MANUALE DELLA CONSERVAZIONE

SISTEMA DI GESTIONE PER LA QUALITÀ - DQ_07.03

Sommario

Emissione del documento 4
Registro delle versioni 5
1. Scopo e ambito del documento 6
1.1. Trattamento dei dati personali 6
2. Terminologia 8
3. Normativa e standard di riferimento 13
3.1. Normativa di Riferimento 13
3.2. Standard di Riferimento 15
4. Ruoli e responsabilità 16
5. Struttura organizzativa per il servizio di conservazione 21
5.1. Organigramma 21
5.2. Strutture organizzative 21
6. Oggetti sottoposti a conservazione 24
6.1 Metadati 24
6.1.1 Metadati minimi del documento informatico 25
6.1.2 Metadati minimi del Registro di protocollo giornaliero 26
6.1.3 Metadati minimi del documento informatico aventi rilevanza tributaria 29
6.1.4 Metadati minimi del fascicolo informatico o dell'aggregazione documentale informatica 33
6.2 Formati 35
6.3 Struttura dati del Pacchetto di versamento 37
6.4 Struttura dati del Pacchetto di archiviazione 42
6.5 Struttura dati del Pacchetto di distribuzione 46
7. Il processo di erogazione del servizio di conservazione 48
7.1 Il processo di conservazione 48
7.2 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico 49
7.3 Verifiche effettuate sui Pacchetti di versamento e sugli oggetti in esso contenuti 50
7.4 Accettazione dei Pacchetti di versamento e generazione del Rapporto di versamento di presa in carico 51
7.5 Rifiuto dei Pacchetti di versamento e modalità di comunicazione delle anomalie 52
7.6 Preparazione e gestione dei Pacchetti di archiviazione 52
7.7 Preparazione e gestione dei Pacchetti di distribuzione ai fini dell'esibizione 53
7.8 Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento 54
7.9 Scarto dei Pacchetti di archiviazione 54
7.10 Predisposizione di misure per l'interoperabilità e la trasferibilità ad altri conservatori 55
7.11 Chiusura del contratto 55
8. Procedure di gestione e di evoluzione 57
8.1 Misure di sicurezza logica 57
8.1.1 Gestione utenze 57
8.1.2 Gestione sistemi di protezione 58
8.1.3 Gestione degli incidenti di sicurezza 59
8.1.4 Gestione dei backup e Disaster Recovery 59
8.1.5 Gestione dei supporti di memorizzazione 60
8.2 Procedure di evoluzione e Change management 61
9. Monitoraggio e controlli 62
9.1 Audit interni e Verifica dell'integrità degli archivi 62
9.2 Gestione delle anomalie 64
9.3 Reportistica di servizio 65
10. La server farm di Unimatica 67
10.1 UniStorage - Il sistema per la conservazione 69
Appendice A 71

Indice delle figure

Figura 1 - Nodo Flusso 38
Figura 2 - Esempio nodo di tipo chiave 38
Figura 3 - Nodo documento 39
Figura 4 - Struttura volumi 47
Figura 5 Modello OAIS 48
Figura 6 - Schema funzionale 64
Figura 7 - Architettura di conservazione 68

Emissione del documento

Redatto da:	Roberta Rosatone (nome, cognome, qualifica)	Data	14/01/2015
Verificato da:	Andrea Anghinolfi (nome, cognome, qualifica)	Data	19/01/2015
Approvato da:	Silvano Ghedini (nome, cognome, qualifica)	Data	17/02/2015

Registro delle versioni

Revisione	Data	Motivo Revisione	Redatto da	Approvato da
1.0	03/10/2009	Emissione	Andrea Anghinolfi	Silvano Ghedini
2.0	12/02/2010	Aggiornamento funzionalità	Andrea Anghinolfi	Silvano Ghedini
3.0	20/06/2010	Aggiornamento funzionalità	Andrea Anghinolfi	Silvano Ghedini
4.0	28/09/2010	Aggiornamento funzionalità	Andrea Anghinolfi	Silvano Ghedini
5.0	15/10/2010	Aggiornamento funzionalità	Andrea Anghinolfi	Silvano Ghedini
6.0	10/02/2011	Modifica gestione anomalie – Ampliamento funzionalità Unistorage	Andrea Anghinolfi	Silvano Ghedini
7.0	20/05/2011	Aggiornamento composizione societaria Unimatica	Andrea Anghinolfi	Silvano Ghedini
8.0	30/11/2012	Aggiornamento Data Center	Andrea Anghinolfi	Silvano Ghedini
8.1	11/12/2012	Personalizzazioni	Andrea Anghinolfi	Silvano Ghedini
8.2	20/06/2013	Aggiornamento compiti e responsabilità della conservazione	Sabina Falcinelli	Andrea Anghinolfi
8.3	04/07/2013	Aggiornamento normative	Sabina Falcinelli	Andrea Anghinolfi
8.4	05/02/2014	Aggiornamento normative	Sabina Falcinelli	Andrea Anghinolfi
8.5	11/02/2014	Aggiornamento Data Center	Sabina Falcinelli	Andrea Anghinolfi
8.6	05/03/2014	Adeguamento normative	Sabina Falcinelli	Andrea Anghinolfi
8.7	17/02/2015	Adeguamento DPCM 03/12/2013	Roberta Rosatone	Silvano Ghedini
8.8	15/10/2015	Passaggio alla ISO 27001:2013 – Aggiornamento ruoli	Roberta Rosatone	Silvano Ghedini
8.9	20/01/2016	Adeguamento Schema Manuale della conservazione AgID	Roberta Rosatone	Silvano Ghedini
9.0	11/04/2017	Modifica ruolo Responsabile della Funzione Archivistica	Roberta Rosatone	Silvano Ghedini
9.1	14/06/2017	Aggiornamento definizioni per termine “Produttore”	Roberta Rosatone	Silvano Ghedini

1. Scopo e ambito del documento

Il presente documento costituisce il Manuale della conservazione fornito da UNIMATICA S.p.A. allo scopo di illustrare la struttura del sistema di conservazione descrivendo analiticamente gli oggetti sottoposti a conservazione, il processo di conservazione e le componenti logiche, tecnologiche e fisiche relative al suo funzionamento. Delinea, inoltre, i soggetti che sono coinvolti nelle attività e nei processi di conservazione i quali hanno la responsabilità del sistema.

Il Manuale della conservazione unitamente alla Scheda Cliente predisposta da UNIMATICA S.p.A. al fine di personalizzare il rapporto contrattuale con il Cliente Soggetto produttore (da ora in poi Soggetto produttore) costituiscono parte integrante del contratto di fornitura del servizio e garantiscono ai propri clienti la disponibilità nel tempo di documenti integri, autentici, legalmente validi e facilmente consultabili.

Ogni Soggetto produttore avrà accesso diretto al Manuale della conservazione, disponibile in formato PDF/A, dal portale messo a disposizione da UNIMATICA S.p.A., nell'apposita sezione di Help.

Torna al sommario

1.1. Trattamento dei dati personali

Ai sensi e per gli effetti dell'articolo 29 del D. Lgs. 30 giugno 2003 n. 196, relativamente e limitatamente ai trattamenti riguardanti la conservazione degli oggetti digitali affidati a UNIMATICA S.p.A., a partire dalla data di sottoscrizione del contratto, il Soggetto produttore affida a UNIMATICA S.p.A. i seguenti compiti e impartisce le seguenti istruzioni per il trattamento dei dati cui UNIMATICA S.p.A. deve attenersi:

1. Il trattamento dei dati in questione sarà da UNIMATICA S.p.A. effettuato esclusivamente per lo svolgimento del servizio di che trattasi, in modo lecito e secondo correttezza, attenendosi alle prescrizioni della normativa sulla protezione dei dati personali nonché alle previsioni della presente delega o successivamente concordate tra le parti; è fatto esplicito divieto di diffondere o comunicare i dati in questione a soggetti che siano estranei all'esecuzione del trattamento.
2. UNIMATICA S.p.A. in particolare dovrà:
   a) effettuare tutte le operazioni in termini di mansioni, definendo regole e modelli di comportamento che assicurino la riservatezza e il rispetto del divieto di comunicazione e diffusione dei dati ai quali si ha accesso;
   b) incaricare per iscritto i soggetti che abbiano le caratteristiche di Responsabili di Sistema e di Amministratori di Sistema, tenerne l'elenco aggiornato a disposizione del Soggetto produttore e fornirne eventualmente copia a semplice richiesta dello stesso;
   c) comunicare prontamente al Soggetto produttore i dati relativi a Società terze cui eventualmente si intendano affidare, in tutto o in parte, le attività in premessa, a seguito di accordi di subappalto e previa autorizzazione del Soggetto produttore stesso, affinché questi provveda alla conseguente Nomina a Responsabile del trattamento dati personali anche nei confronti delle Società subappaltanti;
   d) adottare, se del caso, idonee misure di sicurezza in aggiunta a quelle già previste, in modo da ridurre al minimo i rischi di distruzione e perdita, anche accidentale dei dati/documenti

stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

e) informare immediatamente il Soggetto produttore di qualsiasi richiesta o comunicazione da parte dell'Autorità Garante e/o Giudiziaria, per concordare congiuntamente l'evasione delle stesse;
f) collaborare con il Soggetto produttore per l'attuazione delle prescrizioni eventualmente impartite dal Garante;
g) comunicare al Soggetto produttore qualsiasi accadimento che possa compromettere il corretto trattamento dei dati personali.

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

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

Torna al sommario

2. Terminologia

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.
AE	Agenzia dell'Entrate.
AES	Advanced Encryption Standard.
Affidabilità	Caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico.
AgID	Agenzia per l'Italia Digitale.
AIPA	Autorità per l'Informatica nella Pubblica Amministrazione.
AM	Application Management
ANORC	Associazione Nazionale per Operatori e Responsabili per la Conservazione digitale.
AOO	Area Organizzativa Omogenea.
Apertura (formato)	Conforme a specifiche pubbliche, cioè disponibili a chiunque abbia interesse ad utilizzare quel formato.
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 dall'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.
ASP	Application Service Provider.
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.
BGP	Border Gateway Protocol.
CA	Certification Authority.
CAD	Codice dell'Amministrazione Digitale.
CD	Compact Disk.
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione.
Comunità di riferimento	Comunità di riferimento: il sottoinsieme degli utenti in grado di comprendere autonomamente l'informazione archiviata nella forma in cui è conservata e resa disponibile dall'OAIS.
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 della conservazione.
CRL	Certificate Revocation List.

Termine	Definizione
DC	Data Center.
Destinatario	Identifica il soggetto/sistema al quale il documento informatico è indirizzato.
Diffusione (formato)	Estensione dell'impiego di uno specifico formato per la formazione e la gestione dei documenti informatici.
D.lgs	Decreto Legislativo.
DM	Decreto Ministeriale.
DMZ	Demilitarized zone
DPCM	Decreto del Presidente del Consiglio dei Ministri.
DPR	Decreto del Presidente della Repubbica.
DR	Disaster Recovery.
Duplicazione dei documenti informatici	Produzione di duplicati informatici.
DVD	Digital Versatile Disk.
Extrainfo	Elemento che consente di introdurre metadati soggettivi relativi all'IdPA liberamente definiti con un proprio schema.
Esibizione	Operazione che consente di visualizzare un documento conservato e di ottenerne copia.
ETSI	European Telecommunications Standards Institut.
Formato	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
FTP	File Transfer Protocol.
Generazione automatica di documento informatico	Formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni.
GB	Gigabyte.
Hash	Funzione matematica univoca ed unidirezionale (cioè non può essere invertita), che trasforma un testo di qualunque lunghezza (input) in testo di lunghezza fissa (output) relativamente limitata.
HSM	Hardware Security Module.
HTMLS	Linguaggio di markup per la strutturazione delle pagine web, e da Ottobre 2014 pubblicato come W3C Recommendation.
IDC	Internet Data Centre.
Java J2EE	Java 2 Enterprise Edition.
JBOSS	Java Bean Open Source Server.
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.
IDS	Intrusion Detection System.
IdPA	Indice del Pacchetto di Archiviazione.
IEC	International Electrotechnical Commission.
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 DPCM 3 dicembre 2013 Regole tecniche in materia di sistema di conservazione, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta.

Termine	Definizione
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.
IPS	Intrusion Prevention System.
ISMS	Information Security Management System.
ISO	International Organization for Standardizations.
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 della conservazione	Strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 del DPCM 3 dicembre 2013 Regole tecniche in materia di sistemi conservazione.
Massimario di selezione	Strumento che consente di coordinare razionalmente lo scarto archivistico (cioè la destinazione al macero) dei documenti prodotti dagli enti pubblici e dagli organi centrali e periferici dello Stato. Il massimario riproduce l'elenco delle partizioni (categorie) e sottopartizioni del titolario con una descrizione più o meno dettagliata delle competenze cui ciascuna partizione si riferisce e della natura dei relativi documenti; indica per ciascuna partizione quali documenti debbano essere conservati permanentemente (e quindi versati dopo quarant'anni dall'esaurimento degli affari nei competenti Archivi di Stato) e quali invece possono essere destinati al macero dopo cinque anni, dopo dieci anni, dopo venti anni, ecc.
MEF	Ministero dell'Economia e della Finanza.
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 decreto.
NFS	Network File System.
OAIS	Open Archival Information System.
ORM	Object Relational Mapping.
OTRS	Open-source Ticket Request System.
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 della 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 della conservazione.
Pacchetto informativo	Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche),

Termine	Definizione
	oppure anche i soli metadati riferiti agli oggetti da conservare.
PdA	Pacchetto di Archiviazione.
PdD	Pacchetto di Distribuzione.
PdV	Pacchetto di Versamento.
Piano della sicurezza del sistema 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 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.
Portabilità	Facilità con cui i formati possano essere usati su piattaforme diverse, sia dal punto di vista dell'hardware che del software, inteso come sistema operativo. Di fatto è indotta dall'impiego fedele di standard documentati e accessibili.
Presa in carico	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal Manuale della 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.
RAM	Random Access Memory.
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.
Responsabile della conservazione	Soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 del DPCM Regole tecniche in materia di 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.
RDBMS	Relational DataBase Management System.
RdV	Rapporto di Versamento.
RFA	Responsabile della Funzione Archivistica.
RSC	Responsabile del Servizio di Conservazione.
RSI	Responsabile dei Sistemi Informativi.
RSM	Responsabile della Sviluppo e Manutenzione.
RSSI	Responsabile della Sicurezza dei Sistemi.
RTD	Responsabile per il Trattamento dei Dati personali.
SaaS	Software-as-a-Service.
Scarto	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale.
SFPT	Simple File Transfert Protocol.
SINcRO	Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti Digitali.

Termine	Definizione
Sistema di conservazione	Sistema di conservazione dei documenti informatici di cui all'articolo 44 del CAD.
Sistema di gestione informatica di 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.
SLA	Service Level Agreement.
SOA	Service-Oriented Architecture.
Soggetto produttore	Persona fisica o giuridica 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.
Supporto allo sviluppo (formato)	Modalità con cui si mettono a disposizione le risorse necessarie alla manutenzione e sviluppo del formato e i prodotti informatici che lo gestiscono (organismi preposti alla definizione di specifiche tecniche e standard, società, comunità di sviluppatori, ecc.).
TSM	Tivoli Storage Manager.
Unistorage	Applicazione della società Unimatica per la gestione dei Servizi di Conservazione a Norma dei documenti digitali, sia Autentica che Sostititutiva.
URL	Uniform Resource Locator.
URN	Uniform Resource Name.
USB	Universal Serial Bus.
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.
VPN	Virtual Private Network.
VTL	Virtual Tape Library.
WS	Web Service.
XML	Extensible Markup Language.
XSD	XML Schema Definition.

Torna al sommario

3. Normativa e standard di riferimento

Il sistema di conservazione sviluppato da UNIMATICA S.p.A. è conforme alla normativa e agli standard elencati nei successivi paragrafi.

Torna al sommario

3.1. Normativa di Riferimento

Notazione abbreviata	Riferimento
Codice Civile	[Libro Quinto del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle Scritture contabili], art. 2215 bis – Documentazione informatica.
L. 7 agosto 1990, n. 241	Legge 7 agosto 1990, n. 241, e successive modificazioni e integrazioni. Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.
D.P.R. 28 dicembre 2000, n. 445	Disposizioni legislative in materia di documentazione amministrativa - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.
AIPA, Circolare 7 maggio 2001, n. 28	Standard, modalità di trasmissione, formato e definizione dei tipi di informazioni minime ed accessorie comunemente scambiate tra le pubbliche amministrazioni e associate ai documenti protocollati e successive revisioni.
D. Lgs. 30 giugno 2003, n. 196 (codice sulla privacy)	D. lgs. 30 giugno 2003, n. 196, e successive modificazioni e integrazioni. Codice in materia di protezione dei dati personali.
D. Lgs. 22 gennaio 2004, n. 42 (codice dei beni culturali)	D. lgs. 22 gennaio 2004, n. 42, e successive modificazioni e integrazioni. Codice dei beni culturali e del paesaggio ai sensi dell'articolo 10 della Legge 6 luglio 2002, n. 137.
D. Lgs. 20 febbraio 2004, n. 52	Attuazione della direttiva 2001/115/CE che semplifica ed armonizzale modalità di fatturazione in materia di IVA.
DPR 2 marzo 2004, n. 117	Regolamento concernente la diffusione della carta nazionale dei servizi, a norma dell'articolo 27, comma 8, lettera b), della legge 16 gennaio 2003, n. 3.
DPR 11 febbraio 2005, n. 68	Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della Legge 16 gennaio 2003, n. 3.
Codice dell'amministrazione digitale (CAD)	D. lgs. 7 marzo 2005, n. 82, e successive modificazioni e integrazioni. Codice dell'amministrazione digitale.
Agenzia delle Entrate, Circolare 19 ottobre 2005, n. 45	Circolare esplicativa della fattura elettronica.
Circolare 6 dicembre 2006, n. 36/E	Chiarimenti sull'applicazione del Decreto 23 gennaio, 2004.
DPMC 30 marzo 2009	Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici.
Delibera CNIPA, n. 45 21 maggio 2009	Regole per il riconoscimento e verifica del documento informatico.
DPCM 10 febbraio 2010	Fissazione del termine che autorizza l'autocertificazione circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza.
Determinazione DigitPA n. 69 del 28 luglio 2010	Modifica alla Delibera n. 45/2009.
Provvedimento 25 ottobre 2010	Agenzia delle Entrate: provvedimento attuativo della comunicazione dell'impronta relativa ai documenti informatici rilevanti ai fini tributari.

Notazione abbreviata	Riferimento
D. lgs. 30 dicembre 2010, n. 235	Modifiche e integrazioni al decreto legislativo 7 marzo 2005, n. 82 “NUOVO CAD”.
DPCM 22 febbraio 2013	Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli art. 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71.
DPCM 3 dicembre 2013	Regole tecniche in materia di protocollo informatico ai sensi degli articoli 40-bis , 41, 47, 57-bis e 71 del Codice dell’amministrazione digitale di cui al decreto legislativo n. 82 del 2005.
DPCM 3 dicembre 2013	Regole tecniche in materia di sistema di conservazione ai sensi degli artt. 20, 23ter, 43, 44, 44bis e 71 del CAD di cui al Dlgs n. 82 del 2005.
Circolare AGID 10 aprile 2014, n. 65	Modalità per l’accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all’art. 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.
Decreto MEF 17 giugno 2014	Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005.
Il Regolamento UE n. 910/2014	eIDAS Regulation - Identification and trusted services for electronic transactions in the internal market.

Torna al sommario

3.2. Standard di Riferimento

Sigla	Titolo standard
ISO 14721:2012 OAIS	Open Archival Information System – Sistema informativo aperto per l'archiviazione.
ISO/IEC 27001:2013	Information technology – Security techniques – Information security management systems – Requirements. - Requisiti di un ISMS (Information Security Management System).
ETSI TS 101 533-1 v1.3.1 (2012-04)	Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part. 1: Requirements for Implementation and Management. – Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.
ETSI TR 101 533-2 v1.3.1 (2012-04)	Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part. 2: Guidelines for Assessors. – Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.
UNI 11386:2010	Standard SInCRO – Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.
ISO 15836:2009	Information and documentation – The Dublin Core metadata element set. – Sistema di metadata del Dublin Core

Torna al sommario

4. Ruoli e responsabilità

Ragione sociale	**UNIMATICA S.p.A.**
Codice Fiscale/Partita IVA:	02098391200
Sede legale ed operativa:	Via Cristoforo Colombo, 21 – 40131 Bologna

UNIMATICA S.p.A. utilizza personale altamente specializzato e formato sulle problematiche legate alla conservazione e all'archiviazione digitale.

Tale personale è inoltre costantemente aggiornato sulle nuove normative e sugli aspetti tecnologici, attraverso la consultazione della documentazione, messa a disposizione dall'azienda, e la partecipazione ad appositi corsi di approfondimento, interni ed esterni.

L'impegno e l'attenzione di tutta l'azienda sulla tematica specifica ed i risultati raggiunti nel corso degli anni di attività hanno permesso ad UNIMATICA S.p.A. di ottenere l'iscrizione quale socio sostenitore presso l'associazione ANORC (Associazione Nazionale per Operatori e Responsabili della Conservazione Digitale).

L'art. 6, c.1 del DPCM 3 dicembre 2013 individua all'interno della struttura organizzativa del sistema di conservazione i ruoli di:

- Soggetto produttore,
- Responsabile della Conservazione,
- Utente.

Il **Soggetto produttore** è la persona fisica o giuridica che permette la produzione dei Pacchetti di Versamento[1] ed è il responsabile del trasferimento di questi dal proprio sistema di gestione documentale al sistema di conservazione UNIMATICA S.p.A. Per l'intera durata del contratto, il Soggetto produttore resterà il titolare degli oggetti documentali versati.

A tal proposito è opportuno sottolineare la distinzione tra il Soggetto produttore, da UNIMATICA S.p.A. inteso come responsabile sia della produzione che del versamento e il Produttore responsabile unicamente dell'invio in conservazione del Pacchetto di Versamento.

Il **Responsabile della Conservazione** viene nominato dal Soggetto produttore. In accordo con il Responsabile del trattamento dei dati personali, con il Responsabile della sicurezza e con il Responsabile dei sistemi informativi definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia di documenti da conservare, in conformità alla normativa vigente. Il Responsabile della conservazione, tramite specifico contratto, affida al Responsabile del servizio di conservazione di UNIMATICA S.p.A. le attività di gestione e la supervisione dei processi del sistema di conservazione. In particolare, il Responsabile del servizio di conservazione si occuperà di:

- definire le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente;

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

- gestire il processo di conservazione e di garantirne nel tempo la conformità alla normativa vigente;
- generare il Rapporto di Versamento, secondo le modalità previste dal Manuale della conservazione;
- generare e sottoscrivere il Pacchetto[2] di Distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal Manuale della conservazione;
- effettuare il monitoraggio della corretta funzionalità del sistema di conservazione;
- assicurare la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
- al fine di garantire la conservazione e l'accesso ai documenti informatici, adottare misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; occuparsi, inoltre di adottare analoghe misure con riguardo all'obsolescenza dei formati;
- provvedere alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal Manuale della conservazione;
- adottare le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12 delle Regole tecniche in materia di sistemi di conservazione;
- assicurare la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
- assicurare agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
- provvedere, per gli organi giudiziari e amministrativi dello Stato, al versamento dei documenti conservati all'archivio centrale dello Stato e agli archivi di Stato secondo quanto previsto dalle norme vigenti;
- predisporre il Manuale della conservazione di cui all'art. 8 delle Regole tecniche in materia di sistemi di conservazione e curare l'aggiornamento periodico di questo in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Il **Responsabile del servizio di conservazione**, quindi, si occupa di definire e attuare le politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione e di definire le caratteristiche e i requisiti del sistema di conservazione in conformità alla normativa vigente. Garantisce una corretta erogazione del servizio di conservazione all'ente produttore e gestisce le convenzioni, definisce gli aspetti tecnico-operativi e la validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.

Nominativo	Periodo nel ruolo
Silvano Ghedini	Dal 2004 ad oggi

Silvano Ghedini, Responsabile del servizio di conservazione di UNIMATICA S.p.A., nello svolgere le attività del processo di conservazione, ha delegato l'esercizio complessivo di queste a:

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

Nominativo Delegato Responsabile del Servizio di conservazione	Periodo di delega
Andrea Anghinolfi	01/2009 ad oggi
Roberta Nucci	01/2010 ad oggi

L'Utente è la persona, l'ente o il sistema che interagisce con i servizi del sistema di conservazione allo scopo di usufruire degli oggetti conservati di suo interesse. Gli Utenti costituiscono la comunità di riferimento individuata nel modello OAIS, sulla base della quale il sistema di conservazione struttura le modalità di esibizione.

All'interno della struttura organizzativa del sistema di conservazione, così come specificato nella circolare dell'Agenzia per l'Italia Digitale n. 65 del 10 aprile 2014, in particolare nel documento "Profili professionali", si individuano le seguenti figure responsabili coinvolte nel servizio:

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

Nominativo	Periodo nel ruolo
Massimo Ortensi	Dal 2001 ad oggi

Responsabile della funzione archivistica di conservazione. Si occupa di definire e gestire 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, inoltre, il set di metadati di conservazione dei documenti e dei fascicoli informatici. Monitora il processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema. 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.

Nominativo	Periodo nel ruolo
Sabina Falcinelli	Dal 2012 a Giugno 2017
Roberta Nucci	Da Giugno 2017 ad oggi

Responsabile del trattamento dei dati personali. Si occupa di garantire il rispetto delle vigenti disposizioni in materia di trattamento dei dati personali. Garantisce, inoltre che il trattamento dei dati affidati dai Soggetti produttore avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.

Nominativo	Periodo nel ruolo
Silvano Ghedini	Dal 2004 ad oggi

Responsabile dei sistemi informativi per la conservazione. Si occupa di gestire l'esercizio delle componenti hardware e software del sistema di conservazione e monitora il mantenimento dei livelli di servizio (SLA) concordati con il Soggetto produttore. Segnala le eventuali difformità degli SLA al Responsabile del servizio di conservazione e individua e pianifica le necessarie azioni correttive. Si occupa di pianificazione lo sviluppo delle infrastrutture tecnologiche del sistema di conservazione e verifica i livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.

Nominativo	Periodo nel ruolo
Andrea Anghinolfi	Dal 2008 ad oggi

Responsabile sviluppo e manutenzione del sistema di conservazione. Si occupa di coordinare lo sviluppo e la manutenzione delle componenti hardware e software del sistema di conservazione. Pianifica e monitora i progetti di sviluppo del sistema di conservazione. Monitora inoltre gli SLA relativi alla manutenzione del sistema di conservazione. Si occupa di interfacciarsi con il Soggetto produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche. Gestisce, inoltre lo sviluppo di siti web e portali connessi al servizio di conservazione.

Nominativo	Periodo nel ruolo
Stefano Ghedini	Dal 2008 ad oggi

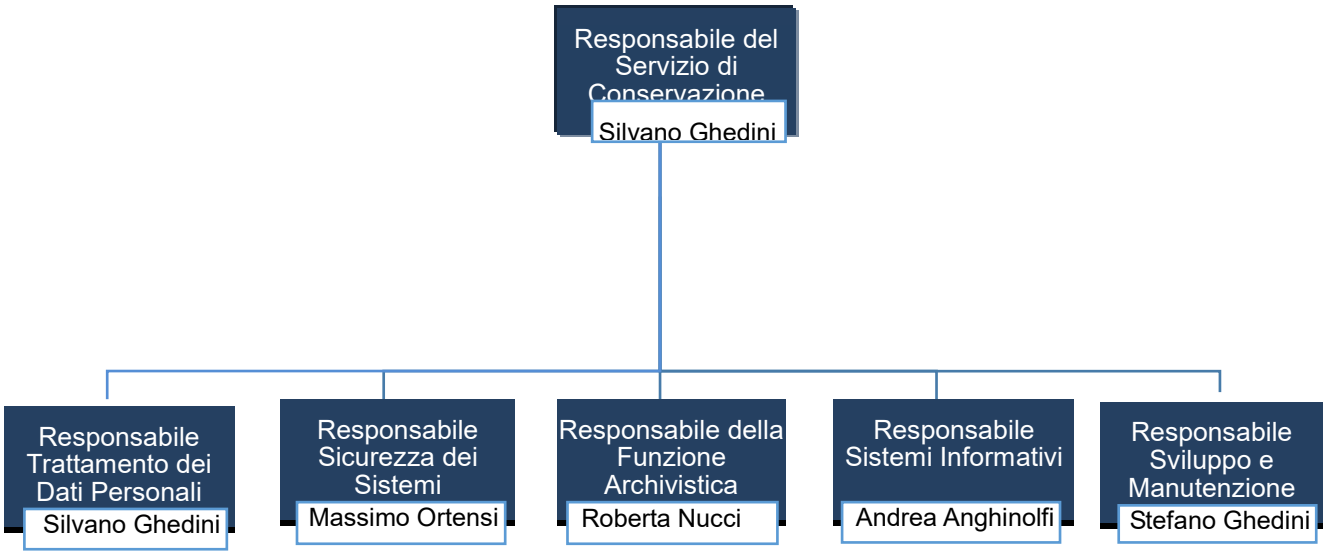
Torna al sommario

5. Struttura organizzativa per il servizio di conservazione

Il presente capitolo ha lo scopo di illustrare la struttura organizzativa del settore conservazione di UNIMATICA S.p.A. L' espletamento di un processo di conservazione prevede una serie di complesse attività, pertanto la società si avvale di personale altamente qualificato e con esperienza decennale. Si riporta di seguito l'organigramma della struttura organizzativa e una sintetica descrizione[3] delle funzioni e delle responsabilità che intervengono nel processo di conservazione.

Torna al sommario

5.1. Organigramma



Torna al sommario

5.2. Strutture organizzative

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

[3] La descrizione dettagliata del processo di conservazione è riportata nel capitolo 7 "Il processo di erogazione del servizio di conservazione".

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

[4] Traduzione di Archival Information Package dal Modello OAIS Open Archival Information Standard che individua nel sistema di archiviazione tre diversi tipi di Pacchetti: Submission Information Package (SIP), Archival Information Package (AIP) e Dissemination Information Package (DIP).
[5] Indice del pacchetto di archiviazione.

	conservazione (al termine di un contratto)	ad UNIMATICA, nei tempi previsti dal manuale, la rescissione del contratto.	RTD

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

Legenda	
RSC	Responsabile del Servizio di Conservazione
RSSI	Responsabile Sicurezza dei Sistemi Informativi per la Conservazione
RFA	Responsabile Funzione Archivistica per la Conservazione
RTD	Responsabile Trattamento Dati Personali
RSI	Responsabile Sistemi Informativi per la Conservazione
RSM	Responsabile Sviluppo e Manutenzione del Sistema di Conservazione

Torna al sommario

6. Oggetti sottoposti a conservazione

UNIMATICA S.p.A. mediante UniStorage, il prodotto applicativo descritto nel capitolo 8 "La server farm di Unimatica", utilizzato per la gestione del processo di conservazione e sviluppato integralmente dalla società, è in grado di gestire diverse tipologie di documenti, relativi a diversi ambiti applicativi, quali:

- Documenti e disposizioni in ingresso e in uscita
- Documenti di sportello bancario
- Contratti ed allegati
- Fatture attive e Fatture passive
- Libri e registri sociali
- Libri e registri contabili
- Libri e registri assicurativi
- Libretto unico del lavoro (LUL)
- Assegni
- Mandati di pagamento e Reversali d'incasso
- Ricevute e quietanze di pagamento
- Delibere, determine, atti e provvedimenti
- Referti, Cartelle cliniche, Immagini diagnostiche
- Registro Giornaliero di protocollo

In accordo con il Soggetto produttore, UNIMATICA S.p.A. si riserva la facoltà di accettare anche documenti non menzionati nel suddetto elenco. L'indicazione di tali documenti, compresa la gestione di questi, verranno indicati nella Scheda Cliente allegata al Manuale della conservazione e al contratto stipulato con il Soggetto produttore.

UNIMATICA S.p.A. accetta e conserva solo documenti digitali. Il sistema di conservazione permette l'acquisizione sia di documenti firmati digitalmente, sia di documenti non firmati. Entrambe le tipologie subiscono il medesimo trattamento eccezion fatta in fase di controllo[6] quando tra le verifiche non verrà effettuata quella sulla firma per i documenti dei quali è stato dichiarato non essere firmati. Con l'ausilio del Responsabile del servizio di conservazione, è il Soggetto produttore a definire nella Scheda cliente allegata al Manuale della conservazione le modalità di trattamento dei documenti firmati o non firmati.

Torna al sommario

6.1 Metadati

Come previsto dall'art. 3, c. 1 del Decreto della Presidenza del Consiglio dei Ministri 3 dicembre 2013 Regole tecniche in materia di sistema di conservazione, il sistema di conservazione assicura dalla presa in carico dal Soggetto produttore fino all'eventuale scarto, la conservazione tramite l'adozione di regole, procedure e tecnologie degli oggetti in esso conservati, garantendone oltre all'autenticità, all'integrità, all'affidabilità e alla leggibilità anche la reperibilità. Al fine di rendere agevole ed efficiente la ricerca di un documento, di un fascicolo, o di un'aggregazione

[6] Le verifiche effettuate sui documenti ricevuti sono descritte al capitolo 7 "Il processo di erogazione del servizio di conservazione", Fase 2.

documentale informatica conservati è necessario individuare dei metadati, ovvero un insieme di dati da associare all'oggetto informatico o al fascicolo informatico che ne descrivano il contenuto e lo identifichino all'interno del sistema.
UNIMATICA S.p.A., in piena conformità con le Regole tecniche, individua un insieme minimo di metadati.
In particolare:

- un set di metadati minimi del documento informatico,
- un set di metadati minimi del Registro di protocollo giornaliero,
- un set di metadati minimi del documento informatico avente rilevanza tributaria,
- un set di metadati minimi del fascicolo informatico o dell'aggregazione documentale informatica.

Torna al sommario

6.1.1 Metadati minimi del documento informatico

Di seguito vengono elencati i metadati minimi del documento informatico:

1. **Identificativo**: è una sequenza di max. 20 caratteri alfanumerici associati in maniera univoca e persistente al documento informatico così da garantirne l'identificazione. Il Dublin Core Metadata Element Set7 raccomanda di identificare la risorsa per mezzo di una sequenza di caratteri alfabetici o numerici secondo un sistema di identificazione formalmente definito. Esempi di tali sistemi di identificazione includono l'Uniform Resource Identifier (URL) (incluso l'Uniform Resource Locator (URN)), il Digital Object Identifier (DOI) e l'International Standard Book Number (ISBN).

Valori ammessi	Tipo dato
Come da Sistema di identificazione formalmente definito	Alfanumerico 20 caratteri

2. **Data di chiusura**: indica la data di creazione del documento informatico, ovvero il momento in cui tale documento è reso immodificabile.

Valori ammessi	Tipo dato
Data	Formato yyyy/mm/dd

3. **Oggetto**: riassume sinteticamente il contenuto del documento informatico e può contenere un riassunto analitico, un indice o una rappresentazione grafica del contenuto.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

[7] Il Dublin Core Metadata si propone come uno standard di descrizione delle risorse in formato elettronico ed è costituito da 15 elementi descrittivi: titolo, autore o creatore, soggetto e parole chiave, descrizione, editore, altro responsabile, data, tipo di risorsa, formato, identificatore della risorsa, lingua, fonte, relazione, copertura e diritti.

4. **Soggetto produttore**: colui che ha la responsabilità della produzione del documento informatico.

Valori ammessi	Tipo dato
Nome: testo libero	Alfanumerico 40 caratteri
Cognome: testo libero	Alfanumerico 40 caratteri
Codice fiscale: codice fiscal	Alfanumerico 16 caratteri

5. **Destinatario**: colui che ha la responsabilità della ricezione del documento.

Valori ammessi	Tipo dato
Nome: testo libero	Alfanumerico 40 caratteri
Cognome: testo libero	Alfanumerico 40 caratteri
Codice fiscale: codice fiscale (Obbligatorio, se disponibile)	Alfanumerico 16 caratteri

Nella Scheda Cliente predisposta da UNIMATICA S.p.A. allegata al Manuale della conservazione e al contratto, è possibile personalizzare i set di metadati in base alle esigenze del Soggetto produttore e alle diverse tipologie documentali conservate. In un'apposita tabella il cliente specificherà i metadati di proprio interesse.

Torna al sommario

6.1.2 Metadati minimi del Registro di protocollo giornaliero

I metadati minimi obbligatori del Registro di protocollo giornaliero sono i seguenti:

1. **Identificativo univoco e persistente:** nome del file.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

2. **Data di chiusura:** data di chiusura del Pacchetto di versamento (Es. la data di chiusura del Registro di protocollo giornaliero del 22 settembre 2015, sarà del 23 settembre 2015).

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

3. **Soggetto produttore:** operatore che ha prodotto il Registro – Nome, Cognome, Codice fiscale; qualora il registro è generato automaticamente dal sistema informatico, il nome dell'operatore può essere sostituito dall'indicazione di tale sistema.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

4. **Soggetto produttore 2:** Operatore che ha prodotto il registro – Nome, cognome, codice fiscale**.**

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

5. **Destinatario:** indicare la dicitura "Interno".

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

6. **Impronta del documento informatico**

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

7. **Codice identificativo dell'amministrazione**: Codice IPA**.**

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

8. **Denominazione dell'amministrazione**:

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

9. **Codice identificativo dell'area organizzativa omogenea**:

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

10. **Responsabile**: Responsabile della gestione documentale o Responsabile del servizio per la tenuta del protocollo informatico – Nome, Cognome, Codice fiscale.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

11. **Oggetto**: Descrizione della tipologia di servizio, ad es. “Registro giornaliero di protocollo”, “Registro giornaliero delle modifiche di protocollo”.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

12. **Codice identificativo del registro**

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

13. **Numero progressivo del registro**

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

14. **Anno**

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

15. **Numero della prima registrazione effettuata sul registro**

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

16. **Numero dell’ultima registrazione effettuata sul registro**

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

17. Data della prima registrazione effettuata sul registro

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

18. Data dell'ultima registrazione effettuata sul registro

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

Eventuali metadati facoltativi possono essere indicati nella Scheda cliente allegata al Manuale della conservazione e al contratto di servizio.

Torna al sommario

6.1.3 Metadati minimi del documento informatico aventi rilevanza tributaria

I metadati minimi dei documenti informatici con rilevanza tributaria**,** laddove tali informazioni siano obbligatoriamente previste[8], sono i seguenti**:**

- per i documenti fiscali di tipo Fattura i metadati obbligatori per il ciclo attivo sono:

1. **Partita IVA emittente:** partita iva dell'emittente.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

2. **Numero documento:** stringa che identifica il numero della fattura.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico255 caratteri

3. **Data documento**

Valori ammessi	Tipo dato
Data	Formato yyyy/mm/dd hh:mm:ss

[8] Rif. Art. 3 del Decreto del Ministero Economia e Finanza **del 17 giugno 2014 -** Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005.

4. **Partita IVA cliente:** partita IVA del cliente.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico255 caratteri

5. **Codice fiscale cliente:** codice fiscale del cliente.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico255 caratteri

6. **Nome Cliente:** nome cliente della fattura in caso di persona fisica.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico255 caratteri

7. **Cognome Cliente:** cognome cliente della fattura in caso di persona fisica.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico255 caratteri

8. **Denominazione:** denominazione in caso di persona giuridica.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico255 caratteri

9. **Valuta:** valuta importo fatture “EUR”.

Valori ammessi	Tipo dato
Valore fisso “EUR”	Alfanumerico 255 caratteri

10. **Totale fattura:** importo totale della fattura.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

UNIMATICA S.p.A., nella Scheda Cliente allegata al Manuale della conservazione, predispone anche i seguenti metadati facoltativi:

- **Totale tasse**

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

- **Data scadenza:** data scadenza documento.

Valori ammessi	Tipo dato
Data	Formato yyyy/mm/dd hh:mm:ss

- **Codice cliente**

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

- **ID documento_sistema:** identificativo del cliente.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

- Per i documenti fiscali di tipo Fattura i metadati obbligatori per il ciclo passivo sono:

1. **Partita IVA ricevente:** partita iva dell'emittente.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

2. **Numero documento:** stringa che identifica il numero della fattura.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

3. **Data documento**

Valori ammessi	Tipo dato
Data	Formato yyyy/mm/dd hh:mm:ss

4. **Partita IVA fornitore:** partita IVA del fornitore.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

5. **Codice fiscale fornitore:** codice fiscale del fornitore.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

6. **Nome fornitore:** nome fornitore della fattura in caso di persona fisica.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

7. **Cognome fornitore:** cognome fornitore della fattura in caso di persona fisica.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

8. **Denominazione:** denominazione in caso di persona giuridica.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

9. **Valuta:** valuta importo fatture, valore fisso “EUR”.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

10. **Totale fattura:** importo totale della fattura.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

UNIMATICA S.p.A., nella Scheda Cliente allegata al Manuale della conservazione predispone anche i seguenti metadati facoltativi:

- **Totale tasse**

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

- **Data scadenza:** data scadenza documento.

Valori ammessi	Tipo dato
Data	Data yyyy/mm/dd hh:mm:ss

- **Codice cliente**

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

- **ID documento_sistema:** identificativo del cliente.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

Si riporta di seguito un estratto di xml:

```
<Profilo>
    <Metadato Chiave="Categoria">REGISTRO IVA ACQUISTI</Metadato>
    <Metadato Chiave="Azienda">Anagrafica</Metadato>
    <Metadato Chiave="C.F.">c.f. </Metadato>
    <Metadato Chiave="Partita IVA">p.iva</Metadato>
    <Metadato Chiave="Oggetto">Oggetto del documento</Metadato>
</Profilo>
```

Nei casi in cui tali metadati non siano ricavabili da particolari tipologie di documenti informatici aventi rilevanza tributaria, nell'apposita Scheda Cliente allegata al Manuale della conservazione il Soggetto produttore potrà indicare i metadati individuabili dal documento come specificato nell' **all'art**. **3**, comma1, lettera b) del **Decreto del 17 giugno 2014 - Min. Economia e Finanze,** Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005.

Torna al sommario

6.1.4 Metadati minimi del fascicolo informatico o dell'aggregazione documentale informatica

I metadati minimi dei fascicoli o delle aggregazioni documentali per i versamenti effettuati dalle pubbliche amministrazioni sono:

1. **Identificativo**: Identificativo univoco e persistente è una sequenza di caratteri alfanumerici associata in modo univoco e permanente al fascicolo o aggregazione documentale informatica in modo da consentirne l'identificazione. Dublin Core raccomanda di identificare il documento per mezzo di una sequenza di caratteri alfabetici o numerici secondo un sistema di identificazione formalmente definito. Esempi di tali sistemi di identificazione includono l'Uniform Resource Identifier (URI), il Digital Object Identifier (DOI) e l'International Standard Book Number (ISBN).

Valori ammessi	Tipo dato
Come da sistema di identificazione formalmente definito	Alfanumerico 20 caratteri

2. **Amministrazione titolare**: Amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo.

Valori ammessi	Tipo dato
Vedi specifiche Codice IPA	Codice IPA

3. **Amministrazioni partecipanti**: Amministrazioni che partecipano all'Iter del procedimento.

Valori ammessi	Tipo dato
Vedi specifiche Codice IPA	Codice IPA

4. **Responsabile del procedimento**:

Valori ammessi	Tipo dato
Nome: testo libero	Alfanumerico 40 caratteri
Cognome: testo libero	Alfanumerico 40 caratteri
Codice fiscale: codice fiscale	Alfanumerico 16 caratteri

5. **Oggetto**: Oggetto, metadato funzionale a riassumere brevemente il contenuto del documento o comunque a chiarirne la natura. Dublin Core prevede l'analoga proprietà "Description" che può includere ma non è limitata solo a: un riassunto analitico, un indice, un riferimento al contenuto di una rappresentazione grafica o un testo libero del contenuto.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 100 caratteri

6. **Documento**: Elenco degli identificativi dei documenti contenuti nel fascicolo che ne consentono la reperibilità.

Valori ammessi	Tipo dato
Identificativo del documento così come definito agli articoli 9 e 19 delle regole tecniche per il protocollo informatico di cui al D.P.C.M. 31 ottobre 2000 e descritti nella Circolare AIPA del 7 maggio 2001, n. 28.	Alfanumerico 100 caratteri

I Metadati minimi dei fascicoli o delle aggregazioni documentali informatiche per i versamenti effettuati dai soggetti privati sono:

1. **Denominazione cliente**: Ragione sociale del Soggetto produttore.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

2. **Identificativo cliente**: sequenza alfanumerica di caratteri associati in maniera univoca e permanente al fascicolo o all'aggregazione documentale informatica in modo da consentirne l'identificazione.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

3. **Oggetto:** Oggetto del fascicolo o dell'aggregazione documentale informatica.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

4. **Data**: Data di presa in carico da parte di UNMATICA S.p.A. del fascicolo o dell'aggregazione documentale informatica.

Valori ammessi	Tipo dato
Data	Formato yyyy/mm/dd hh:mm:ss

5. **Partita IVA**: Partita IVA del Soggetto produttore.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

6. **Codice fiscale cliente**: Codice fiscale del Soggetto produttore.

Valori ammessi	Tipo dato
Testo libero	Alfanumerico 255 caratteri

Torna al sommario

6.2 Formati

UNIMATICA S.p.A., in conformità all'allegato 2 al Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 Regole tecniche in materia di sistema di conservazione, accetta formati che maggiormente garantiscano i principi di interoperabilità tra sistemi di conservazione. Al fine di assicurare una corretta gestione degli oggetti conservati è opportuno che i formati assicurino le seguenti caratteristiche[9]:

- apertura,
- sicurezza,
- portabilità,
- funzionalità,
- supporto allo sviluppo,
- diffusione.

[9] Per maggiori dettagli circa le spiegazioni di tali caratteristiche fare riferimento all'allegato 2 al DPCM 3 dicembre 2013 Regole tecniche in materia di conservazione.

Di seguito viene riportato un breve elenco dei formati più diffusi accettati da UNIMATICA S.p.A. e i relativi dettagli esplicativi.

Formato	Estensione	Tipo MIME	Formato aperto	Specifiche tecniche	Ultima Versione
Portable Document Format	.pdf	application/pdf	si	Pubbliche	1.7
Joint Photographic Experts Group	.jpg .jpeg	image/jpeg	si	Pubbliche	2009
Extensible Markup Language	.xml	application/xml, text/xml	si	Pubbliche	
Office Open XML (OOXML)	.docx .xlsx .pptx		si	Pubbliche	1.1
Tagged Image File Format	.tiff	image/tiff	no	Pubbliche	TIFF 6.0 del 1992 TIFF Supplement 2 del 2002
Open Document Format	.ods .odp .odg .odb	application/vnd.oasis .opendocument.text	si	Pubbliche	1.0
Zip	.zip	application/zip	si	Pubbliche	3.0
Digital Imaging and Communications in Medicine	.dicom	image/x-dicom		Pubbliche	
Health Level-7	.hl7	application/edi-hl7			

In accordo con il Soggetto produttore, UNIMATICA S.p.A. si riserva la facoltà di accettare anche formati non menzionati nell'elenco delle Regole Tecniche ma che il Soggetto produttore ritiene di dover conservare. L'indicazione di tali formati, compresa la gestione di questi, verranno indicati nella Scheda Cliente allegata al Manuale della conservazione e al contratto stipulato con il Soggetto produttore.

Alla ricezione del documento il sistema, attraverso l'uso di una libreria WAZFORMAT, la cui procedura utilizzerà un metodo di indagine diretta con tecniche euristiche, riconosce il formato controllando il valore descritto nel magic number.
Questo passaggio permette di associare il formato al documento per garantirne la corretta visualizzazione e quindi leggibilità utilizzando gli opportuni i visualizzatori.

Torna al sommario

6.3 Struttura dati del Pacchetto di versamento

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

- La ricezione mediante File Transfert Protocol prevede l'upload del Pacchetto di versamento composto da un file indice e da un insieme di file, in formato .zip.

Si riporta di seguito lo schema xml della struttura dati di un Pacchetto di versamento

```
<?xml version="1.0" encoding="utf-8"?>
<Flusso>
  <Testata>
    <Nome>xxxxxxxxxxxxxxx</Nome>
    <DataInvio>yyyy/mm/dd 00.00.00</DataInvio>
    <Tipo>xxxxxxxxxxxxxxx</Tipo>
    <Struttura>xxxxx</Struttura>
  </Testata>
  <NuovoDocumento>
    <Documento>
      <Chiave>
        <Numero>XXXXXXXXXXXXXXXXXXXXXXXX</Numero>
        <Registro />
        <Anno />
      </Chiave>
      <Proprieta>
        <TipoDocumento>xxxxxx</TipoDocumento>
        <Data>yyyy/mm/dd 00:00:00</Data>
        <IdSistemaMittente>xxxxxxxxxxxxxxxxxx</IdSistemaMittente>
      </Proprieta>
      <File>
        <Hash Algoritmo="SHA1" Codifica="B64">xxxxxxxxxxxxxx</Hash>
        <Path>XXXXXXXXXXXXXXXXXXXXXXXX.pdf</Path>
      </File>
      <Profilo>
        <Metadato Chiave="COD_SOC">xx</Metadato>
        <Metadato Chiave="COD_UO">xxxx</Metadato>
        <Metadato Chiave="COD_SPORTELLO">xxxx</Metadato>
        <Metadato Chiave="WORKSTATION">xxxxxx</Metadato>
        <Metadato Chiave="OPERATORE">xxxxxxxx</Metadato>
        <Metadato Chiave="COD_RAPPORTO">xxxxxxxx</Metadato>
        <Metadato Chiave="NDG">xxxxxxxx</Metadato>
        <Metadato Chiave="NOME">xxxxxxxx</Metadato>
        <Metadato Chiave="COGNOME">xxxxxxxx</Metadato>
        <Metadato Chiave="IMPORTO">xxxxxx</Metadato>
        <Metadato Chiave="COD_ADESIONE">xxx</Metadato>
        <Metadato Chiave="FG_ANNULLO">x</Metadato>
        <Metadato Chiave="EMAIL_CLIENTE">xxxxxx</Metadato>
        <Metadato Chiave="TRANSAZIONE">xxxxx</Metadato>
```

```
        <Metadato Chiave="DATA_CONTABILE">yyyy/mm/dd
00:00:00</Metadato>
        <Metadato Chiave="DATA_CREAZIONE">yyyy/mm/dd
00:00:00</Metadato>
        <Metadato Chiave="DATA_FIRMA">yyyy/mm/dd
00:00:00</Metadato>
        <Metadato Chiave="VERSIONE">x</Metadato>
      </Profilo>
      <Referenze />
    </Documento>
  </NuovoDocumento>
</Flusso>
```


Dove il nodo *Flusso* contiene un solo nodo Testata e una serie di nodi di tipo NuovoDocumento,

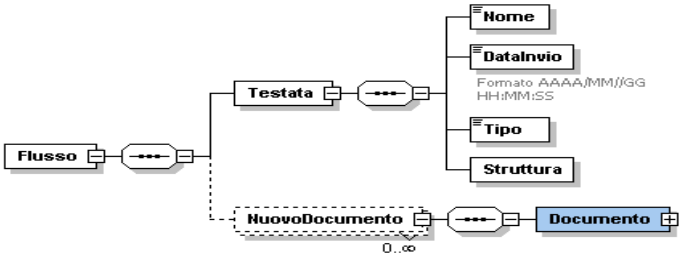


Figura 1 - Nodo Flusso

i nodi di tipo *Chiave* forniscono un identificativo univoco dei documenti,

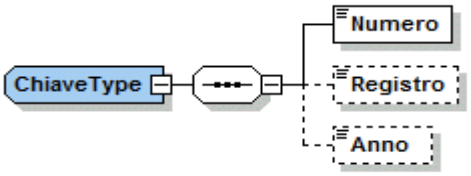


Figura 2 - Esempio nodo di tipo chiave

il nodo *Documento* contiene tutti gli elementi per la sua descrizione.

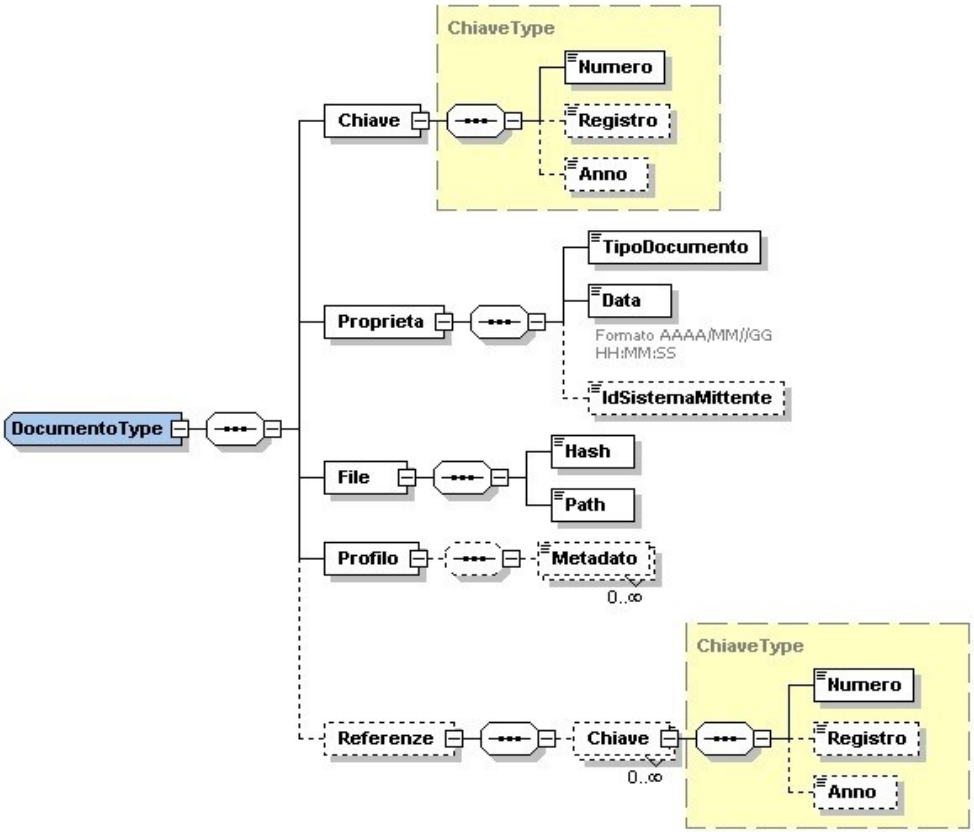


Figura 3 - Nodo documento

Per maggiori dettagli circa la struttura dei Pacchetti di versamento, fare riferimento al documento FlussiConservazione_ver 1.7

- La ricezione tramite Sistema Web Service è possibile da qualsiasi piattaforma che permetta di eseguire e ricevere chiamate Web Service conformi allo standard WS-I Basic Profile 1.0. Con questo servizio il sistema di conservazione riceve singoli documenti ed eventuali allegati, ne verifica la firma digitale se presente e ne gestisce la conservazione autentica.

Si riporta di seguito lo schema xml della struttura dati di un Pacchetto di versamento

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
	<soapenv:Body>
		<ConsegnaAnticipata
xmlns="http://anticipati.versamenti.service.unirepo.unimaticaspa.it/">
			<Documento xmlns="">
				<chiave>
					<proprieta>
						<chiave>NUMERO</chiave>
						<valore>xx</valore>
					</proprieta>
					<proprieta>
						<chiave>ANNO</chiave>
						<valore>xxxx</valore>
```

```
                        </proprieta>
                        <proprieta>
                                <chiave>CLASSIFICAZIONE</chiave>
                                <valore>xxxxxx</valore>
                        </proprieta>
                </chiave>

                <allegati>
                        <proprieta>
                                <chiave>tipo_allegato</chiave>
                                <valore>GENERICO</valore>
                        </proprieta>
                        <proprieta>
                                <chiave>chiave_allegato</chiave>
                                <valore>prova_allegato_1</valore>
                        </proprieta>
                        <versioneOriginale>
                                <proprieta>
                                        <chiave>formato_versione</chiave>
                                        <valore>xml firmato tipo1</valore>
                                </proprieta>
                                        <parti>
                                        <proprieta>

<chiave>formato_parte</chiave>
                                                        <valore>xxx</valore>
                                        </proprieta>
                                        <proprieta>
                                                <chiave>numero_parte</chiave>
                                                <valore>x</valore>
                                        </proprieta>
                                        <files>
                                                <dati></dati>
                                                        <proprieta>

<chiave>ordinePresentazione</chiave>
                                                                <valore>x</valore>
                                                        </proprieta>
                                                <proprieta>
                                                        <chiave>formato_file</chiave>
                                                        <valore>xxx</valore>
                                                        </proprieta>
                                                        <proprieta>

<chiave>nomeFile</chiave>

<valore>ConsegnaAnticipataAllegatoFileAllegato.pdf.p7m</valore>
                                                        </proprieta>
                                                <proprieta>

<chiave>id_cliente</chiave>

<valore>Test_Consegna_Anticipata_Allegato_ALLEGATO</valore>
                                                        </proprieta>
                                        </files>
                                        </parti>
                        </versioneOriginale>
                </allegati>


                <proprieta>
                        <chiave>tipo_documento</chiave>
                        <valore>xxxxxxxx</valore>
                </proprieta>
```

```
                        <proprieta>
                              <chiave>forza_conservazione</chiave>
                              <valore>xxxxx</valore>
                        </proprieta>
                        <proprieta>
                              <chiave>forza_accettazione</chiave>
                              <valore>xxxxx</valore>
                        </proprieta>
                        <profiloArchivistico>
                              <proprieta>
                                    <chiave>Contraente</chiave>
                                    <valore>xxxxxxxxxx</valore>
                              </proprieta>
                              <proprieta>
                                    <chiave>Codice Rivenditore</chiave>
                                    <valore>xxxxxxx</valore>
                              </proprieta>
                              <proprieta>
                                    <chiave>Numero Contratto</chiave>
                                    <valore>xxxxxxxxx</valore>
                              </proprieta>
                              <proprieta>
                                    <chiave>Data Effetto</chiave>
                                    <valore>xxxxxxx</valore>
                              </proprieta>

                              <proprieta>
                                    <chiave>Codice Fiscale</chiave>
                                    <valore>xxxxxxxxxxxxxx</valore>
                              </proprieta>
                              <proprieta>
                                    <chiave>Scadenza</chiave>
                                    <valore>xxxxxxxxx</valore>
                              </proprieta>
                        </profiloArchivistico>

                        <versioneOriginale>
                              <parti>
                                    <files>
                                          <dati></dati>
                                           <documento>
                <xop:Include href="consensi.pdf.p7m"
xmlns:xop="http://www.w3.org/2004/08/xop/include">
                                                      </xop:Include>
              </documento>
                                          <proprieta>

      <chiave>ordine_presentazione</chiave>
                                                <valore>0</valore>
                                          </proprieta>
                                          <proprieta>
                                                <chiave>nome_file</chiave>
                                                <valore>Consenso.pdf.p7m</valore>
                                          </proprieta>
                                          <proprieta>
                                                <chiave>id_cliente</chiave>
                                                <valore>xxx</valore>
                                          </proprieta>
                                          <proprieta>
                                                <chiave>formato_file</chiave>
                                                <valore>xxxxx</valore>
                                          </proprieta>
                                    </files>
                                    <proprieta>
```

```
                                        <chiave>formato_parte</chiave>
                                        <valore>xxxxxx</valore>
                                  </proprieta>
                                  <proprieta>
                                        <chiave>numero_parte</chiave>
                                        <valore>x</valore>
                                  </proprieta>
                            </parti>
                            <proprieta>
                                  <chiave>formato_versione</chiave>
                                  <valore>xxxxxx</valore>
                            </proprieta>
                      </versioneOriginale>
                </Documento>
                <Proprieta xmlns="">
                      <item>
                            <chiave>FAMILY</chiave>
                            <valore>xxxxxxxxxx</valore>
                      </item>
                      <item>
                            <chiave>ORGANIZZAZIONE</chiave>
                            <valore>xxxxxxxxxxxx</valore>
                      </item>
                      <item>
                            <chiave>STRUTTURA</chiave>
                            <valore>xxxxxxxxxxx</valore>
                      </item>
                      <item>
                            <chiave>USER_ID</chiave>
                            <valore>xxxxxxxxxxxx</valore>
                      </item>
                </Proprieta>

            </ConsegnaAnticipata>
      </soapenv:Body>
</soapenv:Envelope>
```


Per ulteriori precisazioni circa la ricezione degli oggetti digitali tramite Sistema Web Service si rimanda al documento “Specifiche del servizio web per la consegna anticipata di documenti nel Sistema di conservazione”.

Torna al sommario

6.4 Struttura dati del Pacchetto di archiviazione

Terminato il processo di acquisizione dei Pacchetti di versamento, il prodotto applicativo UniStorage sotto la supervisione del Responsabile del servizio di conservazione e del Responsabile della funzione archivistica provvede alla creazione dei Pacchetti di archiviazione e dell’Indice del pacchetto di archiviazione previsto dallo standard UNI 11386:2010 SInCRO – Supporto all’interoperabilità nella conservazione e nel recupero degli oggetti digitali.
I Pacchetti di archiviazione contengono[10]:

- l’oggetto o gli oggetti da conservare;

[10] Sono elencate le caratteristiche indicate nell’allegato 4 al DPCM 3 dicembre 2013 Regole tecniche in materia di sistema di conservazione.

- l'Indice del Pacchetto di archiviazione, formato secondo le regole dettate dallo Standard UNI 11386:2010 SInCRO – Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali, è composto da:

- il nodo **Self Description** che contiene i seguenti elementi:

  - **ID**: identificatore dell'Indice del pacchetto di archiviazione;
  - **CreatingApplication**: riferimento all'applicazione che ha creato tale indice. Può assumere tre valori: Name, Producer e Version;
  - **SourceIdc**: eventuali riferimenti ad altri Indici di pacchetti di archiviazione dai quali deriva il presente;

- il **nodo VdC**, con informazioni relative al Pacchetto di archiviazione, il quale contiene gli elementi:

  - **ID**: identificatore del Pacchetto di archiviazione;
  - **SourceVdc**: eventuali riferimenti a ad altri Pacchetti di archiviazione dai quali deriva il presente;
  - **VdcGroup**: informazioni relative ad un'eventuale tipologia/aggregazione di natura logica o fisica cui il Pacchetto di Archiviazione appartiene;
  - **MoreInfo**: permette l'introduzione di metadati soggettivi relativi all'Indice del pacchetto di archiviazione individuati dal Soggetto produttore e indicati con un proprio schema nella Scheda cliente allegata al Manuale della conservazione al Contratto.

- Il nodo **FileGroup**, che comprende indicazione di uno o più raggruppamenti di uno o più file contenuti nel Pacchetto di archiviazione, è composto dai seguenti elementi:

  - **Label**: identificativo univoco descrive il documento, lo identificano mediante il numero del documento, l'anno, il registro e il tipo di documento;
  - **File**: descrizione di ogni file facente parte integrante del documento mediante
    - ID inteso come identificatore del documento,
    - Hash calcolato da UniStorage,
    - PreviousHash, se presente, corrisponde all'impronta calcolata dal cliente,
    - MoreInfo, che riporta informazioni sulle operazioni di controllo in base ai criteri scelti dal cliente nella fase di configurazione del servizio;
  - **MoreInfo**: permette l'introduzione di metadati soggettivi relativi ai raggruppamenti di file inclusi nel Pacchetto di archiviazione.

- Il nodo **Process** con le informazioni sul processo di conservazione del Pacchetto di archiviazione, ovvero:
  - **Agent**: indicazione del nome e del ruolo dei soggetti che intervengono nel processo di produzione dei Pacchetti di archiviazione;
  - **TimeReference**: riferimento temporale adottato;
  - **LawAndRegulation**: indicazione dei riferimenti tecnici e normativi ai quali ci si è attenuti per la realizzazione del processo di produzione dei Pacchetti di archiviazione;
  - **MoreInfo:** permette l'introduzione di metadati soggettivi relativi all'Indice del pacchetto di archiviazione individuati dal Soggetto produttore e indicati con un proprio schema nella Scheda cliente allegata al Manuale della conservazione al Contratto.

Si riporta di seguito lo schema xml dell'Indice del Pacchetto di archiviazione:


```
<?xml version="1.0" encoding="UTF-8"?>
<sincro:IdC xmlns:sincro="http://www.uni.com/U3011/sincro/"
xmlns:unimatica="http://www.unimaticaspa.it/unimatica-SinCRO/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.uni.com/U3011/sincro/IdC.xsd
http://www.unimaticaspa.it/unimatica-SinCRO/TagUnimatica.xsd"
sincro:url="http://www.uni.com/U3011/sincro/" sincro:version="1.0">
  <sincro:SelfDescription>
    <sincro:ID sincro:scheme="local">Marca-blocco_497170_1168_FIRMATI_VALIDI_2014-150112-
051727-106773032</sincro:ID>
    <sincro:CreatingApplication>
      <sincro:Name>Unistorage</sincro:Name>
      <sincro:Version>3.1.41</sincro:Version>
      <sincro:Producer>Unimatica SPA</sincro:Producer>
    </sincro:CreatingApplication>
  </sincro:SelfDescription>
  <sincro:VdC>
    <sincro:ID sincro:scheme="local">497170</sincro:ID>
    <sincro:VdCGroup>
      <sincro:Label>xxxxx</sincro:Label>
      <sincro:ID sincro:scheme="local">1168</sincro:ID>
      <sincro:Description>xxxxxx</sincro:Description>
    </sincro:VdCGroup>
    <sincro:MoreInfo sincro:XMLScheme="http://www.unimaticaspa.it/unimatica-
SinCRO/TagUnimatica.xsd">
      <sincro:EmbeddedMetadata>
        <unimatica:UnimaticaInfo>
          <unimatica:VdCInfo>
            <unimatica:Lista-Crl>
              <unimatica:Crl>
                <unimatica:Issuer>xxxxxxxxxxxx</unimatica:Issuer>
                <unimatica:Crl-Number>xxxxxxx</unimatica:Crl-Number>
                <unimatica:File-Name>xxxxxxxx</unimatica:File-Name>
                <unimatica:Progressivo>xxxx</unimatica:Progressivo>
              </unimatica:Crl>
              <unimatica:Crl>
                <unimatica:Issuer>xxxxxxxxxx</unimatica:Issuer>
                <unimatica:Crl-Number>xxxx</unimatica:Crl-Number>
                <unimatica:File-Name>xxxxxx</unimatica:File-Name>
                <unimatica:Progressivo>x</unimatica:Progressivo>
              </unimatica:Crl>
```

```
            </unimatica:Lista-Crl>
            <unimatica:Lista-Certificati-Trusted>
              <unimatica:Certificato-Trusted>
                <unimatica:Issuer>xxxxxxxxxxxx</unimatica:Issuer>
                <unimatica:Serial>xxxxxxxxxxx</unimatica:Serial>
                <unimatica:File-Name>xxxxxx</unimatica:File-Name>
                <unimatica:Progressivo>x</unimatica:Progressivo>
              </unimatica:Certificato-Trusted>
            </unimatica:Lista-Certificati-Trusted>
          </unimatica:VdCInfo>
        </unimatica:UnimaticaInfo>
      </sincro:EmbeddedMetadata>
    </sincro:MoreInfo>
  </sincro:VdC>
  <sincro:FileGroup>
    <sincro:Label>xxxxxxxxxxx</sincro:Label>
    <sincro:File sincro:encoding="base64" sincro:extension="XML.P7M"
sincro:format="application/octet-stream">
      <sincro:ID>xxxxxxxxxxxx</sincro:ID>
      <sincro:Hash sincro:function="SHA-1">rMBhWqRKsvXhvF1W8LUpGlmlksI=</sincro:Hash>
      <sincro:MoreInfo sincro:XMLScheme="http://www.unimaticaspa.it/unimatica-
SinCRO/TagUnimatica.xsd">
        <sincro:EmbeddedMetadata>
          <unimatica:UnimaticaInfo>
            <unimatica:FileInfo>
              <unimatica:Forza-Accettazione>xx</unimatica:Forza-Accettazione>
              <unimatica:Forza-Conservazione>xx</unimatica:Forza-Conservazione>
              <unimatica:Urn>xxxxxxx</unimatica:Urn>
              <unimatica:Esito-File>
                <unimatica:Valore>xxxxxxx</unimatica:Valore>
                <unimatica:Codice>xxxx</unimatica:Codice>
              </unimatica:Esito-File>
              <unimatica:Firme>
                <unimatica:Firma>
                  <unimatica:Codice-Fiscale>xxxxxx</unimatica:Codice-Fiscale>
                  <unimatica:Nome>xxxxx</unimatica:Nome>
                  <unimatica:Cognome>xxxxx</unimatica:Cognome>
                  <unimatica:Esito-Firma>
                    <unimatica:Valore>xxxxxxx</unimatica:Valore>
                    <unimatica:Codice>xxx</unimatica:Codice>
                    <unimatica:Revoca>xx</unimatica:Revoca>
                    <unimatica:Validita-Temporale>xx</unimatica:Validita-Temporale>
                  </unimatica:Esito-Firma>
                  <unimatica:Verifiche>
                    <unimatica:Esito-Verifica unimatica:tipo-verifica="Conservazione"
unimatica:verifica-alla-data="2015-01-12T05:17:28.000">
                      <unimatica:Controllo-Struttura-
Firma>xxxxxxxxxxxx</unimatica:Controllo-Struttura-Firma>
                      <unimatica:Controllo-
Crittografico>xxxxxxxxxxxxxxxxxxxx</unimatica:Controllo-Crittografico>
                      <unimatica:Controllo-
Certificato>xxxxxxxxxxxxxxxxxxxx</unimatica:Controllo-Certificato>
                      <unimatica:Controllo-Catena-
Trusted>xxxxxxxxxxxxxxxxxx</unimatica:Controllo-Catena-Trusted>
                      <unimatica:Controllo-Certificate-Revocation-
List>xxxxxxxxxxx</unimatica:Controllo-Certificate-Revocation-List>
                      <unimatica:Crl-Progressivo>x</unimatica:Crl-Progressivo>
                    </unimatica:Esito-Verifica>
                    <unimatica:Esito-Verifica unimatica:tipo-verifica="Chiusura-Blocco"
unimatica:verifica-alla-data="2015-01-12T05:17:28.000">
                      <unimatica:Controllo-Struttura-
Firma>xxxxxxxxxxxxxxxxx</unimatica:Controllo-Struttura-Firma>
                      <unimatica:Controllo-
Crittografico>xxxxxxxxxxxxxxxxx</unimatica:Controllo-Crittografico>
```

```
                        <unimatica:Controllo-
Certificato>xxxxxxxxxxxxxx</unimatica:Controllo-Certificato>
                        <unimatica:Controllo-Catena-
Trusted>xxxxxxxxxxxxxx</unimatica:Controllo-Catena-Trusted>
                        <unimatica:Controllo-Certificate-Revocation-
List>xxxxxxxxxxxx</unimatica:Controllo-Certificate-Revocation-List>
                        <unimatica:Crl-Progressivo>x</unimatica:Crl-Progressivo>
                      </unimatica:Esito-Verifica>
                    </unimatica:Verifiche>
                    <unimatica:Certificato-Trusted-Progressivo>x</unimatica:Certificato-
Trusted-Progressivo>
                  </unimatica:Firma>
                </unimatica:Firme>
              </unimatica:FileInfo>
            </unimatica:UnimaticaInfo>
          </sincro:EmbeddedMetadata>
        </sincro:MoreInfo>
      </sincro:File>
    </sincro:FileGroup>
    <sincro:Process>
      <sincro:Agent sincro:type="organization" sincro:role="PreservationManager">
        <sincro:AgentName>
          <sincro:FormalName>Unimatica SPA</sincro:FormalName>
        </sincro:AgentName>
        <sincro:Agent_ID sincro:scheme="TaxCode">xxxxxxx</sincro:Agent_ID>
      </sincro:Agent>
      <sincro:TimeReference>
        <sincro:AttachedTimeStamp sincro:normal="2015-01-12T08:35:10+01:00"/>
      </sincro:TimeReference>
      <sincro:MoreInfo sincro:XMLScheme="http://www.unimaticaspa.it/unimatica-
SinCRO/TagUnimatica.xsd">
        <sincro:EmbeddedMetadata>
          <unimatica:UnimaticaInfo>
            <unimatica:ProcessInfo>
              <unimatica:Blocca-Crl-Scadute unimatica:time="0">xx</unimatica:Blocca-Crl-
Scadute>
              <unimatica:Catena-Trust>si</unimatica:Catena-Trust>
              <unimatica:Certificato-Valido>xx</unimatica:Certificato-Valido>
              <unimatica:Controllo-Crl>si</unimatica:Controllo-Crl>
              <unimatica:Verifica-Crittografica>xx</unimatica:Verifica-Crittografica>
              <unimatica:Verifica-Timestamp>si</unimatica:Verifica-Timestamp>
            </unimatica:ProcessInfo>
          </unimatica:UnimaticaInfo>
        </sincro:EmbeddedMetadata>
      </sincro:MoreInfo>
    </sincro:Process>
</sincro:IdC>
```


Torna al sommario

6.5 Struttura dati del Pacchetto di distribuzione

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

L'esibizione del materiale di interesse avviene mediante memorizzazione su supporto ottico. La descrizione dettagliata delle procedure è indicata nel capitolo 7 "Il processo di erogazione del servizio di conservazione", Fase 6.
I Pacchetti di distribuzione coincidono con i Pacchetti di archiviazione, come previsto delle Regole tecniche in materia di sistemi di conservazione, ma saranno corredati di informazioni aggiuntive

necessarie per la creazione dei DVD, CD, ecc. nel caso di richiesta di esibizione da parte dell'Utente.

UniStorage consente la produzione di supporti rimovibili che possono essere forniti all'Utente.
In ogni supporto vengono trasferiti dei Pacchetti di distribuzione chiamati "Registrazioni", contenenti sia gli oggetti che l'insieme delle evidenze di conservazione.
La registrazione generata è auto-esplicativa, intendendo con questo che i dati sono affiancati da indici e informazioni di riferimento tali da poter permettere la comprensione del contenuto anche da programmi esterni al sistema di conservazione.
La registrazione è contenuta in una directory, il cui nome contiene un'indicazione del blocco dei documenti e data/ora dell'inizio della creazione della registrazione stessa.

Contenuto della directory della registrazione:

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

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

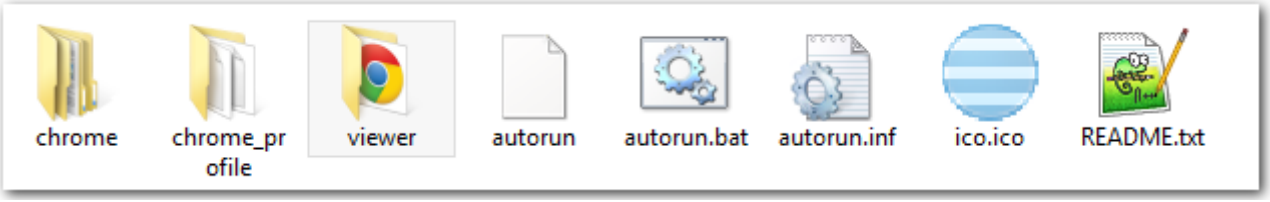


Figura 4 - Struttura volumi

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

Torna al sommario

7. Il processo di erogazione del servizio di conservazione

Il processo di conservazione eseguito da UNIMATICA S.p.A. adotta il modello standard OAIS - Open Archival Information System[11] che definisce concetti e funzionalità degli archivi digitali. Lo schema seguente illustra brevemente gli aspetti principali di un generico processo di conservazione: il Soggetto produttore invia il Pacchetto di versamento, di cui ha piena responsabilità, al Soggetto conservatore il quale provvede a trasformarlo in Pacchetto di archiviazione. Ai fini dell'esibizione e della distribuzione richiesti dalla comunità di riferimento[12], il Soggetto conservatore provvederà a creare i Pacchetti di distribuzione in una forma tale che venga garantita la corretta visualizzazione di questi.

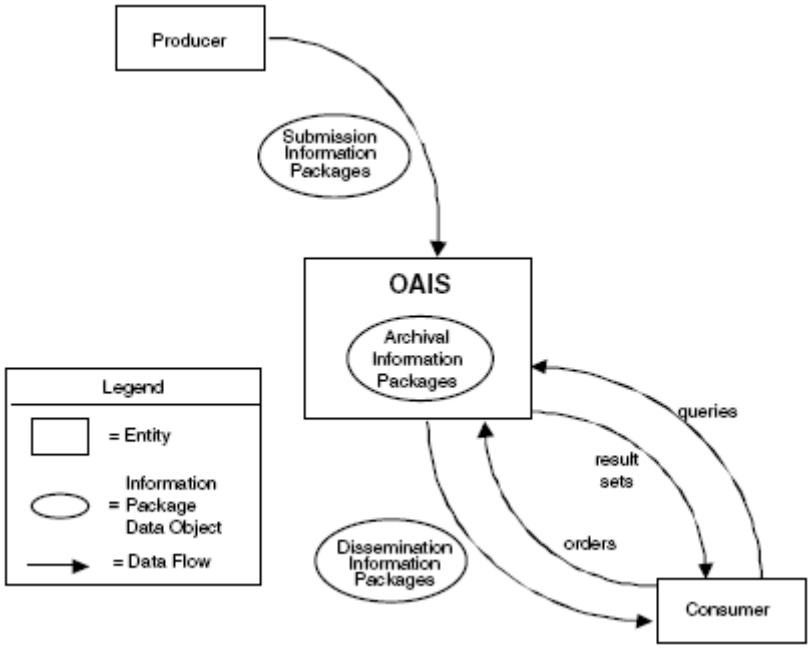


Figura 5 Modello OAIS

Torna al sommario

7.1 Il processo di conservazione

Il servizio offerto da UNIMATICA S.p.A. ad ogni Soggetto produttore viene avviato al termine di un processo di attivazione che segue queste fasi fondamentali:

[11] L'Open Archival Information System è lo standard ISO per la conservazione a lungo termine di archivi digitali.
[12] Comunità di riferimento: il sottoinsieme degli utenti in grado di comprendere autonomamente l'informazione archiviata nella forma in cui è conservata e resa disponibile dall'OAIS

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

Ognuno degli step sopra indicati viene eseguito per ogni tipologia di configurazione richiesta.
Di seguito vengono dettagliate le fasi:

Torna al sommario

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

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

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

- ragione sociale;
- indirizzo;
- partita iva;
- e-mail;
- oggetti documentali gestiti;
- interoperabilità tra sistema del Soggetto produttore e sistema di conservazione;
- tipo di protocollo da utilizzare per lo scambio dei Pacchetti.

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

- i volumi in termini di numero documenti annui previsti da gestire e spazio di occupazione previsto per i dati da Conservare (GB);
- la dimensione massima del Pacchetto di versamento;
- la frequenza di invio dei Pacchetti;
- l'eventuale richiesta di invio di supporti ottici (DVD) di conservazione con la definizione della relativa frequenza.

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

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

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

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

Torna al sommario

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

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

- **identificazione certa del Soggetto produttore**;

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

- verifica che i **formati** degli oggetti da conservare siano conformi con quanto dichiarato nel modulo 'Scheda cliente' e nell'allegato 2 al Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 Regole tecniche in materia di sistema di conservazione e dichiarati nel presente Manuale;
- verifica che i **metadati** siano conformi con i set minimi dichiarati nel modulo 'Scheda cliente' e nell'allegato 5 al Decreto della Presidenza del Consiglio dei Ministri 3 dicembre 2013 Regole tecniche in materia di sistema di conservazione e dichiarati nel presente Manuale.

Torna al sommario

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

L'esito positivo delle verifiche effettuate sui Pacchetti di versamento viene registrato in un Rapporto di versamento di presa in carico. Il Rapporto conterrà un'impronta del file originale comprensivo di algoritmo con la quale tale impronta viene calcolata (hash) e un riferimento temporale certificato che costituisce evidenza dell'esistenza e dell'esatta composizione del Rapporto collegato all'istante indicato (Tcons).
Apponendo un timestamp al Rapporto di versamento, lo si "sigilla" e contemporaneamente si fissa il riferimento temporale. Tale procedimento costituisce un riferimento temporale certificato per il Rapporto di versamento.
Il Rapporto di versamento attesta la corretta esecuzione del processo di immissione dei Pacchetti, ha la funzione di raccogliere evidenze indirette di tutti i documenti del Pacchetto e garantisce due principali funzioni:

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

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

La modalità di conservazione mediante Rapporto di versamento permette di verificare l'integrità di ogni singolo file, a prescindere da tutti gli altri file conservati nello stesso pacchetto. Infatti sarà sufficiente essere in possesso di un file "candidato" e conoscere il suo URN identificativo per poter eseguire la funzione di hash e confrontare l'impronta ricalcolata con la stringa riportata nel Rapporto.
In questa fase vengono associate all'indice tutte le evidenze di autenticità delle firme digitali che verranno verificate all'istante del riferimento temporale:

- i certificati di firma di tutte le firme presenti nel Pacchetto di versamento,
- tutti i certificati appartenenti alle catene di certificazione (trusting chain),

- le liste di revoca dei singoli certificati (CRL).

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

Torna al sommario

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

Le verifiche effettuate sui Pacchetti di versamento possono risultare negative. Nei casi in cui anche solo su uno dei controlli indicati nella fase 2 si dovesse riscontrare una mancanza o non corrispondenza di informazioni viene generato un file di Comunicazione delle anomalie che verrà comunicato mediante un file di esito al Soggetto produttore. Tale Comunicazione comprenderà i dettagli delle verifiche eseguite sui Pacchetti di versamento comprensive delle precisazioni sulle anomalie. Le anomalie, in relazione a quanto descritto nella fase 2, possono essere identificate nella mancata corrispondenza di ciò che viene versato a quanto dichiarato dal Soggetto produttore nella Scheda cliente in termini di firma digitale, formati e metadati.

Sulla Comunicazione delle anomalie verrà apposto un riferimento temporale e conservata così come viene conservato il Rapporto di versamento.

Torna al sommario

7.6 Preparazione e gestione dei Pacchetti di archiviazione

I Pacchetti versati in UniStorage, con la supervisione del Responsabile del servizio di conservazione e del Responsabile della funzione archivistica vengono raggruppati in Pacchetti di archiviazione. Questi pacchetti vengono assemblati dal sistema nei tempi e con i criteri di raggruppamento scelti e concordati con il Soggetto produttore, indicati nella Scheda Cliente (ad es. Pacchetti di archiviazione per tipologie documentali o in base alla cadenza temporale di consegna).
Il processo di costruzione dei Pacchetti di archiviazione, così come previsto dallo standard SInCRO UNI 11386:2010 – Supporto all'interoperabilità nella conservazione e nel recupero degli oggetti digitali, avviene con le seguenti modalità:

- individuazione dei documenti destinati a far parte del Pacchetto di archiviazione sulla base dei criteri scelti. Tali criteri vengono concordati con il cliente e sono definiti nella Scheda Cliente allegata al Manuale della conservazione e si possono basare sia su caratteristiche legate allo stato del documento, sia su sui metadati minimi indicati nell'allegato 5 al Decreto del presidente del consiglio dei ministri Regole tecniche in materia di sistemi di conservazione. Un esempio del primo tipo di caratteristiche può essere lo stato della firma: firmato valido, non firmato, firmato invalido;
- i Pacchetti di archiviazione vengono chiusi in seguito a due tipi di regole:
    - automatiche: impediscono ad un documento di scadere una volta inserito in un Pacchetto di archiviazione. Questa tipologia di regole ha la precedenza su quelle descritte nel punto successivo, le quali riguardano la dimensione massima del

Pacchetto di archiviazione e il tempo limite oltre il quale un Pacchetto di archiviazione deve essere forzatamente chiuso,

- attuate dal Responsabile del servizio di Conservazione in accordo con il Soggetto produttore: definite nella Scheda Cliente allegata al Manuale della conservazione.

Nei casi in cui i Pacchetti di archiviazione contengano referti sanitari, questi vengono crittografati mediante crittografia simmetrica con chiave AES a 1024 bit.
I Pacchetti di archiviazione vengono sottoscritti con firma digitale dal Responsabile del servizio di conservazione e marcati temporalmente.
La sottoscrizione dei Pacchetti di archiviazione effettuata da UNIMATICA S.p.A. attesta esclusivamente la corretta esecuzione del processo di conservazione secondo la normativa vigente in materia di conservazione. UNIMATICA S.p.A. non è responsabile dell'errato contenuto informativo degli oggetti versati.

Torna al sommario

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

La gestione dei Pacchetti di distribuzione fa capo al Responsabile del Servizio di Conservazione, al Responsabile della Funzione archivistica e al Responsabile del trattamento dei dati personali.

La produzione di Pacchetti di distribuzione avviene in seguito alla richiesta da parte dell'Utente, così come indicato all'art. 9, c.1, lett. h). Tali Pacchetti, però, posso differire nei casi in cui l'utente richiede l'esibizione tramite supporto ottico in quanto questo dovrà necessariamente contenere elementi utili all'avvio del supporto e alla visualizzazione dei contenuti informativi.

UniStorage, prevedendo la conservazione dei Pacchetti di archiviazione firmati, implementa un formato di composizione delle marche tale da permettere l'esibizione probatoria di un singolo documento. Quindi, ogni singolo file può essere esibito insieme ai suoi metadati, registrati nel data base, e alle sue prove di conservazione in maniera assolutamente INDIPENDENTE dagli altri documenti.
UNIMATICA S.p.A. permette l'accesso ai Pacchetti di distribuzione esclusivamente agli utenti autorizzati. I livelli di accesso vengono definiti in base alle esigenze delle richieste effettuate, rendendo disponibile soltanto il materiale richiesto grazie all'utilizzo di filtri predefiniti che selezionano i canali previsti per la visualizzazione di un determinato pacchetto.

È possibile visualizzare i documenti tramite duplice canale:

- via web: i Soggetti produttori titolari dei documenti potranno ricercare e visualizzare tutti i documenti conservati direttamente sul portale di UNIMATICA S.p.A. attraverso l'apposita funzionalità. L'accesso avviene tramite il portale al quale è demandata la sicurezza e la gestione della sessione. I documenti saranno disponibili per l'esibizione on-line per tutto il periodo di conservazione. La descrizione di dettaglio dell'interfaccia web per le richieste di esibizione dei documenti è contenuta nell'allegato 'Manuale dell'interfaccia web'. Vengono inoltre resi disponibili servizi web (Web Services) per le eventuali integrazioni con i portali dei Soggetti produttori.

- copia del documento su supporto ottico. La descrizione dettagliata circa la visualizzazione dei Pacchetti di distribuzione mediante supporto ottico è presente nel capitolo 6 Oggetti sottoposti a conservazione, paragrafo 6.5.

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

Torna al sommario

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

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

Nei casi in cui, come previsto dall'art. 23-bis, c. 2 del Codice dell'Amministrazione Digitale[13] il Soggetto produttore richieda la presenza di un pubblico ufficiale, UNIMATICA S.p.A. garantirà tale presenza mettendo a disposizione tutte le necessarie risorse che serviranno all'espletamento delle attività, rimandando in ogni caso la scelta al Soggetto produttore al quale saranno addebitate le spese.

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

Torna al sommario

7.9 Scarto dei Pacchetti di archiviazione

Sette mesi prima della scadenza del periodo di conservazione dei documenti, UNIMATICA S.p.A. comunica al Soggetto produttore, in modalità certa, che in assenza di ulteriori comunicazioni, trascorsi i termini previsti, provvederà alla cancellazione dei documenti.
In caso di proroga della conservazione, UNIMATICA S.p.A. rinnova la marca temporale sui documenti per il periodo richiesto (uno o più anni).

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

Lo scarto dei Pacchetti di archiviazione in caso di pacchetti versati da Pubbliche amministrazioni avviene previa autorizzazione della Soprintendenza archivistica così come prevede la normativa vigente in materia.
I tempi di scarto vengono dettati dal Soggetto produttore mediante il proprio Massimario di selezione. Il Soggetto produttore è tenuto a compilare un lista del materiale che intende scartare e a sottoporre tale lista alla Soprintendenza archivistica competente la quale rilascerà il nulla osta alla procedura di scarto.
UNIMATICA S.p.A. permette al Soggetto produttore l'accesso diretto ai Pacchetti mediante un'apposita interfaccia attraverso la quale potrà selezionare direttamente i Pacchetti che intende scartare. Come prova di tale processo, UNIMATICA S.p.A. rilascerà un rapporto di scarto che verrà firmato dal Soggetto produttore e controfirmato da UNIMATICA e sul quale verrà apposta una marca temporale così da provare quali Pacchetti siano stati scartati. Il rapporto di scarto viene conservato all'interno del sistema UniStorage.

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

Una volta rilasciato il rapporto di scarto, verranno fisicamente eliminati i Pacchetti e le relative prove di conservazione.

Torna al sommario

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

Il sistema di conservazione di UNIMATICA S.p.A., in caso di acquisizione del servizio da parte di un altro Soggetto conservatore è in grado di gestire la presa in carico di Pacchetti di versamento coincidenti con i Pacchetti di archiviazione. Per assicurare, inoltre, interoperabilità e trasferibilità ad altri conservatori in caso di chiusura del contratto per scelta del Soggetto produttore, UNIMATICA S.p.A. crea Pacchetti di distribuzione coincidenti con quelli di archiviazione, così come indicato all'art. 9, comma 1, lettera h) delle Regole tecniche in materia di sistema di conservazione.

Torna al sommario

7.11 Chiusura del contratto

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

1. Invio dell'originale cartaceo con firma autografa tramite posta all'indirizzo:
   Unimatica S.p.A.
   Via Cristoforo Colombo, 21
   40131 Bologna

2. Invio dell'originale firmato digitalmente dal rappresentante legale, all'indirizzo di posta elettronica certificata (PEC): fatturaelettronica@pec.unimaticaspa.it

Il soggetto produttore che intende disdire il servizio di conservazione a norma dei documenti digitali affidato alla società Unimatica S.p.A. può scegliere di:

- mantenere la conservazione a norma dei documenti digitali già versati in conservazione fino al termine precedentemente concordato mantenendo la possibilità di utilizzare le credenziali di accesso al sistema per i soli scopi di consultazione

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

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

Torna al sommario

8. Procedure di gestione e di evoluzione

A coordinare la gestione del sistema, l'aggiornamento di questo e le procedure di adeguamento all'evoluzione tecnologica è la figura del Responsabile sviluppo e manutenzione che esegue una costante attività di controllo dell'attività di conservazione in conformità agli standard di qualità e sicurezza ISO 9001 e ISO 27001.
Affinché venga garantito un controllo totale sul sistema e un buon funzionamento di questo, le attività di manutenzione vengono svolte sia sui processi che sulle strutture hardware e software e viene condotta una quotidiana verifica delle attività sulle infrastrutture parallelamente ad una pianificazione delle eventuali procedure straordinarie da condurre in caso di anomalie.

Torna al sommario

8.1 Misure di sicurezza logica

Il presente paragrafo ha l'obiettivo di descrivere le misure di sicurezza adottate per l'erogazione del Servizio e per la protezione dei dati che fanno riferimento al Piano per la sicurezza del sistema di conservazione di UNIMATICA S.p.A. In particolare, verranno descritte:

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

Torna al sommario

8.1.1 Gestione utenze

La policy di riferimento per la gestione delle utenze applicative e di sistema adottata da UNIMATICA S.p.A. prevede che le utenze siano rilasciate da un ente (o persona) differente dall'ente o persona che le utilizzerà.
Nell'ambito del servizio di conservazione, le utenze applicative e di sistema sono gestite secondo i criteri che seguono le misure minime di sicurezza di cui all'allegato B del D. Lgs 196/2003, in ottemperanza alla policy di UNIMATICA S.p.A.:

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

- non può contenere l'username invertito,
- non può' contenere porzioni della data di nascita,
- non può' contenere due (o più) caratteri uguali consecutivi,
- non può' essere una delle ultime 5 utilizzate;

- La scadenza della password è configurabile attraverso un parametro;
- il sistema deve forzare l'utente a cambiare la password al primo utilizzo;
- il sistema deve avvertire l'utente della necessità di rinnovare la password;
- l'utenza deve essere disabilitata in seguito a ripetuti tentativi di accesso non andati a buon fine;

- Applicazione del principio 'segregation of duty' nel rilascio delle credenziali (utente, password e profilo), vale a dire separazione tra chi rilascia e chi utilizza le credenziali di accesso ai dati;
- Applicazione del principio 'need to know' nel rilascio dei profili, vale a dire rilascio dei soli diritti per eseguire le attività di competenza;
- Assegnazione ad ogni utente di credenziali (user e password) personali, uniche e non assegnabili ad altri utenti;
- Revisione periodica degli utenti e dei relativi profili.

Torna al sommario

8.1.2 Gestione sistemi di protezione

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

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

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

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

8.1.3 Gestione degli incidenti di sicurezza

Gli incidenti di sicurezza (e più in generale tutti gli incidenti che avvengono) sono segnalati al servizio Service Desk aziendale tramite uno strumento elettronico di Help Desk (OTRS - Open-source Ticket Request System). Obbiettivo del servizio di Service Desk è:

- ripristinare la normale operatività del servizio (processo di produzione) il più rapidamente possibile, minimizzando l'impatto negativo sull'operatività, nel rispetto degli SLA concordati;
- soddisfare le richieste dei Soggetti produttori nell'ambito dell'utilizzo dell'infrastruttura tecnologica in ambiente di produzione;
- identificare le corrette modalità di escalation verso i livelli superiori del management.

Gli addetti del servizio Service Desk, prendono in carico le richieste e, in base ad una valutazione della gravità, seguendo la procedura di incident management definita, possono decidere di:

- gestire e risolvere direttamente il problema e chiudere la richiesta;
- scalare il problema al supporto tecnico di 2° livello e seguirne lo sviluppo;
- in caso di incidente grave (disastro) attivare l'unità di crisi preposta tramite chiamata telefonica al Responsabile della sicurezza dei sistemi che coordina le azioni di comunicazione e operative.

Ogni attività di questo tipo è tracciata in modo da poter evidenziare tempi di risposta, tempi e modalità di risoluzione, autori della risoluzione.
Nel caso specifico di incidenti di sicurezza viene eseguita una analisi sul tipo di incidente e viene deciso se:

- archiviare il fatto per successive statistiche;
- eseguire analisi più approfondite (forensic analisys) con coinvolgimento del Responsabile della sicurezza dei sistemi;
- attivare enti giuridici di controllo (autorità sulla privacy, polizia postale).

Torna al sommario

8.1.4 Gestione dei backup e Disaster Recovery

Il sistema di backup è organizzato in differenti modalità in relazione alle informazioni da salvare:
le funzionalità di Backup e Restore dei dati e delle configurazioni, sono state implementate utilizzando il software Tivoli Storage Manager (TSM), il cui client è stato installato su tutti i sistemi virtuali. Il server TSM utilizza la piattaforma Storage EMC-DL4100, costituita da due librerie di nastri virtuali (Virtual Tape Library) sul sito di Settimo Torinese e Moncalieri.
La funzionalità di backup sulla base dati è stata implementata utilizzando Oracle RMAN, con cadenza giornaliera e settimanale.

Vengono effettuate le seguenti policy di salvataggio:

- Backup Full settimanale e incrementale giornaliero (utilizzando RMAN)
- Copia mensile con retention 1 anno
- Copia annuale

- il salvataggio dei documenti su CD-ROM con consegna al Soggetto produttore, può essere eseguito su richiesta;
- il salvataggio dell'applicazione sia server che client è realizzato su supporto fisico esterno (Data tape o CD-ROM) per eseguire una rapida reinstallazione in caso di necessità;
- i supporti di backup hanno rotazione con frequenza settimanale.

Per le attività di salvataggio si eseguono i seguenti controlli:

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

I servizi di conservazione di Unimatica sono erogati tramite un Data Center Primario ed un Data Center Secondario che svolge il compito di Backup Remoto e di Disaster Recovery (D/R), al fine di garantire gli opportuni livelli di continuità del servizio.
I due Data Center hanno una distanza fra loro superiore a 300 Km. e la disponibilità di servizio è H24 per entrambi.
Il Data Center secondario permette di usufruire dei servizi in Produzione anche in caso di indisponibilità del Data Center Primario.
Per questo servizio Unimatica definisce con il Cliente il livello dei parametri che caratterizzano il servizio di D/R e di continuità operativa.

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

Torna al sommario

8.1.5 Gestione dei supporti di memorizzazione

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

- i media di memorizzazione elettronica sono correttamente etichettati in modo da fornire le seguenti informazioni: tipologia del media, tecnica della scrittura, data delle scrittura, contenuto. Per tecnica della scrittura si intende il formato in cui il media è stato preparato, nel nostro caso formato ISO, dipendentemente dal tipo supporto (CD o DVD);
- in caso di media che vengano riutilizzati per altri dati, essi vengono preventivamente riformattati tramite le tecniche di formattazione a basso livello, allo scopo di evitare che le informazioni ed i dati in essi contenuti possano essere presi e divulgati a soggetti non autorizzati;
- nel caso in cui i dati registrati sui media non più utilizzati non possano essere definitivamente cancellati si procede alla distruzione del media stesso, impedendone quindi il riutilizzo;

- i media sui quali sono eseguiti i salvataggi aziendali sono conservati in una sede differente rispetto a quella dove sono le strumentazioni cui i salvataggi si riferiscono ed in un luogo non accessibile se non al personale autorizzato,
- periodicamente è eseguita una verifica dei media e della disponibilità degli strumenti di accesso ai medesimi. In caso che per qualche media sia verificata la non disponibilità (anche prevista nel breve futuro) degli strumenti di accesso a qualche media si procede allo svecchiamento dei media tramite riversamento del loro contenuto in altro media.

Torna al sommario

8.2 Procedure di evoluzione e Change management

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

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

Il Responsabile del servizio di conservazione e il Responsabile della sicurezza dei sistemi informativi periodicamente si occuperanno di aggiornare la normativa e gli standard di riferimento in base all'evoluzione di questi.
La dettagliata descrizione delle procedure di evoluzione è riportata nel paragrafo 3.2.2 del documento "Piano della sicurezza del sistema di conservazione".

Torna al sommario

9. Monitoraggio e controlli

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

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

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

I log file degli applicativi contengono almeno le seguenti informazioni:

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

I file di log non sono modificabili o eliminabili da parte degli Utenti che usano il sistema (che non dispongono dei diritti di accesso).
I log di sistema sono analizzati da parte dei sistemisti qualora si rendesse necessaria un'indagine a seguito di un malfunzionamento del sistema.
La dettagliata descrizione dei processi relativi alle attività di monitoraggio e controlli è riportata nel documento "Piano della sicurezza del sistema di conservazione", capitolo 3.
I log vengono successivamente inviati in conservazione per mantenere traccia delle comunicazioni tra Soggetto produttore e sistema di conservazione.

Torna al sommario

9.1 Audit interni e Verifica dell'integrità degli archivi

Le verifiche ispettive interne vengono pianificate dal Responsabile sviluppo e manutenzione del sistema di conservazione, dal Responsabile sicurezza dei sistemi per la conservazione in accordo con il Responsabile del servizio di conservazione tenendo conto dello stato e dell'importanza dei processi e delle aree oggetto di verifica, nonché dei risultati delle precedenti verifiche. La frequenza con la quale vengono disposte le verifiche ispettive interne è almeno annuale. Al termine delle verifiche viene predisposto il relativo verbale di verifica.

I verbali di verifica possono essere consultati dal Soggetto produttore facendo richiesta al Responsabile del sistema di conservazione e al Responsabile sviluppo e manutenzione.
La scelta del personale verificatore viene fatta in modo da garantire obiettività ed imparzialità nel processo di verifica.
Il libro delle comunicazioni e dei verbali delle verifiche periodiche allegato al Manuale, che UNIMATICA S.p.A. mantiene aggiornato, tiene traccia di:

- verifiche periodiche sullo stato di conservazione dei supporti di memorizzazione, tendenti a verificare con l'ausilio di software appropriati, lo stato di conservazione dei supporti di memorizzazione e a ricercare eventuali difetti,
- verifiche periodiche sui documenti conservati, tendenti a verificare periodicamente, con cadenza non superiore a cinque anni, l'effettiva integrità dei documenti stessi. La procedura che gestisce il processo di conservazione presenta delle funzionalità di controllo massivo dei dati conservati: tali tipologie di controllo consistono nell'impostare/configurare a livello informatico la periodicità dei controlli da effettuare; attualmente, il sistema è configurato per verificare giornalmente un milione di documenti, eseguendo controlli a rotazione su documenti diversi. L'applicazione informatica che gestisce il processo di conservazione, effettua un check automatico loggando per ogni Pacchetto conservato, la data/ora in cui è stata eseguita l'ultima verifica di integrità. Il sistema segnala eventuali difettosità sulla console di sistema. Nel caso ciò si verifichi le figure responsabili competenti dovranno preoccuparsi di recuperare la copia di backup ed effettuarne immediatamente la duplicazione. Tale verifica viene eseguita sia sui dati contenuti nell'archivio digitale on-line (sito primario) che sui dati presenti nell'archivio digitale in Disaster Recovery (sito secondario).

Il "libro delle comunicazioni e dei verbali delle verifiche periodiche" contiene le seguenti informazioni:

- variazioni Famiglie documentali oggetto di conservazione
- variazioni normative
- registro delle variazioni di ruoli e funzioni dei soggetti coinvolti nel processo di conservazione
- registro delle variazioni del processo di conservazione
- registro delle comunicazioni all'Agenzia delle Entrate
- registro delle edizioni del Manuale della conservazione
- scadenziario delle comunicazioni
- registro delle comunicazioni effettuate
- registro delle modifiche all'archivio
- registro delle anomalie
- registro dei riversamenti diretti o sostitutivi
- piano delle verifiche
- registro delle verifiche ispettive
- registro dei documenti distrutti

Torna al sommario

9.2 Gestione delle anomalie

UNIMATICA S.p.A. gestisce le anomalie attraverso l'utilizzo di due funzioni aziendali che fanno parte del settore tecnico di UNIMATICA: il Service desk e l'AM Settore conservazione e Settore sistemi.
Le suddette funzioni garantiscono la gestione di tutte le anomalie relative al servizio di Conservazione assicurando due tipologie di interventi:

- interventi **reattivi** a fronte delle segnalazioni degli utenti;
- Interventi **proattivi** a fronte di generazioni spontanee di eventi e segnalazioni generati dai sistemi di monitoraggio infrastrutturale e applicativo.

Le anomalie sono gestite attraverso l'utilizzo del processo di Incident Management di UNIMATICA, il cui processo è rappresentato dal seguente schema funzionale:

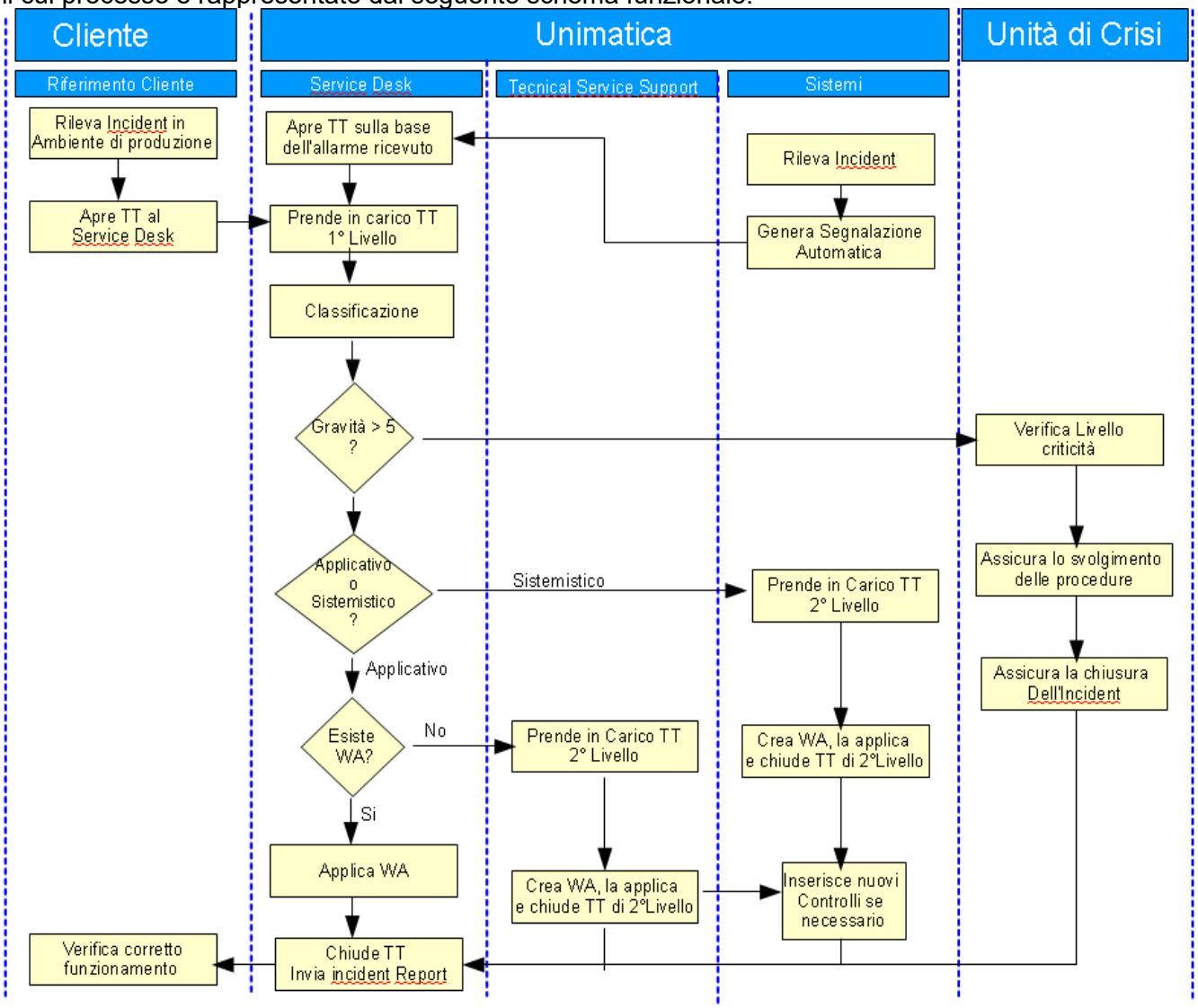


Figura 6 - Schema funzionale

Di seguito vengono descritti gli step del processo più significativi:

1. apertura e presa in carico della segnalazione al Service Desk UNIMATICA;
2. classificazione dell'Incident secondo il livello di criticità, macrotipologia e livello di competenza IT;
3. implementazione workaround, soluzione Incident;
4. compilazione Incident Report.

Fase 1:
il Service Desk UNIMATICA prende in carico la segnalazione dell'incident, che può provenire dal Soggetto produttore o dai sistemi, tracciandolo sul sistema di Trouble Ticketing e verificando se sono correlabili eventi di Tipo Critical segnalati in quel momento.

Fase 2:
Il Service Desk classifica l'incident secondo i parametri di criticità segnalati e/o rilevati secondo l'area di competenza e verifica la possibilità di applicare autonomamente il workaround necessario per risolvere l'Incident.

Fase 3:
Nel caso in cui esista un workaround da applicare, il Service Desk UNIMATICA la applica, notifica la soluzione dell'incident all'utente che ha segnalato l'anomalia attendendo la conferma relativa alla soluzione applicata.
Nel caso in cui non esista un workaround applicabile, il Service Desk UNIMATICA inoltra il problema al secondo livello specialistico, sia esso applicativo (Service Support) o infrastrutturale (Sistemi). Il Secondo livello specialistico definisce il workaround necessario e lo implementa notificando la chiusura dell'intervento al Service Desk UNIMATICA.
Il Secondo livello specialistico valuta se è necessario implementare nuove sonde di monitoraggio in Control Room, in caso affermativo le implementa e le rende operative.

Fase 4:
Al termine dell'intervento viene fornito un Incident Report contenente questo set minimo di informazioni:

- Data/Ora Segnalazione Anomalia;
- Descrizione dell'anomalia Segnalata;
- Data/Ora Presa in Carico Anomalia;
- Descrizione problema tecnico rilevato;
- Data/Ora Chiusura Anomalia;
- Tipo di WA Applicata (se di 1° o 2° Livello) e descrizione WA;
- Necessità di implementare una soluzione definitiva (Si/No);
- Descrizione Soluzione Definitiva;
- Tempi di implementazione.

Torna al sommario

9.3 Reportistica di servizio

Il sistema di conservazione UniStorage gestisce un sistema di tracciatura nel quale vengono registrati tutti i singoli eventi che riguardano sia la gestione dei Pacchetti, dalla fase di versamento a quella di distribuzione, sia i singoli documenti. Questa tracciatura, costruita per implementare un

“forensic log”, è in un formato rigido e non disabilitabile. La tracciatura è prerequisito indispensabile per l’esecuzione delle operazioni.
Nel dettaglio, il sistema di log prevede la registrazione di informazioni relative alle diverse funzioni del processo di conservazione per tutte le fasi descritte nel capitolo 7 “Il processo di erogazione del servizio di conservazione”.

La reportistica di servizio che UNIMATICA gestisce è di due Tipologie:

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

Tipologia 1:
vengono prodotti periodicamente i seguenti report:

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

Tipologia 2:
viene prodotto un report di Servizio che fornirà le seguenti evidenze:

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

Periodicità: Semestrale

Torna al sommario

10. La server farm di Unimatica

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

Lo schema seguente rappresenta l'implementazione hardware/software dell'architettura di conservazione presso i siti di Settimo Torinese e Firenze, nei quali sono allocati i data center, rispettivamente Primario e Secondario:

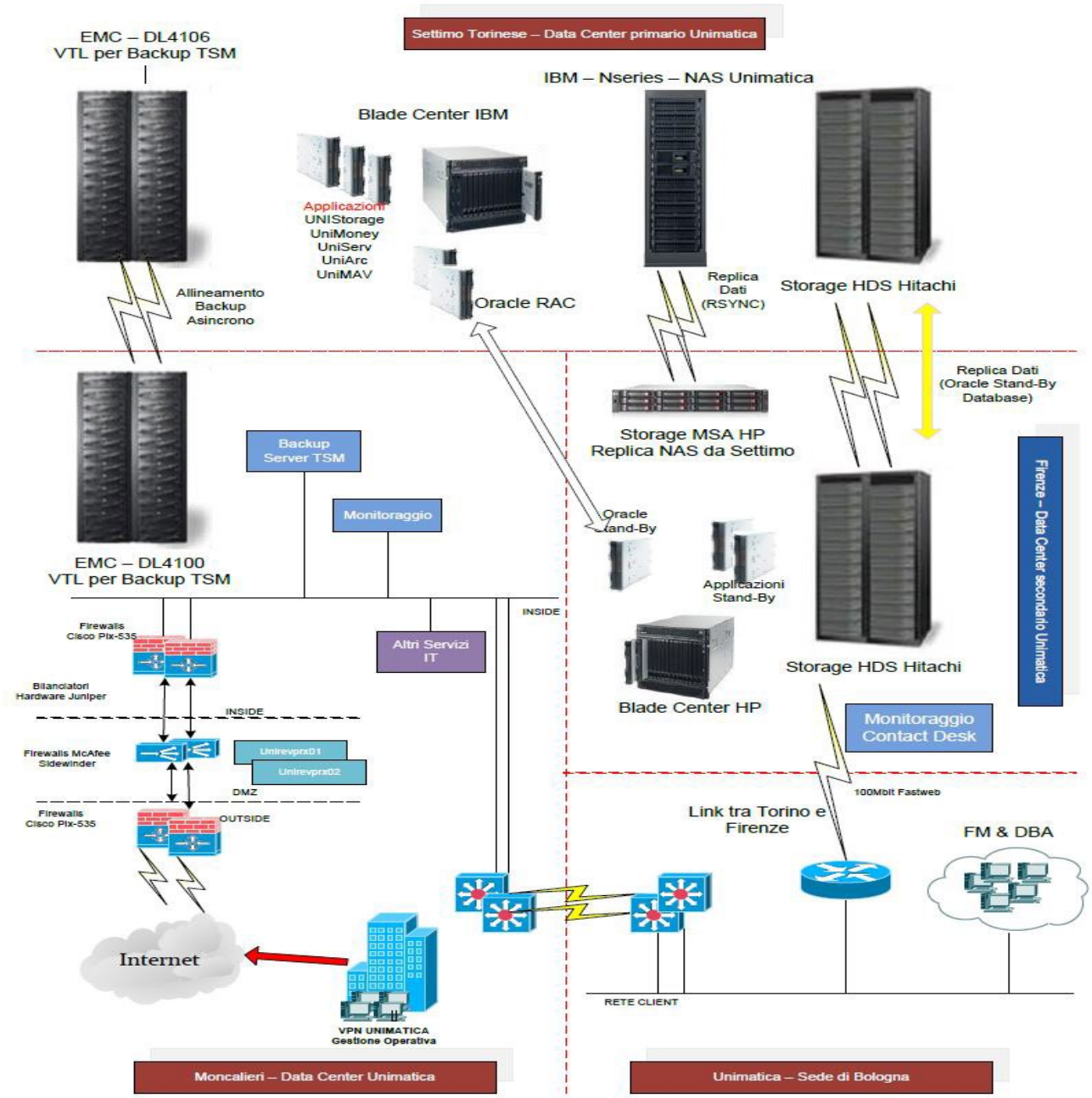


Figura 7 - Architettura di conservazione

Torna al sommario

10.1 UniStorage - Il sistema per la conservazione

Il sistema software utilizzato per la gestione del processo di conservazione dei documenti digitali è costituito dal prodotto applicativo UniStorage.
UniStorage, sviluppato internamente e totalmente da UNIMATICA S.p.A., è un sistema integrato e completo per la conservazione dei documenti digitali che viene fornito in modalità Outsourcing/ASP/SaaS congiuntamente a tutti i servizi di gestione e supporto correlati, oppure in modalità pacchetto applicativo, installando le applicazioni presso il Data Center del Soggetto produttore.
I servizi offerti, oltre che di tipo applicativo e tecnologico, comprendono tutto il necessario supporto normativo, organizzativo e contrattuale (deleghe, privacy, ecc.).

UniStorage esegue la conservazione nel tempo dei documenti sottoscritti con firma digitale e rispetta il 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 e presenta le seguente caratteristiche generali:

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

garantendo:

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

Il sistema è progettato per partizionare in maniera opportuna i dati gestiti al fine di garantire la separazione per contesto organizzativo e la consistenza dei dati. Il partizionamento opera tra i dati di Aziende diverse o di diversi dipartimenti o uffici afferenti ad una stessa Azienda (Aree Organizzative Omogenee). I Pacchetti versati provenienti anche da flussi diversi di conservazione, vengono mantenuti separati tramite una chiave primaria che li identifica, fin dal loro ingresso in conservazione, come appartenenti ad una data AOO e non ad un'altra. Il sistema di partizionamento è direttamente collegato al sistema di controllo degli accessi e tracciatura, viene quindi garantita la riservatezza dei dati presenti in archivio.
UniStorage è una applicazione Web a tre livelli (desktop, application e database) e utilizzabile da posti di lavoro dotati di sistema operativo Windows o Linux, per mezzo di browser standard quali ad esempio Internet Explorer vers. 11 o superiore, Mozilla Firefox 3.6 o superiore, Google Chrome 11.0.696.7 o superiore, Apple Safari 5.0.5 o superiore. Per le postazioni che dovranno operare sulle funzionalità di firma è necessario che localmente siano attivi i driver del dispositivo di firma (lettore, smart card o token USB di firma, tablet per la firma grafometrica, ecc.), oppure che sia utilizzato un dispositivo HSM (Hardware Security Module) raggiungibile via rete.

Il servizio in outsourcing ASP del servizio di conservazione dei documenti digitali prodotti ed inviati dal Soggetto produttore prevede lo svolgimento da parte di UNIMATICA S.p.A., dietro apposita nomina e delega da parte del Soggetto produttore, delle funzioni e responsabilità di conservazione dei documenti.

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

Torna al sommario

Appendice A

Allegati al Manuale della conservazione:

- Allegato ‘Infrastrutture’.

Specificità del contratto e documenti di riferimento:

- Scheda Cliente.
- FlussiConservazione_ver 1.7
- Specifiche del servizio web per la consegna anticipata di documenti nel Sistema di conservazione.
- ‘Manuale dell’interfaccia web'.
- ‘Libro delle comunicazioni e dei verbali delle verifiche periodiche’.

Torna al sommario