, nel caso delle pubbliche amministrazioni, non già presenti nel manuale di gestione.

Il presente Manuale recepisce appieno le disposizioni contenute nel D.Lgs n. 82/2005 e s.m.i. (Codice dell'Amministrazione Digitale – di seguito anche solo CAD), oltre alle ulteriori norme e indicazioni riportate nei provvedimenti di legge o di prassi, anche amministrativa, richiamati nel capitolo "*normativa e standard di riferimento*".

Il presente Manuale è reso pubblico in formato PDF firmato digitalmente dal legale rappresentante di Omniadoc SpA.

Torna al Sommario

2. TERMINOLOGIA (GLOSSARIO E ACRONIMI)

TERMINE	DEFINIZIONE
accesso	operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici
accreditamento	riconoscimento, da parte **dell'Agenzia per l'Italia digitale**, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione
affidabilità	caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico
aggregazione documentale informatica	aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente
archivio	complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività
archivio informatico	archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico
area organizzativa omogenea	un insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445
attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico
autenticità	caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico
base di dati	collezione di dati registrati e correlati tra loro
certificatore accreditato	soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, **dall' Agenzia per l'Italia digitale**, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
ciclo di gestione	arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo

TERMINE	DEFINIZIONE
classificazione	attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati
Codice	decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni
codice eseguibile	insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici
conservatore accreditato	soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, **dall'Agenzia per l'Italia digitale,** il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, **dall'Agenzia per l'Italia digitale**
conservazione	insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione
Coordinatore della Gestione Documentale	responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 nei casi di amministrazioni che abbiano istituito più Aree Organizzative Omogenee
copia analogica del documento informatico	documento analogico avente contenuto identico a quello del documento informatico da cui è tratto
copia di sicurezza	copia di *backup* degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 delle presenti regole tecniche per il sistema di conservazione
destinatario	identifica il soggetto/sistema al quale il documento informatico è indirizzato
duplicazione dei documenti informatici	produzione di duplicati informatici
esibizione	operazione che consente di visualizzare un documento conservato e di ottenerne copia
estratto per riassunto	documento nel quale si attestano in maniera sintetica ma esaustiva fatti, stati o qualità desunti da dati o documenti in possesso di soggetti pubblici
evidenza informatica	una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica
fascicolo informatico	Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del Codice**.**
formato	modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file

TERMINE	DEFINIZIONE
funzionalità aggiuntive	le ulteriori componenti del sistema di protocollo informatico necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni
funzionalità interoperative	le componenti del sistema di protocollo informatico finalizzate a rispondere almeno ai requisiti di interconnessione di cui all'articolo 60 del D.P.R. 28 dicembre 2000, n. 445
funzionalità minima	la componente del sistema di protocollo informatico che rispetta i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445
funzione di *hash*	una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
generazione automatica di documento informatico	formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni
identificativo univoco	sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione
immodificabilità	caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso
impronta	la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di *hash*
insieme minimo di metadati del documento informatico	complesso dei metadati, la cui struttura è descritta nell'allegato 5 del presente decreto, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta
integrità	insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato
interoperabilità	capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi
leggibilità	insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti
log di sistema	registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati
manuale di conservazione	strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 delle regole tecniche del sistema di conservazione
manuale di gestione	strumento che descrive il sistema di gestione informatica dei documenti di cui all'articolo 5 delle regole tecniche del protocollo informatico ai sensi delle regole tecniche per il protocollo informatico D.P.C.M. 31 ottobre 2000 e successive modificazioni e integrazioni
TERMINE	DEFINIZIONE

memorizzazione	processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici
metadati	insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 del presente
pacchetto di archiviazione	pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del presente decreto e secondo le modalità riportate nel manuale di conservazione
pacchetto di distribuzione	pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta
pacchetto di versamento	pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione
pacchetto informativo	contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare
piano della sicurezza del sistema di conservazione	documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza
piano della sicurezza del sistema di gestione informatica dei documenti	documento, che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi nell'ambito dell'organizzazione di appartenenza
piano di conservazione	strumento, integrato con il sistema di classificazione per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445
piano generale della sicurezza	documento per la pianificazione delle attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza
presa in carico	accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione
processo di conservazione	insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 10 delle regole tecniche del sistema di conservazione
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 responsabile della gestione documentale.
TERMINE	**DEFINIZIONE**

rapporto di versamento	documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore
registrazione informatica	insieme delle informazioni risultanti da transazioni informatiche o dalla presentazione in via telematica di dati attraverso moduli o formulari resi disponibili in vario modo all'utente
registro particolare	registro informatico di particolari tipologie di atti o documenti; nell'ambito della pubblica amministrazione è previsto ai sensi dell'articolo 53, comma 5 del D.P.R. 28 dicembre 2000, n. 445
registro di protocollo	registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti
repertorio informatico	registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche con cui si formano altri atti e documenti o indici di atti e documenti secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica
responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi	dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione.
responsabile della conservazione	soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 delle regole tecniche del sistema di conservazione
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 **storico** culturale
sistema di classificazione	strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata
sistema di conservazione	sistema di conservazione dei documenti informatici di cui all'articolo 44 del Codice
sistema di gestione informatica dei documenti	nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445; per i privati è il sistema che consente la tenuta di un documento informatico

TERMINE	DEFINIZIONE
staticità	Caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione
transazione informatica	particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche della base di dati
Testo unico	decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni
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
versamento agli archivi di stato	operazione con cui il responsabile della conservazione di un organo giudiziario o amministrativo dello Stato effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali

ACRONIMI	
TERMINE	**DEFINIZIONE**
AE	Agenzia delle Entrate
AgiD	Agenzia per l'Italia Digitale
CAD	Codice dell'Amministrazione Digitale
FTP	File Transfer Protocol
SFTP	SSH File Transfer Protocol o SFTP è un protocollo di rete che prevede il trasferimento dei dati e funzionalità di manipolazione. Usato con protocollo SSH-2 per il trasferimento dei file sicuro
IpdA	Indice del Pacchetto di Archiviazione
IpdD	Indice del Pacchetto di Distribuzione (o Rapporto di distribuzione)
IPdV	Indice del Pacchetto di Versamento
ISO	International Organization for Standardization
OAIS	Open Archival Information System ISO 14721:2012
PdD	Pacchetto di Distribuzione
PdS	Pacchetto di Scarto
PdV	Pacchetto di Versamento
RdV	Rapporto di Versamento
RSC	Responsabile del servizio di conservazione
RSI	Responsabile dei servizi informativi per la conservazione
RSM	Responsabile sviluppo e manutenzione del sistema di conservazione
RSSC	Resposanbile sicurezza dei sistemi per la conservazione
RTP	Responsabile Trattamento Dati Personali
SHA	Secure Hash Algoritm
SHA-256	Algoritmo di hash a 256 caratteri sviluppato da National Security Agency e pubblicato da NIST (National Institute of Standards and Technologies)

SinCRO	Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali
W3C	World Wide Web Consortium, è un'organizzazione non governativa internazionale che ha come scopo quello di sviluppare tutte le potenzialità del World Wide Web
XML linguaggio XML	acronimo di eXtensible Markup Language, è un linguaggio marcatore basato su un meccanismo sintattico che consente di definire e controllare il significato degli elementi contenuti in un documento o in un testo
ZIP	formato di compressione dei dati che supporta vari algoritmi di compressione, uno dei quali è basato su una variante dell'algoritmo LZW

Torna al Sommario

3. NORMATIVA E STANDARD DI RIFERIMENTO

3.1 Normativa di riferimento

La normativa di riferimento alla data ordinata secondo la gerarchia delle fonti.
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;

- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;

- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;

- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);

- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;

- 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 Ministero dell'Economia e delle Finanze del 17 giugno 2014 - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto

- Decreto del Presidente del Consiglio dei Ministri del 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

- 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;

- Deliberazione Cnipa del 21 maggio 2009, n. 45 (come modificata dalla determinazione dirigenziale DigitPA n. 69/2010). Regole per la creazione dei certificati di firma e di marca che quelle per il loro utilizzo, riconoscimento e verifica;

- Direttiva 2010/45/UE del 13 luglio 2010 recante modifica della direttiva 2006/112/CE relativa al sistema comune d'imposta sul valore aggiunto per quanto riguarda le norme in materie di fatturazione. Recepita in Italia dalla Legge 228/2012, legge di stabilità 2013 del 24 dicembre 2012.

- Circolare dell'Agenzia delle Entrate n. 45/E del 19 ottobre 2005;

- Circolare dell'Agenzia delle Entrate n. 36/E del 06 dicembre 2006;

- Circolare dell'Agenzia delle Entrate n. 18/E del 24 giugno 2014;

- Risoluzione Agenzia delle Entrate nr. 161E del 9 luglio 2007;

- Risoluzioni Agenzia delle Entrate nr. 158E del 15 giugno e nr. 196E del 30 luglio 2009;

- Risoluzione Agenzia delle Entrate nr. 81/E del 25 settembre 2015.

Torna al Sommario

3.2 Standard di riferimento

Si riportano di seguito gli standard di riferimento elencati nell'allegato 3 delle Regole Tecniche in materia di Sistema di conservazione con indicazione delle versioni aggiornate al 1° ottobre 2014.

- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;

- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);

- ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;

- ETSI TR 101 533-2 V1.3.1 (2012-04)Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;

- UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;

- ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

- ISO 15489-1:2016 Information and documentation -- Records management

Torna al Sommario

4. RUOLI E RESPONSABILITA'

Il processo di conservazione impone alle aziende l'istituzione di una struttura e di una organizzazione, coerente con le proprie politiche di efficienza gestionale, che garantisca la piena osservanza di tale normativa. A tal scopo, in base alle specifiche necessità aziendali, il Responsabile del Servizio di Conservazione, sia dal punto di vista dell'impostazione operativa delle attività di conservazione, sia dal punto di vista della scelta delle risorse coinvolte nel processo, deve organizzare il lavoro affinché esso venga svolto secondo i principi stabiliti dalla legislazione vigente.

Il processo di conservazione realizzato da Omniadoc vede coinvolte, a vario titolo, differenti figure e differenti professionalità. Tutte le figure coinvolte sono coordinate dal responsabile del servizio di conservazione che è il punto di riferimento per le attività del conservatore.

Il responsabile del servizio di conservazione

Il responsabile del servizio di conservazione è colui che si occupa di definire e attuare le politiche complessive del sistema di conservazione, nonché di governare la gestione del sistema di conservazione; inoltre a lui spetta la definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente. E' il garante della corretta erogazione del servizio di conservazione all'ente produttore, gestisce tutte le convenzioni, definisce gli aspetti tecnico-operativi e valida i disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.

In caso di impossibilità a svolgere i compiti ad esso assegnati, viene nominato un "Delegato del responsabile del servizio di conservazione" che opera presso il soggetto conservatore.

Il responsabile della funzione archivistica

Il responsabile della funzione archivistica è colui che definisce e gestisce il 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; Definisce il set di metadati di conservazione dei documenti e dei fascicoli informatici; - Gestisce il monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione; - Collabora con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.

Il responsabile del trattamento dati personali

Il responsabile del trattamento dei dati personali è il garante del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; garantisce che il trattamento dei dati affidati dai Clienti avvenga nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.

Il responsabile della sicurezza dei sistemi per la conservazione

Il responsabile della sicurezza dei sistemi per la conservazione si occupa del monitoraggio continuo e del rispetto dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; è suo dovere segnalare ogni eventuale difformità al' responsabile del servizio di conservazione" e individuare e pianificare le necessarie azioni correttive.

Il responsabile dei sistemi informativi per la conservazione

Il responsabile dei sistemi informativi per la conservazione gestisce il corretto funzionamento di tutte le componenti hardware e software del sistema di conservazione. Tiene monitorati i livelli di servizio (SLA) concordati con il Cliente e segnala eventuali difformità degli SLA al Responsabile del servizio di conservazione individuando e pianificando le necessarie azioni correttive.

Controlla e verifica anche i livelli di servizio erogati da terzi segnalando le eventuali difformità al Responsabile del servizio di conservazione.

Infine pianifica lo sviluppo delle infrastrutture tecnologiche del sistema di conservazione.

Il Responsabile dello sviluppo e della manutenzione del sistema di conservazione

A tale responsabile compete il coordinamento dello sviluppo e della manutenzione delle componenti hardware e software del sistema di conservazione. Pianifica e tiene monitorati i progetti di sviluppo del sistema di conservazione oltre agli SLA relativi alla manutenzione del sistema di conservazione. Si interfaccia, inoltre, con il Cliente relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche. A lui, infine, compete la gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.

ruoli	nominativo	periodo nel ruolo
Responsabile del servizio di conservazione	Marcello Avolio	Dal 2006
Delegato del responsabile del servizio di conservazione	Marco Dallaturca	Dal 2006
Responsabile Sicurezza dei sistemi per la conservazione	Marco Dallaturca	Dal 2006
Responsabile funzione archivistica di conservazione	Cecilia Tamagnini Matteo del Basso	Dal luglio 2015 alla data di approvazione da parte di AgID della revisione 4 Dalla data di approvazione da parte di AgID della revisione 4
Responsabile trattamento dati personali	Marco Dallaturca	Dal 2006
Responsabile sistemi informativi per la conservazione	Marcello Avolio	Dal 2006
Responsabile sviluppo e manutenzione del sistema di conservazione	Lorenzo Braidi	Dal 2006

Torna al Sommario

5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Organigramma

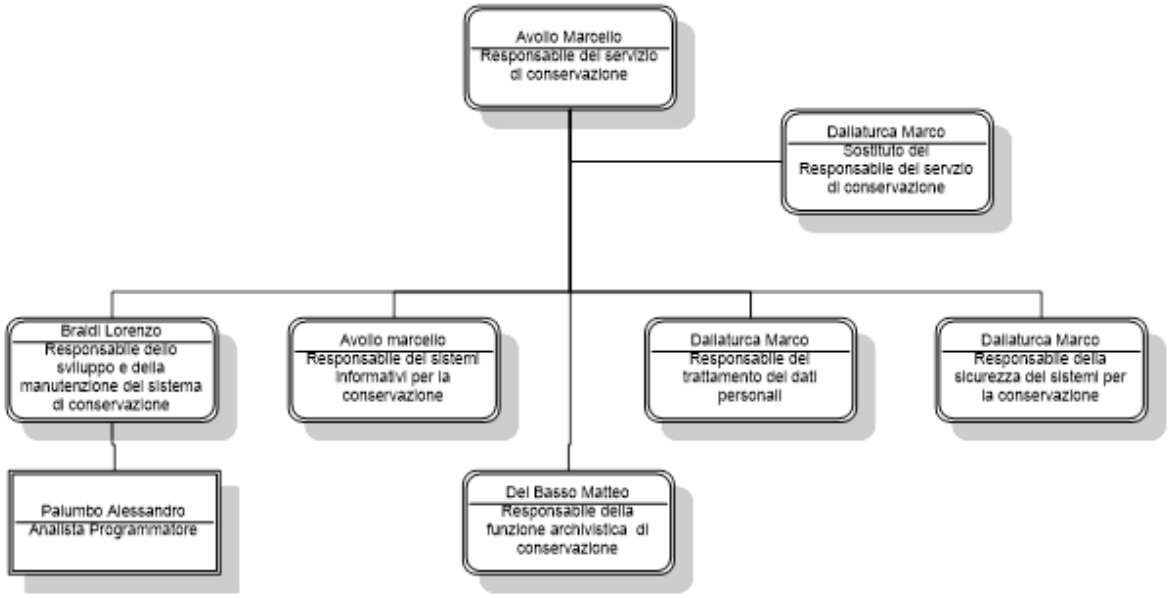


Figura 1. Organigramma

Torna al Sommario

5.2 Strutture organizzative

Di seguito si descrivono le strutture organizzative che intervengono nel processo di un contratto di conservazione di un cliente.

- **Attivazione del servizio di conservazione** (a seguito della sottoscrizione di un contratto);

A seguito della sottoscrizione di un contratto di conservazione il Conservatore definisce un capoprogetto che ha il compito di concordare e definire con il cliente il documento di progetto "Specificità di contratto cliente". Il documento redatto in base alle informazioni condivise con il cliente descrive i requisiti essenziali del servizio, l'analisi della conformità alla normativa vigente e la definizione dei processi che sono messi in atto per il trattamento dei dati. Il documento è revisionato dal Responsabile della funzione archivistica di conservazione, dal Responsabile del trattamento dei dati personali e ove necessario e dal Responsabile del servizio di conservazione.

Le successivo variazioni al servizio che possono nascere nel tempo comportano l'aggiornamento sistematico del documento di progetto.

- **Impostazione e collaudo**

Terminata la fase di definizione del progetto, sono attivate le aree organizzative di sviluppo e di produzione. L'area organizzativa di sviluppo ha il compito di generare / attivare , laddove necessario, i programmi software definiti nel documento di progetto per il trattamento dei dati.

L'area organizzativa di produzione gestisce le componenti hardware e software del servizio e presidia, controlla e monitora il corretto funzionamento dei sistemi.

L'intero processo di gestione dei dati è sottoposta ad una fase di collaudo al fine di verificare che il comportamento sia coerente con quanto indicato nel documento di progetto. Il collaudo deve essere validato dal cliente per poter poi passare al passaggio in produzione.

- **Produzione**

L'area organizzativa di produzione, supervisionata dal responsabile del servizio della conservazione di Omniadoc, provvede a svolgere le attività volte alla conservazione dei documenti e garantirne la leggibilità e la tenuta nel tempo:

- acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento;
- preparazione e gestione del pacchetto di archiviazione;
- preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta;
- scarto dei pacchetti di archiviazione;
- chiusura del servizio di conservazione (al termine di un contratto).
- Supporto agli utenti/ clienti produttori dei documenti
- Rilevazione e catalogazione delle segnalazioni di anomalie da gestire mediante i processi di change management
- Rilevazione e catalogazione delle proposte migliorative da gestire mediante i processi di change management

Torna al Sommario

6. OGGETTI SOTTOPOSTI A CONSERVAZIONE

6.1 Oggetti conservati

Gli oggetti sottoposti a conservazione sono specificati nel documento di progetto "Specificità di contratto cliente" concordato tra il Conservatore ed il Cliente e le relative logiche di conservazione distinte per ciascuna tipologia documentale.
Per ogni tipologia documentale si definiscono :

- la natura e l'oggetto della tipologia documentale;
- l'elenco e la descrizione dei metadati associati ai documenti;
- il periodo di conservazione;
- l'elenco e la descrizione dei formati dei file utilizzati;
- l'indicazione dei visualizzatori relativi ai formati gestiti, necessari per garantire la leggibilità nel tempo dei documenti conservati;
- I livelli di servizio (SLA) concordati con l'ente produttore;
- Eventuali logiche specifiche che caratterizzano il processo di conservazione.

Torna al Sommario

6.1.2 Formati dei documenti

I formati idonei alla conservazione devono assolvere all'esigenza che il documento assuma le caratteristiche di immodificabilità e di staticità previste dalle regole tecniche.

Formato File	Estensione	Standard	Visualizzatore	Produttore del visualizzatore
PDF	.pdf	ISO32000-1	Adobe Reader	Adobe Systems www.adobe.com
PDF/A	.pdf	ISO 19005-1:2005 (vers. PDF 1.4) ISO 19005-2:2011 (vers. PDF 1.7)	Adobe Reader	Adobe Systems www.adobe.com
XML	.xml		Mozilla,Chrome,Internet Explorer, notepad++, Qualsiasi editor di testo	Mozilla,Google,Microsoft,produttori vari
TXT	.txt		Mozilla,Chrome,Internet Explorer, notepad++, Qualsiasi editor di testo	Mozilla,Google,Microsoft,produttori vari
TIFF	.tif		Vari visualizzatori.	Produttori vari
EML	.eml		Client di posta che supportano il formato	Produttori vari

È possibile che sia necessaria la conservazione di formati non previsti in elenco. I formati specifici sono concordati con il Responsabile della conservazione e inseriti nell'allegato "Specifica del contratto" insieme ai riferimenti ai rispettivi viewer.

Torna al Sommario

6.1.3 Classi documentali e metadati

La classe documentale definisce le caratteristiche di una determinata tipologia documentale da sottoporre a procedura di conservazione digitale. Si definiscono le informazioni indispensabili per qualificarla e identificarne gli elementi distintivi.

I metadati di ogni classe documetale sono indicati nel documento di progetto "Specificità di contratto cliente" concordato tra il Conservatore ed il Cliente.

In ogni caso, per ciascuna classe documentale, il Conservatore garantisce l'uso dei metadati minimi di cui all'allegato 5 del DPCM 3 dicembre 2013.

Il cliente può decidere di associare al documento eventuali ulteriori metadati che al pari del set minimo di metadati saranno oggetto di indicizzazione nel sistema di conservazione.
Torna al Sommario

6.1.4 Metadati minimi del documento informatico avente rilevanza tributaria

Sulla base di quanto disposto dall'art. 3, del decreto del Ministero dell'Economia e delle Finanze del 23 gennaio 2004, devono essere consentite le funzioni di ricerca e di estrazione delle informazioni dagli archivi contenenti documenti informatici rilevanti ai fini delle disposizioni tributarie in relazione ai metadati di seguito riportati:

- cognome;
- nome;
- denominazione;
- codice fiscale;
- partita Iva;
- data documento;
- periodo d'imposta di riferimento;
- tipo documento

Torna al Sommario

6.2 Pacchetti di Versamento

Il Cliente Produttore fornisce al Conservatore i documenti informatici da conservare mediante un pacchetto di versamento (detto PdV). Il PdV è un file in formato .zip contenente i documenti informatici e un file di indici (detto IPdV) in formato xml conforme allo standard UNI - SINCRO che ne descrive il contenuto e i dati relativi alla richiesta di versamento in conservazione.

Informazioni presenti nell' indice del pacchetto di versamento (IPdV)

Nel IPdV sono riportate le seguenti informazioni strutturate :

- Informazioni sul produttore dei documenti
  - Sono riportati i dati identificativi del cliente che produce i documenti informatici
- Informazioni relative alla classe documentale oggetto del versamento
  - Sono riportate le informazioni relative alla classe documentale oggetto del versamento quali le descrizione dei metadati associati, la tipologia di documento, le regole per la tenuta quali la durata della conservazione, le logiche per la dismissione.
- Metadati
  - Sono riportati i metadati valorizzati di ogni documento informatico
  - il nome del file informatico.

E' possibile che sia necessaria la gestione di pacchetti di versamento formati di versamento rispetto allo standard UNI SINCRO. Omniadoc in accordo con il produttore, sulla base di accordi definiti nel documento di progetto "Specificità di contratto cliente", potrà fornire un apposito applicativo per la generazione dei Pacchetti di Versamento.

La rappresentazione grafica dello schema del PDdV fare riferimento a quanto riportato nel paragrafo 6.3.

Torna al Sommario

6.3 Pacchetti di Archiviazione

Il pacchetto di archiviazione (PdA) è composto da un file in formato .xml strutturato secondo lo standard SinCro UNI 11386:2010, contiene le informazioni descrittive della tipologia di documento conservato.

Un pacchetto di archiviazione descrive :

- Le logiche di tenuta dei documenti
- I metadati identificativi di ogni documento
- L'impronta del documenti informatico
- Il puntamento al documento informatico
- I dati relativi alla generazione del PdA
- I dati della marca temporale
- I dati del firmatario del PdA
- I dati dell'applicazione utilizzata per la generazione del PdA

Di seguito si riporta la rappresentazione grafica dell'indice del Pacchetto di Archiviazione

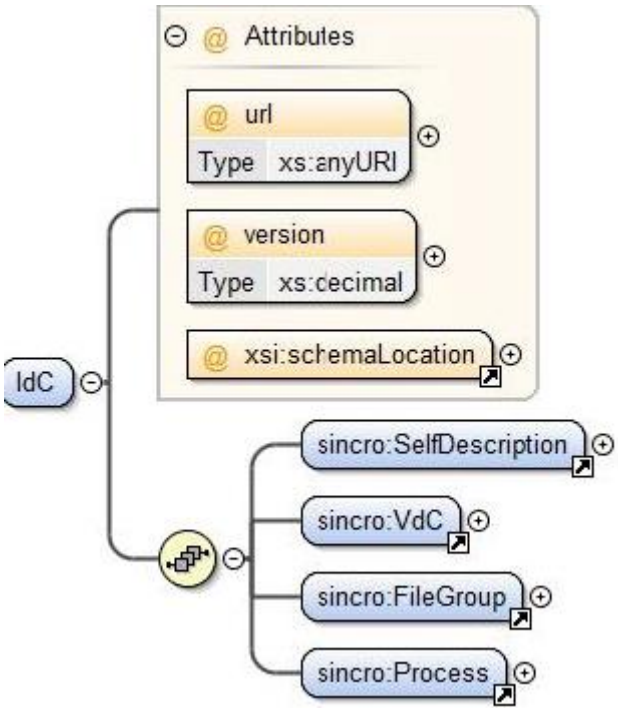


Figura 2. Descrizione Livello Globale

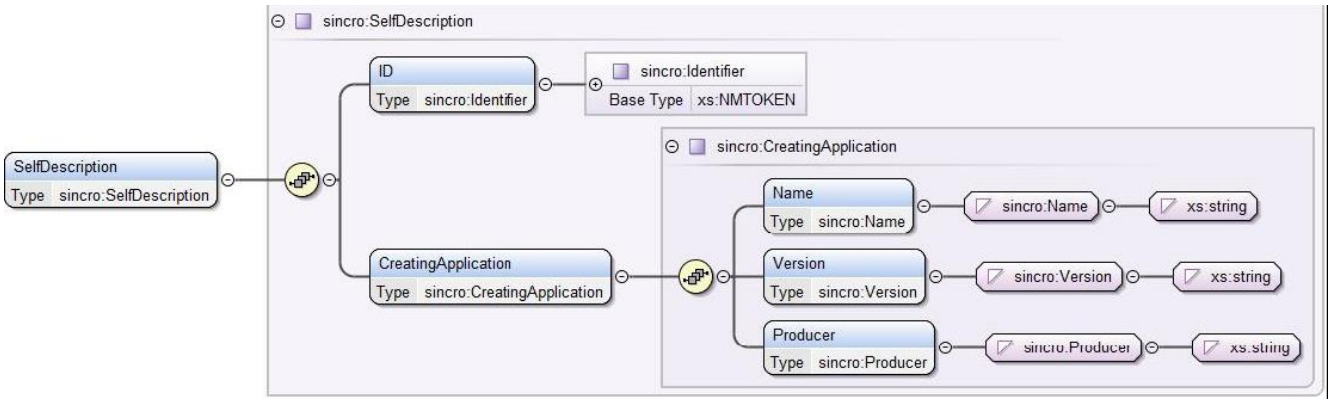


Figura 3. Dettaglio descrizione generale

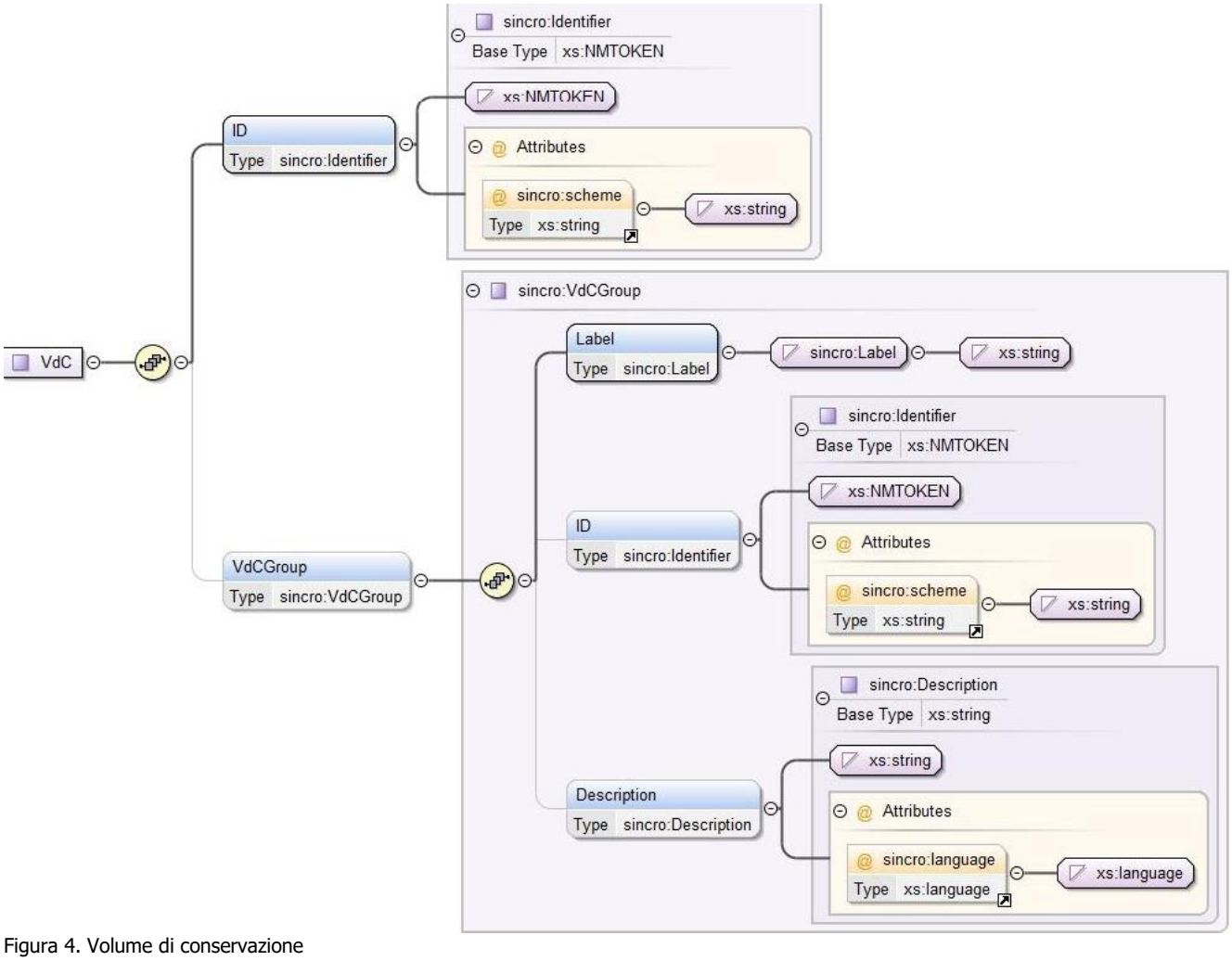


Figura 4. Volume di conservazione

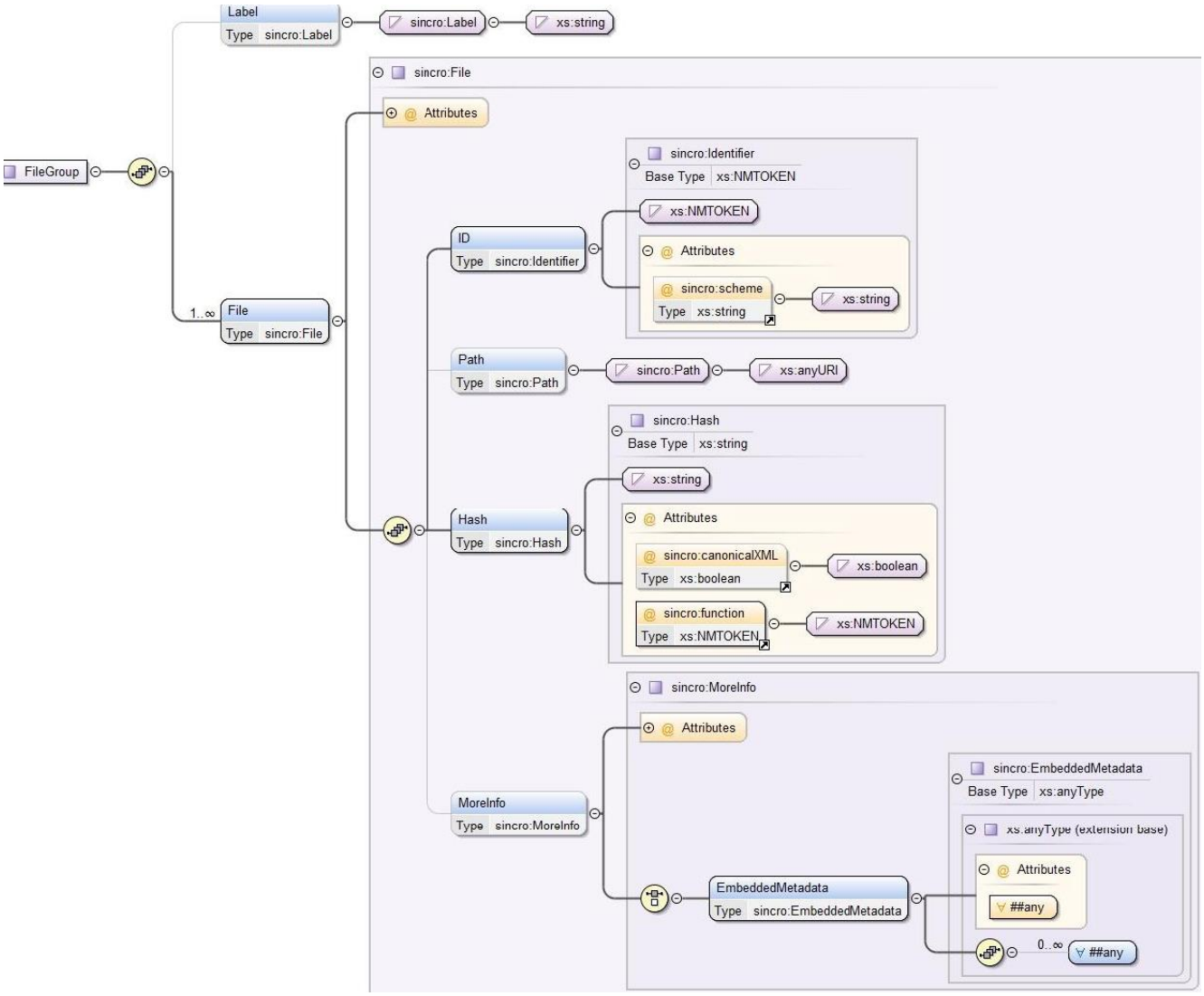


Figura 5. Dettaglio – File Group

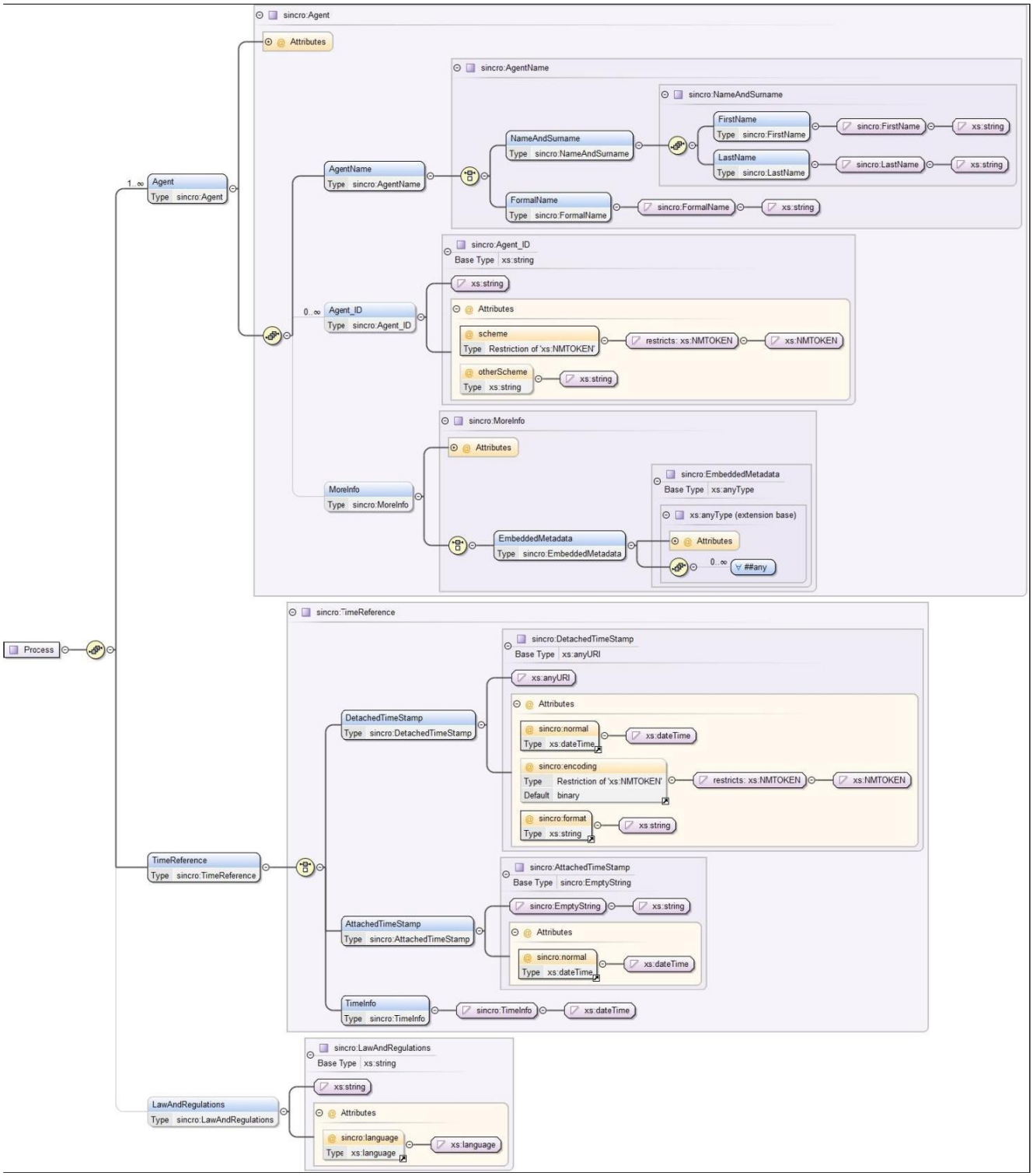


Figura 6. Dettaglio Processo

Torna al Sommario

6.4 Pacchetti di distribuzione

Il pacchetto di distribuzione è un file in formato .zip contenente copia dei documenti digitali in conservazione insieme ad un file indice di distribuzione strutturato in formato XML ed avente la medesima struttura dell'indice del pacchetto di archiviazione. Il pacchetto di distribuzione contiene, inoltre, un file in formato HTML che permette all'utente la consultazione del pacchetto di distribuzione nonchè la possibilità di svolgere delle ricerche sul contenuto.

Il file in formato .zip è nominato con l'id del pacchetto di distribuzione, corrispondente all'id univoco del pacchetto di archiviazione e messo a disposizione del cliente, il quale potrà scaricare i file mediante una connessione FTP / SFTP in base agli accordi contrattuali

Personalizzazioni del pacchetto di distribuzione. Qualora un contratto preveda personalizzazioni del pacchetto di distribuzione tali personalizzazioni sono riportate nel documento 'Specificità di contratto cliente'.

Torna al Sommario

7 Processo di Conservazione

Il processo di conservazione dei documenti è gestito tramite il software GiadaCD interamente progettato e realizzato da Omniadoc spa.

Le fasi del processo sono riassumibili come segue:

Ricezione del pacchetto di versamento	Il Cliente invia il PdV mediante uno dei metodi condivisi. sftp – web service
Verifica del pacchetto di versamento e generazione del rapporto di versamento	Presa in carico del PdV; Esecuzione di una serie di verifiche formali sulla completezza e sulla correttezza delle informazioni contenute nel file indice Generazione del rapporto di versamento o del ripudio del pacchetto di versamento in caso di anomalie bloccanti.
Generazione dei pacchetti di archiviazione	Generazione dei pacchetti di archiviazione per i documenti che hanno superato le verifiche e sono stati correttamente versati nel sistema.
Generazione pacchetti di distribuzione	Generazione dei pacchetti di distribuzione, su richiesta del Cliente, per consentire la consultazione / esibizione dei documenti.
Scarto / Restituzione	Individuazione dei pacchetti di archiviazione il sui termine di conservazione è scaduto, generazione della proposta di scarto da sottoporre al cliente. Esecuzione delle cancellazione dei documenti e dei pacchetti di archiviazione che il cliente ha accettato di cancellare.

Torna al Sommario

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

Il cliente può inviare i pacchetti di versamento mediante due procedure :

Procedura Sincrona a mezzo WebServices
Procedura Asincrona a mezzo trasferimento SFTP

Procedura Sincrona

Il cliente invia il PdV mediante web services
Il pacchetto viene interpretato subito dopo la ricezione
Il cliente riceve via web service l'esito della lavorazione.

Procedura Asincrona

Il Cliente invia il PdV mediante un trasferimento SFTP
Il PdV viene processato mediante un job di processo schedulato
Generazione del rapporto di versamento

In base ad accordi contrattuali, il cliente delega Omniadoc alla creazione dei pacchetti di versamento. Il cliente archivia i documenti nel sistema di archiviazione Giada e concorda quali classi documentali versare nel sistema di conservazione e con quale periodicità.
I metodi di versamento sono equivalenti a quelli sopra descritti.
Le attività di acquisizione dei pacchetti di versamento sono tracciate in appositi file di log distinti per giornata di attività.

Il sistema Omniadoc prevede procedure di salvataggio sia dei file di log che dei pacchetti di versamento ricevuti dal produttore. Il tempo di mantenimento della copia del PdV è definito con il soggetto produttore e riportata nel documento 'Specificità di contratto cliente'

Lo storico dei PdV gestiti è riportato in una apposita tabella del database consultabile anche dal produttore mediante l'accesso Web del sistema di conservazione.

L'intero sistema di storage di Omniadoc è riversato nel sito di disaster e recovery con allineamento immediato.

Torna al Sommario

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

I pacchetti di versamento sono sottoposti a controlli formali e di contenuto al fine di verificarne la validità.

Le verifiche sono volte ad assicurare che i metadati siano sintatticamente coretti, congruenti con la tipologia di documento a cui si riferiscono e che il formato del documento informatico sia tra quelli previsti nel manuale della conservazione.

Per ogni pacchetto di versamento sono verificati i seguenti requisiti:

- Identificazione certa del soggetto produttore. Tra i metadati presenti nel IPdV è obbligatorio l'identificativo fiscale del soggetto produttore che al momento del versamento è confontrato con la tabella dei produttori autorizzati da Omniadoc. Un ulteriore controllo è svolto mediante il metodo di trasmissione dei PdV basato sempre su una logica di invio previa autenticazione con credenziali diverse per ogni produttore. La logica delle credenziali è valida sia per le trasmissioni a mezzo WebServices che via SFTP
- Conformità dei formati dei documenti contenuti
- Conformità delle firme digitali apposte sui documenti
- Verifica dei metadati obbligatori
- Conformità tra il numero di documenti dichiarati nel IPdV e i documenti effettivamente presenti nel PdV
- Verifica de formato XML del IPdV
- Check che il documento non sià già presente nel sistema (documenti doppi)
- I documenti di natura tributaria sono soggetti al controllo della progressione numerica al fine i identificare eventuali "buchi di numerazione". I PdV che presentano "buchi di numerazione" sono rifiutati. Il responsabile del servizio di conservazione, previo esplicito accordo con il cliente potrà forzare l'accettazione del PdV.

Ulteriori controlli possono essere definiti in accordo con il cliente e dichiarati nel documento "specificità di contratto cliente".

L'esito dei controlli è riportato nel rapporto di versamento unitamente alle motivazioni dello scarto.

Le attività di controllo dei pacchetti di versamento sono tracciate in appositi file di log distinti per giornata di attività che sono oggetto di salvataggio da parte delle procedure Omniadoc per la gestione dei file di log.

Torna al Sommario

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

Il sistema di conservazione per ogni pacchetto di versamento gestito genera un rapporto di versamento(Rdv) previsto dalle regole tecniche (DPCM 3 dicembre 2013) come esito delle verifiche eseguite.

I pacchetti di versamento sono registrati nel database dell'applicazione in una tabella ed identificati univocamente mediante un codice progressivo numerico detto "idpacchettoversamento". In tabella sono riportati anche la data di elaborazione, l'esito della lavorazione, il numero di documenti processati,il numero di pagine e l'impronta del file .zip contenitore dei documenti e dell'IPdV.

Ogni documento presente nel PdV viene registrato nel database riportando l'impronta del documento calcolata mediante l'algoritmo SHA256. La stessa impronta calcolata è riportata nel rapporto di versamento.

I pacchetti di versamento danno vita ad una cartella fisica contenente i documenti del PdV ed il rapporto di versamento RdV.
RdV è un file in formato XML avente la stessa struttura del IPdV riportante l'elenco dei file versati, l'impronta (HASH) per ogni file e l'esito della lavorazione per ogni documento, l'identificativo univoco associato al documento nel sistema di conservazione che può essere utilizzato dai Clienti per aggiornare i propri sistemi informativi e il riferimento temporale indicante il momento di generazione del rapporto di versamento con riferimento al Tempo universale coordinato (UTC).

Il tempo universale è calcolata attraverso i server di Omniadoc sincronizzati con i server NTP (network time protocol) di Microsoft.

Di seguito uno stralcio del rapporto di versamento riportante i dati dell' esito

```
<ESITO>
    <STATO>OK</STATO>
    <NOTE/>
    <IMPRONTA>6555467fa3c8515e2043d752cc8fbc55a63f059c743f39bab23c0c2cc740a616</IMPRONTA>
    <IDPDV>3103</IDPDV>
    <IDUNIVOCO>1011742</IDUNIVOCO>
</ESITO>
<DATARAPPORTOVERSAMENTO>2015-10-22T13:51:07.183+01:00</DATARAPPORTOVERSAMENTO>
<PDV>Provmi_2210201512.ZIP</PDV>
<PDVIMPRONTA>559ab574c1e0a3d834bf6a149601c7cef57cbb356cad2da06b1c6ae14087aff5</PDVIMPRONTA
>
```

Il rapporto di versamento è reso disponibile al cliente tramite i canali previsti o su canali diversi in base agli accordi specifici riportati nel socumento 'Specificità di contratto cliente'

I canali previsti sono :

- HTTPS. Il cliente può eseguire il download del RdV mediante l'interfaccia Web del sistema di conservazione. Il download del RdV è possibile previa autenticazione nel sistema che tiene traccia dell'utente che si è autenticato e che svolge l'azione di download.

- FTPS. Il RdV è reso disponibile mediante il canale FTPS. L'accesso al canale è possibile solo previa autenticazione mediante credenziali personalizzate per ogni utente. Il sistema FTPS tiene traccia degli accessi eseguiti e scarica le informazioni in file di log memorizzati nello storage di Omniadoc.

I processi di gestione generano file di log distinti per data di lavorazione che sono salvati dalle procedure di gestione dei log di Omniadoc.

Torna al Sommario

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

Le verifiche dei PdV possono rilevare delle anomalie che generano il rifiuto del dei pacchetti di versamento:

- PdV non contiene l'IPdV
- Il File IPdV non valido rispetto allo schema XSD previsto.
- Fallita Identificazione del Produttore dei documenti
- Numero di files presenti nel PdV non corrispondente al numero di files dichiarati nell'IPdV;
- Nomi dei files presenti nel PdV non corrispondenti ai nomi files definiti nell'IPdV;
- Formato dei files differente dai formati accettati.
- Fallita verifica della validità della firma digitale solo se il IPdV è firmato;
- I metadati settati come obbligatori non sono presenti nell'IPdV;
- La firma digitale posta sul singolo documento non è valida.
- La firma del PdV qualora questo sia firmato non è valida.
- In caso di documenti tributari, è stata verificata la presenza di un "buco di numerazione", cioè è stata accertata la non continuità nella progressione numerica dei documenti.

Il sistema di conservazione, successivamente alla sua generazione, prevede la possibilità di inoltro al produttore dei documenti il file del RdV tramite e-mail ordinaria o Pec oppure resa disponibile via SFTP.

L'email di comunicazione viene formattata in modo automatico dal Sistema e in allegato viene inserito il RdV riportante l'esito del versamento.

RdV è un file in formato XML avente la stessa struttura del IPdV riportante per ogni documento ricevuto, l'impronta (HASH) calcolato con algoritomo SHA 256, l'esito della lavorazione, la motivazione dello scarto e il riferimento temporale indicante il momento di generazione del rapporto di versamento con riferimento al Tempo universale coordinato (UTC).

Il produttore può accedere mediante l'interfaccia Web del sistema e verificare gli esiti delle lavorazioni e scaricare il rapporto di versamento.

Torna al Sommario

7.5 Preparazione e gestione del pacchetto di archiviazione

Il pacchetto di archiviazione è composto da un file in formato .xml strutturato secondo lo standard SinCro, contiene le informazioni descrittive della tipologia di documento conservato.

Un pacchetto di archiviazione contiene una sola tipologia documentale, le logiche di tenuta dei documenti, i metadati identificativi di ogni documento, l'hash dei file dei documenti ed il puntamento al file del documento.
I pacchetti di archiviazione sono generati fisicamente in una cartella nominata con il nome univoco del pacchetto.
Il file fisico riporta nel nome i seguenti dati separati dal carattere underscore '_' :

identificativo fiscale dell'azienda conservata

tipologia documentale contenuta

anno di riferimento dei documenti

Identificativo univoco del pacchetto.

Esempio : 00163130248_2014_COMUNICAZIONI_149.xml

La generazione dei pacchetti di archiviazione è svolta mediante il seguente processo :

Generazione delle code di archiviazione

Il responsabile del servizio di conservazione o un suo delegato genera le "code di archiviazione" che sono una rappresentazione logica dei documenti che saranno conservati (andranno a formare i pacchetti di archiviazione).

Generazione dei pacchetti di archiviazione

Il responsabile del servizio di conservazione può selezionare le code per le quali desidera generare i pacchetti di archiviazione. Genera i pacchetti di archiviazione (file .xml) per le code selezionate.

Firma e marca temporale dei pacchetti di archiviazione

Il responsabile firma e pone la marca temporale sui pacchetti di archiviazione generati.

La firma digitale e la marca temporale sono poste, in conformità alla normativa vigente, da Omniadoc mediante sistemi di firma digitale remota e marcatura temporale remota resi disponibili da Certification Authority (CA) e Time Stamping Authority conformi alla normativa vigente.

Il sistema, anche nel caso della generazione dei PdA, registra i log per la tracciatura delle azioni effettuate sui pacchetti di archiviazione.

L'intero sistema di storage di Omniadoc è riversato nel sito di disaster e recovery con allineamento immediato per far fronte e limitare i rischi di perdita dati.

Il sistema Omniadoc prevede il sistematico svolgimento dei backup dello storage dove sono presenti i PdA e i documenti conservati. In caso di corruzione o perdita dei dati si provvede al controllo,recupero delle informazioni e ripristino del PdA attraverso l'utilizzo delle copie di backup.

Specifici casi in cui è necessario adottare metodi di crittografia per proteggere i dati conservati nei PdA sono descritti nell'allegato "Scheda Servizio Cliente - Specificità del contratto", che rappresenta l'accordo sulle condizioni di servizio specifiche tra Ente Conservatore ed Ente Produttore.

Periodicamente vengono effettuati dei controlli sui PdA prodotti tali verifiche vengono inserite come annotazione sul sistema di conservazione.

Torna al Sommario

7.6 Pacchetto di distribuzione

La produzione dei pacchetti di distribuzione è composta da due fasi.

La prima fase si compone della ricezione della richiesta e censimento della stessa.

Il cliente accede tramite le interfacce di condivisione web ai documenti conservati di sua pertinenza e indica tramite apposite funzioni quali sono i documenti di cui richiede la distribuzione.

La richiesta viene registrata nel sistema e messa disposizione del responsabile del servizio di conservazione.

La seconda fase è eseguita dal responsabile del servizio di conservazione o da un suo delegato, che provvedono ad evadere le richieste di duplicazione generando i pacchetti di distribuzione ed inviandoli secondo i canali stabiliti al cliente.

Il pacchetto di distribuzione dove previsto con il Produttore ed indicato nell'allegato "Scheda Servizio Cliente - Specificità del contratto" può essere firmato dal responsabile del servizio di conservazione.

I canali previsti per la trasmissione del pacchetto di distribuzione sono :

- HTTPS. Il cliente può eseguire il download del PdD mediante l'interfaccia Web del sistema di conservazione. Il download del PdD è possibile previa autenticazione nel sistema che tiene traccia dell'utente che si è autenticato e che svolge l'azione di download .
- FTPS. Il PdD è reso disponibile mediante il canale FTPS. L'accesso al canale è possibile solo previa autenticazione mediante credenziali personalizzate per ogni utente. Il sistema FTPS tiene traccia degli accessi eseguiti e scarica le informazioni in file di log memorizzati nello storage di Omniadoc.
- Supporto Fisico. Il PdD viene salvato su un supporto fisico (dischо esterno, Pen Drive Usb) consegnato al cliente il quale firma una nota di avvenuta consegna. Il supporto fisico non presenterà riferimenti esterni che possano permettere l'identificazione dell'ente produttore, dei dati contenuti e della loro tipologia. Il personale incaricato del trasporto dei supporti fisici è scelto sulla base dei requisiti definiti dal resposanbile del servizio di conservazione.

I dati trasmessi o resi disponibili al produttore sono protetti da un appropriato sistema crittografico.

Le attività di richiesta dei PdD sono tracciate nel sistema di conservazione ed identificate tramite un identificativo univoco. Alla richiesta è associato un riferimento temporale.
Le attività di produzione del PdD generano dei file di log archiviati nel sistema di storage di Omniadoc e salvati dalle procedure di gestione dei Log

L'intero sistema di storage di Omniadoc è riversato nel sito di disaster e recovery con allineamento immediato limitando al minimo possibile la possibilità di perdita di dati.

Torna al Sommario

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

L'utente ha accesso al sistema documentale tramite l'interfaccia Web. L'accesso avviene su protocolli sicuri https previa autenticazione con userid e password.

L'operazione di duplicazione, ovvero la copia di uno o più documenti da un supporto di memorizzazione ad un altro, senza alterarne la rappresentazione informatica, è svolta mediante l'interfaccia web, attraverso la quale accedere al documento ed al pacchetto di archiviazione contenente i dati del documento, l'hash, la firma del responsabile del servizio di conservazione e la marca temporale.
Allo stesso tempo le attività di copia sono svolte per la gestione dei processi di backup ai fini della business continuity.
Per tale processo non è previsto l'intervento di un Pubblico Ufficiale.

L'operazione di copia di uno o più documenti che comporti la modifica della rappresentazione informatica può rendersi necessaria in alcuni casi come ad esempio per obsolescenza dei formati.
Questo tipo di operazione si conclude con la creazione di una evidenza informatica contenente le impronte dei documenti, l'apposizione del riferimento temporale e della firma digitale da parte del Responsabile del servizio di Conservazione e nel caso di documenti originali unici, con l'ulteriore apposizione del riferimento temporale e della firma digitale da parte di un Pubblico Ufficiale.
Qualora sia necessario l'intervento di un pubblico ufficiale, questo rilascerà una dichiarazione formale mediante la quale attesta la conformità all'originale della copia prodotta.

Torna al Sommario

7.8 Scarto dei pacchetti di archiviazione

Il responsabile del servizio di conservazione definisce in accordo con il produttore i tempi di conservazione di ogni classe documentale riportandoli nelle specificità di contratto.
Il produttore definisce periodicamente l'elenco dei documenti da scartare, in quanto sono scaduti i termini di conservazione.
Il produttore può decidere se prolungare il tempo di conservazione della classe documentale o procedere all'eliminazione.
I pacchetti di archiviazione gestiti sono omogenei per periodo, pertanto lo scarto riguarda sempre tutti i documenti presenti in un pacchetto di archiviazione. Fisicamente si provvede a cancellare tutti i documenti informatici presenti in un pacchetto di archiviazione e modificare lo stato del pacchetto di archiviazione in "cancellato", aggiornando la data di scarto. Il file del pacchetto di archiviazione è comunque conservato nel sistema e non viene cancellato.
Il produttore può richiedere prima della cancellazione fisica la creazione di un pacchetto di distribuzione dei documenti che saranno cancellati, al fine di avere una copia da conservare su altri sistemi.

Qualora I documenti conservati appartengano ad una Amministrazione pubblica e abbiano comunque carattere o valenza pubblica, fermi restando i principi cogenti della normativa codicistica, si rendono applicabili alcune disposizioni di carattere speciale tra cui quella concernente i beni culturali e ambientali di cui al D.Lgs 10 gennaio 2004, n. 42 (Codice dei beni culturali e ambientali).

Indipendentemente dalla natura giuridica del soggetto titolare dei documenti oggetto di conservazione, particolare attenzione viene prestata alla rilevanza di interesse storico-artistico che gli stessi possono ricoprire. In questi casi,

lo scarto del PdA può essere realizzato solamente previa autorizzazione del Ministero per i beni e le attività culturali, richiesta a cura del Cliente, così come previsto dalla vigente normativa in materia.

Torna al Sommario

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

Il Sistema di Conservazione è in grado di garantire l'interoperabilità con altri sistemi in quanto esso gestisce Pacchetti di archiviazione conformi allo standard UNI 11386:2010 – SInCRO.
In caso di trasferimento dei documenti verso altri sistemi di conservazione i Pacchetti di archiviazione sono resi disponibili mediante download da interfaccia applicativa web oppure mediante download a mezzo SFTP.
Ulteriori modalità di consegna dei documenti al Produttore possono essere concordate fra quest'ultimo e il Responsabile del servizio di Conservazione.

Torna al Sommario

7.10 Piano di cessazione servizio di Conservazione

Il servizio di conservazione può essere cessato per le seguenti motivazioni:

- Scadenza contratto
- Recesso da parte del cliente
- Cessazione attività di conservazione (per scelta di business, cessazione attività, etc.)

In caso di cessazione del servizio di conservazione, qualunque sia la causa o motivazione, l'azienda si impegna a mantenere operativo il servizio per il tempo strettamente necessario al completamento del processo di restituzione dei dati e dei documenti conservati.

L'azienda metterà in atto il seguente processo:

- Comunicazione ai clienti via PEC del proposito di cessazione del servizio, se di propria iniziativa
- Condivisione con i clienti del piano di restituzione dei documenti conservati:
  - Modalità operative e tecniche come descritto al par. 7.9
  - Elenco dei pacchetti di archiviazione
  - Tempistiche di lavorazione
- Evidenza da parte dei clienti dell'avvenuta restituzione delle informazioni
- Cancellazione dei dati conservati secondo i processi di sicurezza descritti nel Piano della Sicurezza e nel SGSI
- Comunicazione al cliente dell'avvenuta cancellazione dei dati, dei documenti e delle credenziali di accesso all'applicazione

Torna al Sommario

8 IL SISTEMA DI CONSERVAZIONE

Il software utilizzato per la gestione del processo di conservazione è GIADACD® sviluppato internamente secondo gli standard qualitativi e di sicurezza previsti all'interno del processo di sviluppo software adottato nel SGSI certificato ISO 27001:2013 (emissione corrente).

Il sistema adottato si avvale delle opportune tecniche per la realizzazione delle funzionalità di Firma Digitale, fornisce supporto per la gestione dei certificati/chiavi dei responsabili di conservazione, operatori ed eventuali pubblici ufficiali che operano all'interno del sistema di conservazione e per il trattamento e la custodia delle informazioni relative alle quantità crittografiche che dovranno essere integrate negli archivi digitali su idonei supporti di memorizzazione.

Il sistema ha come oggetto la realizzazione di un insieme di funzionalità atte a consentire la conservazione documentale digitale e garantire:

- Integrità: il contenuto dei dati non deve subire alterazioni;
- Confidenzialità: solo il personale autorizzato deve essere in grado di accedere ai dati;
- Disponibilità: è garantita la fruizione dei dati nel rispetto degli SLA definiti in sede contrattuale.

Torna al Sommario

8.1 Componenti Logiche e Tecnologiche

GIADACD® è una web application scritta in tecnologia J3EE a tre livelli.

I componenti logici di Giada sono:

- Front End. Applicazione WEB, pubblicata e raggiungibile via Web dagli utenti dell'applicativo. In questa componente risiedono le pagine web che comunicano con l'application server. Implementato su tecnologia Apache Tomcat (o semplicemente Tomcat) è un application server nella forma di contenitore servlet open source sviluppato dalla Apache Software Foundation. Implementa le specifiche JavaServer Pages (JSP) eServlet, fornendo quindi una piattaforma software per l'esecuzione di applicazioni Web sviluppate in linguaggio Java. La sua distribuzione standard include anche le funzionalità di web server tradizionale, che corrispondono al prodotto Apache.
- Back End Server Side. Vi risiedono i programmi Java che compongono GiadaCd, svolgono le operazioni di accesso ai dati e composizione delle pagine che poi saranno presentate all'utente finale tramite il Web Server. Implementato su tecnologia JBoss AS o semplicemente JBoss, è un application server open source che implementa le specifiche Java EE. WildFly è un sistema multipiattaforma, interamente realizzato in Java.
- DataBase Server. Vi risiede il database relazionale che ospita i dati logici degli oggetti archiviati nel sistema Giada. Implementato su DataBase POSTGRES 11
- File Repository. Vi risiedono i dati archiviati in giadaCd, quindi sia le immagini dei documenti che i PDA prodotti. Il protocollo di accesso al File Repository è Swift Stack S3

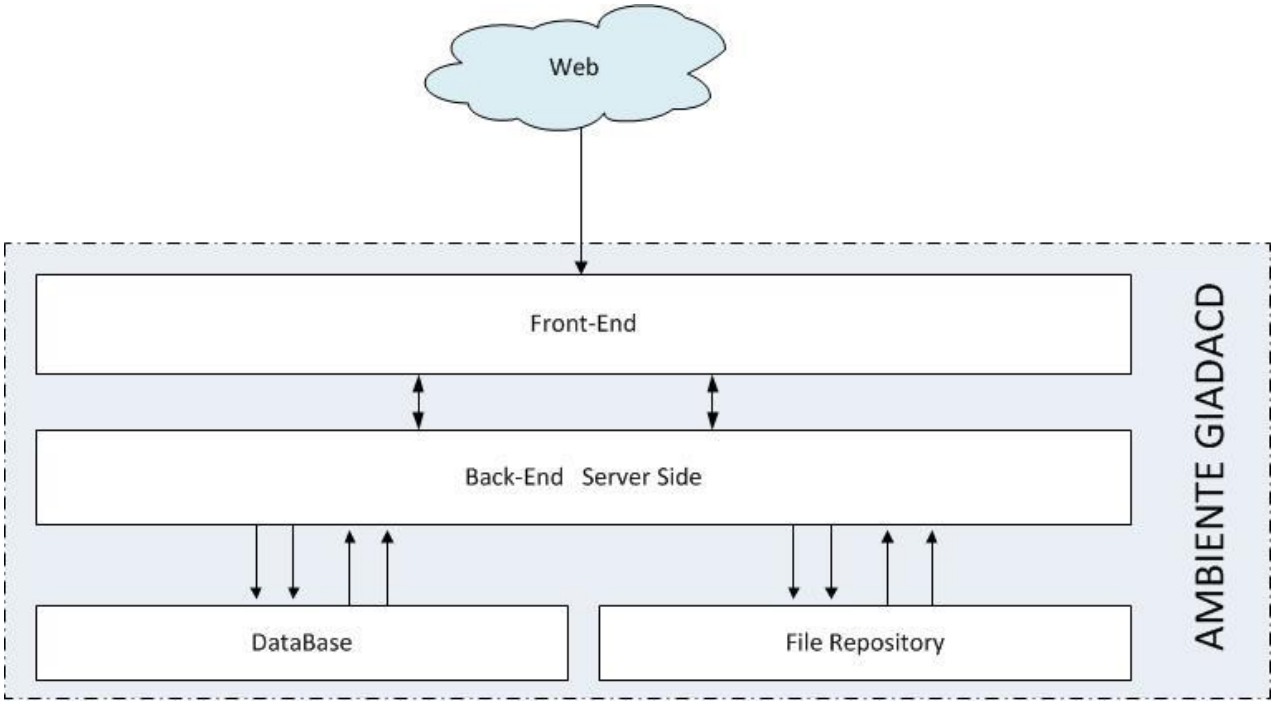


Figura 7. Ambiente Tecnologico

I componenti funzionali dell'applicazione sono :

- Sistema di archiviazione documentale (GiadaCD)
- Sistema batch di trattamento dei dati
- Sistema web di accesso ai dati.

Torna al Sommario

8.1.2 Processi Batch

Il sistema batch di trattamento dati è composto da un insieme di programmi batch (privi di interfaccia grafica) che svolgono i seguenti compiti:

- Caricamento dei documenti nel sistema di conservazione
- Gestione dei pacchetti di versamento
- Generazione dei rapporti di versamento
- Conservazione dei documenti
  - Generazione dei pacchetti di archiviazione
  - Generazione dei pacchetti di distribuzione
  - Generazione del rapporto di generazione dei pacchetti di distribuzione

Torna al Sommario

8.1.3 Sistema web di accesso ai dati

Il sistema interattivo di presentazione dei dati è una applicazione web disponibile sia al responsabile del servizio di conservazione che al cliente. Le funzionalità disponibili per il cliente sono le seguenti:

- Consultazione dei documenti conservati
- Consultazione dei pacchetti di versamento
- Consultazione dei pacchetti di archiviazione
- Richiesta di esibizione di un documento.
- Generazione di una copia del documento conservato
- Consultazione del monitor di controllo dei documenti che evidenzia la presenza di eventuali buchi di numerazione o documenti con indici anomali.

Il responsabile del servizio di conservazione oltre alle funzioni sopra elencate ha a disposizione:

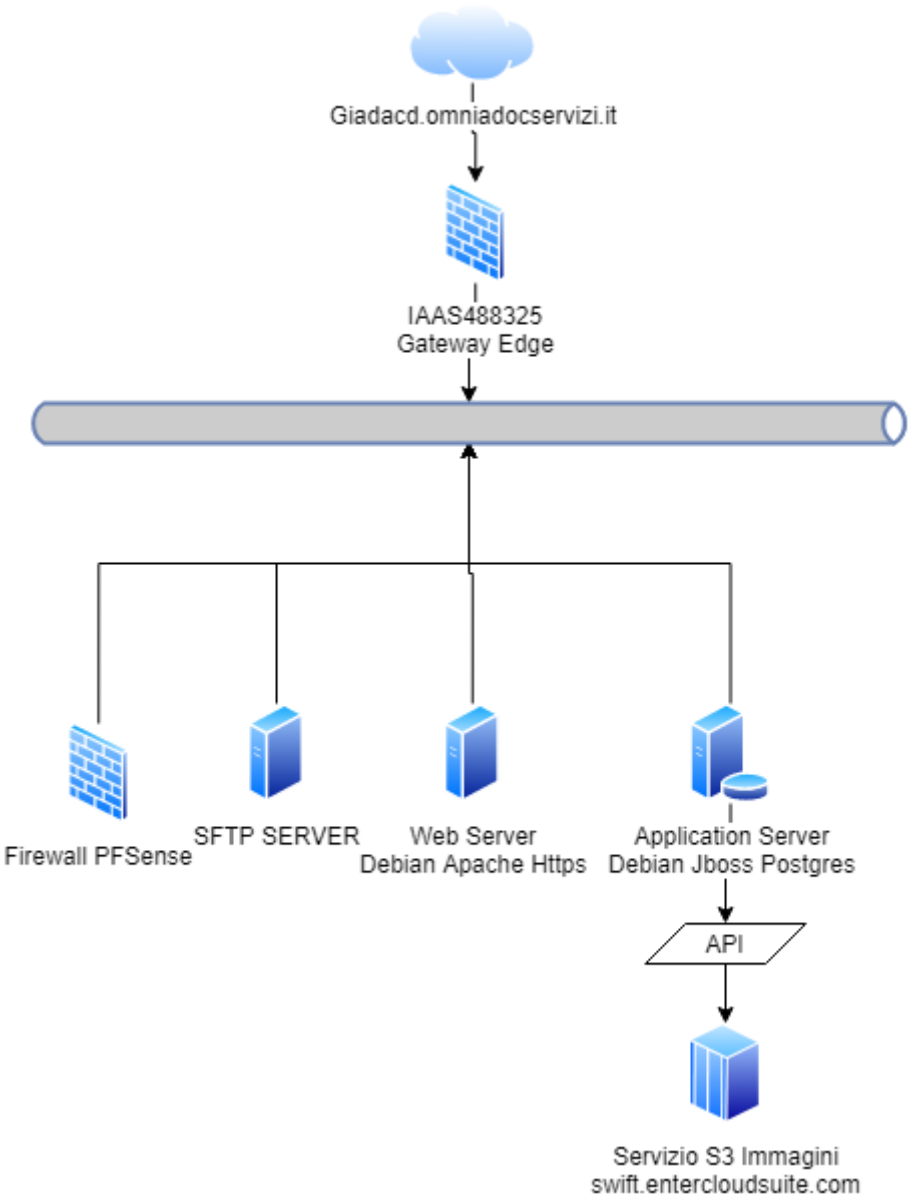
- Funzioni per la firma dei pacchetti di archiviazione
- Funzioni di controllo per la verifica dei buchi di numerazione
- Funzioni di supporto al responsabile del servizio di conservazione per la generazione dei pacchetti di archiviazione
- Accettazione delle richieste di esibizione documenti

Torna al Sommario

8.2 Componenti Fisiche

GIADACD® e i dati relativi ai processi sono installati presso i datacenter di Cloud Italia P.Iva 07543230960.

Il Deploy è stato realizzato su 3 livelli:



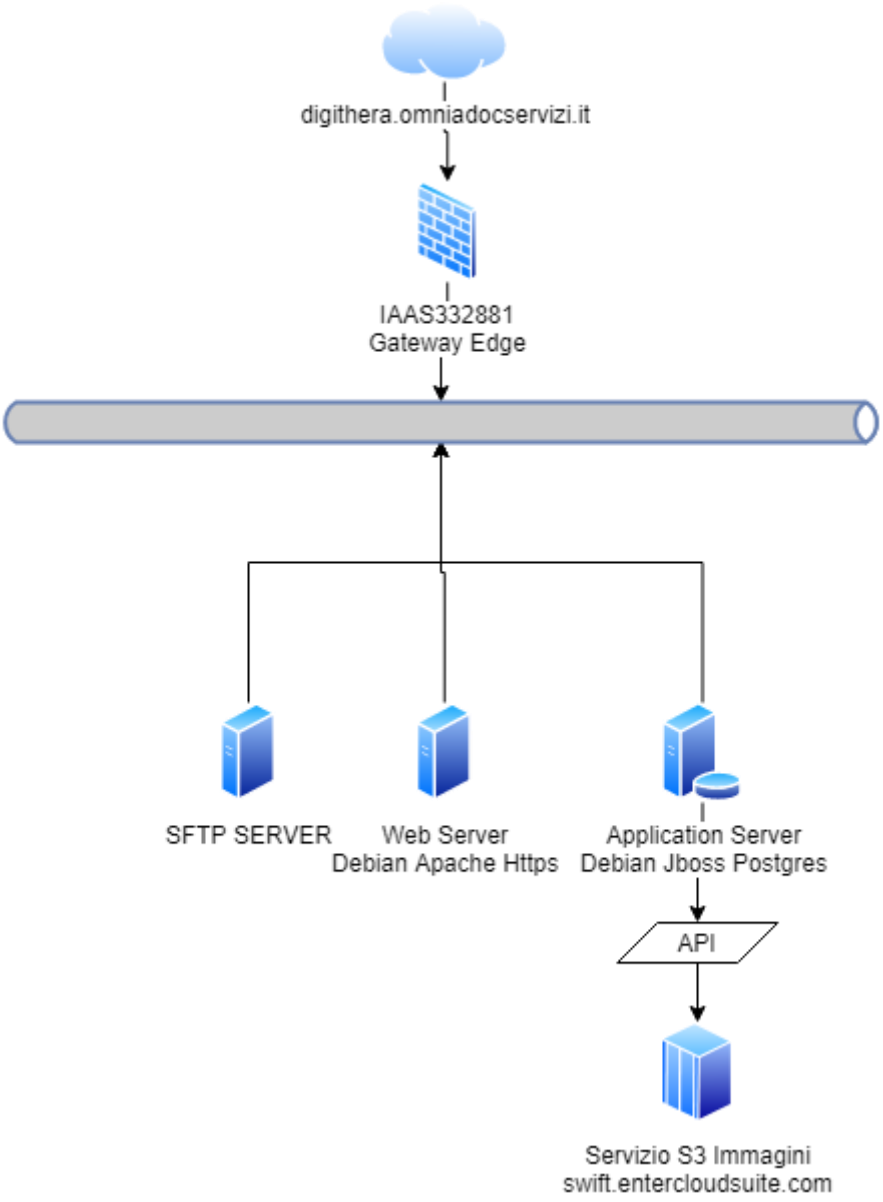


Figura 8 Componenti fisiche

L'accesso ai sistemi avviene unicamente via WEB tramite comunicazione HTTPS. La cifratura dei dati è in essere sia durante le fasi di Login che durante l'accesso ai dati archiviati. I dati sono cifrati tramite l'utilizzo di un certificato SSL.

Il sistema di conservazione è attivo sui datacenter primario e secondario indicati nel paragrafo Infrastruttura Hardware, con allineamento continuo tra i due siti.

In caso di indisponibilità del datacenter primario è possibile attivare il datacenter secondario.
Torna al Sommario

8.3 Procedure di gestione e di evoluzione

Il sistema di Conservazione di Omniadoc è stato implementato con l'obiettivo di garantire i punti elencati di seguito

• Che il sistema sia conforme alla normativa vigente e alle continue evoluzioni tecnologiche in modo da garantire prestazioni in linea alle attese ed al contesto tecnologico.

• Garantire la riservatezza, l'integrità, la leggibilità, la reperibilità e la disponibilità dei documenti e dei dati gestiti dal sistema;

• Gestire in modo consono ed adeguato i livelli di rischio della continuità operativa

• monitorare e gestire la sicurezza;

La gestione e la conduzione del Sistema seguono gli standard di qualità e di sicurezza internazionali formalizzati nelle ISO 9001 ed ISO 27001:2013 che Omniadoc ha adottato.

I requisiti di sicurezza (sicurezza fisica, sicurezza logica e sicurezza organizzativa) adottati nella conduzione e manutenzione del sistema di conservazione, nelle politiche di gestione dell'incident management e della continuità operativa del servizio di conservazione sono specificati e riportati nel piano della sicurezza.

I clienti di Omniadoc hanno a disposizione un servizio di assistenza contattabile mediante molteplici canali: email, telefono che gestisce e supporta il cliente nella gestione e consultazione del sistema di conservazione.

Qualora sia evidenziata una segnalazione non gestibile il servizio di assistenza si interfaccia con le risorse aziendali identificate per la gestione delle segnalazioni di II livello, tipicamente possono essere il capoprogetto assegnato al cliente o direttamente il team di sviluppo.

Torna al Sommario

8.3.2 Change Management

Le evoluzione del Sistema di Conservazione possono scaturire da richieste di natura normativa, di mercato, di sicurezza o di performance. Al manifestarsi di uno o più eventi sopra descritti che possa avere impatto sul sistema di conservazione, il responsabile del sistema redige un documento di proposta di intervento per l'adeguamento delle applicazioni ai nuovi requisiti; il progetto viene condiviso con la direzione e con il responsabile dello sviluppo per essere approvato e attivato.
Ogni evoluzione è tracciata mediante appositi documenti che descrivono il processo produttivo. Di seguito se ne riporta l'elenco

- ***studio di fattibilità*** si descrivono le funzionalità da gestire (modifica o creazione ex novo), le eventuali ricadute sulle funzionalità già esistenti e si valuta il rischio di impatto sulla sicurezza dei dati e sull'integrità. Il documento deve essere approvato dal responsabile del servizio di conservazione, dal responsabile dei sistemi informativi, dal responsabile della sicurezza, dal responsabile degli sviluppi e dal responsabile archivistico.

- ***Analisi funzionale*** si disegna il processo da realizzare, le funzioni da implementare le interfacce utente e la modalità di esposizione delle informazioni e di aggiornamento della base dati. Inoltre si compila l'elenco dei test da svolgere al fine di verificare che le funzioni eseguano quanto atteso e la non regressione delle altre funzioni già disponibili.

- **Analisi Tecnica** si descrivono nel dettaglio le componenti tecniche per la realizzazione delle funzioni riportate nell'analisi funzionale

- **Report Unit Test** Si descrivono l'esito dei test eseguiti sulle nuove funzionalità.

- **System Test** Si descrivono i test svolti dopo il deploy della nuove versione per verificare il corretto funzionamento e la non regressione delle funzioni precedentemente disponibili.

A seguito dello svolgimento dei System test, il responsabile del sistema di conservazione autorizza il rilascio in produzione del pacchetto di change.

Torna al Sommario

8.3.3 Gestione e conservazione dei Log

I log generati dal sistema possono essere di due tipi : log descrittivi , log applicativi.

I log descrittivi sono generalmente il risultato di procedure di gestione dati che tracciano le operazioni svolte il riferimento temporale dell'operazione e i relativi esiti. Sono tenuti tipicamente su file di dati distinti per periodo di produzione.

I log applicativi sono generati dalle applicazioni che richiedono l'interazione con un operatore, questo può essere sia una figura del produttore dei documenti che del conservatore. Le operazioni svolte dall'operatore sono salvate nelle basi dati e tracciano il riferimento temporale dell'operazione svolta, l'operatore che la effettuata e la tipologia.

In accordo con il produttore si definisce il periodo di conservazione dei log generati.

Torna al Sommario

9 MONITORAGGIO E CONTROLLI

Il sistema è sottoposto ad un'attività di monitoraggio costante al fine di garantire la piena funzionalità di ogni componente del sistema.

9.1 Procedure di monitoraggio

Le attività di monitoraggio possono essere distinte in monitoraggio applicativo e monitoraggio sistemistico.

L'utilizzo quotidiano da parte dell'area di produzione Omniadoc per lo svolgimento delle sue funzioni e dai produttori dei documenti per la consultazione dei documenti versati è la prima forma di monitoraggio svolto sul sistema.

L'eventuale non disponibilità o eventuali errori di funzionamento sono subito evidenziati e generano l'apertura di una segnalazione di incidente o di non conformità come previsto dalle procedure ISO 27001:2013

Il monitoraggio sistemistico consiste nella verifica della disponibilità e del corretto funzionamento dell'infrastruttura Hardware. Un eventuale malfunzionamento solitamente genera una non disponibilità dell'applicazione che viene rilevata dal monitoraggio applicativo.

Il monitoraggio sistemistico è volto ad evidenziare le situazioni che potrebbero generare malfunzionamenti ed evitare che avvengano. Per esempio verifica che i componenti di backup siano funzionanti (verifica degli alimentatori secondari delle schede di rete secondarie)

Torna al Sommario

9.1.2 Verifica dell'integrità degli archivi

Il Sistema di Conservazione prevede da parte degli operatori preposti l'esecuzione di un processo di verifica con cadenza annuale che assicuri l'integrità, e leggibilità degli oggetti conservati.

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 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.
Leggibilità	verifica leggibilità dei documenti affidata a degli operatori preposti che effettuano con cadenza periodica un controllo visivo su documenti a campione.

Le verifiche di integrità degli archivi sono tracciate in appositi Log riportanti il riferimento temporale del momento in cui è stato svolto il controllo e gli esiti. L'esecuzione dei controlli genera un verbale firmato digitalmente dal Responsabile del servizio di Conservazione e conservato nel sistema di conservazione.
Torna al Sommario

9.2 Soluzioni adottate in caso di anomalie

La procedura di conservazione digitale in atto presenta dei rischi che per loro natura non è possibile evitare.
I rischi di malfunzionamento sono riconducibili ai seguenti fattori:

- Malfunzionamento software
- Malfunzionamento Hardware
- Malfunzionamento del dispositivo di firma
- Indisponibilità del sito della certification authority

Torna al Sommario

9.2.2 MALFUNZIONAMENTO SOFTWARE.

Il software utilizzato per la procedura di conservazione è sviluppato e manutenuto secondo le procedure definite nel SGSI certificato 27001:2013 precedentemente illustrate, allo scopo di gestire le casistiche al momento presenti in azienda ed isolando i casi non gestiti. Per questo motivo si ritiene siano state attivate le misure di mitigazione del rischio di malfunzionamento software, giudicato basso.
Allo stesso modo sono preventivamente verificati possibili casi di incompatibilità tra il software GIADACD e altri software di base o di servizio (es. antivirus).
In ogni caso il software è presente in azienda in due istanze su due diversi computer in modo da avere un'istanza di backup da utilizzare in caso di malfunzionamento. Il responsabile del servizio di conservazione o i suoi delegati al termine di qualsiasi operazione svolta sul software GIADACD provvedono ad effettuare una copia dei dati ed aggiornare la situazione sull'istanza di backup tenendo di fatto le istanze allineate e quindi in qualsiasi momento interscambiabili.
Nel caso, per quanto improbabile, si presenti una casistica non prevista dal software GIADACD, l'azienda ha tra i suoi dipendenti i tecnici sviluppatori e i sistemisti in grado di affrontare l'eventuale malfunzionamento e porvi correzione, applicando le procedure già citate.

Torna al Sommario

9.2.3 MALFUNZIONAMENTO HARDWARE.

Il software GIADACD è presente su due hardware in due istanze tenute costantemente aggiornate, in caso di malfunzionamento hardware che impedisca l'utilizzo dell'istanza principale si deve utilizzare l'istanza di backup.

Torna al Sommario

9.2.4 MALFUNZIONAMENTO DEL DISPOSITIVO DI FIRMA.

Il responsabile del servizio di conservazione di Omniadoc, nel caso in cui si renda conto che la non disponibilità del servizi di firma avvenga o sia prevista in tempi eccessivi che possano comportare la scadenza dei limiti per rendere sostitutivi i documenti, provvede a produrre su carta i documenti in scadenza e ad annotare sul registro degli eventi del presente manuale l'accadimento, segnalando i singoli documenti che saranno resi sostitutivi oltre il limite di tempo stabilito dalla legge.

Torna al Sommario

9.2.5 INDISPONIBILITÀ DEL SITO DELLA CERTIFICATION AUTHORITY

In caso di indisponibilità della certification authority o della connettività per raggiungere il sito, nel caso vi siano documenti in scadenza per la conservazione, il responsabile del servizio di conservazione provvede ad annotare l'accadimento sul registro degli eventi del presente manuale e indica i singoli documenti o il range, tramite l'indicazione del primo e ultimo numero progressivo interessato in caso di documenti rilevanti ai fini tributari, che saranno conservati oltre il termine stabilito dalla legge.

A partire da dicembre 2012 vengono utilizzati i servizi di firma digitale e marcatura temporale forniti da Namirial S.p.a., inscritta nell'Elenco Pubblico AGID dal 03/11/2010.

Torna al Sommario

9.3 Apposizione firma digitale e marca temporale

L'apposizione delle firme digitali e delle marche temporali è svolta mediante l'utilizzo della tecnologia di firma digitale remota di Namirial spa.
Il certificato di firma digitale è memorizzato presso la certification Authority, svincolando Omniadoc ed il responsabile del servizio di conservazione dalla tenuta di un qualsiasi supporto fisico.
L'apposizione di una firma o di una marca temporale è svolta mediante l'applicazione GiadaCd che invia una apposita richiesta ai Web Services esposti da Namirial, i quali rispondo con un codice di sicurezza inviato via SMS al cellulare del responsabile del servizio di conservazione, il quale per concludere l'operazione dovrà digitare il codice di ricevuta in una apposita maschera di conferma.

Torna al Sommario

10 Infrastruttura Hardware

INFRASTRUTTURA

La Rete, basata su un'infrastruttura a banda larga di ultima generazione, flessibile, scalabile, a copertura nazionale, costituisce il patrimonio di Clouditalia

La Rete proprietaria in fibra ottica di circa 14000 km garantisce performance e sicurezza delle trasmissioni ed è completata al Sud da ulteriori 2800 km realizzati tramite sistemi a 2,5 Gbit/s attrezzati su Lambda in affitto.

Rete in fibra ottica terrestre: 7800 Km
Rete in fibra ottica aerea: 1500 Km
Rete in ponte radio: 2400 Km
Rete metropolitana in fibra ottica: 2000 Km

Clouditalia rende disponibili due Data Center autonomi, ma tra loro collegati attraverso una linea dedicata proprietaria. L'attuale configurazione prevede la seguente collocazione:

Sito Primario	via Savona, 125 – 20144 Milano
Sito Secondario (backup e Disaster Recovery	Via Cornelia 498 – 00166 Roma

Sono di nuovissima concezione e sfruttano le migliori tecnologie high-density di ultima generazione presenti sul mercato: Cisco, NetApp, VMware, Tintri e EMC2.
La soluzione messa in campo da Clouditalia è rappresentata da un mix di elementi hardware, software e di infrastruttura di rete strettamente correlati tra loro.

Torna al Sommario

10.1 Servizi tecnici ed impianti

Clouditalia ha implementato due datacenter gemelli, di ultima generazione. Essi si trovano in siti geograficamente distinti, come descritto nel paragrarafo precedente.
Ogni datacenter concentra su uno spazio esiguo, grandi risorse di calcolo, memoria, di storage e di apparati di rete.

Equipaggiamento per ogni singolo polo – Tre layer hardware
La parte di computing è realizzata per mezzo di lame Cisco UCS.
I Dischi di storage si appoggiano su sistemi NetApp
Per la parte network, vengono impiegati apparati Cisco Nexus

Computing
Per entrambi i siti sono state previste e installate Blade Cisco UCS B200 M3, distribuite. Ogni singola Blade si compone di due processori Intel E5 2680 da 2,7 GHz con 8 core, 256 GB di RAM, Virtual Interface Card 1240, I/O Module 2204 e Fabric Interconnect 6296.

Storage
L'architettura di storage è affidata a sistemi:
- NetApp FAS 6240A;
- Tintri T880;
- Synology RS3614xs+.

Ogni sistema NetApp FAS 6240A si avvale di due Controller in configurazione HA; ciascun controller è dotato di 2TB di cache in lettura (la cache, deduplication aware, a bordo di schede dotate di memoria flash montate sulla motherboard delle teste).
Il FAS 6240A si compone di:
- Shelves da dischi SAS;
- Shelves da dischi SATA;
- 8 porte 10GBE (fibra multimodo) on board con protocollo di storage: NFS;
- porte 100Mb (UTP) per il management;
- sistema di replica asincrona SnapMirror;
- gestione totalmente integrata con VMware mediante Virtual Storage Console.

Tintri T880 è un datastore ad alte prestazioni, il più performante della sua serie. E' un datastore ibrido dedicato specificamente alle virtual machine (si chiama appunto Vmstore). Le sue elevate prestazioni sono possibili grazie ad un software di gestione evoluto ed una parte di dischi SSD.
Clouditalia impiega 3 T880 nei suoi due Data Center.

Synology RS3614xs+ è la soluzione Storage, che si poggia su dischi SATA e collegamenti in fibra 10GB/s, impiegata per le attività di supporto, a basse prestazioni, come l'archiviazione di backup.

Networking
Da un punto di vista del networking ogni singolo polo dispone di Nexus 7010 così equipaggiati:
- Doppia Supervisor 1;
- 5x fabric N7K-C7010-FAB-2;
- Tre alimentatori 6.0 KW AC;
- 2x linecard 8 porte 10G (N7K-M108X2-12L);

- 1x linecard 32 porte SFP (N7K-F132XP-15);
- Licenze per L2, L3, OTV, VDC, DCNM, MPLS;

I Nexus 7000 svolgono i ruoli di Access/Aggregation/Core per il singolo polo e garantiscono la visibilità layer 2 Extension tra i due siti (Data Center Interconnection-DCI).
Connessione inter DC – Collegamenti DWDM
Le tratte tra tra i due siti sono realizzate tramite connessioni 10G DWDM (Siemens); le singole tratte sono sono protette a livello DWDM ma il down di una di esse viene propagato verso gli apparati di networking direttamente connessi Nexus 7k (Remote Laser Shutdown).
Le lambda 10G formano una magliatura tra i due Nexus 7k in oguno dei due siti in modo che ogni Nexus veda gli altri due dell'altro sito con una via corta e con una via lunga.
I collegamenti 10G tra i Nexus e DWDM, 2 per ogni Nexus, sono in fibra ottica monomodale.
La banda complessiva tra i due Data Center è pari a 2x10G; il protocollo di routing sceglie sempre la via migliore (tipicamente la più corta) e la via più lunga sarà usata solo in caso di fault.
Tre layer software
Al fine di ridistribuire le risorse relative all'hardware appena descritto, secondo le logiche proprie della virtualizzazione, i Data Center si compongono di tre livelli software.
Il primo livello è quello in cui le risorse hardware vengono "astratte" e quindi rese ridistribuibili. Questa attività è demandata all'hypervisor e quello scelto da CloudItalia è VMware vSphere.
I vari hypervisor vengono quindi aggregati in cluster e VMware vCenter è la componente che consente di gestire, amministrare, configurare più hypervisor contemporaneamente, con una granularità che arriva sino alla configurazione delle singole virtual machine che vi si attestano.
Nell'ultimo livello le risorse vengono esportate e organizzate in servizio: VMWare vCloud Director è il layer software che si sovrappone al vCenter e che rende possibile l'erogazione di servizi di virtualizzazione ai clienti di CloudItalia. Il servizio erogato è il c.d. IaaS (Infrastructure as a Service) che consente al cliente di creare, amministrare, modificare in autonomia e sicurezza, i propri server virtuali e apparati di rete; cioè: la propria server farm virtuale.
Torna al Sommario

10.2 Impianto di anti intrusione e verifica accessi fisici

Roma: L'accesso e la sicurezza del Data Center sono gestite nel modo seguente:

- POP di Roma di via Cornelia 498: accesso garantito attraverso un servizio di guardiania della proprietà Fezia Group S.r.l., presso cui il sito è ubicato, dove sono presenti le seguenti regole di accesso/sicurezza:
  - Lista di nominativi che possono accedere al sito tecnico;
  - se nominativo non presente, controllo ed identificazione della persona tramite chiamata al NOC Sielte che lavora per Clouditalia che valida la richiesta di accesso;
  - accesso tramite bussola antirapina con apertura biometrica (impronta digitale);
  - accesso ai locali tecnici attraverso Smart card abilitata solo agli utenti autorizzati;
  - telecamere H24 controllate dal NOC Sielte che lavora per Clouditalia.

Milano: L'accesso e la sicurezza del Data Center sono gestite nel modo seguente:
- Acceso richiesto dal NOC attraverso la compilazione di apposito modulo
- Area dedicata con accesso ai rack tramite smart card e codice per sbloccare la caged area
- Intera area videosorvegliata

Torna al Sommario

10.3 Impianto antincendio

Sia nel sito primario che nel sito secondario sono presenti due impianti di rilevazione incendi spegnimento a gas inerte.

Gli impianti sono manutenuti regolarmente ogni 6 mesi

Torna al Sommario

10.4 Ridondanza geografica

I parametri quantitativi più indicativi di un sistema di Business Continuity sono:
- il tempo necessario al pieno ripristino dell'operatività di un sistema, in caso di "Recovery" a seguito di "Disaster" (RTO);
- il tempo necessario a mettere in sicurezza un dato residente nell'ambiente di produzione, nel sito di Recovery (RPO).

Al fine di garantire continutà operativa, Clouditalia si avvale di Zert0. Esso è un'infrastruttura realizzata per garantire la Business Continuity attraverso un sistema di Disaster Recovery ad alte prestazioni grazie a:

- RTO (Recovery Time Objective) dell'ordine di minuti;
- RPO (Recovery Point Objective) dell'ordine di secondi.

Zert0 è una piattaforma che è nata per operare in multi-tenancy e che si integra perfettamente con VMware vCloud Director e vCenter.

La rapidità di Zert0 è dovuta al fatto che esso opera le sue repliche a livello di singola virtual machine, e non sugli storage, garantendo tuttavia un impatto nullo sulle virtual machine in produzione.

La piattaforma in questione è impiegata per la replica delle virtual machine ad uso interno, cioè le vm che eseguono gli applicativi esecutivi e documentali; ma anche per quelle vm che espongono i servizi ai clienti. Inoltre, Clouditalia espone questo servizio ai clienti sia quei servizi IaaS erogati all'interno dei Data Center di Clouditalia, con dislocazione geografica differenziata, che per quelle infrastrutture ibride, cioè anche esterne al perimetro infrastrutturale di Clouditalia.

Torna al Sommario

10.5 Politica di gestione, dismissione e smaltimento dei supporti

Gli storage di Clouditalia sono realizzati su infrastrutture ad alto grado di resilienza. Pertanto le informazioni sono ridistribuite nei dischi secondo le logiche architetturali RAID 5 o RAID 6.
In caso di rimozione di un disco guasto, questo viene sostituito dal vendor. I dati al suo interno non sono comunque leggibili perché i dischi in quella configurazione non permettono una lettura autonoma dei dati ivi contenuti; e perché il disco è, appunto, guasto.
Quando un cliente chiude un contratto, è autonomo nella cancellazione dei dati prensenti nel servizio IaaS, qualora lo desideri.
In ogni caso, a meno di esplicite richieste contrattuali, al momento della soluzione di un rapporto contrattuale, i dati all'interno del servizio stesso, vengono resi non leggibili attraverso la loro cancellazione.

Torna al Sommario

10.6 Accreditamento e affidamento all'esterno di attività a supporto del processo di conservazione

- L'infrastruttura di Data Center virtuale erogata all'interno di un servizio IaaS (Infrastructure as a Service) multitenant, acquisita mediante contratto, è nella piena disponibilità di Omniadoc che l'amministra con proprio personale e ne governa l'utilizzo secondo le proprie procedure e misure di sicurezza.
- Omniadoc, inoltre, con il servizio "IaaS Adaptive" ha pieno ed esclusivo accesso e controllo ai propri sistemi virtuali e al proprio sistema IaaS volti all'erogazione dei servizi di conservazione digitale laddove CLOUDITALIA offre il servizio di manutenzione ordinaria sempre rispettando procedure e misure concordate con Omniadoc, accettando i controlli che quest'ultima ritenesse di operare (*).

- Conseguentemente l'attività del fornitore consiste nella fornitura di un'infrastruttura di data center virtuale ospitata all'interno di una infrattruttura IaaS multitenant caratterizzata da elevati livelli di sicurezza, gestita con processi certificati ISO9001 e ISO27001 per quanto attiene l'accesso e trattamento dei dati e le attività di manutenzione: Omniadoc mantiene un governo ed un controllo pieno ed esclusive nel caso di servizio "IaaS adaptive" che prevede :
Allocazione di risorse garantite ad uso esclusivo, con possibilità di configurarle e suddiverle in vApp e virtual machine e, ove necessari più servizi IaaS può suddividere in "organizzazioni" in modo da garantire sia le perfomance computazionali, di storage necessarie e di network, sia la totale indipendenza e disaccoppiamento rispetto ad altre organizzazioni dello stesso cliente e /o ad altri clienti presenti, sia dal punto di vista funzionale che dal punto di vista della sicurezza e privacy).

Torna al Sommario