MANUALE DEL SISTEMA DI CONSERVAZIONE

Sommario

Registro delle versioni 4
1. Scopo e ambito del documento 6
1.1. Trattamento dei dati personali 6
1.2. Trasparenza 8
2. Terminologia 10
3. Normativa e standard di riferimento 11
3.1. Normativa di Riferimento 11
3.2. Standard di Riferimento 12
4. Ruoli e responsabilità 14
4.1. Ruoli di ausilio al processo di conservazione 17
4.2. Precedenti responsabili 17
5. Struttura organizzativa per il servizio di conservazione 18
5.1. Organigramma 18
5.2. Strutture organizzative 19
6. Oggetti sottoposti a conservazione 21
6.1. Metadati 21
6.1.1 Metadati del documento informatico 22
6.1.2 Metadati del documento amministrativo informatico 24
6.1.3 Metadati delle aggregazioni documentali informatiche 26
6.1.4 Metadati del documento informatico di natura fiscale e contabile 29
6.2 Formati 29
6.2.1 Riversamento 29
6.3 Struttura dati del Pacchetto di versamento 30
6.4 Struttura dati del Pacchetto di archiviazione 30
6.5 Struttura dati del Pacchetto di distribuzione 31
7. Il processo di erogazione del servizio di conservazione 33
7.1 Il processo di conservazione 34
7.2 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico 34
7.3 Verifiche effettuate sui Pacchetti di versamento e sugli oggetti in esso contenuti 35
7.4 Accettazione dei Pacchetti di versamento e generazione del Rapporto di versamento di presa in carico 36
7.5 Rifiuto dei Pacchetti di versamento e modalità di comunicazione delle anomalie 37
7.6 Preparazione e gestione dei Pacchetti di archiviazione 37
7.7 Preparazione e gestione dei Pacchetti di distribuzione ai fini dell'esibizione 38
7.8 Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento di un pubblico ufficiale 39
7.9 Scarto dei Pacchetti di archiviazione 40
7.10 Predisposizione di misure per l'interoperabilità e la trasferibilità ad altri conservatori 40
7.11 Chiusura del contratto 41
8. Procedure di gestione e di evoluzione 42
8.1. Misure di sicurezza logica 42
8.1.1 Gestione utenze 42
8.1.2 Gestione sistemi di protezione 43
8.1.3 Gestione degli incidenti di sicurezza 43
8.1.4 Gestione dei backup e Disaster Recovery 44
8.1.4.1 Siti Settimo e Firenze 44
8.1.4.2 Siti di Bologna e Acilia (Roma) 45
8.1.4.3 Disaster Recovery 46
8.1.5 Gestione dei supporti di memorizzazione 46
8.2. Procedure di evoluzione e Change management 47
8.3. Cessazione del Servizio di conservazione 47
9. Monitoraggio e controlli 49

9.1 Audit interni e Verifica dell'integrità degli archivi 49
9.2 Reportistica di servizio 50
10. La server farm di Unimatica-RGI 52
10.1 UniStorage - Il sistema per la conservazione 55
Appendice A 57

Indice delle figure

Figura 1 - Struttura volumi 31
Figura 2 - Modello OAIS 33
Figura 3 - Architettura di conservazione 54

Registro delle versioni

Revisione	Data	Motivo Revisione	Redatto da	Approvato da
1.0	03/10/2009	Emissione	Andrea Anghinolfi	Silvano Ghedini
2.0	12/02/2010	Aggiornamento funzionalità	Andrea Anghinolfi	Silvano Ghedini
3.0	20/06/2010	Aggiornamento funzionalità	Andrea Anghinolfi	Silvano Ghedini
4.0	28/09/2010	Aggiornamento funzionalità	Andrea Anghinolfi	Silvano Ghedini
5.0	15/10/2010	Aggiornamento funzionalità	Andrea Anghinolfi	Silvano Ghedini
6.0	10/02/2011	Modifica gestione anomalie – Ampliamento funzionalità Unistorage	Andrea Anghinolfi	Silvano Ghedini
7.0	20/05/2011	Aggiornamento composizione societaria Unimatica-RGI	Andrea Anghinolfi	Silvano Ghedini
8.0	30/11/2012	Aggiornamento Data Center	Andrea Anghinolfi	Silvano Ghedini
8.1	11/12/2012	Personalizzazioni	Andrea Anghinolfi	Silvano Ghedini
8.2	20/06/2013	Aggiornamento compiti e responsabilità della conservazione	Sabina Falcinelli	Andrea Anghinolfi
8.3	04/07/2013	Aggiornamento normative	Sabina Falcinelli	Andrea Anghinolfi
8.4	05/02/2014	Aggiornamento normative	Sabina Falcinelli	Andrea Anghinolfi
8.5	11/02/2014	Aggiornamento Data Center	Sabina Falcinelli	Andrea Anghinolfi
8.6	05/03/2014	Adeguamento normative	Sabina Falcinelli	Andrea Anghinolfi
8.7	17/02/2015	Adeguamento DPCM 03/12/2013	Roberta Rosatone	Silvano Ghedini
8.8	15/10/2015	Passaggio alla ISO 27001:2013	Roberta Rosatone	Silvano Ghedini
8.9	20/01/2016	Adeguamento Schema Manuale della conservazione AgID	Roberta Rosatone	Silvano Ghedini
9.0	11/04/2017	Modifica ruolo Responsabile della Funzione Archivistica	Roberta Rosatone	Silvano Ghedini
9.1	14/06/2017	Aggiornamento definizioni per termine “Produttore”	Roberta Rosatone	Silvano Ghedini
9.2	05/10/2017	· Aggiornamento Server farm · Visualizzazione di 200 risultati da portale	Roberta Rosatone	Silvano Ghedini
9.3	20/10/2017	· Capitolo Trasparenza · Aggiornamento elenco formati · Aggiunto testo alternativo mancante su alcune immagini · Sostituita immagine 7 precedentemente con parti nascoste	Roberta Rosatone	Silvano Ghedini
9.4	25/10/2018	· Aggiornamento par. 1.1 adeguamento GDPR · Modifica ruolo Privacy Manager cap. 4 · Aggiornamento tabella normativa par. 3.1 · Aggiunto ruolo DPO al par.4.1	Roberta Rosatone	Silvano Ghedini
9.5	29/01/2019	· Recepimento N.C. AgID Recepimento Oss. Audit interno · Aggiornamento Nomina ad Interim Responsabile della funzione archivistica · Aggiornamento proc. Gestione Incident par. 8.1.3	Roberta Rosatone	Silvano Ghedini

9.6	19/04/2019	· Revoca nomina ad Interim per la Responsabilità della funzione archivistica · Aggiornamento nomina ad interim DPO	Roberta Rosatone	Silvano Ghedini
9.7	27/09/2019	· Aggiornamento Ruoli (Delegato Responsabile del servizio di conservazione – Responsabile dello sviluppo e della manutenzione – Responsabile dei sistemi informative – DPO) · Aggiornamento proc. Gestione Incident par. 8.1.3 · Aggiornamento estensioni ISO 27017 – 27018 · Aggiornamento descrizione par. 7.5 Rifiuto PDV	Roberta Rosatone Paolo Vandelli	Silvano Ghedini
9.8	20/12/2019	· Aggiornamento capp. 4 e 5 a seguito della sostituzione del Delegato alla Responsabilità del servizio di conservazone, della Responsabile della funzione archivistica e della Responsabile dello sviluppo e manutenzione · A seguito delle NC ricevute in fase di audit è stato eliminato il par. 9.2 ed aggiornato il par. 8.1.3 sulla Gestione degli incident di sicurezza.	Roberta Rosatone Paolo Vandelli	Silvano Ghedini
9.9	13/01/2021	· Aggiornamento cap. 4 a seguito di Oss da Audit interno. Aggiunto nominativo Resp. dello sviluppo in carica. · Aggiornamento tabella formati par. 6.2	Roberta Rosatone	Silvano Ghedini
10	13/09/2021	· Aggiornamenti a seguito del cambio ragione sociale · Aggiornamento par. 1.1 sulla privacy · Aggiornamento par. 1.2 per certificazione ISO 14001 · Aggiornamento modifica sito d/r secondario Acilia (RM)	Roberta Rosatone	Silvano Ghedini
11	30/12/2021	· Aggiornamento a seguito dell'adeguamento alle Linee guida per la formazione, gestione e conservazione del documento informatico (revisionati cap. 1-2-3-4-6-7)	Eleonora Luzi	Paolo Vandelli
12	21/06/2022	· Capitolo 4.1.: riportato nuovo responsabile del servizio; rimossa evidenza della delega assegnata a Paolo Vandelli dal precedente responsabile del servizio; · Aggiunto capitolo '4.2. Precedenti responsabili' · Rivisto capitolo '5.1. Organigramma' in funzione della nuova nomina	Eleonora Luzi	Paolo Vandelli
13	01/09/2022	· Indicazione socio unico a piede pagina	Eleonora Luzi	Paolo Vandelli

1. Scopo e ambito del documento

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

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

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

Torna al sommario

1.1. Trattamento dei dati personali

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

1. Unimatica-RGI per espletare le attività pattuite per conto del Soggetto produttore potrebbe trattare direttamente o anche solo indirettamente una o più delle seguenti categorie di dati:
- dati personali,
- dati rientranti nelle categorie "particolari" di dati personali,
- dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza,

di cui è Titolare il Soggetto produttore. Per i dettagli, occorre fare riferimento a quanto pattuito nel contratto/ordine/accordo.

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

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

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

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

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

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

c) non divulgare o rendere noti a terzi - per alcuna ragione ed in alcun momento, presente o futuro ed anche una volta cessati i trattamenti oggetto del contratto/ordine/accordo - i dati personali ricevuti dal Titolare o pervenuti a sua conoscenza in relazione all'esecuzione del servizio prestato, se non previamente autorizzato per iscritto dal Titolare, fatti salvi eventuali obblighi di legge o ordini dell'Autorità Giudiziaria e/o di competenti Autorità amministrative;

d) collaborare con il Titolare per garantire la puntuale osservanza e conformità alla normativa in materia di protezione dei dati personali;

e) incaricare per iscritto i soggetti che abbiano le caratteristiche di Responsabili di Sistema e di Amministratori di Sistema, tenerne l'elenco aggiornato a disposizione del Soggetto produttore e fornirne eventualmente copia a semplice richiesta dello stesso;

f) adottare, se del caso, adeguate misure di sicurezza, in modo da ridurre al minimo i rischi di distruzione e perdita, anche accidentale dei dati/documenti stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

g) informare immediatamente il Soggetto produttore di qualsiasi richiesta o comunicazione da parte dell'Autorità Garante e/o Giudiziaria, per concordare congiuntamente l'evasione delle stesse;

h) collaborare con il Soggetto produttore per l'attuazione delle prescrizioni eventualmente impartite dall'Autorità Garante;

i) comunicare al Soggetto produttore qualsiasi accadimento che possa compromettere il corretto trattamento dei dati personali;

j) segnalare eventuali criticità al Soggetto produttore che possono mettere a repentaglio la sicurezza dei dati, al fine di consentire idonei interventi da parte dello stesso;

k) prestare particolare attenzione all'eventuale trattamento di dati personali rientranti nelle categorie particolari e/o relative a condanne penali o reati degli interessati conosciuti, anche incidentalmente, in esecuzione dell'incarico affidato, procedendo alla loro raccolta e archiviazione solo ove ciò si renda necessario per lo svolgimento delle attività di competenza e istruendo in tal senso le persone autorizzate che operano all'interno della propria struttura.

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

6. Unimatica-RGI, nella sua qualità di Responsabile esterno del trattamento, si impegna a notificare al Soggetto produttore, Titolare del trattamento, senza ingiustificato ritardo dall'avvenuta conoscenza, e comunque entro 24 ore dalla scoperta con comunicazione da inviarsi all'indirizzo PEC del Soggetto produttore, (salvo diversa email indicata) ogni violazione dei dati personali (*data breach*). Unimatica-RGI si impegna a prestare ogni più ampia assistenza al Soggetto produttore al fine di consentirgli di assolvere agli obblighi di cui agli artt. 32 - 34 del GDPR.
Una volta definite le ragioni della violazione, Unimatica-RGI di concerto con il Soggetto produttore e/o altro soggetto da quest'ultimo indicato, si attiverà per implementare nel minor tempo possibile tutte le misure di sicurezza fisiche e/o logiche e/o organizzative atte ad arginare il verificarsi di una nuova violazione della stessa specie di quella verificatasi.

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

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

9. Premesso che l'accesso ai dati personali da parte degli interessati esercitato ai sensi degli artt. 15 e seguenti del GDPR sarà gestito direttamente dal Soggetto produttore, Unimatica-RGI si rende disponibile a collaborare con il Soggetto produttore stesso fornendogli tutte le informazioni necessarie a soddisfare le eventuali richieste ricevute in tal senso.
10. Unimatica-RGI – ove tale obbligo si applichi anche alla stessa, nella sua qualità di Responsabile del trattamento e in base alle disposizioni del comma 5 dell'art. 30 del GDPR - mantiene un registro di tutte le categorie di attività relative al trattamento svolte per conto del Soggetto produttore.
11. Unimatica-RGI si impegna a mettere a disposizione del Soggetto produttore tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di sicurezza descritti nel presente documento e, in generale, il rispetto delle obbligazioni assunte in forza del GDPR, consentendo e, su richiesta, contribuendo alle attività di audit, comprese le ispezioni, realizzate dal Soggetto produttore o da altro soggetto da esso incaricato.
12. L'autorizzazione al trattamento dei dati personali avrà la medesima validità ed efficacia della durata della conservazione legale dei documenti, stabilita dalla normativa.

Torna al sommario

1.2. Trasparenza

La conservazione a norma di Unimatica-RGI è rivolta a Pubbliche amministrazioni, banche, assicurazioni, strutture sanitarie ed ai privati in genere.
Al fine di rendere tali servizi agevoli ed accessibili ad un pubblico variegato e disomogeneo, Unimatica-RGI rende disponibili una serie di strumenti ed informazioni utili a garantire una totale trasparenza delle proprie attività mediante canali diretti ed indiretti.
In generale, nel sito internet aziendale www.unimaticaspa.it sono disponibili:

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

Oltre alle certificazioni sopra elencate, Unimatica-RGI sta implementando un sistema di gestione anticorruzione ISO 37001:2016.
Tale certificazione, obbligatoria ai fini dell'adeguamento alle Linee guida per la formazione, gestione e conservazione dei documenti informatici in vigore dal 1° gennaio 2022, verrà aggiunta alle altre presenti nella sezione Trasparenza.

Negli anni, il settore Conservazione di Unimatica-RGI ha ottemperato a tutti gli obblighi normativi applicabili. Nello specifico, infatti, da marzo del 2015 ha mantenuto l'accreditamento presso l'Agenzia per l'Italia Digitale (AgID) con la pubblicazione del Manuale della conservazione nell'apposita area a ciò dedicata sul sito web di AgID.
Dall'ottobre del 2017 fino ad abrogazione, in continuità con le disposizioni normative, ha ottenuto e mantenuto la certificazione in conformità all'art. 24 del Regolamento Eidas e alla check list "*Lista di riscontro per la visita ispettiva AgID e la certificazione di conformità*".
Tali strumenti, oltre ad essere sinonimo di eccellenza, sono risultati negli anni passi indispensabili per la crescita dell'azienda, del team e per migliorare continuamente il prodotto Unistorage e il servizio offerto ai clienti.

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

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

Torna al sommario

2. Terminologia

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

Torna al sommario

3. Normativa e standard di riferimento

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

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

Torna al sommario

3.1. Normativa di Riferimento

Notazione abbreviata	Riferimento
Codice Civile	[Libro Quinto del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle Scritture contabili], art. 2215 bis – Documentazione informatica.
RD 1163/1911	Regolamento per gli archivi di Stato
DPR 1409/1963	Norme relative all'ordinamento ed al personale degli archivi di Stato
Legge 241/1990	Nuove norme sul procedimento amministrativo
DPR 445/2000	Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
DPR 37/2001	Regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli uffici dello Stato
D.lgs 196/2003	Recante il Codice in materia di protezione dei dati personali
D.lgs 42/2004	Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002,n.137
Legge 9 gennaio 2004, n. 4 aggiornata dal decreto legislativo 10 agosto 2018, n. 106	Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici
D.lgs 82/2005 e ss.mm.ii.	Codice dell'amministrazione digitale
D.lgs 33/2013	Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni
DPCM 22 febbraio 2013	Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71
DPCM 21 marzo 2013	Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni;

Reg. UE 910/2014	In materia di identificazione elettronica e servizi fiduciari per le transazionielettroniche nel mercato interno e che abroga la direttiva 1999/93/CE - Regolamento eIDAS;
Circolare 40 e 41 del 14 dicembre 2015 della Direzione generale degli archivi	Autorizzazionealla distruzione di originali analogici riprodotti secondo le regole tecniche di cui al DPCM 13.11.2014 econservati secondo le regole tecniche di cui al DPCM 13.12.2013;
Reg. UE 679/2016 (GDPR)	Relativo alla protezione delle persone fisiche con riguardo al trattamento deidati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
Circolare 18 aprile 2017 n. 2/2017 dell'Agenzia per l'Italia Digitale	Recante le misure minime disicurezza ICT per le pubbliche amministrazioni;
Circolare n. 2 del 9 aprile 2018	Recante i criteri per la qualificazione dei Cloud Service Provider per laPA;
Circolare n. 3 del 9 aprile 2018	Recante i criteri per la qualificazione di servizi SaaS per il Cloud dellaPA;
Reg. UE 2018/1807	Relativo a un quadro applicabile alla libera circolazione dei dati non personalinell'Unione europea;
DPCM 19 giugno 2019 n. 76	Regolamento di organizzazione del Ministero per i beni e le attivitàculturali, degli uffici di diretta collaborazione del Ministro e dell'Organismo indipendente di valutazione dellaperformance.
Linee guida AgID ed Allegati	Linee guida sulla Formazione, Gestione, Conservazione dei documenti informatici Allegato 1 Glossario dei termini e degli acronimi Allegato 2 Formati di File e Riversamento Allegato 3 Certificazione di processo Allegato 4 Standard e specifiche tecniche Allegato 5 Metadati
Regolamento AgID ed Allegati	Regolamento sui criteri di conservazione Allegato A Requisiti per l'erogazione del servizio di conservazione per conto delle pubbliche amministrazioni Allegato B Piano di cessazione del servizio di conservazione dei documenti informatici

Torna al sommario

3.2. Standard di Riferimento

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

SIARD	Software Independent Archiving of Relational Databases 2.0 Ministère de la culture et de la communication, Service interministériel des Archives de France, Standard d'échange de donnéès pour l'archivage. Transfert – Communication – Élimination – Restitution - Modification, ver. 2.1, 2018
METS	Metadata Encoding and Transmission Standard
PREMIS	PREservation Metadata: Implementation Strategies.
EAD (3)/ISAD (G)	
EAC (CPF)/ISAAR (CPF)/NIERA (CPF)	
SCONS2/EAG/ISDIAH	

Torna al sommario

4. Ruoli e responsabilità

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

- **Titolare dell'oggetto della conservazione** (citato nel manuale come soggetto produttore), identificato come il soggetto produttore degli oggetti di conservazione.
- **Produttore dei PdV**, ovvero la persona fisica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione, identificato con il responsabile della gestione documentale nelle pubbliche amministrazioni
- **Utente abilitato**, ossia la persona, l'ente o il sistema che interagisce con i servizi di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse
- **Responsabile della conservazione**, ovvero il soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.
- **Conservatore**, identificato come l'insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti.

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

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

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

1. definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato
2. gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
3. genera e sottoscrive il Rapporto di Versamento, secondo le modalità previste dal manuale di conservazione;
4. genera il pacchetto di archiviazione conforme allo Standard SInCRO UNI 11386 - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali e lo sottoscrive con firma digitale;
5. genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione, ai fini dell'esibizione richiesta dall'utente;
6. effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
7. effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;

8. al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità. Adotta analoghe misure con riguardo all'obsolescenza dei formati;
9. provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
10. adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione;
11. assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
12. assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
13. provvede per le amministrazioni statali centrali e periferiche a versare i documenti informatici, le aggregazioni informatiche e gli archivi informatici, nonché gli strumenti che ne garantiscono la consultazione, rispettivamente all'Archivio centrale dello Stato e agli archivi di Stato territorialmente competenti, secondo le tempistiche fissate dall'art. 41, comma 1, del Codice dei beni culturali

garantendo un particolare riguardo alla:

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

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

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

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

- definire e gestire il processo di conservazione, incluse le modalità di trasferimento da parte del produttore dei PDV, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato
- monitorare set di metadati di conservazione dei documenti, dei fascicoli informatici e delle aggregazioni documentali informatiche
- monitorare il processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema
- collaborare con il Produttore dei PDV ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.

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

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

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

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

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

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

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

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

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

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

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

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

Torna al sommario

4.1. Ruoli di ausilio al processo di conservazione

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

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

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

Torna al sommario

4.2. Precedenti responsabili

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

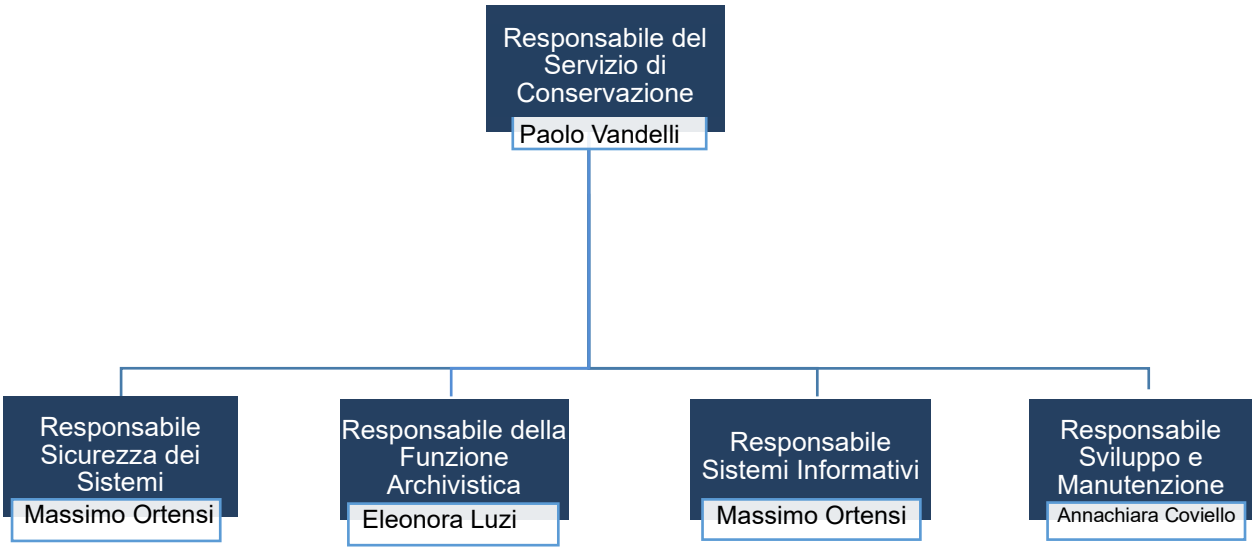
Torna al sommario

5. Struttura organizzativa per il servizio di conservazione

Il presente capitolo ha lo scopo di illustrare la struttura organizzativa del settore conservazione di Unimatica-RGI. L' espletamento di un processo di conservazione prevede una serie di complesse attività, pertanto la società si avvale di personale altamente qualificato e con esperienza decennale. Si riporta di seguito l'organigramma della struttura organizzativa e una sintetica descrizione[1] delle funzioni e delle responsabilità che intervengono nel processo di conservazione.

Torna al sommario

5.1. Organigramma



Torna al sommario

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

5.2. Strutture organizzative

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

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

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

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

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

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

Torna al sommario

6. Oggetti sottoposti a conservazione

Unimatica-RGI mediante il proprio sistema di conservazione Unistorage, sviluppato integralmente dalla società, è in grado di accettare e gestire, come richiesto ai sensi dell'art. 44, comma 1-bis, del CAD[4],

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

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

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

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

Torna al sommario

6.1. Metadati

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

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

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

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

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

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

Torna al sommario

6.1.1 Metadati del documento informatico

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

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

Il metadato è costituito dai seguenti:

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

Modalità di formazione: modalità di generazione del documento informatico

Sono previste le seguenti modalità:

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

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

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

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

Sono previsti i seguenti campi:

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

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

Sono definiti i seguenti attributi:

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

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

È costituito da seguenti campi:

- Oggetto: testo libero

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

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

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

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

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

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

É costituito da:

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

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

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

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

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

Versione del documento: versione del documento.

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

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

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

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

Torna al sommario

6.1.2 Metadati del documento amministrativo informatico

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

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

Il metadato è costituito dai seguenti:

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

Modalità di formazione: modalità di generazione del documento informatico

Sono previste le seguenti modalità:

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

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

Sono definiti i seguenti attributi:

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

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

È costituito da seguenti campi:

- Oggetto: testo libero

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

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

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

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

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

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

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

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

É costituito da:

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

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

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

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

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

Versione del documento: versione del documento.

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

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

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

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

6.1.3 Metadati delle aggregazioni documentali informatiche

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

Identificativo dell'Aggregazione documentale: si tratta di una sequenza di caratteri alfanumerici associata in modo univoco all'aggregazione documentale informatica in modo da consentirne l'identificazione, indica se si tratta di un Fascicolo o di una Serie Documentale o di una Serie di Fascicoli.
Il fascicolo è una aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento.
Le serie documentarie sono costituite da documenti singoli accorpati per ragioni funzionali in base alla tipologia di riferimento.
Le serie di fascicoli sono costituite da fascicoli accorpati per ragioni funzionali in base alla classe di riferimento o alla tipologia di fascicoli.

Sono definiti i seguenti attributi:

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

Tipologia fascicolo: I fascicoli sono organizzati per:

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

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

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

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

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

Il metadato ha una struttura ricorsiva.

Data Apertura: data di apertura dell'aggregazione documentale.

Classificazione: classificazione dell'aggregazione:

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

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

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

È costituito da seguenti campi:

- Oggetto: testo libero

Data Chiusura: data di chiusura dell'aggregazione documentale.

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

È costituito da seguenti campi:

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

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

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

È costituito da seguenti campi:

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

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

6.1.4 Metadati del documento informatico di natura fiscale e contabile

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

Torna al sommario

6.2 Formati

Unistorage, in conformità all'*Allegato 2 "Formati di file e riversamento"* alle Linee guida AgID, accetta e gestisce formati aperti, non proprietari, standard de iure, estendibili, parlanti, completamente robusti, indipendenti dal dispositivo e che garantiscano i principi dell'interoperabilità.
Tuttavia, in accordo con il soggetto produttore, Unimatica-RGI permette anche l'accettazione di formati non esplicitati nell'Allegato 2. Infatti qualora l'ordinamento giuridico preveda degli obblighi relativamente all'uso di formati specifici per alcuni Titolari, questi assolvendo tali obblighi, sono chiamati ad effettuare una valutazione di interoperabilità utile anche per garantire la conservazione e la fruibilità degli stessi nel tempo. L'indicazione di tali formati, compresa la gestione di questi, verrà indicata nella scheda cliente.

Torna al sommario

6.2.1 Riversamento

Unistorage, in relazione all'obsolescenza dei formati, tiene un censimento dei formati di file ricevuti in conservazione a seguito di un'attività di ingestion (compreso il recupero da precedente conservatore). Il responsabile del servizio di conservazione, assieme al responsabile della funzione archivistica, al responsabile sviluppo e manutenzione del sistema di conservazione e al responsabile sicurezza dei sistemi per la conservazione, con cadenza non superiore ai 5 anni, fatta una fotografia dei formati di file censiti al momento sul sistema, ne valuta il grado di obsolescenza.
In fase di analisi dei formati, come da procedura stabilita, per ogni formato si attribuisce un grado di obsolescenza, basandosi sulle caratteristiche di apertura, sicurezza, portabilità, funzionalità,

supporto allo sviluppo e diffusione. Al termine della verbalizzazione di questo processo di verifica, a fronte di evidenze di formati di file per cui è impossibile individuare soluzioni in grado di rappresentare fedelmente il contenuto di questi file, il responsabile del servizio di conservazione attiva il processo di riversamento dei file appartenenti ai formati risultati a rischio di obsolescenza, previa certificazione di processo.
Per tutti i dettagli inerenti l'intero processo di gestione del riversamento si rimanda al documento di sistema "PRO_CONS01 - Procedure di Conservazione".

Torna al sommario

6.3 Struttura dati del Pacchetto di versamento

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

- La ricezione mediante SSH File Transfert Protocol prevede l'upload del Pacchetto di versamento composto da un file indice e da un insieme di file, in formato .zip. Per maggiori dettagli circa la struttura dei Pacchetti di versamento, fare riferimento al documento Flusso per la conservazione dei Documenti in Unistorage.

- La ricezione tramite Sistema Web Service è possibile da qualsiasi piattaforma che permetta di eseguire e ricevere chiamate Web Service conformi allo standard WS-I Basic Profile 1.0. Con questo servizio il sistema di conservazione riceve singoli documenti ed eventuali allegati, ne verifica la firma digitale se presente e ne gestisce la conservazione autentica. Per maggiori dettagli circa la ricezione degli oggetti digitali tramite Sistema Web Service si rimanda al documento "Specifiche del servizio web per la consegna anticipata di documenti nel Sistema di conservazione".

Torna al sommario

6.4 Struttura dati del Pacchetto di archiviazione

Terminato il processo di acquisizione dei Pacchetti di versamento, il prodotto applicativo UniStorage sotto la supervisione del Responsabile del servizio di conservazione e del Responsabile della funzione archivistica provvede alla creazione dei Pacchetti di archiviazione e dell'Indice del pacchetto di archiviazione previsto dallo standard UNI 11386 SInCRO – Supporto all'interoperabilità nella conservazione e nel recupero degli oggetti digitali.
I Pacchetti di archiviazione contengono[5]:

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

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

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

Torna al sommario

6.5 Struttura dati del Pacchetto di distribuzione

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

L'esibizione del materiale di interesse avviene via interfaccia web o mediante memorizzazione su supporto ottico. La descrizione dettagliata delle procedure è indicata nel capitolo 7 "Il processo di erogazione del servizio di conservazione", Fase 6.
Per quanto riguarda i Pacchetti di distribuzione memorizzati su supporto ottico, questi coincidono con i Pacchetti di archiviazione, come previsto delle Regole tecniche in materia di sistemi di conservazione, ma saranno corredati di informazioni aggiuntive necessarie per la creazione dei DVD, CD, ecc. nel caso di richiesta di esibizione da parte dell'Utente.

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

Contenuto della directory della registrazione:

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

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

Figura 1 - Struttura volumi

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

Torna al sommario

7. Il processo di erogazione del servizio di conservazione

Il processo di conservazione eseguito da Unimatica-RGI adotta il modello standard OAIS - Open Archival Information System[6] 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[7], il Soggetto conservatore provvederà a creare i Pacchetti di distribuzione in una forma tale che venga garantita la corretta visualizzazione di questi.

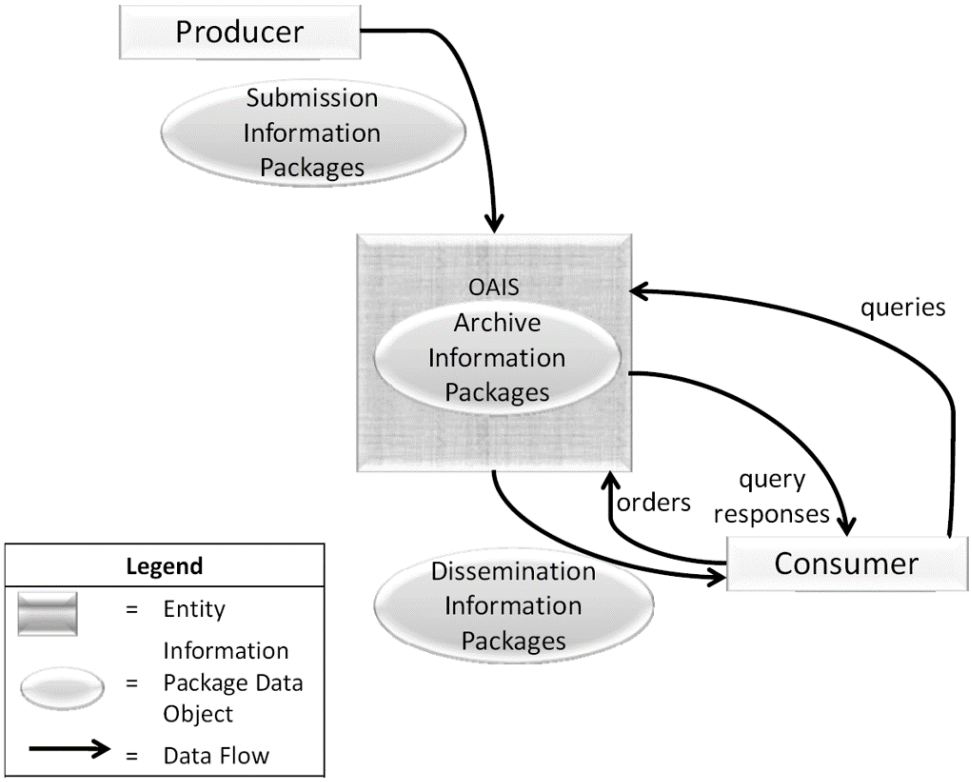


Figura 2 - Modello OAIS

Torna al sommario

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

7.1 Il processo di conservazione

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

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

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

Di seguito vengono dettagliate le fasi del processo.

Torna al sommario

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

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

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

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

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

- i volumi in termini di numero documenti annui previsti da gestire e spazio di occupazione previsto per i dati da Conservare (GB);
- la dimensione massima del Pacchetto di versamento;
- la frequenza di invio dei Pacchetti;

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

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

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

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

Torna al sommario

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

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

- **identificazione certa del Soggetto produttore**;

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

una “catena di certificazione” (trust chain) per cui l'autorità di un certificato vada a sua volta identificata risalendo ad un'autorità terza.

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

Torna al sommario

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

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

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

Il Rapporto di versamento è un file in formato XML che riporta, per ognuno dei file inclusi nel Pacchetto, alcune informazioni tra cui un “URN” (unified resource name) e un “hash”. L'URN è una stringa univoca che identifica l'oggetto digitale, mentre l’hash è un'impronta del documento, ovvero una sequenza di bit che può essere ricavata dal file in modo ripetibile e standardizzato e che

garantisce una corrispondenza esatta col contenuto originale (in modo pratico possiamo dire di avere la garanzia che a due file differenti corrispondono sempre due impronte distinte).

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

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

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

Torna al sommario

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

Le verifiche effettuate sui Pacchetti di versamento possono risultare negative. Nei casi in cui anche solo su uno dei controlli indicati nella fase 2 si dovesse riscontrare una mancanza o non corrispondenza di informazioni viene generato un file di Comunicazione delle anomalie che verrà comunicato mediante un file di esito al Soggetto produttore. Tale Comunicazione comprenderà i dettagli delle verifiche eseguite sui Pacchetti di versamento comprensive delle precisazioni sulle anomalie.
Le anomalie, in relazione a quanto descritto nella fase 2, possono essere identificate nell'assenza dei metadati obbligatori ovvero nella mancata corrispondenza di ciò che viene versato a quanto dichiarato dal soggetto produttore nella scheda cliente in termini di firma digitale, formati e metadati. Qualora l'anomalia venisse riscontrata soltanto su una parte di documenti inclusi nel Pacchetto di versamento, è facoltà del soggetto produttore decidere se bloccare l'intero pacchetto o soltanto i documenti segnalati. In questo ultimo caso i file conformi vengono inviati in conservazione e gli altri spediti successivamente mediante nuovo Pacchetto di versamento.

Torna al sommario

7.6 Preparazione e gestione dei Pacchetti di archiviazione

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

- individuazione dei documenti destinati a far parte del pacchetto di archiviazione sulla base dei criteri scelti. Tali criteri vengono concordati con il cliente e sono definiti nella scheda cliente e si possono basare sia su caratteristiche legate allo stato del documento, sia sui metadati.
- i Pacchetti di archiviazione vengono chiusi in seguito a due tipi di regole:
  - automatiche: collocano nel pacchetto i documenti per i quali ci sia almeno un certificato di firma prossimo alla scadenza. Questa tipologia di regole ha la precedenza su quelle descritte nel punto successivo, le quali riguardano la dimensione massima del Pacchetto di archiviazione e il tempo limite oltre il quale un Pacchetto di archiviazione deve essere forzatamente chiuso,
  - attuate dal Responsabile del servizio di conservazione in accordo con il soggetto produttore: definite nella scheda cliente.

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

I Pacchetti di archiviazione vengono sottoscritti con firma digitale dal Responsabile del servizio di conservazione e marcati temporalmente.
La sottoscrizione dei Pacchetti di archiviazione effettuata da Unimatica-RGI attesta esclusivamente la corretta esecuzione del processo di conservazione secondo la normativa vigente in materia di conservazione. Unimatica-RGI non è responsabile dell'errato contenuto informativo degli oggetti versati.

Torna al sommario

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

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

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

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

È possibile visualizzare i documenti tramite duplice canale:

- via web: i Soggetti produttori titolari dei documenti potranno ricercare e visualizzare tutti i documenti conservati direttamente sul portale di Unimatica-RGI attraverso l'apposita funzionalità. L'accesso avviene tramite il portale al quale è demandata la sicurezza e la gestione della sessione. I documenti saranno disponibili per l'esibizione on-line per tutto il

periodo di conservazione. Per maggiore chiarezza si precisa che al fine di garantire una veloce e corretta visualizzazione dei documenti conservati, tramite ricerca libera il portale permette la visualizzazione di 200 risultati. Per la ricerca di tutti gli altri documenti sarà necessario valorizzare gli appositi campi delle maschere di ricerca con i metadati dichiarati in fase di versamento. La descrizione di dettaglio dell'interfaccia web per le richieste di esibizione dei documenti è contenuta nell'allegato 'Funzionalita_portale'. Vengono inoltre resi disponibili servizi web (Web Services) per le eventuali integrazioni con i portali dei Soggetti produttori.

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

La struttura 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 propri documenti, in base alle credenziali e alle politiche di accesso attivate.

Torna al sommario

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

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

Nei casi in cui, come previsto dall'art. 23-bis, c. 2 del Codice dell'Amministrazione Digitale[8] il Soggetto produttore richieda la presenza di un pubblico ufficiale, Unimatica-RGI garantirà tale presenza mettendo a disposizione tutte le necessarie risorse che serviranno all'espletamento delle attività, rimandando in ogni caso la scelta al Soggetto produttore al quale saranno addebitate le spese.

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

Torna al sommario

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

7.9 Scarto dei Pacchetti di archiviazione

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

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

In caso degli archivi pubblici o privati dichiarati di interesse storico particolarmente importante l'autorizzazione finale è rilasciata ai sensi della normativa vigente in materia di beni culturali[9].

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

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

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

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

Torna al sommario

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

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

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

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-RGI utilizzando una delle modalità di seguito indicate:

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

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

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

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

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

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

Torna al sommario

8. Procedure di gestione e di evoluzione

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

Torna al sommario

8.1. Misure di sicurezza logica

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

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

Torna al sommario

8.1.1 Gestione utenze

La policy di riferimento per la gestione delle utenze applicative e di sistema adottata da Unimatica-RGI prevede che le utenze siano rilasciate da un ente (o persona) differente dall'ente o persona che le utilizzerà.
Nell'ambito del servizio di conservazione, le utenze applicative e di sistema sono gestite secondo criteri idonei a garantire il rispetto dell'applicazione di misure di sicurezza tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio ai sensi dell'art. 32 del GDPR. Si riportano di seguito alcune delle misure di sicurezza adottate:

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

  - non può contenere l'username dell'utente,
  - non può essere una delle ultime 4 utilizzate;

- la scadenza della password è configurabile attraverso un parametro;
- il sistema deve forzare l'utente a cambiare la password al primo utilizzo;
- il sistema deve avvertire l'utente della necessità di rinnovare la password;

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

Torna al sommario

8.1.2 Gestione sistemi di protezione

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

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

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

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

Torna al sommario

8.1.3 Gestione degli incidenti di sicurezza

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

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

La segnalazione di anomalie può scaturire

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

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

Una volta preso in carico il ticket dal Responsabile del settore Conservazione o da un operatore designato egli diventa Incident Owner, cui sono delegate le azioni di: Contenimento[10], Eliminazione delle cause[11], Ripristino[12].

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

Torna al sommario

8.1.4 Gestione dei backup e Disaster Recovery

8.1.4.1 Siti Settimo e Firenze

L'architettura del sistema backup è composta da un master server per ogni sito e da differenti media server che hanno il compito di archiviare i dati ed inserirli in una rete dedicata, parallela a quella di erogazione dei singoli servizi, per non impattare sulle prestazioni e sulla disponibilità di questi ultimi, durante la normale esecuzione delle attività di backup.
I singoli agent installati sull'infrastruttura di virtualizzazione e sui server non virtualizzati comunicano con il backup server che esegue il salvataggio dei dati su un appliance Data Domain. Il salvataggio dei dati su un appliance Data Domain viene replicato sul sito secondario. Questo sistema consente:

- Semplicità di integrazione anche con future evoluzioni del software di backup
- De-duplicazione del dato ad alta velocità

[10] **Contenimento**: processo che rappresenta la fase di esecuzione delle attività di contrasto, atte a mitigare le compromissioni della sicurezza derivanti da un incidente. Una delle attività principali del processo di contenimento è quella di determinare il patrimonio informativo che viene messo a rischio a seguito di un incidente.
[11] **Eliminazione delle cause**: processo che elenca le azioni indirizzate alla rimozione delle cause che scatenano un incidente informatico. E' opportuno sottolineare l'importanza che rappresenta la comprensione del problema che è all'origine dell'incidente; a tale scopo appare determinante descrivere con il maggior dettaglio possibile il modo con cui l'evento di sicurezza si è verificato.
[12] **Ripristino**: processo tramite il quale viene attuato il ritorno alle normali condizioni di operatività aziendale e di chiusura formale dell'incidente. Un obiettivo determinante che emerge dalla corretta applicazione delle misure qui contemplate, è garantire che per i dati e per i sistemi/applicazioni siano ristabilite le funzionalità e performance in essere prima dell'incidente.

- Replica efficiente in rete
- Scalabilità dell'infrastruttura

L'architettura di backup utilizza le seguenti tecnologie:

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

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

Torna al sommario

8.1.4.2 Siti di Bologna e Acilia (Roma)

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

Le categorie di dati oggetto del backup sono:

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

Nell'ambito del backup dei dati appartenti alla categoria Directory di sistema, è eseguito anche il backup delle cartelle di rete utilizzate dal personale Unimatica-RGI.
Il backup avviene in due modalità:

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

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

- i dati di backup sono conservati per 7 giorni su Dischi, i backup full eseguiti ogni fine settimana sono conservati per 1 mese su dischi;
- vengono eseguiti backup mensili su dischi rimuovibili, in singola copia, conservati in cassaforte ignifuga, con retention di un anno;
- l'ultimo backup mensile su disco di ogni anno viene conservato con ritenzione infinita;
- backup su disco di dati con esigenze di retention specifiche (superiori all'anno), sono eseguiti in doppia copia, in base a specifiche degli "owner" dei dati;
- il salvataggio dei documenti su CD-ROM con consegna al Soggetto produttore, può essere eseguito su richiesta;

- il salvataggio dell'applicazione sia server che client è realizzato su supporto fisico esterno (Data tape o CD-ROM) per eseguire una rapida reinstallazione in caso di necessità;
- i supporti di backup hanno rotazione con frequenza settimanale.

Per le attività di salvataggio si eseguono i seguenti controlli:

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

Torna al sommario

8.1.4.3 Disaster Recovery

I servizi di conservazione di Unimatica-RGI sono erogati tramite due Data Center Primari due Data Center Secondari che svolgono il compito di Backup Remoto e di Disaster Recovery (D/R), al fine di garantire gli opportuni livelli di continuità del servizio.
I Data Center hanno una distanza fra loro superiore 200 e 300 Km e la disponibilità di servizio è H24 per tutti e 4.
I Data Center secondari permettono di usufruire dei servizi in Produzione anche in caso di indisponibilità dei Data Center Primari.
Per questo servizio Unimatica-RGI definisce con il Cliente il livello dei parametri che caratterizzano il servizio di D/R e di continuità operativa.

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

Torna al sommario

8.1.5 Gestione dei supporti di memorizzazione

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

- i media di memorizzazione elettronica sono correttamente etichettati in modo da fornire le seguenti informazioni: tipologia del media, tecnica della scrittura, data 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, si procede allo svecchiamento dei media tramite riversamento del loro contenuto in altro media.

Torna al sommario

8.2. Procedure di evoluzione e Change management

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

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

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

Torna al sommario

8.3. Cessazione del Servizio di conservazione

Il servizio di Conservazione digitale a norma è, dal 2005, uno dei principali asset di Unimatica-RGI e gli obiettivi della Direzione per gli anni futuri sono di continuare ad evolvere il sistema ed il servizio di conservazione per mantenerlo adeguato alla tecnologia ed alla normativa e di espandere sempre più nel mercato target, non solo italiano, la penetrazione dell'azienda.
A fronte dei suddetti obiettivi, è stata comunque stabilita una procedura per definire le modalità secondo le quali dovrà essere gestito l'evento, ad oggi non prevedibile, di cessazione del servizio di Conservazione da parte di Unimatica-RGI
La gestione della cessazione del Servizio di Conservazione, in fase iniziale, è in carico alla Direzione la quale stabilisce un tempo di almeno 10 mesi prima della data di attuazione prevista.

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

Alla ricezione della comunicazione suddetta il Responsabile del servizio di conservazione coinvolge i Responsabili delle diverse aree inerenti la Conservazione (Sicurezza, Servizio, Archivistica,

Sviluppo) con i quali deve collaborare strettamente per la gestione della cessazione e la relativa pianificazione delle attività.
La procedura e le attività che verranno eventualmente eseguite sono descritte nel dettaglio all'interno del documento PRO_CONS - Piano di Cessazione, qualora venga richiesto, tale procedura viene resa disponibile fornendola al soggetto produttore interessato.

Torna al sommario

9. Monitoraggio e controlli

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

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

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

I log file degli applicativi contengono almeno le seguenti informazioni:

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

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

Torna al sommario

9.1 Audit interni e Verifica dell'integrità degli archivi

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

La scelta del personale verificatore viene fatta in modo da garantire obiettività ed imparzialità nel processo di verifica.
Unimatica-RGI prevede in allegato al Manuale "Elenco delle modifiche apportate al Manuale della conservazione e dei documenti obsoleti" tenente traccia delle seguenti informazioni:

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

Torna al sommario

9.2 Reportistica di servizio

Il sistema di conservazione UniStorage gestisce un sistema di tracciatura nel quale vengono registrati tutti i singoli eventi che riguardano sia la gestione dei Pacchetti, dalla fase di versamento a quella di distribuzione, sia i singoli documenti. Questa tracciatura, costruita per implementare un "forensic log", è in un formato rigido e non disabilitabile. La tracciatura è prerequisito indispensabile per l'esecuzione delle operazioni.
Nel dettaglio, il sistema di log prevede la registrazione di informazioni relative alle diverse funzioni del processo di conservazione per tutte le fasi descritte nel capitolo 7 "Il processo di erogazione del servizio di conservazione".

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

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

Tipologia 1:
vengono prodotti periodicamente i seguenti report:

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

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

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

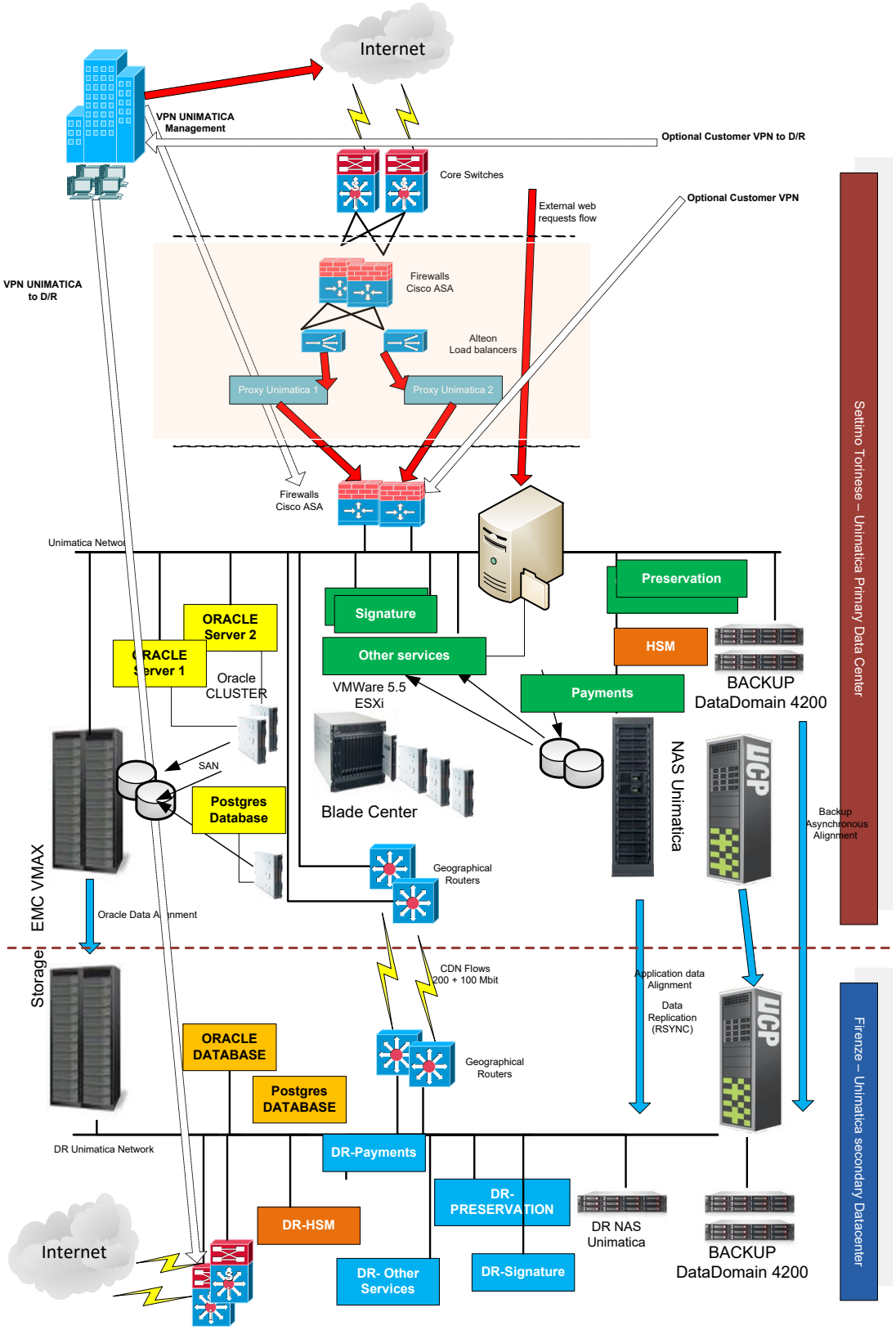
- Media Tempo di Chiusura Service Request

Torna al sommario

10. La server farm di Unimatica-RGI

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

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


Internet
VPN UNIMATICA Management
Optional Customer VPN to D/R
Core Switches
External web requests flow
Optional Customer VPN
VPN UNIMATICA to D/R
Firewalls Cisco ASA
Alteon Load balancers
Proxy Unimatica 1
Proxy Unimatica 2
Firewalls Cisco ASA
Unimatica Network
Settimo Torinese – Unimatica Primary Data Center
Preservation
Signature
Other services
HSM
ORACLE Server 2
ORACLE Server 1
Oracle CLUSTER
VMWare 5.5 ESXi
Payments
BACKUP DataDomain 4200
SAN
Postgres Database
Blade Center
NAS Unimatica
UCP
Backup Asynchronous Alignment
EMC VMAX
Geographical Routers
Oracle Data Alignment
Storage
CDN Flows 200 + 100 Mbit
Application data Alignment
Data Replication (RSYNC)
ORACLE DATABASE
Postgres DATABASE
Geographical Routers
DR Unimatica Network
DR-Payments
DR-PRESERVATION
DR-HSM
DR NAS Unimatica
BACKUP DataDomain 4200
Internet
DR- Other Services
DR-Signature
Firenze – Unimatica secondary Datacenter

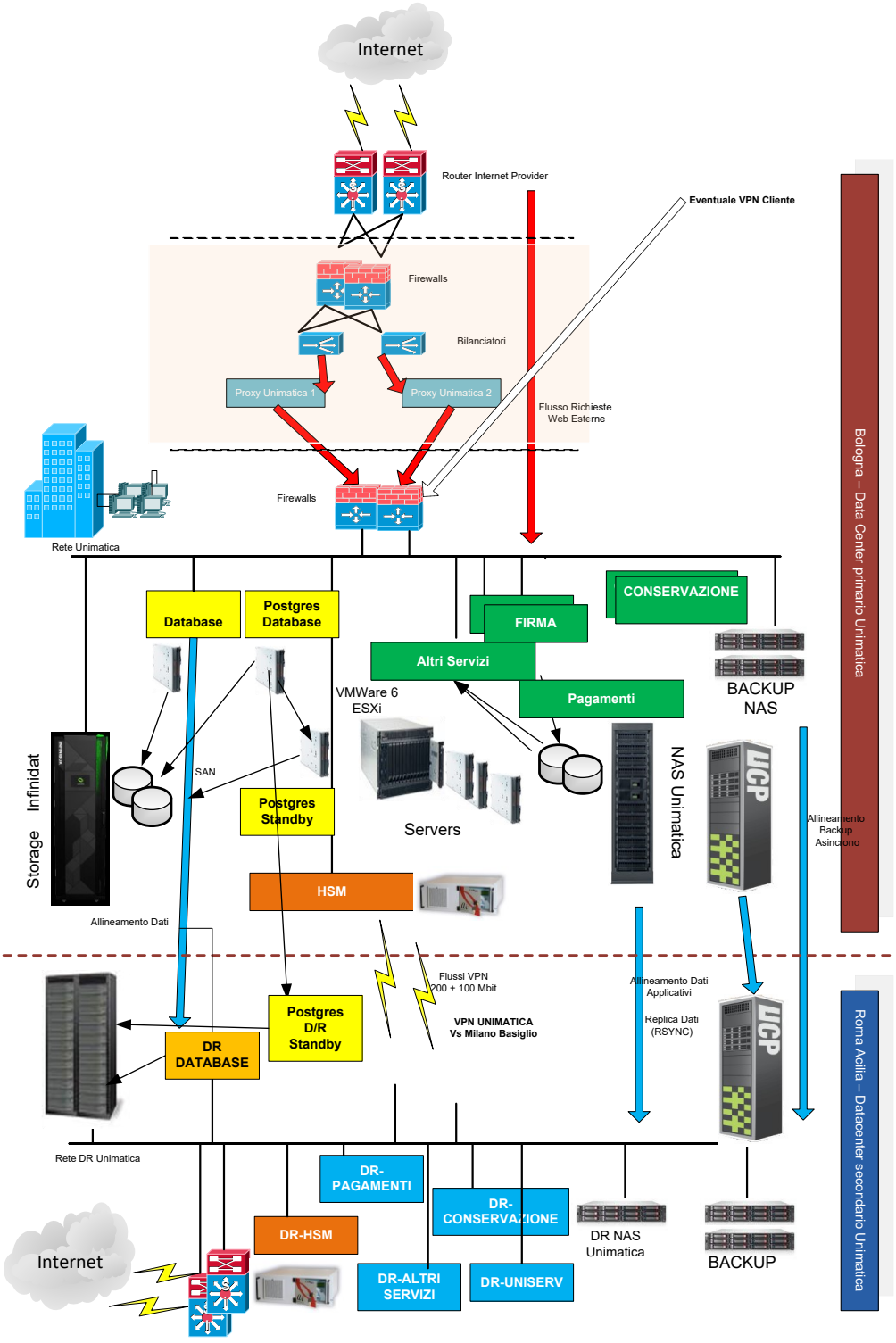


Figura 3 - Architettura di conservazione

Torna al sommario

10.1 UniStorage - Il sistema per la conservazione

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

UniStorage esegue la conservazione nel tempo dei documenti sottoscritti con firma digitale e le 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 dei principali browser di riferimento sul mercato. Per le postazioni che dovranno operare sulle funzionalità di firma è necessario che localmente siano attivi i driver del dispositivo di firma (lettore, smart card o token USB di firma, tablet per la firma grafometrica, ecc.), oppure che sia utilizzato un dispositivo HSM (Hardware Security Module) raggiungibile via rete.

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

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

Torna al sommario

Appendice A

Allegati al Manuale del sistema di conservazione:

- Allegato ‘Infrastrutture’.
- PRO_CONS - Piano di Cessazione

Specificità del contratto e documenti di riferimento:

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

Torna al sommario