Manuale di Conservazione

di **RCM Italia Srl**

EMISSIONE DEL DOCUMENTO

AZIONE	DATA	NOMINATIVO	FUNZIONE
Redazione	25.05.2020	D'ANGELO dott. Marcello	*Responsabile della funzione archivistica di conservazione*
Verifica	25.05.2020	D'ANGELO dott. Gennaro	*Responsabile del servizio di conservazione*
Approvazione	25.05.2020	D'ANGELO dott. Marcello	*Responsabile della funzione archivistica di conservazione*

REGISTRO DELLE VERSIONI

N°VER/REV/BOZZA	DATA EMISSIONE	MODIFICHE APPORTATE	OSSERVAZIONI
0	15.03.2017	Prima stesura	-
1	18.01.2018	Indicazioni certificazioni possedute	-
2	13.06.2019	Aggiornamento nominativo responsabile sviluppo applicativo	-
3	25.05.2020	Specifica dettaglio indice di versamento sezione 6.2	

INDICE DEL DOCUMENTO

1. SCOPO E AMBITO DEL DOCUMENTO

RCM Italia S.r.l. nasce dalla gestione dei microfilm (1994) e progressivamente si è specializzata nei processi e servizi di archiviazione dei dati per la PA e la media azienda; dalla archiviazione dei dati clienti fino alla conservazione a norma avviata a luglio 2015.
Il presente Manuale illustra l'organizzazione, i soggetti coinvolti, il processo, l'architettura, l'infrastruttura e le misure di sicurezza del sistema di conservazione sviluppato da RCM ITALIA e che la stessa offre come servizio ai suoi clienti. Il servizio è stato disegnato e realizzato secondo quanto previsto dalle regole tecniche sui sistemi di conservazione di cui al DPCM (Decreto del Presidente del Consiglio dei Ministri) del 3 Dicembre 2013, dalla circolare n°65/2014 di AgID (Agenzia per l'Italia Digitale) e più in generale in ottemperanza a quanto previsto dal quadro normativo attualmente in vigore.

Il presente Manuale, quindi:

- è realizzato come documento nativamente informatico
- contiene le modalità operative con cui vengono erogati i servizi indicati;
- descrive le regole e le procedure utilizzate per implementare il processo di conservazione dei documenti informatici, trasferiti dal Cliente/Produttore a RCM Italia S.R.L.;
- descrive le modalità per l'esibizione dei documenti informatici sottoposti al processo di conservazione;
- descrive le procedure di sicurezza adottate nell'erogazione del servizio;
- descrive le competenze, i compiti e le responsabilità del Conservatore e dei vari Responsabili da questo individuati all'interno della propria organizzazione.
- è stato redatto al fine di poter essere pubblicato a garanzia dell'affidabilità del servizio nei confronti dei Clienti che lo utilizzano.
-

DATI IDENTIFICATIVI DEL SOGGETTO PRODUTTORE

Denominazione sociale	**RCM Italia S.R.L.**
Indirizzo sede legale	**Via Paolo Borsellino 123 80025 Casandrino (Na)**
Amministratore Unico	**Marcello D'Angelo**
P.IVA	**06736060630**
Telefono (centralino)	**+390817361552**
FAX	**+390813953335**
Sito internet	**www.rcmitalia.it**
Indirizzo PEC	**rcmitalia@pec.it**

Torna al sommario

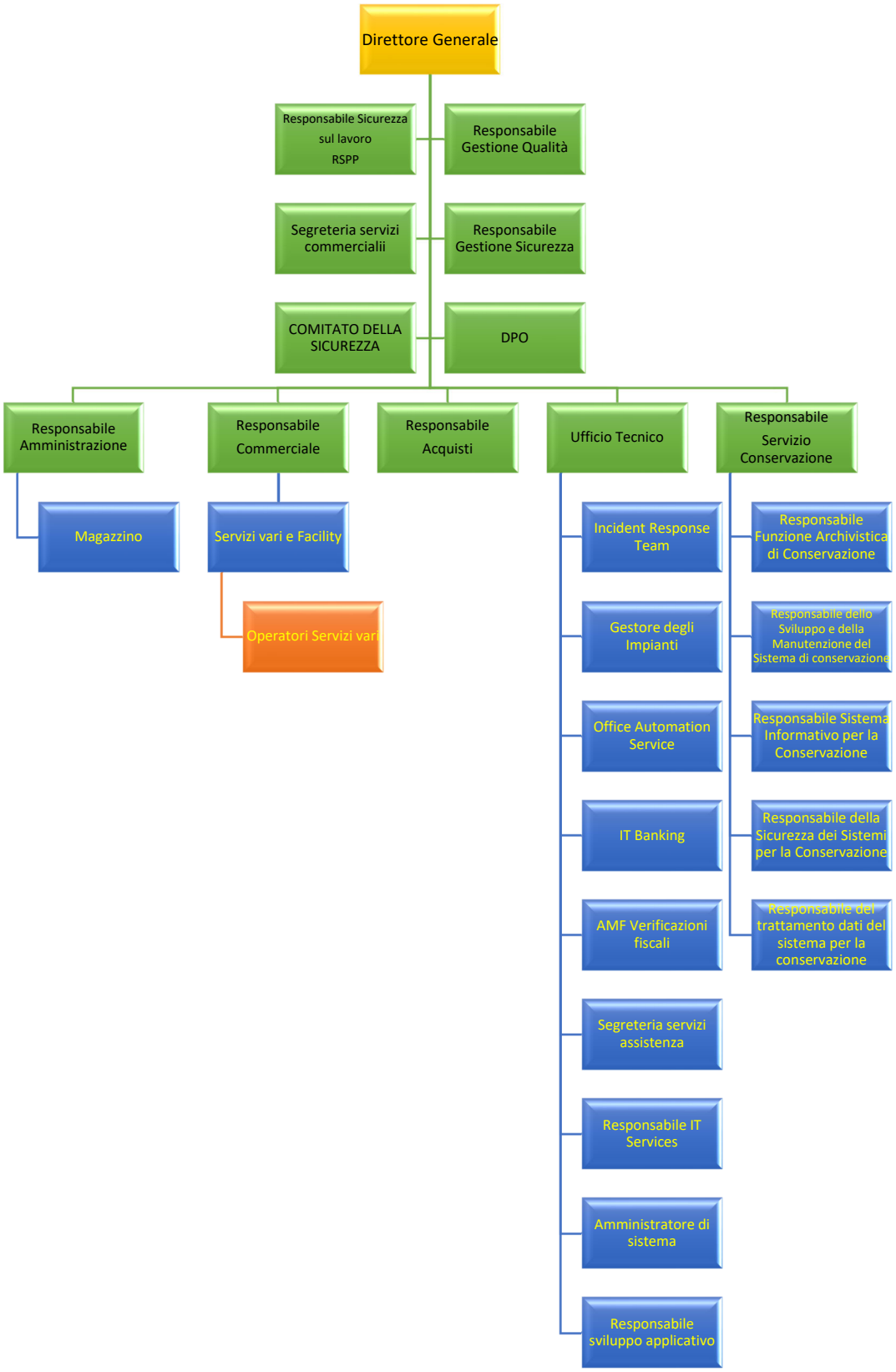

Figura 1 Organigramma rev. 6 del 13 Giugno 2019

FUNZIONE	NOMINATIVO
1. ***DIRETTORE GENERALE (DG)***	*D'Angelo Gennaro*
2. ***RESPONSABILE SICUREZZA (RSPP)***	*D'Angelo Marcello*
3. ***RESPONSABILE GESTIONE QUALITA' (RGQ)***	*D'Angelo Marcello*
4. ***RESPONSABILE GESTIONE SICUREZZA (RGS)***	*D'Angelo Marcello*
5. ***COMITATO DELLA SICUREZZA***	*(DG; RGS; RGQ; UTC; RSPP)*
6. ***DPO***	*Pinto Gianpaolo*
7. ***SEGRETERIA SERVIZI COMMERCIALI***	*Di Serio Concetta*
8. ***RESPONSABILE AMMINISTRAZIONE (AMM)***	*Pinto Gianpaolo*
9. ***DIREZIONE COMMERCIALE (COM)***	*D'Angelo Gennaro*
10. ***DIREZIONE ACQUISTI (ACQ)***	*D'Angelo Gennaro*
11. ***DIREZIONE UFFICIO TECNICO (UTC)***	*D'Angelo Carlo*
12. ***RESPONSABILE SERVIZIO CONSERVAZIONE***	*D'Angelo Gennaro*
13. ***RESPONSABILE FUNZIONE ARCHIVISTICA***	*D'Angelo Marcello*
14. ***RESPONSABILE DELLO SVILUPPO E DELLA MANUTENZIONE DEL SISTEMA DI CONSERVAZIONE***	*Elviri Simone*
15. ***RESPONSABILE SISTEMA INFORMATIVO PER LA CONSERVAZIONE***	*Farella Giovanni*
16. ***RESPONSABILE DELLA SICUREZZA DEI SISTEMI PER LA CONSERVAZIONE***	*D'Angelo Gennaro*
17. ***RESPONSABILE DEL TRATTAMENTO DATI DEL SISTEMA PER LA CONSERVAZIONE***	*D'Angelo Marcello*
18. ***RESPONSABILE MAGAZZINO (MAG)***	*Napolano Pasquale*
19. ***RESPONSABILE SERVIZI VARI e FACILITY***	*Barretta Francesco*
20. ***INCIDENT RESPONSE TEAM***	*D'Angelo Marcello e D'Angelo Carlo*
21. ***GESTORE DEGLI IMPIANTI***	*D'Angelo Marcello e D'Angelo Carlo*
22. ***OFFICE AUTOMATION SERVICE***	*D'Angelo Carlo*
23. ***IT BANCKING***	*D'Angelo Marcello*
24. ***AMF VERIFICAZIONI FISCALI***	*D'Angelo Carlo*
25. ***SEGRETERIA SERVIZI ASSISTENZA***	*Perone Carmela*
26. ***RESPONSABILE IT SERVICES***	*D'Angelo Marcello*
27. ***AMMINISTRATORE DI SISTEMA***	*Elviri Simone*
28. ***RESPONSABILE SVILUPPO APPLICATIVO***	*de Lorenzo Pietro*

2. TERMINOLOGIA (GLOSSARIO, ACRONIMI)

GLOSSARIO

TERMINE	DEFINIZIONE
Accesso	Operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici
Accreditamento	Riconoscimento, da parte dell'Agenzia per l'Italia digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione
Affidabilità	Caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico
Aggregazione documentale informatica	Aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente
Allegato	Documento che compone l'Unità documentaria per integrare le informazioni contenute nel documento principale. È redatto contestualmente o precedentemente al documento principale. La sua presenza è facoltativa
Annesso	Documento che compone l'Unità documentaria, generalmente prodotto e inserito nell' unità documentaria in un momento successivo a quello di creazione dell'Unità documentaria, per fornire ulteriori notizie e informazioni a corredo del Documento principale
Apertura	Un formato si dice "aperto" quando è conforme a specifiche pubbliche, cioè disponibili a chiunque abbia interesse ad utilizzare quel formato. Gli organismi di standardizzazione internazionali considerati dalla normativa sono ISO e ETSI
Application server	Tipologia di server che fornisce l'infrastruttura e le funzionalità di supporto, sviluppo ed esecuzione di applicazioni nonché altri componenti server in un contesto distribuito. Si tratta di un complesso di servizi orientati alla realizzazione di applicazioni ad architettura multilivello ed enterprise, con alto grado di complessità, spesso orientate per il web (applicazioni web)
Archivio	Complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività
Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico
Autenticità	Caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico
Certificatore accreditato	Soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, dall' Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
Ciclo di gestione	Arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo
Classificazione	Attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati
Cluster	Insieme di dispositivi di elaborazione connessi in maniera più o meno stretta che operano insieme in modo tale da poter essere considerati un unico sistema
Codice	Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni
Comunità di riferimento	Un gruppo ben individuato di potenziali Utenti che dovrebbero essere in grado di comprendere un particolare insieme di informazioni. La Comunità di riferimento può essere composta da più comunità di Utenti. [da OAIS]

Conservatore accreditato	Soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, dall'Agenzia per l'Italia digitale
Conservazione	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione
Contenuto informativo	L'insieme delle informazioni che costituisce l'obiettivo originario della conservazione. E' composto dall'Oggetto-dati e dalle Informazioni di rappresentazione [da OAIS]
Data center	Struttura utilizzata per ospitare computer e componenti associati quali dispositivi di telecomunicazioni e di storage, in generale con adeguati livelli di prestazioni e di sicurezza.
Diffusione	È l'estensione dell'impiego di uno specifico formato per la formazione e la gestione dei documenti informatici affinché sia più probabile che esso venga supportato nel tempo. La questione ha impatti sul fatto che un formato possa avere la disponibilità di più prodotti informatici idonei alla sua gestione e visualizzazione
Disaster recovery	Insieme delle misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi di business per imprese, associazioni o enti, a fronte di gravi emergenze che ne intacchino la regolare attività
Esibizione	Operazione che consente di visualizzare un documento conservato e di ottenerne copia
Evidenza informatica	Una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica
Fascicolo informatico	Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del Codice
File di indice	Indice dei PdA: file XML che contiene tutti gli elementi del Pacchetto di archiviazione, derivati sia dalle informazioni contenute nel PdV (o nei PdV) trasmessi dal Produttore, sia da quelle generate dal Sistema di conservazione nel corso del processo di conservazione
Formato	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
Funzionalità	La possibilità da parte di un formato di essere gestito da prodotti informatici, che prevedono una varietà di funzioni messe a disposizione dell'utente per la formazione e gestione del documento informatico
Funzione di hash	Una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
Identificativo univoco	Sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione
Impronta	La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash
Informazioni descrittive	Descrivono il pacchetto informativo e consentono di ricercarlo nel sistema di conservazione. In base alle caratteristiche della tipologia di oggetto contenuto nel Pacchetto, tali informazioni possono essere un sottoinsieme di quelle presenti nel pacchetto informativo, possono coincidere o possono anche essere diverse
Informazioni sulla conservazione (PDI)	Informazioni necessarie a conservare il Contenuto informativo e garantiscono che lo stesso sia chiaramente identificato e che sia chiarito il contesto in cui è stato creato. Sono costituite da metadati che definiscono la provenienza, il contesto, l'identificazione e l'integrità del Contenuto informativo oggetto della conservazione [da OAIS]
Informazioni sulla rappresentazione	Informazioni che associano un Oggetto-dati a concetti più significativi.

Informazioni sull' impacchettamento	Informazioni che consentono di mettere in relazione nel Sistema di conservazione, in modo stabile e persistente, il Contenuto informativo con le relative Informazioni sulla conservazione
Integrità	Insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato
Interoperabilità	Capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi
Leggibilità	Insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti
Log di sistema	Registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati
Manuale di conservazione	Strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 delle regole tecniche del sistema di conservazione
Marca temporale	Sequenza di caratteri che rappresentano una data e/o un orario per accertare l'effettivo avvenimento di un certo evento. La data è di solito presentata in un formato compatibile, in modo che sia facile da comparare con un'altra per stabilirne l'ordine temporale. La pratica dell'applicazione di tale marca temporale è detto timestamping
Memorizzazione	Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici
Metadati	Insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 del DPCM 3 dicembre 2013
Pacchetto di archiviazione	Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del presente decreto e secondo le modalità riportate nel manuale di conservazione
Pacchetto di distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta
Pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione
Pacchetto informativo	Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare
Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza
Piano di conservazione	Strumento, integrato con il sistema di classificazione per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445
Portabilità	La facilità con cui i formati possano essere usati su piattaforme diverse, sia dal punto di vista dell'hardware che del software, inteso come sistema operativo. RCM Italia, utilizzando gli standard sopra descritti, è possibile rispettare questo criterio. La portabilità è fondamentale perché un cliente possa esportare i propri dati presso un altro outsourcer qualora, alla fine del contratto, non intenda rinnovarlo. Essa è altresì importante per poter viceversa importare i dati di un nuovo cliente provenienti da un altro outsourcer che utilizzi gli standard descritti dalla normativa
Presa in carico	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione
Processo di conservazione	Insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 10 delle regole tecniche del sistema di conservazione
Produttore	Persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale
Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore

Responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi	Dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione
Responsabile della conservazione	Soggetto responsabile dell'insieme delle attività elencate nell'articolo 7, comma 1 delle regole tecniche del sistema di conservazione
Responsabile del servizio di conservazione	Soggetto individuato dai profili professionali, indicato nell'allegato alla circolare n. 65 del 10 aprile 2014, AGID
Responsabile del trattamento dei dati	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali
Responsabile della sicurezza	Soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza
Riferimento temporale	Informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento
Scarto	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale
Serie	Unità Archivistiche o Unità Documentarie ordinate secondo un sistema di classificazione o conservati insieme perché: - sono il risultato di un medesimo processo di sedimentazione o archiviazione o di una medesima attività; - appartengono ad una specifica tipologia documentaria; - a ragione di qualche altra relazione derivante dalle modalità della loro produzione, acquisizione o uso (fonte: ISAD)
Sicurezza	La sicurezza di un formato dipende da due elementi: il grado di modificabilità del contenuto del file e la capacità di essere immune dall'inserimento di codice maligno. Nel sistema di i pacchetti di riversamento vengono sottoposti a scansione antivirus con verifica dei file e archivi compressi multilivello. Ogni file compresso è quindi controllato anche se si tratta di compressioni ripetute (tecnica utilizzata per evitare che l'antivirus controlli i file di un archivio compresso). Gli antivirus utilizzati sono costantemente aggiornati. L'invio dei file, inoltre, avviene attraverso linee controllate da firewall e Intrusion detector
Sistema di classificazione	Strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata
Sistema di conservazione	Sistema di conservazione dei documenti informatici di cui all'articolo 44 del Codice
Sistema di gestione informatica dei documenti	Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445; per i privati è il sistema che consente la tenuta di un documento informatico
Supporto allo sviluppo	E' la modalità con cui si mettono a disposizione le risorse necessarie alla manutenzione e sviluppo del formato e i prodotti informatici che lo gestiscono (organismi preposti alla definizione di specifiche tecniche e standard, società, comunità di sviluppatori, ecc.)
Testo unico	Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni
Unità archivistica	Insieme organizzato di Unità documentarie o Documenti raggruppati dal Produttore per le esigenze della sua attività corrente in base al comune riferimento allo stesso oggetto, attività o fatto giuridico. Può rappresentare una unità elementare di una Serie
Unità documentaria	Unità minima, concettualmente non divisibile, di cui è composto un archivio, per esempio, una lettera, un memorandum, un rapporto, una fotografia, una registrazione sonora (ISAD (G)
Versamento	Azione di trasferimento di PdV dal Produttore al Sistema di conservazione
Versamento agli archivi di Stato	Operazione con cui il responsabile della conservazione di un organo giudiziario o amministrativo dello Stato effettua l'invio agli Archivi di Stato o all'Archivio Centrale

	dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali
Utente	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse

ACRONIMI

ACRONIMO	SIGNIFICATO
AgID	Agenzia per l'Italia digitale
AIP (PdA)	Archival Information package (Pacchetto di archiviazione)
CA	Certification Autorithy / Prestatore di servizio fiduciario qualificato
CAD	Codice dell'amministrazione digitale
CRL	Certificate Revocation List, è la lista dei certificati revocati o sospesi, ovvero lista di certificati che sono stati resi non validi prima della loro naturale scadenza
DIP (PdD)	Dissemination Information Package (Pacchetto di distribuzione)
HSM	Hardware Security Module, è l'insieme di hardware e software che realizza dispositivi sicuri per la generazione delle firme in grado di gestire in modo sicuro una o più coppie di chiavi crittografiche
ISO	International organization for Standardization
IR	Informazioni sulla rappresentazione
IRse	Informazioni sulla rappresentazione semantiche
IRSI	Informazioni sulla rappresentazione sintattiche
OAIS	Open archival information system di cui allo standard ISO 14721
PDI	Preservation description information (Informazioni sulla conservazione)
PEC	Posta Elettronica Certificata
SIP (PdV)	Submission Information Package (Pacchetto di versamento).
SMTP	Simple Mail Transfer Protocol (SMTP) è il protocollo standard per la trasmissione via internet di e-mail.
TSA	Time Stamping Autorithy, è il soggetto che eroga la marca temporale.
UNI SinCRO	UNI 11386:2010 – Supporto all'Interoperabilità nella conservazione e nel Recupero.

Torna al sommario

3. NORMATIVA E STANDARD DI RIFERIMENTO

3.1 Normativa di riferimento

Il presente elenco riporta la normativa nazionale italiana di riferimento in ambito di conservazione dei documenti informatici.

Regolamento UE n. 910/2014 – eIDAS, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE
Regolamento UE n.679/2016 – GDPR, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE
Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. Codice dell’amministrazione digitale (CAD);
Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
Circolare AGID 10 aprile 2014, n. 65 - Modalità per l’accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.

Torna al sommario

3.2 Standard di riferimento

ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
ETSI TR 101 533-2 V1.3.1 (2012-04)Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

3.3 Certificazioni

- La RCM Italia è certificata ISO 9001:2015 e ISO/IEC 27001:2013

- I servizi di connettività e la gestione dei servizi di rete sono in gestione alla Società Retelit, certificata ISO 9001 e ISO/IEC 27001: 2013, presso i cui siti sono erogati i servizi di housing nei Data Center di Roma e Napoli con certificazione ISO/IEC 27001:2013

- I servizi fiduciari sono affidati alla Società Actalis, iscritta al Pubblico Elenco dei Certificatori della firma digitale e all'Elenco dei gestori di Posta Elettronica Certificata (PEC) presso l'Agenzia per l'Italia Digitale (AgID).

I servizi, i prodotti e le soluzioni di Actalis sono realizzati nel rispetto degli standard di qualità, sicurezza e solidità richiesti dalle leggi e dalle norme vigenti.

I dispositivi crittografici offerti da Actalis sono dotati di una o più delle seguenti certificazioni di sicurezza:

- ITSEC, a livello E3 HIGH o superiore;
- Common Criteria a livello EAL4 o superiore;
- FIPS PUB 140-2 Level 3 o superiore;

Actalis è certificata ISO 9001:2015, ISO/IEC 27001:2013 ed è accreditata eIDAS.

Torna al sommario

4. RUOLI E RESPONSABILITÀ

Il modello organizzativo di un sistema di conservazione preveda l'interazione tra:

a) il produttore (ruolo svolto da persone o sistemi che versano i pacchetti di versamento al sistema di conservazione);
b) il responsabile della conservazione;
c) l'utente (ruolo che ha la possibilità di richiedere al sistema di conservazione l'accesso al pacchetto di distribuzione).

Lo svolgimento del processo di conservazione richiede la presenza di più figure coinvolte, ognuna delle quali ha la responsabilità di specifiche attività da svolgere.
Nella tabella di seguito riportata sono indicati le attività svolte e i nominativi delle persone che ricoprono i ruoli richiesti per lo svolgimento del processo di conservazione, cosi come individuati nel documento "Profili professionali", allegato alla circolare n°65/2014 di AgID. Per ogni figura interna al sistema di conservazione sono richiesti specifici requisiti di onorabilità e di esperienza minima nel ruolo. Peraltro, così com'è previsto che alcune attività possano essere svolte dal medesimo soggetto è, altresì, previsto che alcune funzioni possano essere affidate ad altri soggetti, fermo restando i predetti vincoli di onorabilità e di requisiti di esperienza del delegato. In tal caso per ciascuna delega saranno indicati i dati identificativi del delegato, il relativo periodo di riferimento e le attività, oggetto di delega.

Ruolo	Attività di competenza	Nominativo	Periodo nel ruolo	Eventuali deleghe
Responsabile del servizio di Conservazione	Definizione e attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione; - definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente; - corretta erogazione del servizio di conservazione all'ente produttore; - gestione delle convenzioni, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.	Gennaro D'Angelo	Dal 1/10/2015	
Responsabile della funzione archivistica di conservazione	- Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; - definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici; - monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione; - collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.	Marcello D'Angelo	Dal 1/10/2015	
Responsabile del trattamento dei dati personali	- Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; - garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni	Marcello D'Angelo	Dal 1/10/2015	

	impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza			
Responsabile della sicurezza dei sistemi per la conservazione	Rispetta e monitora i requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; - Segnala eventuali difformità al Responsabile del servizio di conservazione e individua e pianifica le necessarie azioni correttive.	Gennaro D'Angelo	Dal 1/10/2015	
Responsabile dei sistemi informativi per la conservazione	Gestisce l'esercizio delle componenti hardware e software del sistema di conservazione; - Monitora il mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore; - Segnala eventuali difformità degli SLA al Responsabile del servizio di conservazione e individua e pianifica le necessarie azioni correttive; - Pianifica lo sviluppo delle infrastrutture tecnologiche del sistema di conservazione; - Controlla e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.	Giovanni Farella	Dal 1/10/2015	Nomina D.G. del 30/09/2015
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	- Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione; - pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione; - monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione; - interfaccia con l'ente produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche; - gestione dello sviluppo di siti web e portali connessi al servizio di conservazione. - oordina lo sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione;	Simone Elviri	Dal 1/10/2015	Nomina D.G. del 30/09/2015

Torna al sommario

5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Organigramma

RCM Italia si configura come soggetto conservatore che svolge attività di conservazione. RCM Italia definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia. Secondo quanto stabilito dall'art. 6 comma 8 del DPCM 3 dicembre 2013 e, secondo quanto previsto dal Codice in materia di protezione dei dati personali, il conservatore RCM Italia assume il ruolo di responsabile del trattamento dei dati (art. 28 GDPR), come individuato anche con specifico atto scritto.
Tutte le persone coinvolte nel servizio di conservazione sono state istruite rispetto al trattamento dei dati da effettuare nell'ambito delle attività di conservazione. Nel contratto di affidamento del servizio di conservazione con il soggetto Produttore si riconosce a quest'ultimo la titolarità del trattamento dei dati contenuti nei documenti oggetto di conservazione in capo al soggetto Produttore.

Figura 2 Organigramma RCM Italia srl

Torna al sommario

5.2 Strutture organizzative

Attività proprie di ciascun contratto di servizio di conservazione

L'attività del servizio di conservazione e presa in carico da parte di RCM Italia viene espletata a seguito della sottoscrizione di un contratto per il servizio di conservazione con il soggetto produttore. RCM Italia predispone la redazione del contratto attraverso l'area commerciale-amministrativa della società.

Il contratto consente l'avvio delle attività di attivazione del servizio. La responsabilità di tale sotto processo è del responsabile del servizio di conservazione. Attraverso l'area del *Provisioning*, detto responsabile coordina e gestisce l'attivazione del servizio di conservazione per il Soggetto Produttore.

La prima parte del processo di conservazione, relativa all'acquisizione e verifica dei pacchetti di versamento, da parte del soggetto produttore, viene gestita dal responsabile del servizio di conservazione.

Se il pacchetto di versamento è accettato significa che risponde a tutti i controlli di presa in carico previsti tramite contratto di affidamento del servizio con il cliente.

Se il pacchetto di versamento non risponde pienamente a tutte le verifiche di presa in carico il pacchetto viene rifiutato. Il conservatore RCM Italia è responsabile della conservazione dei soli pacchetti di versamento accettati.

La generazione del rapporto di versamento sarà effettuata di conseguenza dopo le verifiche di conformità alla normativa e agli standard di riferimento, da parte del responsabile del servizio di conservazione, coadiuvato dal responsabile del servizio archivistico.

Il responsabile del servizio di conservazione, per i pacchetti accettati, provvede alla preparazione e alla gestione del pacchetto di archiviazione. Detto pacchetto viene così firmato e marcato digitalmente.

Per quanto concerne il processo di esibizione sarà cura del responsabile del servizio di conservazione mettere a disposizione i pacchetti di distribuzione all'utente.

Il processo di *deprovisioning* si attiva qualora un Soggetto Produttore arriva alla scadenza naturale del suo contratto con RCM Italia e non intenda rinnovarlo. La gestione e la responsabilità di tali attività sono in carico al responsabile del servizio di conservazione.

Infine, l'eventuale attività di scarto della documentazione conservata, su richiesta del Produttore o in conseguenza del processo di *deprovisioning,* è realizzata dal Responsabile del servizio di conservazione con il supporto del Responsabile della funzione archivistica.

La seguente tabella, descrive nel dettaglio le attività, le responsabilità e chi si occupa della loro realizzazione, relativamente al ciclo di vita contrattuale dell'adesione al servizio.

Attività	Responsabilità	Area di competenza
Attivazione del servizio di conservazione (a seguito della sottoscrizione di un contratto).	Responsabile del servizio di conservazione, supporto del Responsabile della funzione archivistica di conservazione; Responsabile del trattamento dei dati	Provisioning
Acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento.	Responsabile del servizio di conservazione, supporto del Responsabile della funzione archivistica di conservazione	Controlli di processo e di sistema
Preparazione e gestione del pacchetto di archiviazione. Il pacchetto di archiviazione è firmato digitalmente dal responsabile del servizio di conservazione e viene apposta una validazione temporale qualificata al pacchetto di archiviazione.	Responsabile del servizio di conservazione	Controlli di processo e di sistema
Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione.	Responsabile del servizio di conservazione	Controlli di processo e di sistema
Scarto dei pacchetti di archiviazione.	Responsabile del servizio di conservazione, supporto del Responsabile della funzione archivistica di conservazione, previa autorizzazione da parte del soggetto produttore	Controlli di processo e di sistema
Chiusura del servizio di conservazione (al termine di un contratto).	Responsabile del servizio di conservazione, supporto del Responsabile della funzione archivistica di conservazione, Responsabile del trattamento dei dati	Deprovisioning

Tabella 1 Attività, responsabilità e ruoli nelle attività del processo di conservazione

Attività proprie di gestione dei sistemi informativi

Per ciò che riguarda i processi di gestione dei sistemi informativi dedicati al servizio di conservazione, le attività di conduzione e manutenzione del sistema di conservazione sono garantite dal responsabile dei sistemi informativi per la conservazione.

Il monitoraggio del sistema di conservazione è in carico al responsabile dei sistemi informativi per la conservazione per quanto concerne i sistemi informativi e le soluzioni per garantire lo SLA (Service Level Agreement). Il responsabile della sicurezza dei sistemi per la conservazione è invece colui che coordina e garantisce il monitoraggio dei requisiti per la sicurezza dei sistemi e degli ambienti.

Il *change management* della piattaforma dedicata al servizio di conservazione è invece un processo controllato e seguito dal responsabile dello sviluppo e della manutenzione del sistema di conservazione. Esso serve per garantire la leggibilità nel tempo dei documenti conservati ed evitare che l'obsolescenza dei sistemi possa pregiudicarne l'esibizione.

Per quanto riguarda gli adeguamenti dei sistemi informativi della conservazione agli standard e alle normative specifiche, le indicazioni provengono dal responsabile della funzione archivistica di conservazione, che si occupa delle verifiche periodiche di conformità a normativa e standard di riferimento. Il responsabile della funzione archivistica di conservazione ha quindi il compito di aggiornare RCM Italia sulle normative a gli standard di riferimento e provvederà a tenere dei corsi di aggiornamento alle strutture organizzative coinvolte nel processo di conservazione.

La seguente tabella, descrive nel dettaglio le attività, le responsabilità e chi si occupa della loro realizzazione, relativamente alla gestione dei sistemi informativi:

Attività	Responsabilità	Area di competenza
Conduzione e manutenzione del sistema di conservazione	Responsabile dei sistemi informativi	Esercizio piattaforme applicative e sistemi
Monitoraggio del sistema di conservazione	Responsabile dei sistemi informativi e Responsabile Sicurezza	Esercizio piattaforme applicative e sistemi
Change management	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Manutenzione e delivery
Verifica periodica di conformità a normativa e standard di riferimento	Responsabile della funzione archivistica di conservazione e Responsabile Sicurezza	Normative e standard

Tabella 2 Attività, responsabilità e ruoli nei processi dei sistemi informativi

Torna al sommario

6. OGGETTI SOTTOPOSTI A CONSERVAZIONE

RCM Italia S.r.l. è in grado di gestire diverse tipologie di documenti, relativi a diversi ambiti applicativi, quali ad esempio:

- Contratti ed allegati
- Fatture attive e Fatture passive
- Documenti di trasporto
- Libri e registri sociali
- Libri e registri contabili
- Libretto unico del lavoro (LUL)
- Libri, registri e documenti di amministrazione del personale
- Documenti correlati con la gestione delle notifiche

Torna al sommario

6.1 Oggetti conservati

Il Sistema di conservazione KeepEasy conserva documenti informatici, in particolare documenti amministrativi informatici, con i metadati ad essi associati e le loro aggregazioni documentali informatiche (aggregazioni), che includono i fascicoli informatici.

Il sistema gestisce gli oggetti digitali sottoposti a conservazione distinti per ogni singolo soggetto produttore, anche per singola struttura (generalmente corrispondenti alle Aree Organizzative Omogenee), consentendo di definire configurazioni e parametrazioni *ad hoc* per ogni soggetto produttore, in base agli accordi stipulati all'atto della sottoscrizione del servizio.

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

Le serie ed i fascicoli possono essere versati nel sistema quando sono completi e dichiarati chiusi, descritti da un set di metadati che include obbligatoriamente, oltre alle informazioni di identificazione, classificazione e descrizione, anche il tempo di conservazione previsto. Nel caso delle serie, la chiusura può avvenire a cadenza annuale o comunque secondo una definizione temporale definita dal soggetto produttore.

I documenti informatici (unità documentarie), e i fascicoli delle amministrazioni pubbliche sono classificati e gestiti secondo il piano di classificazione. La classificazione è una attività basilare per la gestione e la conservazione dei documenti degli archivi, ha lo scopo di garantire un'organizzazione logica dei documenti, basata su fondamenti oggettivi e condivisi. Il piano di classificazione o titolario è il sistema precostituito di partizioni astratte, gerarchicamente ordinate (dal generale al particolare), fissate sulla base dell'analisi delle funzioni dell'ente, al quale deve ricondursi la molteplicità dei documenti prodotti, per organizzarne la sedimentazione ordinata. Il titolario si sviluppa su più livelli, denominati dalla dottrina: titolo, classe, sottoclasse.

Le tipologie documentarie (trattate e i loro specifici metadati e articolazioni), sono indicate nell'allegato di servizio concordato con ogni soggetto produttore e riportate nelle funzionalità di amministrazione del

sistema. Un elenco delle tipologie documentali conservate all'interno del sistema di conservazione gestito da RCM Italia è allegato al presente manuale (rif. Elenco tipologie e metadati).

L'unità documentaria rappresenta l'unità minima elementare di riferimento di cui è composto un archivio, pertanto rappresenta il riferimento principale per la costruzione dei pacchetti informativi secondo il modello OAIS.

Con riferimento a quanto indicato nello standard ISO 23081-2, l'unità documentaria, rappresenta la più piccola *"unit of records*" individuabile e gestibile come una entità singola gestita nel sistema, anche se al suo interno contiene elementi come ad esempio un messaggio di posta elettronica con i suoi allegati.

All'unità documentaria e agli elementi che la compongono sono associati set di metadati che li identificano e li descrivono. Coerentemente con quanto sopra riportato l'unità documentaria è pertanto logicamente strutturata su tre livelli: unità documentaria, documento, File.

Il sistema di conservazione utilizza come formati di conservazione quelli della Tabella 9- "*Formati ammessi per la conservazione*" e, inoltre, è in grado di gestire, su richiesta del soggetto produttore, anche formati non compresi nel suddetto elenco, ma che il soggetto produttore utilizza nei propri sistemi e che ritiene di dover conservare.

Tutti i formati gestiti sono elencati e descritti in un registro interno al sistema di conservazione "Registro dei Formati" in cui ogni formato è corredato da informazioni descrittive relative alla eventuale versione, e al *mimetype*.

Con ogni soggetto produttore è concordato un elenco di formati ammessi, che individua i formati che il sistema può accettare da ogni produttore e per ogni tipologia documentaria gestita. L'elenco dei formati ammessi è riportato (e gestito) nelle funzionalità "Amministrazione strutture versanti" del sistema ed è aggiornato continuamente in base alle esigenze del produttore. Le modalità con cui si procede a tale aggiornamento sono concordate con ogni Produttore e riportate nell'allegato "Registro dei Formati".

Il sistema identifica i formati al momento della ricezione del PdV mediante l'analisi dei *magic number* o del contenuto del file, in modo tale da consentire l'individuazione dello specifico *mimetype.* L'informazione sul formato è parte dei metadati dei componenti dell'unità documentaria e costituisce un elemento delle informazioni sulla rappresentazione.

Formato	Proprietario	Estensione	Tipo	Aperto	Standard
PDF - PDF/A	Adobe Systems	.pdf	application/pdf	Si	ISO 32000-1 (PDF); ISO 19005-1:2005 (vers. PDF 1.4); ISO 19005-2:2011 (vers. PDF 1.7)
TIFF	Aldus Corporation (acquisita Adobe)	.tif	image/tiff	No	ISO 12639 (TIFF/IT); ISO 12234 (TIFF/EP)
JPG e JPEG 2000	Joint Photographic Experts Group	.jpg, .jpeg, .jp2 (JPEG 2000)	image/jpeg	Si	ISO/IEC 10918:1 (JPG); ISO/IEC 15444-1 (JPEG 2000)
Office Open XML (OOXML)	Microsoft	.docx, .xlsx, .pptx	MIME	Si	ISO/IEC DIS 29500:2008

ODF Open Document Format	OASIS	.ods, .odp, .odg, .odb	application/vnd.oasis.opendocument.text	Si	ISO/IEC 26300:2006; UNI CEI ISO/IEC 26300
XML Extensible Markup Language	W3C	.xml	application/xml text/xml	Si	
TXT	-	.txt	ASCII, UTF-8,UNICODE	Si	ISO 646, RFC 3629, ISO/IEC 10646
PEC ed EMAIL	-	.eml	MIME	No	RFC 2822/MIME
ZIP	PKWARE	.ZIP	application/zip	SI	ISO/IEC 21320:2015
RAR	Eugene Roshal	.rar	application/x-rar-compressed	NO	

Al fine di soddisfare l'eventuale necessità di una disponibilità immediata dell'oggetto conservato, il sistema di conservazione Keep Easy conserva gli strumenti per la leggibilità (visualizzatori) degli oggetti dati da conservare.

Torna al sommario

6.2 Pacchetto di versamento

Si tratta del pacchetto informativo inviato dal produttore al sistema di conservazione. Ogni pacchetto di versamento ricevuto sarà trasformato in Pacchetto di Archiviazione.

La fase relativa alla preparazione del pacchetto di versamento (PdV) e il conseguente versamento nel sistema di conservazione può avvenire in modi diversi, poiché dipende dalla situazione specifica del soggetto produttore e dagli accordi stipulati con il conservatore.

Il sistema di conservazione KeepEasy prevede le seguenti modalità di versamento:

1. automatica - via web service: tale modalità prevede l'invio automatico in conservazione di PdV prodotti dai sistemi gestionali in uso del Produttore che richiamano una funzione remota pubblicata da KeepEasy il quale costruirà il PdA e gestirà i metadati verificandone la congruenza.

2. via interfaccia web mediante upload manuale dei documenti: tramite apposita interfacia presente in KeepEasy il Produttore può selezionare i documenti da conservare, inserire (tramite apposta maschera) i metadati ad essi relativi e procedere con l'invio degli stessi al sistema di conservazione.

Trattandosi, di elaborazioni effettuate direttamente mediante sistemi forniti da RCM Italia, i controlli sulla corretta formazione del PDV vengono effettuati contestualmente alla creazione stessa del PDV e la sua struttura sarà identica a quella del PdA poi successivamente conservato così come specificato nei paragrafi successivi.

I PdV sono corredati di un file indice avente la struttura come da esempio seguente:

```
<?xml version="1.0" encoding="UTF-8"?>
<ArchieasyIndex documentClass="ae_lot_fat_in">
 <ID>L_FTIN_4_9</ID>
 <CreatingApplication>
  <Name>KeepEasy</Name>
  <Version>1.1</Version>
  <Producer>RCM ITALIA SRL</Producer>
 </CreatingApplication>
 <FileGroup>
  <field1 name="descrizione_lotto_ftin">Fatture mese 01 Anno 2019</field1>
  <field2 name="anno_fiscale">2019</field2>
  <field3 name="data_inizio_numerazione_ftin">2019-01-01</field3>
  <field4 name="data_fine_numerazione_ftin">2019-01-01</field4>
  <Group Tipo="Fatture Attive" Numero="2">
   <Data>
    <field_D1 name="Nome File">IT06736060630_07036.xml</field_D1>
    <field_D2
name="Hash">1f05714af4b30f6ba4de5fb0505ecc14f6882761f3e013e96e79a2e05d09b5c3</field_D2>
    <field_D3 name="Indentificativo SDI">582825303</field_D3>
    <field_D4 name="Tipo Fattura">FPA12</field_D4>
    <field_D5 name="Ragione Sociale">Cliente1</field_D5>
    <field_D6 name="P.iva/Codice Fiscale">10987654321</field_D6>
    <field_D7 name="Num.Fattura">02/1</field_D7>
    <field_D8 name="Data Fattura">2019-01-01</field_D8>
   </Data>
   <Data>
    <field_D1 name="Nome File">IT06736060630_07037.xml</field_D1>
    <field_D2
name="Hash">fafa6132e1370c640c1a413868bec87bebc58b612b88782ec0d315c1e026c5f6</field_D2>
    <field_D3 name="Indentificativo SDI">839023917</field_D3>
    <field_D4 name="Tipo Fattura">FPA12</field_D4>
    <field_D5 name="Ragione Sociale">cliente2</field_D5>
    <field_D6 name="P.iva/Codice Fiscale">12345678901</field_D6>
    <field_D7 name="Num.Fattura">02/2</field_D7>
    <field_D8 name="Data Fattura">2019-01-01</field_D8>
   </Data>
  </Group>
  <Group Tipo="Fatture Passive" Numero="1">
   <Data>
    <field name="Nome File">IT04705810150_00V3B.xml</field>
    <field
name="Hash">f06a687b750b868f61ed232364f33122da03e234489ab5d07f2c937563472611</field>
    <field name="Indentificativo SDI">445779977</field>
    <field name="Tipo Fattura">FPR12</field>
    <field name="Ragione Sociale">Fornitore1</field>
    <field name="P.iva/Codice Fiscale">10293847560</field>
    <field name="Num.Fattura">01</field>
    <field name="Data Fattura">2019-01-01</field>
   </Data>
  </Group>
  <Group Tipo="Esiti">
   <Data>
    <field name="Nome File">IT06736060630_07036_RC_002.xml</field>
```

```
    <field
name="Hash">21daea80cb30b4e13c569a4d7bdc08413666d91c4382a5e46f1b0cd4ba94ba5e</field>
    <field name="Indentificativo SDI">173760330</field>
    <field name="Tipo Fattura">FPR12</field>
    <field name="Ragione Sociale">Cliente1</field>
    <field name="P.iva/Codice Fiscale">10987654321</field>
    <field name="Num.Fattura">02/1</field>
    <field name="Data Fattura">2019-01-01</field>
   </Data>
   <Data>
    <field name="Nome File">IT06736060630_07037_RC_002.xml</field>
    <field
name="Hash">ea879c49e5ea5d30ec0ee530739441dc53f796b9bd6305e4b59020c448e76859</field>
    <field name="Indentificativo SDI">173760634</field>
    <field name="Tipo Fattura">FPR12</field>
    <field name="Ragione Sociale">Cliente2</field>
    <field name="P.iva/Codice Fiscale">12345678901</field>
    <field name="Num.Fattura">02/2</field>
    <field name="Data Fattura">2019-01-01</field>
   </Data>
  </Group>
 </FileGroup>
 <Process>
  <Agent type="person" role="OtherRole">
   <AgentName>
    <NameAndSurname>
     <FirstName>Marcello</FirstName>
     <LastName>D'Angelo</LastName>
    </NameAndSurname>
   </AgentName>
   <Agent_ID></Agent_ID>
  </Agent>
  <Agent type="Organization" role="OtherRole">
   <AgentName>
    <FormalName>RCM ITALIA SRL</FormalName>
   </AgentName>
   <Agent_ID>06736060630</Agent_ID>
  </Agent>
  <Agent type="person" role="PreservationManager">
   <AgentName>
    <NameAndSurname>
     <FirstName>Gennaro</FirstName>
     <LastName>D'Angelo</LastName>
    </NameAndSurname>
   </AgentName>
   <Agent_ID>DNGGNR63L05F839F</Agent_ID>
  </Agent>
  <TimeReference>
   <TimeInfo>2020-05-20T21:23:54+01</TimeInfo>
  </TimeReference>
  <LawAndRegulations>DPCM 13 Novembre 2014</LawAndRegulations>
 </Process>
</ArchieasyIndex>
```


Torna al sommario

6.3 Pacchetto di archiviazione

Il pacchetto di archiviazione (PdA) è l'elemento fondamentale del sistema di conservazione. È il pacchetto informativo che racchiude in sé tutti gli elementi sufficienti e necessari per una conservazione a lungo termine. Contiene gli oggetti digitali e le informazioni di conservazione ovvero le informazioni di identificazione, provenienza, contesto, integrità, contenuto. Un pacchetto di archiviazione è un oggetto informativo, contenitore a sua volta di altri oggetti informativi. All'interno del pacchetto di archiviazione, si trova l'oggetto informativo individuato per la conservazione, ovvero il contenuto informativo.
Il principio su cui si basa l'architettura del modello dati del sistema di conservazione è quello di un'auto-consistenza del pacchetto informativo nel momento in cui è costituito il PdA stesso, tale obiettivo viene raggiunto grazie all'aderenza al modello funzionale e al modello-dati previsto in OAIS.
La coerenza di un pacchetto informativo è data da due componenti logiche fondamentali:

- l'insieme delle informazioni statiche che prevedono un set complesso di metadati che descrivono in maniera "piatta" tutti gli elementi identificativi, descrittivi, gestionali, tecnologici, etc., relativi ad uno e uno solo pacchetto informativo;
- l'insieme delle relazioni di contesto che permettono la correlazione logica del pacchetto informativo agli altri pacchetti informativi e in generale ad un qualsiasi contesto di natura archivistico-gerarchica.

Quest'ultimo elemento è quello che ci permette di ricostruire il vincolo archivistico e quindi di ricondurre, ad esempio, ad una stessa pratica o ad uno stesso fascicolo tutti i documenti relativi ad un medesimo procedimento amministrativo.
Il PdA è costituito da:

- l'oggetto digitale possibilmente in un formato standard non proprietario;
- l'Indice del pacchetto di archiviazione (IdPA) realizzato secondo lo standard UNI SinCRO e contenente un hash dell'oggetto digitale conservato.

Per comodità si riporta la struttura dell'indice del pacchetto di archiviazione.

In un sistema OAIS *compliant*, si definisce pacchetto di archiviazione un pacchetto informativo composto dall'insieme delle informazioni che costituiscono l'obbiettivo originario della conservazione e dalle relative informazioni sulla conservazione. In un contesto OAIS il pacchetto di archiviazione dove essere auto-consistente, ovvero, deve prevedere tutte le informazioni necessarie al recupero e alla ricostruzione dell'oggetto digitale conservato e delle informazioni ad esso associate.

La struttura del PdA è la seguente:

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified" attributeFormDefault="unqualified">
 <!-- ********************************************************************** -->
 <!--  -->
 <xs:complexType name="IdC">
  <xs:sequence>
   <xs:complexType name="SelfDescription">
    <xs:sequence>
     <xs:element name="ID" type="xs:string" minOccurs="0"/>
     <xs:complexType name="CreatingApplication">
      <xs:sequence>
       <xs:element name="Name" type="xs:string" minOccurs="0"/>
```

```
                                        <xs:element name="Version" type="xs:string"
minOccurs="0"/>
                                        <xs:element name="Producer" type="xs:string"
minOccurs="0"/>
                                    </xs:sequence>
                                </xs:complexType>
                                <xs:complexType name="MoreInfo">
                                    <xs:complexType name="ExternalMetadata">
                                        <xs:sequence>
                                            <xs:element name="ID" type="xs:string"
minOccurs="0"/>
                                            <xs:element name="Path" type="xs:string"
minOccurs="0"/>
                                            <xs:element name="Hash" type="xs:string"
function="SHA256" minOccurs="0"/>
                                        </xs:sequence>
                                    </xs:complexType>
                                </xs:complexType>
                            </xs:sequence>
                        </xs:complexType>
                        <xs:complexType name="VdC">
                            <xs:sequence>
                                <xs:element name="ID" type="xs:string" minOccurs="0"/>
                                <xs:complexType name="VdCGroup">
                                    <xs:sequence>
                                        <xs:element name="Label" type="xs:string"
minOccurs="0"/>
                                        <xs:element name="ID" type="xs:string" minOccurs="0"/>
                                        <xs:element name="Description" type="xs:string"
minOccurs="0"/>
                                    </xs:sequence>
                                </xs:complexType>
                            </xs:sequence>
                        </xs:complexType>
                        <xs:complexType name="FileGroup">
                            <xs:sequence>
                                <xs:element name="Label" type="xs:string" minOccurs="0"/>
                                <xs:complexType name="File">
                                    <xs:sequence>
                                        <xs:element name="ID" type="xs:string" minOccurs="0"/>
                                        <xs:element name="Path" type="xs:string"
minOccurs="0"/>
                                        <xs:element name="Hash" type="xs:string"
minOccurs="0"/>
                                        <xs:complexType name="MoreInfo">
                                            <xs:complexType name="ExternalMetadata">
                                                <xs:sequence>
                                                    <xs:element name="ID"
type="xs:string" minOccurs="0"/>
                                                    <xs:element name="Path"
type="xs:string" minOccurs="0"/>
                                                    <xs:element name="Hash"
type="xs:string" minOccurs="0"/>
                                                </xs:sequence>
                                            </xs:complexType>
                                        </xs:complexType>
```

```
                                        </xs:sequence>
                                    </xs:complexType>
                                </xs:sequence>
                            </xs:complexType>
                            <xs:complexType name="Process">
                                <xs:complexType name="Agent">
                                    <xs:complexType name="AgentName">
                                        <xs:complexType name="NameAndSurname">
                                            <xs:sequence>
                                                <xs:element   name="FirstName"   type="xs:string"
minOccurs="0"/>
                                                <xs:element   name="LastName"   type="xs:string"
minOccurs="0"/>
                                            </xs:sequence>
                                        </xs:complexType>
                                    </xs:complexType>
                                    <xs:element name="Agent_ID" type="xs:string" minOccurs="0"/>
                                </xs:complexType>
                                <xs:complexType name="Agent">
                                    <xs:complexType name="AgentName">
                                        <xs:complexType name="NameAndSurname">
                                            <xs:sequence>
                                                <xs:element name="FormalName" type="xs:string"
minOccurs="0"/>
                                            </xs:sequence>
                                        </xs:complexType>
                                    </xs:complexType>
                                    <xs:element name="Agent_ID" type="xs:string" minOccurs="0"/>
                                </xs:complexType>
                                <xs:complexType name="TimeReference">
                                    <xs:element name="TimeInfo" type="xs:dateTime" minOccurs="0"/>
                                </xs:complexType>
                                <xs:element name="LawAndRegulations" type="xs:string" minOccurs="0"/>
                            </xs:complexType>
   </xs:sequence>
  </xs:complexType>
   <!--  -->
  <!-- ********************************************************************** -->
</xs:schema>
```

Torna al sommario

6.4 Pacchetto di distribuzione

Nel modello OAIS, il pacchetto di distribuzione (PdD) è strutturato nel modello dati come il pacchetto di archiviazione (PdA). La differenza sta nella sua destinazione in quanto esso viene concepito per essere fruito ed utilizzato dall'utente finale (esibizione).
Anche ai fini dell'interoperabilità tra i sistemi di conservazione, viene garantita la coincidenza tra PdD e rispettivo PdA.

Torna al sommario

7. IL PROCESSO DI CONSERVAZIONE

Il processo di conservazione si attiva al seguito della sottoscrizione del contratto di affidamento del servizio di conservazione, le cui procedure vengono descritte nell'allegato di specifiche tecniche. Tutti i processi a partire dall'acquisizione del PDV all'accettazione, alla validazione, degli oggetti digitali alla trasformazione del PDV in PDA e infine alla distribuzione del PDV sono tracciati dai LOG. I files Log vengono conservati a norma a tempo indeterminato.
Il servizio di conservazione erogato è regolato dai seguenti documenti:

- contratto di affidamento del servizio di conservazione;
- specifiche tecniche (allegato del contratto);
- atto di nomina responsabile del servizio di conservazione;
- nomine dei responsabili delle aree coinvolte nel processo di conservazione;
- oggetti da sottoporre a conservazione (parte integrante delle specifiche tecniche, allegato del contratto di affidamento del servizio di conservazione);
- manuale operativo del software di conservazione.

Torna al sommario

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

La prima fase del processo di conservazione è l'acquisizione dei pacchetti di versamento nel sistema di conservazione. L'acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico avviene tramite upload automatico o upload manuale.

L'upload automatico avviene attraverso un Web Services (A2A) con credenziali personalizzate e accesso consentito dal *layer* di sicurezza ad un set predefinito di IP statici riservati alle applicazioni gestionali del Cliente fornite da RCM Italia. La modalità è detta Application To Application (A2A). L'applicazione del Cliente, dopo l'autenticazione, potrà utilizzare le chiamate di cui saranno fornite le specifiche per eseguire tutte le operazioni previste dalla conservazione.

L'upload manuale avviene tramite l'autenticazione al sito di erogazione della conservazione digitale. Una apposita Web-App, presentata in seguito, consente agli utenti, autorizzati dal cliente e profilati sulla piattaforma, di accedere e caricare uno ad uno i file da conservare inserendo di volta in volta i metadati che serviranno a ricercare i dati conservati e ad effettuarne l'esibizione.

Tutte le attività effettuate vengono tracciate attraverso la generazione e registrazione di appositi log applicativi.

Torna al sommario

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

Il sistema di conservazione esegue, contestualmente alla formazione e acquisizione dei PdV i seguenti controlli:

- la conformità dell'Indice del pacchetto di versamento allo schema stabilito dal sistema di conservazione;
- la conformità delle tipologie documentarie che devono essere congruenti con quanto previsto nell'ambito delle pattuizioni contrattuali stipulate con i singoli soggetti produttori;
- la conformità dei metadati da quanto previsto dagli accordi;
- l'integrità dei componenti, verificando per ogni file versato, che l'impronta fornita dal produttore coincida con quella calcolata dal sistema di conservazione;

- il controllo di ammissibilità dei formati (effettuato attraverso l'analisi del cd. *magic number*).

L'identità del produttore che ha creato e trasmette il PdV al sistema di conservazione è assicurata dalla corretta autenticazione dello stesso alla web-app che permette il caricamento del file e dei relativi metadati.

Nel caso di upload automatico dei PdV, l'identità del sistema mittente, trattandosi di un colloquio *machine to machine* è accertata in automatico.

In entrambi i casi la trasmissione del PdV al sistema di conservazione avviene tramite canali sicuri (con protocollo https).

Torna al sommario

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

Il sistema di conservazione di RCM Italia effettua, come abbiamo visto, numerosi controlli già in fase di predisposizione del PdV: per tale motivo la fase di formazione del PdV si conclude positivamente solo se tutti i controlli preliminari siano stati superati.
Il sistema effettua anche un calcolo dell'hasj del PdV correttamente formato che viene inserito, unitamente al risultato dei controlli, all'interno del Rapporto di versamento – RdV-.
Di seguito viene descritta la struttura dell'RdV:

```
<RapportoDiVersamento>
   <Versione>1.0</Versione>
   <UrnRDV>URN:RdV:RCMITALIA:FTAC:L:4</UrnRDV>
   <DataRDV>22-03-2019</DataRDV>
   <EsitoExt>POSITIVO</EsitoExt>
   <Versatore>
         <Ambiente>KEEPEASY</Ambiente>
         <Ente></Ente>
         <Struttura>RCM ITALIA Srl</Struttura>
         <UserID>m.dangelo</UserID>
   </Versatore>
   <PDVType>
         <URNindexPDV>URN:index:RCMITALIA:FTAC:L:4</URNindexPDV>
         <HashIndexPDV>15b4c3a6ef2c8ea290b96aa906c43b4bc415bcfa6d157049dcdf382ffd77ab9a</Has
         hIndexPDV>
         <AlgoritmoHashIndexPDV>SHA-256</AlgoritmoHashIndexPDV>
         <DataPDV>2019-03-22 09:58:58</DataPDV>
   </PDVType>
   <UnitaDocumentaria>
         <TipoUnitaDocumentaria>L_FT</TipoUnitaDocumentaria>
         <IdentificativoDocumento>Aci-bollettini.rar</IdentificativoDocumento>
         <HashUnitaDocumentaria>fc07a40ecb0264984842777cb1c3b8f82f2c38530ee8b1af281fd340772d5
         7ce</HashUnitaDocumentaria>
         <AlgoritmoHashUnitaDocumentaria>SHA-256</AlgoritmoHashUnitaDocumentaria>
   </UnitaDocumentaria>
</RapportoDiVersamento>
```

Il Rdv viene quindi firmato e marcato digitalmente e messo a disposizione dell'ente produttore come evidenza della presa in carico degli oggetti.
Per i soggetti che effettuano i versamenti tramite l'upload da web, il PDV è a disposizione dalla stessa interfaccia *web based*, attraverso una pagina di ricerca che consente la visualizzazione e il download.
Per i soggetti che effettuano i versamenti tramite *web services* ricevono il PDV attraverso un apposito comando dallo stesso applicativo che invia i documenti.

Tutti i rapporti di versamento sono conservati insieme ai oggetti digitali sottoposti al processo conservazione e per lo stesso periodo di tempo relativo agli oggetti stessi.
Tutti i soggetti, a prescindere dalla modalità di versamento dei dati, sono in grado di recuperare i rapporti di versamento delle conservazioni effettuate attraverso l'interfaccia *web based* a disposizione del personale designato dall'ente produttore.
La generazione di ogni RdV viene tracciata mediante la registrazione di appositi log applicativi.

Torna al sommario

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

Il PdV viene sottoposto ai controlli di validazione descritti nel paragrafo 7.2 contestualmente alla sua formazione.
Qualora non vengano superati tutti i controlli previsti, il sistema rifiuta la generazione stessa del pacchetto di versamento e notifica all'utente l'avvenuto errore. La notifica avviene attraverso interfaccia grafica nell'area designata alle notifiche e, in caso di upload automatico. attraverso l'invio di un messaggio PEC. In aggiunta, oltre alla notifica PEC e web il sistema dettaglia nei log la causa d'errore.

Torna al sommario

7.5 Preparazione e gestione del pacchetto di archiviazione

Una volta a disposizione i pacchetti informativi presso la piattaforma, il processo di conservazione può avere inizio.
Il sistema di conservazione trasforma i pacchetti di versamento (PdV) in pacchetto di archiviazione (PdA) contenti tutti i file necessari alla loro ricostruzione e ricerca, collegando i documenti alle informazioni sulla rappresentazione loro associate e ai viewer associati al relativo formato file.

Il PdA creato sarà composto dal file ricevuto e prevede la creazione di un apposito Indice del pacchetto di archiviazione conforme a quanto previsto dalla standard Uni SinCRO.

La conservazione si conclude con la firma digitale e la marca temporale dell'indice UNISincro e termina con la messa a disposizione del cliente di questa evidenza di avvenuta conservazione (indice in formato P7M) da parte del responsabile del servizio di conservazione.

Il sistema di conservazione si occupa autonomamente di tutte le fasi di conservazione, tracciandone ogni passaggio e ogni esito in appositi file di log.

Torna al sommario

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

I pacchetti di archiviazione (PdA) sono nel sistema. In un momento successivo alla generazione dei PdA, utenti con profilo di esibizione o ricerca possono accedere, tramite apposite credenziali, da remoto al sistema di conservazione e interrogarlo per ottenere un pacchetto di distribuzione.

Ci possono essere varie generazioni di PdD

- PdD coincidente con il PdA che contiene:
  - tutti gli elementi presenti nel PdA;
  - i documenti del PdA richiesto;
  - un'estrazione delle informazioni di conservazione degli oggetti conservati;
  - l'indice di conservazione firmato e marcato e le informazioni sulla conservazione associate agli oggetti digitali;

- i *viewer* necessari alla visualizzazione dei documenti del pacchetto e le informazioni sulla rappresentazione;
- le informazioni sull'impacchettamento e le informazioni descrittive associate al pacchetto informativo.

Inoltre è possibile inserire tutta la catena di documentazione necessaria a rispondere alle esigenze del modello OAIS.

- PdD dell'unità documentaria che contiene:
  - I metadati che la compongono;
- PdD del documento che contiene:
  - Le informazioni aggiuntive del documento**.**

In linea generale il pacchetto di distribuzione può essere erogato dal sistema di conservazione come unico file in formato ZIP e in formato ISO a seconda della richiesta dell'utente.
Nei contratti standard non è previsto da parte del soggetto conservatore il rilascio di copie cartacee conformi agli originali digitali conservati, né l'accesso diretto alla documentazione da parte di colui che, dovendo tutelare situazioni giuridicamente rilevanti, abbia presentato istanza di consultazione.

Pertanto, in merito all'esercizio del diritto d'accesso ai documenti conservati dal soggetto conservatore, questo si limita a fornire al soggetto produttore, su precisa richiesta di quest'ultimo e senza che su di esso debba gravare alcun particolare onere, il documento informatico conservato, qualora per un qualsiasi motivo l'ente produttore stesso abbia deciso di non acquisirlo direttamente, mediante le modalità delineate nel presente manuale. Permane in carico all'ente produttore sia la responsabilità di valutare la fondatezza giuridica della domanda di accesso, sia l'onere di far pervenire il documento (o sua eventuale copia cartacea conforme) al soggetto richiedente la consultazione.

L'esibizione è un atto da svolgersi in ottemperanza di quanto previsto dall'ultimo comma dell'art. 2220 del Codice Civile, ribadito nell'art. 10 del D.P.C.M. del 3 Dicembre 2013. Essa consiste nel rendere leggibili, con mezzi messi idonei, tutte le scritture e i documenti conservati a norma.
L'articolo 10 del D.P.C.M. del 3 Dicembre 2013 ribadisce le norme vigenti e specifica che ai fini dell'esibizione il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, al documento informatico conservato, attraverso la produzione di un pacchetto di distribuzione (PdD) selettivo secondo le modalità descritte nel manuale di conservazione.

Il sistema di conservazione garantisce l'esibizione dell'archivio informatico. Il sistema permette di richiedere, di generare e di scaricare i PdD, completi di file di evidenza della conservazione e delle informazioni di rappresentazione. Inoltre, nei PdD è contenuta tutta la catena di documentazione necessaria a rispondere alle esigenze del modello di riferimento OAIS.

L'ente Produttore, in fase di attivazione del servizio segnala al *provisioning*, su apposita documentazione correlata dagli allegati autorizzativi e di identificazione, i propri delegati alla visualizzazione e al download dei documenti informatici originali ai fini dell'esibizione.

Il conservatore genera gli account e il sistema invia le credenziali all'utente per accedere al portale del sistema di conservazione.
Il collegamento avviene tramite connessione sicura SSL con certificato rilasciato da Certification Authority accreditata presso AgID.
Verranno così inviate le credenziali per accedere al portale Keep Easy via mail e un manuale di utilizzo del portale. Una volta accreditato al portale, l'utente ha accesso ai servizi opportunamente profilati alla sua utenza.
A quel punto i produttori sono in grado di:

- Visualizzare direttamente i documenti informatici originali conservati da remoto;
- Scaricare i documenti informatici conservati (duplicati) e i file di evidenza della conservazione (indice di conservazione Unisincro);
- Richiedere e scaricare i (PdD) da consegnare alle autorità competenti, in caso di necessità.

Il soggetto produttore avrà cura di produrre una copia conforme richiedendo la presenza di un pubblico ufficiale.
In merito alla produzione delle copie sarà cura del produttore produrre le copie e richiedere, quando necessario, la presenza di un Pubblico Ufficiale.
Nel pacchetto informativo è compreso anche il necessario per la rappresentazione (*viewer* nella versione coerente alla visualizzazione dei PdD) e le informazioni sul sistema operativo in grado di supportare l'applicazione.
Va sottolineato che l'esibizione dei oggetti digitali conservati deve avvenire in modo che le autorità possano verificare la coerenza della firma digitale e la marca temporale apposta durante il processo di conservazione. Tale processo, non potendo essere effettuata stampando l'evidenza firmata della conservazione, deve necessariamente prevedere un supporto informatico.

Torna al sommario

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

Il Soggetto Produttore, in fase di attivazione del servizio segnala al *provisioning*, su apposita documentazione correlata dagli allegati autorizzativi e di identificazione, i propri delegati alla visualizzazione e al download dei documenti informatici originali.
Verranno così inviate le credenziali per accedere al *portale della conservazione* via mail e un manuale di utilizzo del portale.
Il conservatore genera gli account e il sistema invia le credenziali all'utente per accedere al portale del sistema di conservazione Keep Easy.
Detta piattaforma, consente al Soggetto Produttore di fruire sia della produzione di duplicati e copie informatiche che l'esibizione a norma degli oggetti digitali conservati. (PdD)
Una volta accreditato dal portale, l'utente ha accesso ai servizi opportunamente profilati alla sua utenza.
A quel punto gli enti produttori sono in grado di:

- Visualizzare direttamente i documenti informatici originali conservati
- Scaricare i documenti informatici conservati (duplicati) e i file di evidenza della conservazione (indice di conservazione Unisincro)
- Richiedere e scaricare i (PdD) da consegnare alle autorità competenti, in caso di necessità.
- Produrre eventualmente una copia conforme richiedendo la presenza di un pubblico ufficiale.

La procedura per visualizzare i documenti informatici conservati è semplice e intuitiva. E' tuttavia disponibile online un manuale, presso lo stesso portale della conservazione.
Il soggetto produttore o un suo delegato all'attività di consultazione e produzione di duplicati informatici, ricerca i documenti attraverso i campi che l'interfaccia grafica mette a disposizione. Si tratta degli stessi metadati con i quali sono stati accompagnati i file durante l'invio al sistema di conservazione.
Una volta visualizzati i file conservati, l'ente produttore può richiedere al responsabile del servizio di conservazione una copia, attraverso una funzione disponibile sul portale. Detta funzione consente di scaricare un file di tipo ISO o di tipo ZIP, attraverso il canale criptato SSL del portale.
Sarà così possibile per il soggetto produttore avere una copia del pacchetto di distribuzione (PdD) contenente i documenti conservati, il *viewer* per la loro corretta visualizzazione, l'indice di conservazione firmato e marcato e un'estrazione dei metadati associati ai documenti.
Il sistema di conservazione è stato progettato anche in termini organizzativi di preservation planning, proprio con l'obiettivo di prevenire l'obsolescenza dei formati trattati.
Qualora fosse richiesta la presenza di un pubblico ufficiale per l'attestazione di conformità all'originale di copie di documenti informatici originali, conservati dal sistema di conservazione, il produttore avrà cura di gestire tale scelta. Il conservatore rimanda la gestione di tale attività al soggetto produttore le cui modalità di intervento sono esplicitate nel contratto di affidamento. Il conservatore garantisce la messa a disposizione dell'originale informatico attraverso un PdD eventualmente firmato dal responsabile del servizio di conservazione.

Torna al sommario

7.8 Scarto dei pacchetti di archiviazione

L'art. 9 comma 2, lett. K del DPCM 3 dicembre 2013 stabilisce che deve essere effettuato lo scarto dal sistema di conservazione, alla scadenza dei termini di conservazione previsti dalla norma, dandone informativa al soggetto produttore.
Il Sistema di Gestione Dati, grazie alla propria concezione, permette di gestire al meglio lo scarto del materiale documentario non destinato alla conservazione permanente, ma caratterizzato invece da tempi di conservazione limitati e diversificati. Negli archivi correnti, gestiti secondo criteri aggiornati è presente un metadato, definibile per ciascuna tipologia documentaria o fascicolo, che stabilisce i tempi di conservazione. Sarà dunque il sistema di gestione dati (SGD) ad avvisare il responsabile del servizio di conservazione, attraverso una o più notifiche impostabili, riguardo la scadenza dei tempi di conservazione dei documenti, a supportarlo materialmente nella procedura di scarto e a mantenere al proprio interno, ove richiesto, i metadati della documentazione logicamente scartata.
Il sistema di conservazione produrrà quotidianamente un elenco dei PdA che hanno superato il tempo di conservazione che sarà inviato al soggetto produttore. Una volta validato definitivamente l'elenco di scarto dal produttore, questi provvederà a trasmettere l'autorizzazione di scarto al conservatore. Solo dopo aver ricevuto l'autorizzazione, il conservatore provvederà alla cancellazione dei pacchetti di archiviazione, contenuti nell'elenco di scarto. Nei casi di archivi pubblici o privati di particolare interesse culturale, le procedure di scarto avvengono previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo. L'ente produttore, una volta ricevuto il nulla-osta dal Ministero, provvede ad adeguare, se necessario, l'elenco di scarto. Una volta che l'elenco di scarto è definitivo, l'ente produttore lo trasmette a RCM Italia. Solo dopo aver ricevuto l'autorizzazione, il conservatore provvederà alla cancellazione dei pacchetti di archiviazione, contenuti nell'elenco di scarto.
Il sistema di conservazione è quindi dotato di un processo di scarto che si occupa di controllare quotidianamente se esistono pacchetti di archiviazione che devono essere scartati. Alla presenza di uno o più pacchetti, il processo avvisa il responsabile del servizio di conservazione, che avrà a disposizione una interfaccia che gli permetterà di decidere se scartare o meno i documenti. In caso affermativo, il processo di selezione e scarto provvederà ad eliminare fisicamente i file presenti nel *file system* e a cancellare tutti i riferimenti nel database, mantenendo però l'indice di conservazione (in quanto contiene la lista dei file scartati) e aggiungendo automaticamente ai metadati dei PdA, una nota che indica il fatto che il PdA è stato sottoposto a processo di scarto includendo data e ora di esecuzione.

Torna al sommario

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

Per una corretta erogazione di un servizio di conservazione a norma che risponda alle caratteristiche richieste dal modello OAIS, una qualsiasi applicazione di conservazione deve essere in grado di esportare i documenti conservati in un formato che garantisca l'integrità della conservazione stessa.
L'applicazione del sistema di conservazione, essendo progettata secondo il modello di riferimento OAIS è in grado di esportare i singoli pacchetti di archiviazione generati durante gli anni, seguendo le regole che permettono successivamente di importare i pacchetti in un altro sistema OAIS *compliant*.
Sono di seguito presentate le situazioni e le soluzioni previste per i flussi di migrazione dei dati conservati da un soggetto conservatore ad un altro.
Si ricorda che, in accordo con il modello di riferimento OAIS, tutti i conservatori aderenti sono tenuti all'interoperabilità dei sistemi, che si concretizza con l'adozione e la produzione di pacchetti di distribuzione in formato standard, importabili su qualunque sistema di conservazione a norma.
In caso di movimentazione di dati da un soggetto conservatore ad un altro o da un conservatore ad un utente autorizzato, è sempre obbligatorio l'uso di canali sicuri e criptati.

- Per i download dei PdD eseguiti da web, il requisito è evaso utilizzando gli appositi servizi https esposti;
- Per gli upload, anche massivi, eseguiti con chiamate SOAP (A2A) è sempre utilizzato il protocollo sicuro https;

- Per il riversamento dei PdD su supporti ottici, fisici o altro hardware (e.g. flash-memory), allo scopo di trasportare i dati da un conservatore ad un altro o in generale per il mantenimento dei dati conservati all'esterno dei CED del conservatore accreditato, è necessario utilizzare supporti criptati.

RCM Italia è in grado di importare dati di altri *outsourcer* qualora dette informazioni, precedentemente soggette a conservazione, rispettino alcune caratteristiche. La verifica di dette caratteristiche è preventiva rispetto all'accettazione degli oggetti conservati da migrare. I contratti avranno pertanto una componente di valutazione preventiva della fattispecie.
Di seguito viene tracciato l'iter procedurale del *de-provisioning,* cioè della sequenza temporale relativa alle azioni da effettuare al termine naturale dei contratti con i clienti, qualora tali contratti non vengano rinnovati.
Il produttore aveva già nominato gli utenti abilitati all'accesso della piattaforma web, all'atto della sottoscrizione del contratto.Tali utenti sono invitati tramite tre avvisi via mail a collegarsi alla piattaforma web per generare e scaricare i PdD contenenti tutti i documenti conservati.
L'ex cliente è tenuto a verificare la coerenza dei dati consegnati entro i tempi prestabiliti. RCM Italia fornirà supporto telefonico in orario di ufficio, per eventuali problemi. Gli utenti avranno a disposizione un manuale, scaricabile direttamente dal portale web, che descrive tutte le attività da espletare per queste operazioni.
In alternativa, per PdA di grandi dimensioni, RCM Italia restituirà le conservazioni all'ex-cliente o ai delegati autorizzati con apposita lettera firmata, previa consultazione con il Responsabile dei Dati del Soggetto Produttore, su appositi supporti. Infine, verrà disattivato l'account relativo al portale web e i dati verranno cancellati.

Torna al sommario

8. IL SISTEMA DI CONSERVAZIONE

Il modello dei dati che viene utilizzato come base per l'implementazione del sistema di conservazione è ISO 14721: OAIS Open Archival Information System esplicato nella gestione di tre differenti tipologie di pacchetti informativi:

- Il pacchetto di versamento (PdV): il documento digitale o l'insieme dei documenti digitali, corredati da tutti i metadati descrittivi, versati dal soggetto produttore nel sistema di conservazione.
- Il pacchetto di archiviazione (PdA): uno o più PdV sono trasformati in pacchetto di archiviazione per la conservazione. Il PdA ha un insieme completo di informazioni sulla conservazione che si aggiungono al file di metadati. Il PdA è comprensivo di UniSincro;
- Il pacchetto di distribuzione (PdD): l'oggetto digitale o l'insieme degli oggetti digitali, corredati da tutti o da parte dei metadati previsti nel PdA, finalizzati alla fruibilità della comunità di riferimento.

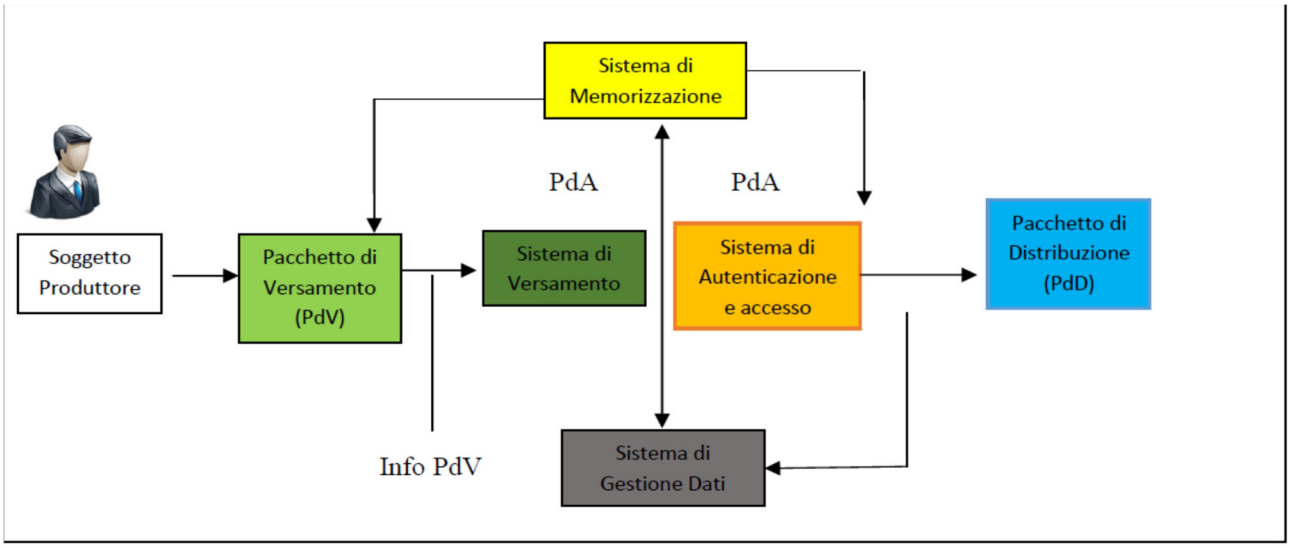

Figura 3 ISO 14721: OAIS Open Archival Information System

In termini generali, il modello OAIS definisce le componenti logiche comuni a tutti e tre i pacchetti informativi sopra descritti. Il modello dati utilizzato dal sistema di conservazione prevede una strettissima aderenza a tale modello concettuale rivisitandolo ed ampliandolo con elementi di contestualizzazione provenienti dalla tradizione archivistica italiana.
Inoltre l'obiettivo del sistema di conservazione è quello di garantire non solo la gestione e la conservazione dell'insieme informativo e descrittivo del singolo oggetto (o collezione di documenti, nell'accezione OAIS, in riferimento a AIC, *Archival Information Collection*), ma anche di tutte le informazioni di contesto dei metadati e, soprattutto, delle relazioni fra i documenti che servono per la ricostruzione del vincolo archivistico e, quindi, del fascicolo digitale di riferimento.

Come illustrato nella seguente figura il sistema di conservazione è conforme al modello OAIS.

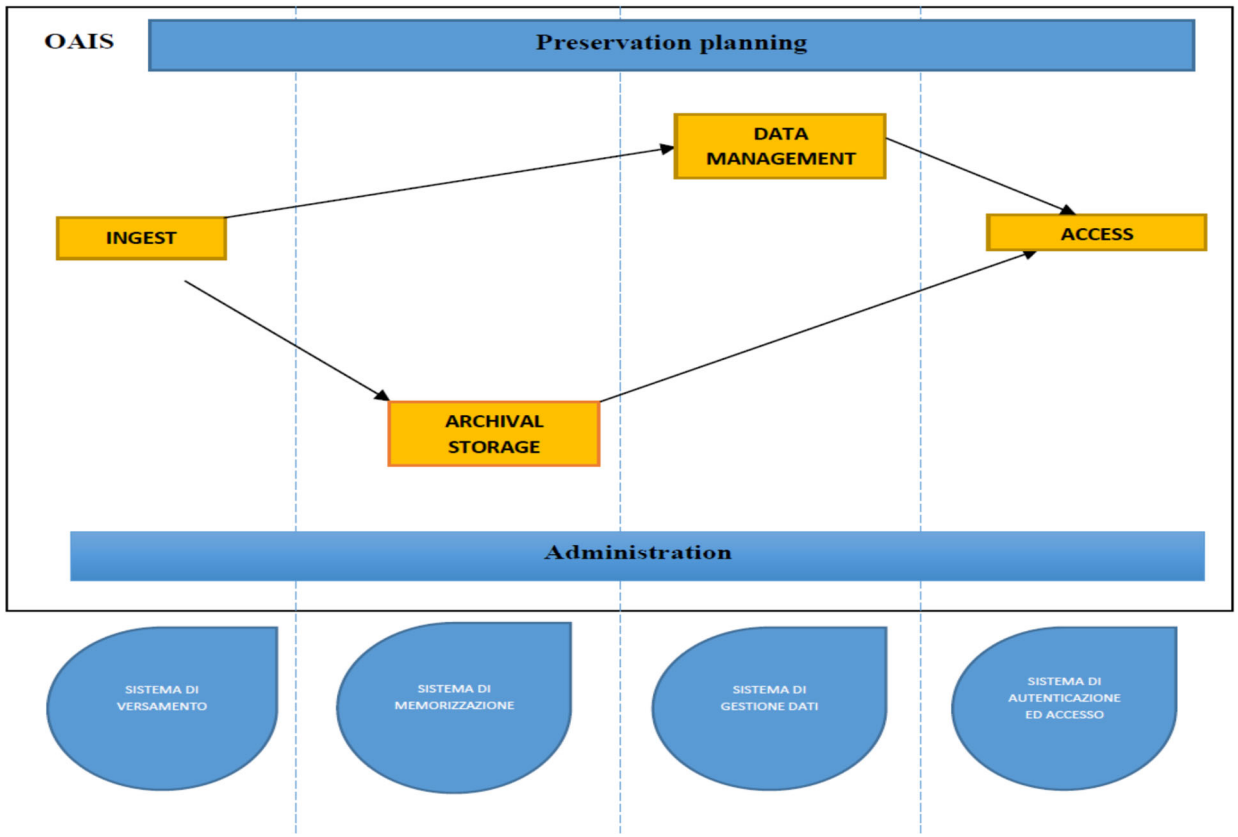

Figura 4 Componenti OAIS del sistema di conservazione

Torna al sommario

8.1 Componenti Logiche

Nel rispetto dello standard, il sistema è formato da quattro macrocomponenti funzionali:

- Sistema di versamento (SdV);
- Sistema di gestione dati (SGD);
- Sistema di memorizzazione (SM);
- Sistema di autenticazione e accesso (SAA).

Sistema di versamento (SdV).

Il sistema di versamento, è la porta di ingresso dell'intero sistema ed ha il compito di gestire la ricezione dei pacchetti di versamento da parte dei soggetti produttori, di verificarne l'aderenza al contratto di servizio di conservazione e ai requisiti di conservazione, di preparare i pacchetti di archiviazione ed infine di inviare ai sistemi opportuni, le informazioni e i dati per garantire la conservazione degli oggetti digitali ricevuti.
Rispetto alla pluralità di situazioni documentarie possibili, il sistema si comporterà applicando le regole d'ingresso che saranno definite nell'accordo di servizio. Esattamente come avviene in un archivio di deposito tradizionale, le regole avranno lo scopo di stabilire:

- Le caratteristiche minime che la documentazione deve possedere per poter essere accettata in ingresso;
- I tempi di versamento della documentazione dotata di tali caratteristiche;
- Le modalità di versamento;
- I metadati di ciascun versamento che dovranno anch'essi essere conservati dal sistema.

Una volta che la documentazione avrà superato i controlli previsti, il sistema di versamento dovrà applicare le regole previste dal *preservation planning* per costruire i pacchetti di archiviazione a partire dai PdV inviati dal soggetto produttore.
Innanzitutto viene generata la cosiddetta "descrizione del pacchetto informativo" che consiste in una serie di informazioni descrittive (descrizioni associate) che consentirà l'accesso al documento informatico da parte dell'utente. Infatti, sulla base di queste descrizioni, è possibile effettuare delle ricerche ed è a partire da queste descrizioni che verranno costruiti i *Dissemination Information Package* (PdD – Pacchetti di distribuzione) differenti, a seconda delle necessità dell'utente.
Sui documenti versati nel sistema di conservazione è possibile quindi avviare un'attività di validazione sia dei file che dei metadati rispetto alle regole ed agli standard previsti dalle descrizioni archivistiche di appartenenza. I risultati della convalida possono essere allegati al documento oggetto della convalida per essere eventualmente portati in conservazione insieme al documento. Il processo di convalida include:

- La verifica dell'integrità del documento memorizzato sul supporto rispetto all'impronta associata allo stesso;
- La verifica che il formato del contenuto binario sia coerente con quanto dichiarato nei suoi metadati, oppure, si potrebbe consentire l'invio di formati di file non adatti alla conservazione;
- La verifica delle eventuali firme digitali apposte su di esso, comprensiva di convalida del certificato rispetto ad uno *store* locale ed alle liste di revoca on-line;
- L'eventuale verifica della presenza in archivio di un documento identico (i.e.: stessa impronta e/o metadati);
- La compilazione metadati: alcuni metadati potrebbero essere compilati in questa fase in maniera automatica

Sistema di gestione dati (SgD)

Il sistema di gestione dati ha il compito di gestire le informazioni legate al contesto archivistico e alle descrizione dei documenti. Il Sistema di Gestione Dati è il cuore archivistico del sistema ed è la componente che consente di avere una visione unitaria dell'archivio e quindi consente di accedervi.
Il Sistema di Gestione Dati ha una duplice valenza: da una parte offre servizi al Sistema di Accesso per consentire le ricerche e la navigazione e dall'altra consente all'ente produttore di gestire il proprio deposito digitale secondo canoni archivistici, offrendo funzionalità come la descrizione e il riordino, la selezione e scarto, la ricollocazione del materiale non digitale, ecc. Il Sistema di Gestione Dati rappresenta il collante archivistico dell'intero sistema di conservazione e per questo riteniamo questa componente essenziale per consentire ad un soggetto produttore di gestire al meglio il proprio deposito digitale.
L'ente produttore attraverso questo modulo potrà vedere l'archivio come il complesso sistema di relazioni che in effetti è e, tramite le funzionalità che esso offre, potrà compiere tutte quelle operazioni tipicamente archivistiche necessarie per la gestione di un archivio (di deposito). Per esempio, il Sistema di Gestione Dati, grazie alla propria particolare concezione, permette di gestire al meglio lo scarto del materiale documentario non destinato alla conservazione permanente, ma caratterizzato invece da tempi di conservazione limitati e diversificati.

Sistema di memorizzazione (SdM)

Il Sistema di memorizzazione ha lo scopo di gestire in modo semplice e sicuro la conservazione a lungo termine dei documenti informatici, integrando una serie di servizi specifici di monitoraggio dello stato fisico e logico dell'archivio ed effettuando, per ogni documento conservato, una continua verifica di caratteristiche come la leggibilità, l'integrità, il valore legale, l'obsolescenza del formato e la possibilità di applicare la procedura di scarto d'archivio.
Nell'ambito del sistema complessivo, quindi, il Sistema di memorizzazione ha il compito di garantire il mantenimento della validità nel tempo dei singoli "documenti digitali", preoccupandosi di aspetti quali l'affidabilità, l'autenticità e l'accessibilità.
Il Sistema di memorizzazione, in primo luogo acquisisce quanto inviato dal Sistema di versamento durante la fase di versamento e, verificandone preventivamente l'affidabilità, provvederà a gestirne lo storage. Sui documenti conservati verranno applicate opportune politiche di gestione atte a garantire, non solo la catena ininterrotta della custodia dei documenti, ma anche la piena tracciabilità delle azioni conservative finalizzate a garantire nel tempo la salvaguardia della fonte.

Sistema di autenticazione e accesso (SAA)

Il modulo per la gestione degli accessi orchestra il flusso di informazioni e servizi necessari per fornire le funzionalità di accesso al cosiddetto "consumer" ovvero all'utente che ha la necessità di accedere ad un determinato documento.

A seguito di una ricerca impostata dall'utente il modulo di Gestione Accesso richiede i risultati della ricerca al Sistema di Gestione Dati che, organizzando le informazioni descrittive dei PdA, è in grado di rispondere alla richiesta; l'utente una volta individuato il documento desiderato (o i documenti, o addirittura un intero fascicolo o PdA) potrà inoltrare una richiesta di accesso ai dati, questa genererà la richiesta al modulo di Generazione PdD il quale interagendo sia con il Sistema di Gestione Dati che con il Sistema di Memorizzazione recupererà le informazioni necessarie (PdA e informazioni descrittive) per produrre il Pacchetto di Distribuzione (PdD) corrispondente alla richiesta.

Inoltre, il sistema consente anche ricerche trasversali tra tipologie documentali differenti.

Attraverso la piattaforma di conservazione è possibile definire più ruoli attraverso la definizione di profili d'uso che verrà illustrata più avanti.

Le funzionalità di ricerca saranno implementate dal Sistema di Gestione Dati, mentre il Sistema di Accesso fornirà le interfacce per l'interrogazione e per la ricezione e visualizzazione dei risultati.

Le modalità dell'accesso, in generale, permettono quindi di poter ricercare il documento singolo o le aggregazioni di documenti, mediante tutti i criteri derivabili dai metadati ad esso direttamente associati, per poi risalire al suo contesto archivistico.

L'accesso alle funzionalità offerte dal sistema è regolato anche da un sottosistema di autorizzazione che permette di suddividere l'utenza applicativa in gruppi ai quali è possibile assegnare permessi di esecuzione di specifiche operazioni. I singoli permessi (*capabilities*) sono assegnabili ad un gruppo tramite la definizione di "Profilo d'uso". Grazie ai "profili d'uso", definibili autonomamente dall'amministratore dell'applicazione, ogni utente autorizzato potrà accedere ad uno o più Soggetti Produttori e avere visibilità su uno o più descrizioni archivistiche, nonché è possibile assegnare visualizzazioni di singoli pulsanti e/o menù.

CODICE ATTIVITA'	SISTEMA DI RIFERIMENTO	DESCRIZIONE
REQUISITI	Sistema di versamento	Viene verificato che: - il soggetto produttore non sia bloccato; - non siano stati raggiunti i limiti di contratto; - sia definito almeno un certificato di firma; - sia definito un responsabile della conservazione per il soggetto produttore; - sia definito un account di marca temporale per la descrizione archivistica; - siano definite delle informazioni di rappresentazione valide;

CREASOTTOPROCESSI	Sistema di versamento	Per ogni PdV vengono creati dei sottoprocessi per migliorare le performance di conservazione
TRADUCIPdV	Sistema di versamento	Normalizzazione del file di metadati del pacchetto di versamento
CREATEMPDATA	Sistema di versamento	Caricamento nel database dei metadati del pacchetto di versamento
VALIDATEMPDATA	Sistema di versamento	Validazione dei metadati secondo le specifiche concordate con il soggetto produttore
DELETETEMPDATA	Sistema di versamento	Cancellazione delle tabelle temporanee create per la fase di validazione
CREAPdA	Sistema di versamento	Creazione del pacchetto di archiviazione
CREAFILEMETADATI	Sistema di versamento	Crea il file di metadati per il pacchetto di archiviazione
CREAIdC	Sistema di versamento	Crea l'indice di conservazione secondo lo standard UNI SINCRO
FIRMAIdC	Sistema di versamento	Firma l'indice di conservazione
MARCAIdC	Sistema di versamento	Marca l'indice di conservazione
MEMORIZZAPdA	Sistema di Gestione Dati	Memorizza nel database tutte le informazioni inerenti al pacchetto di archiviazione
COPIAPdA	Sistema di Memorizzazione	Copia il pacchetti di archiviazione nel repository di destinazione
VALIDAPdA	Sistema di Gestione Dati	Verifica che la copia sia andata a buon fine (controllo di hash)
COLLEGAIR	Sistema di Gestione Dati	Collega il pacchetto di archiviazione alle Informazioni sulla rappresentazione

DELETEFILE	Sistema di Memorizzazione	Se previsto dalle impostazioni della descrizione archivistica cancella i file in input
ENCRYPTMETADATA	Sistema di Memorizzazione	Cripta i metadati con tipo di privacy impostato a giudiziario o sanitario
CREARdV	Sistema di versamento	Genera il rapporto di versamento
FIRMARdV	Sistema di versamento	Firma il rapporto di versamento
MARCARdV	Sistema di versamento	Marca il rapporto di versamento

Sottosistema di firma digitale

Il sottosistema per la firma digitale nel contesto della conservazione digitale si configura come elemento fondamentale per consentire di attuare la conservazione a norma dei documenti di un preciso flusso di lavoro. Il processo essenziale per completare la procedura consiste nella firma dell'indice di conservazione (UNI 11386) dei PdA nonché nell'apposizione di una marca temporale su tale file.

Essendo presenti diversi dispositivi in grado di fornire queste funzionalità, l'architettura del sistema di conservazione prevede di demandare ad un apposito sottosistema il compito di interfacciarsi con essi. Ciò consente al Sistema di Memorizzazione di utilizzare qualunque dispositivo di firma digitale, dato che le eventuali differenze nell'implementazione vengono mascherate dal sottosistema stesso.

Resta l'obbligo che la firma digitale, in questo contesto relativa al responsabile del servizio di conservazione ed eventualmente anche ad un pubblico ufficiale (o ruolo equivalente), deve essere apposta utilizzando un dispositivo di firma di un tipo approvato da AgID ed un certificato rilasciato da un prestatore di servizio fiduciario qualificato appartenente all'elenco dei certificatori accreditati presso AgID.

Il sistema di conservazione è in grado di applicare la firma digitale utilizzando certificati rilasciati da tutti i prestatori di servizio fiduciario qualificato accreditati presso AgiD.

La marca temporale consiste in un'ulteriore firma digitale apposta da un soggetto esterno, Time Stamping Authority (TSA), il quale registra e memorizza presso la propria struttura organizzativa l'impronta del file e la relativa data di firma. In questo caso il soggetto esterno non è, dunque, una persona fisica ma un Ente certificatore.

Il sistema di conservazione è in grado di richiedere in modo automatico ed on-line la marca temporale alle TSA utilizzate nel sistema.

Il Sistema di conservazione si avvale per la firma digitale e la marca temporale di Actalis (Aruba), prestatore di servizio fiduciario qualificato, compliant eIDAS. Il Piano per la Sicurezza del Certificatore è depositato presso AgID.

Sotto Sistema per l'apposizione della marca temporale

La marca temporale consiste in un'ulteriore firma digitale apposta da un soggetto esterno [Time Stamping Authority (TSA)] che, presso la propria struttura organizzativa, registra e memorizza l'impronta del file e la relativa data di firma. Dunque, in questo caso il soggetto esterno non è una persona fisica, ma un ente certificatore.

In linea di massima le TSA coincidono con le Certification Authority e questo servizio è offerto on-line utilizzando protocolli di comunicazione standard.

Il sistema è in grado di richiedere in modo automatico ed on-line la marca temporale alle TSA utilizzate nel sistema.

Per i servizi di marca temporale il conservatore si avvale di Certification Authority iscritte alla Trust List Europea.

Torna al sommario

8.2 Componenti Tecnologiche

I moduli e le componenti necessarie alla conservazione sono tutti erogati internamente da Rcm Italia. Le componenti core del sistema di conservazione sono suddivise in modo da rispettare i più ristrettivi standard di sicurezza:

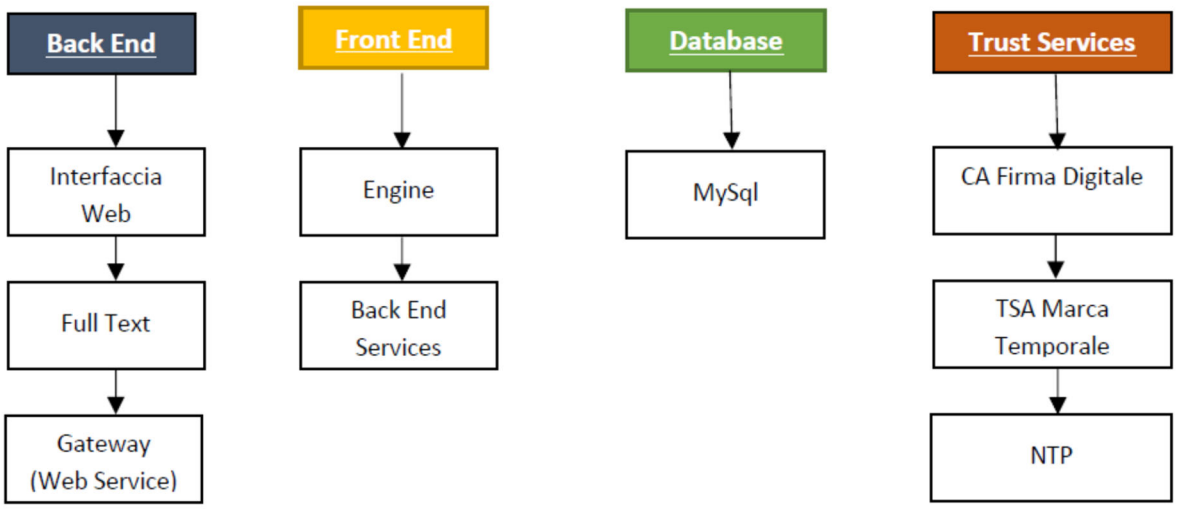

Figura 5 Componenti core del sistema di conservazione

Front End

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

- **Full-text Engine**: è l'applicazione che abilita le funzionalità di full-text;
- **Web Services**: sono un insieme di servizi web che permettono, ad applicazioni di terze parti, di versare oggetti digitali nel sistema di conservazione o di interrogare lo stesso sullo stato di un oggetto digitale;
- **File System**: è un sottoprocesso di Back End che permette di effettuare polling su folder per il versamento automatico dei documenti al sistema di conservazione.

L' interfaccia Web è erogata e protetta ed espone i servizi di consultazione, esibizione e download.

Back End

I Back End Services rappresentano il core della logica applicativa e l'interfaccia verso le basi dati (MySql) e gli storage. Il Back End ha in carico la gestione e la distribuzione dei processi tra i vari nodi del cluster.

Database

Il database, gli storage e le componenti critiche degli ambienti di conservazione sono soggette a procedure di backup tali da mantenere correttamente allineati gli ambienti di erogazione e di DR.
Vista l'esperienza di RCM Italia nella gestione dei grandi volumi di dati è sempre stato un obiettivo per l'azienda il creare una architettura elastica: che può essere espansa in caso di aumento del carico di lavoro oppure ridotta nel caso di un calo delle necessità.
L'intera soluzione è stata progettata per essere in grado di gestire l'elaborazione di grandi volumi di dati. A tale scopo, il sistema può essere scalato sia verticalmente che orizzontalmente e, le singole componenti, possono essere distribuite su più server. La compatibilità con la virtualizzazione e il *cloud computing* è garantita previa raggiungibilità dei certificati di firma.
L'architettura è basata su una soluzione multi-tier a 3 livelli:

- Presentation layer;

- Business logic (o application) layer;
- Database layer.

L'estrema elasticità del prodotto permette di sostituire, upgradare a caldo oppure di aggiungere a piacere applicazioni in uno o più nuovi nodi di un eventuale cluster:

- **Back End** (Services): rappresenta il core della logica applicativa e l'interfaccia verso le basi dati (MySql) a cui l'applicazione attinge. Il Back End ha in carico la gestione e la distribuzione dei processi.
- **Engine**: è il motore di conservazione.
- **Front End** (Interfaccia Web): è un'applicazione realizzata attraverso l'uso di pagine web dinamiche. Attraverso Front End gli utenti potranno accedere per configurare e monitorare il sistema.

Di seguito la lista dei browser dichiarati compatibili:

- Android 2.3 o superiore.
- Google Chrome 23 o superiore.
- Internet Explorer 8 o superiore.
- iOS 5 o superiore.
- Mozilla Firefox 17 o superiore.
- Opera 12 o superiore.
- Safari 6 o superiore.

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

- **Full-text Engine**: è l'applicazione che abilita le funzionalità di full-text.
- **Web Services**: sono un insieme di servizi web che permettono, ad applicazioni di terze parti, di versare documenti nel sistema di conservazione o di interrogare lo stesso sullo stato di un documento.
- **File System**: è un sottoprocesso di Back End che permette di effettuare polling su folder per il versamento automatico dei documenti al sistema di conservazione.

In un'ottica di installazione su ambienti virtuali, il sistema consente un'ampia scalabilità al crescere degli utenti coinvolti e, cosa più importante, al crescere del volumi di documenti da conservare, permettendo di reagire tempestivamente alle nuove esigenze del cliente.

Trust service - Firma Digitale Remota

Il servizio di firma digitale remota è basato sull'acquisizione da parte del Certificatore Accreditato Aruba, di certificati di firma da utilizzare attraverso un'infrastruttura HW e SW che permette di realizzare la cd. Firma remota.
Con "firma digitale remota" si intende la firma digitale apposta sui documenti, eseguita con una chiave privata non residente su un dispositivo personale dell'utente (es. lettore di smart card) bensì su un dispositivo remoto idoneo alla conservazione di dette chiavi. Questo rende il servizio estremamente pratico da utilizzare, in quanto l'utente non deve installare driver e librerie sulla propria postazione e può firmare digitalmente "da remoto" qualunque documento. La sicurezza è garantita in quanto l'utente deve accedere al servizio utilizzando un sistema di autenticazione a due fattori (conoscenza e possesso) basato su token OTP.
Nel caso del servizio di ***Firma digitale remota***, la chiave privata risiede presso un server sicuro (HSM, Hardware Security Module) dislocato nel Centro servizi della CA, che ne garantisce sempre la disponibilità ogni volta che è necessario (sia per apporre la firma che per verificarne la validità). Tale dispositivo impedisce che la chiave privata dell'utente possa essere rivelata, in quanto ne rende impossibile l'estrazione. Le operazioni di firma sono quindi eseguite all'interno del'HSM stesso.
RCM Italia ha integrato i propri applicativi col sistema di firma remota attraverso l'invocazione di ***web services*** (WS) con protocollo SOAP. Allo scopo è realizzato presso il Centro Servizi un servizio di Integrazione Applicativa per le soluzioni di Firma Remota, denominato ARSS (Aruba Remote Sign Server) che consente a

RCM di integrare il sistema di firma remota con i propri applicativi o di utilizzarla direttamente da interfaccia web tramite il portale. Poiché le applicazioni di RCM sono ospitate in infrastrutture IT diverse da quella dove risiede il sistema di Firma Digitale Remota di Aruba, il componente ARSS provvede a dialogare su canale sicuro HTTPS con i Sistemi della Certification Authority di Aruba limitatamente all'invio delle richieste di generazione di certificati alla Certification Authority e all'eventuale verifica dei file sottoscritti con certificati Aruba.

Di seguito è descritta l'architettura utilizzata e le componenti Hardware e Software utilizzate per l'erogazione del servizio.

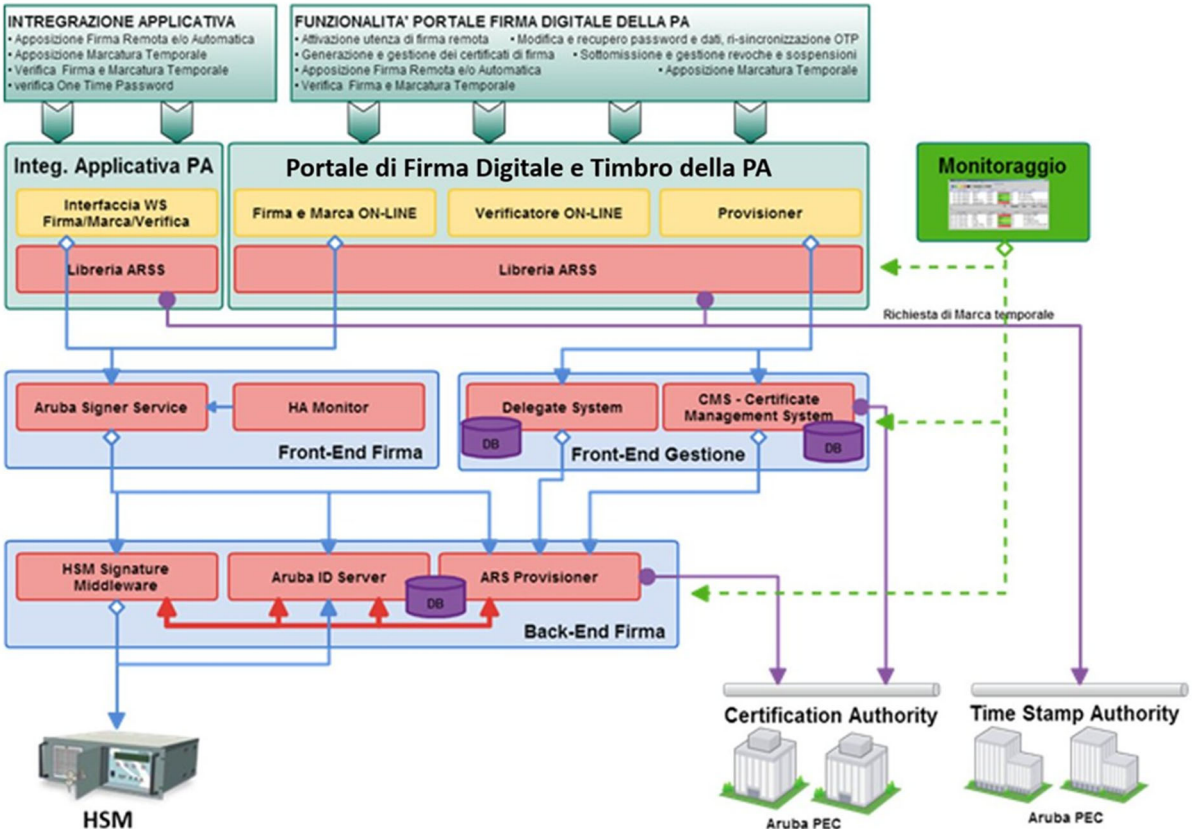

Figura 6 Architettura software del servizio di Firma digitale remota

Tutte le componenti hardware e software sono installate presso i centri servizi di Aruba e, limitatamente all'interfaccia di front-end (Aruba Remote Signing Server – ARSS), presso la sede di RCM.
La soluzione è predisposta, sul sito di produzione, con più nodi che lavorano in alta affidabilità, utilizzando una particolare architettura active-active sviluppata per garantire in ogni situazione la coerenza della firma ed il rispetto della normativa vigente. Il sistema è costantemente controllato da un apposito strumento di monitoraggio, implementato direttamente dalla componente HA Monitor, che consente di verificare la regolare operatività del sistema e di segnalare tempestivamente il verificarsi di anomalie hardware o applicative.

Torna al sommario

8.3 Scalabilità sui volumi

La conservazione dei documenti, rispetto ai volumi, è soggetto a due variabili:

- Crescita dei documenti;
- Crescita dei dati.

La crescita dei documenti, vista la dimensione fisica degli oggetti, è sicuramente la parte più critica in termini di scalabilità. Per questo motivo il sistema di conservazione è stato sviluppato per essere indipendente dal sistema hardware che conserva i file. Oltre ad essere svincolato dal sistema hardware, il software è in grado di distribuire i documenti da conservare su più storage in funzione di regole che dipendono dalla tipologia di documenti o dalla disponibilità di risorse. Per questo motivo, al crescere dei volumi, è possibile affiancare agli esistenti altri storage con caratteristiche tecnologiche anche differenti rispetto ai presenti.
Il Sistema di Conservazione è stato progettato per supportare numeri elevati di utenti che vi accedono per consultare documenti in esso conservati. In ogni caso, trattandosi di un applicativo sviluppato a tre livelli ed impiegando le più moderne tecnologie di implementazione software, è possibile far crescere la componente Interfaccia Web in funzione del numero di utenti. Anche la componente database è assolutamente scalabile in funzione del numero di utenti.
Riepilogando:

- necessità di maggiore capacità elaborativa => si aggiungono application server e/o core e RAM;
- necessità di maggiore capacità elaborativa sui Database e Repository/Content Server => si aggiungono ulteriori server ai rispettivi cluster e/o core e RAM;
- necessità di archiviare una maggior quantità di dati => si aggiungono nuovi dischi agli storage;
- Alla saturazione di uno storage se ne aggiunge un altro;
- necessità di maggiore banda fra il sito principale e l'eventuale sito di disaster recovery: la presenza di accessi in Fibra Ottica sulle due sedi consente di ampliare agevolmente la banda disponibile per il collegamento.

Torna al sommario

8.4 Componenti Fisiche

Piattaforma di esercizio primario del servizio

La piattaforma è stata implementata sia su una piattaforma di esercizio primario che su una piattaforma gemella, per la funzionalità di Disaster Recovery. La piattaforma di test è separata fisicamente e logicamente da quella di sviluppo: entrambi gli ambienti di test e sviluppo sono presenti nel sito operativo della RCM Italia.
La piattaforma di esercizio primario eroga il servizio di conservazione con macchine fisiche ridondate, che garantiscono cioè l'alta affidabilità dei processi, in modo che, qualora un processo relativo ad un software dovesse avere un blocco nell'erogazione, la piattaforma continua ad erogare il servizio con la macchina gemella.
Per questo motivo, esistono 2 macchine gemelle di erogazione dei processi relativi al Front End e 2 macchine gemelle per i processi del Back End.
La configurazione sfrutta l'algoritmo di Round Robin, garantendo così oltre all'alta affidabilità, anche la scalabilità dei processi. Infine, i bilanciatori sul sito primario consentono di erogare i servizi in alta affidabilità mentre, il cluster dei servizi di backend, permette di estendere le stesse garanzie all'intera infrastruttura.
È disponibile un sito di *Disaster Recovery*, nel Data Center Extratel al Centro Direzionale Isola F10 Napoli, come ulteriore protezione dei sistemi dagli eventi di natura disastrosa che si possono verificare sul sito di erogazione principale di Roma. La piattaforma sul sito secondario è realizzata con caratteristiche funzionali simili a quelle del sito primario.
I Data Center di Roma e Napoli sono conformi ai principali standard di sicurezza internazionale ed in particolare il DC di Roma implementa un Sistema di Gestione della Sicurezza delle Informazioni certificato ISO 27001. I dischi sul sito Primario e DR per il sistema di conservazione sono crittografati al fine di garantire un elevato livello di sicurezza del dato.
L'architettura *High Level* distribuita sui 2 siti (Produzione e DR) si compone di diverse tecnologie abilitanti al fine di indirizzare in modo ottimale le esigenze per ogni linea di erogazione.
Per il sito di DR si ottengono RPO (*Recovery Point Objective,* riferito alla perdita dei dati) tendente a zero con l'utilizzo delle seguenti tecniche:

- Replica dei dati residenti su DB utilizzando tecnologie di replica a livello software (log *shipping e standbyDB*), che consentono di avere sul sito remoto una copia consistente a livello applicativo per architetture complesse multi-istanza;
- Replica dei dati residenti su file system effettuata attraverso tecnologie di data *replication host-based;*
- Replica dei dati residenti su DB in modo sincrono su NAS sul DC Primario.

Tale soluzione consente di garantire protezione e ridondanza dei dati rendendo possibile la ricostruzione completa degli ambienti tramite funzionalità di allineamento massivo offerte dalle tecnologie di *data replication* a livello *array.*
Per maggiori dettagli si richiama il piano della sicurezza, capitolo 5 "Perimetro del sistema di conservazione"

Torna al sommario

8.5 Procedure di gestione e di evoluzione

Gli interventi di manutenzione, a qualunque tipologia appartengano, oltre a garantire operatività e funzionalità ai sistemi, hanno un alto profilo di qualità in termini sia di manutenibilità che di verificabilità delle applicazioni; per ottenere tali risultati è condizione essenziale un approccio di tipo metodologico e strutturato, che consente di:

- valutare l'impatto: prima di operare la modifica, in sede di definizione degli interventi di manutenzione, deve essere valutato con precisione l'impatto che la modifica avrà sul funzionamento dell'intero sistema;
- controllare l'azione: è necessario procedere nell'esecuzione degli interventi rispettando sia gli standard e le regole proprie del processo di produzione del software che le modalità di erogazione del servizio, aggiornando coerentemente la documentazione al fine di preservare nel corso del tempo il livello di manutenibilità del sistema.

Vengono di seguito sinteticamente illustrati i processi di sviluppo e manutenzione evidenziando in particolare le fasi connesse alla gestione della configurazione:

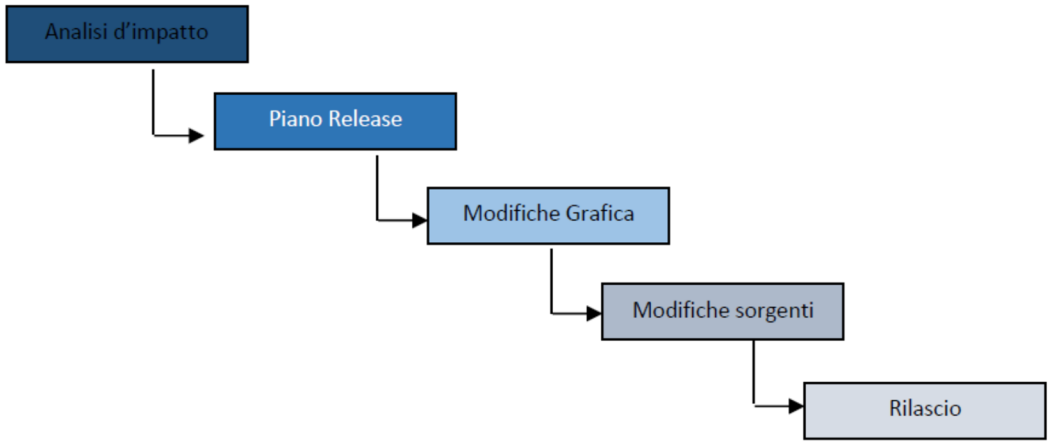

Figura 7 Processi di sviluppo e manutenzione

L'analisi di impatto ha l'obiettivo di determinare la portata dell'intervento richiesto ai fini della sua pianificazione e relativa implementazione. Si articola in:

- valutare la richiesta di manutenzione per ciò che riguarda l'impatto potenziale sui sistemi software esistenti, sulla documentazione, sulle strutture dati;
- determinare una stima preliminare delle risorse necessarie;
- documentare la portata della modifica e conseguentemente aggiornare il documento di richiesta di modifica.

Dopo la loro analisi, le modifiche possono essere raggruppate come una **release** di manutenzione schedulata, con conseguente pianificazione, il cui obiettivo è determinarne i contenuti e la tempificazione.
Le principali attività sono:

- selezione delle richieste di modifica per la prossima release;
- raggruppamento delle modifiche e schedulazione del lavoro;
- preparazione di un documento di pianificazione della release e, introduzione nel sistema di gestione delle configurazioni;
- aggiornamento della richiesta di modifiche approvata.

Attività afferenti alle modifiche design prevedono:
- analisi della richiesta approvata ed eventuale revisione della struttura architetturale;
- revisione e sviluppo della progettazione funzionale e tecnica;
- aggiornamento della documentazione di progetto e del dizionario dati;
- recupero e rimpiazzo di tutti i documenti modificati;
- aggiornamento della richiesta di intervento.

Le principali attività relative alle modiche sorgenti sono:
- realizzare ed eseguire lo unit test delle modifiche nel codice;
- memorizzare o rimpiazzare il codice, sotto il controllo del sistema di gestione delle configurazioni;
- aggiornare la richiesta di manutenzione in modo da rispecchiare i moduli o le unità modificate.

I rilasci saranno strutturati e qualificati; il significato della codifica usata da RCM Italia è chiara ed univoca. In particolare, sono previste le seguenti tipologie di rilasci:
- Livello di manutenzione (Maintainance Level);
- Rilascio di aggiornamento (Release);
- Versione (Version).

Gli interventi di manutenzione evolutiva sono assimilabili ad un insieme di piccoli progetti con durate ipotizzabili che oscillano secondo i requisiti individuati. Tali attività presentano le caratteristiche tipiche di ogni progetto, ovvero:
- definizione dei requisiti, definizione di una soluzione tecnica, stima dei costi e dei tempi, formalizzazione dell'incarico, pianificazione, analisi dei rischi ed esecuzione delle attività progettuali, accettazione del prodotto e autorizzazione dei pagamenti.

Il processo operativo per la gestione degli interventi seguirà un modello iterativo incrementale suddiviso in due fasi descritte nei paragrafi seguenti:
- Pianificazione intervento;
- Sviluppo e rilascio.

La pianificazione dell'intervento avverrà come segue:
- L'attivazione dell'intervento: l'intervento manutentivo viene sempre avviato in relazione ad una Richiesta di Sviluppo Modifiche (RSM) di manutenzione evolutiva proveniente dal Committente che comunicherà, via fax o e-mail, la richiesta di comprensiva dei requisiti e dei vincoli temporali ai quali deve sottostare l'intervento richiesto (affidamento). Il team di manutenzione, nel momento dell'attivazione dell'intervento, provvederà alla predisposizione di una Scheda di Intervento attraverso la quale le suddette richieste saranno formalizzate, corredate da informazioni utili al raggiungimento dell'obiettivo quali: data prevista di inizio attività; data richiesta per completamento fase di definizione; eventuali vincoli (ad esempio richieste utente di date di esercizio).
- Studio di evoluzione funzionale: il Responsabile del progetto, entro 5 giorni naturali consecutivi, analizza la richiesta e predispone il documento "Studio di evoluzione funzionale" comprendente l'analisi di fattibilità dell'intervento richiesto, le figure professionali da utilizzare, la pianificazione dello sviluppo, la tempificazione di svolgimento dell'intervento (e relativa data di rilascio) e la stima economica espressa come impegno in termini di giorni uomo per figura professionale. Lo Studio di evoluzione funzionale sarà sottoposto all'approvazione del responsabile del contratto del Committente.

- Affidamento: La realizzazione dell'intervento verrà affidata dal Committente attraverso una specifica richiesta di prestazione, a seguito dell'approvazione del suddetto "Studio di evoluzione funzionale" da parte del responsabile del contratto del Committente stesso.

Lo sviluppo ed il rilascio avverranno come segue:

- Definizione delle attività realizzative: il Responsabile del Servizio (RDS) di RCM Italia, alla ricezione della richiesta di prestazione, provvede alla formulazione del documento di "Definizione delle attività realizzative" articolato in: definizione e pianificazioni; analisi; disegno; pianificazione delle attività.
- Realizzazione: Una volta approvato il documento di "Definizione delle attività realizzative, il piano di dettaglio correlato diventa esecutivo e il team di manutenzione prende in carico la gestione dell'intervento e diviene, quindi, responsabile del completamento dell'intervento; ove necessario, potrà contattare l'utente finale per richiedere ulteriori informazioni d'approfondimento sulla richiesta inviata. Il Responsabile del Servizio (RDS) sulla base del suddetto piano avvia le attività allocando le risorse e controllando la realizzazione fino alla consegna del prodotto secondo le scadenze pianificate.
- Collaudo e Rilascio: a conclusione delle attività realizzative, a seguito del test e del "collaudo di conformità" con esito positivo d p dotti realizzati.

La manutenzione correttiva consiste nell'adeguamento del software in relazione ad un difetto o malfunzionamento. Le attività di manutenzione correttiva, mirate alla risoluzione dei problemi, sono svolte nel rispetto dei livelli di servizio (SLA) richiesti.
La richiesta di azione correttiva (RAC) avverrà di norma attraverso la notifica formale via e-mail o fax al Capo Progetto da parte del Responsabile del contratto del Committente.
Il team di manutenzione prende in carico la gestione della Richiesta e diventa, quindi, responsabile per il completamento dell'intervento; ove necessario, potrà contattare l'Utente finale per richiedere ulteriori informazioni d'approfondimento sulla richiesta inviata. Se non diversamente specificato dal Committente, l'attivazione dell'intervento è tracciata mediante un sistema di ticketing; mediante questo sarà possibile avere evidenza dello stato del singolo processo e dei livelli di servizio raggiunti.
Il gruppo di lavoro impegnato individua gli oggetti coinvolti dall'attività, eventuali effetti collaterali su altri oggetti software, attua la manutenzione richiesta, nel rispetto delle modalità definite (fasi e prodotti per le singole fasi), dichiarando, alla terminazione dei lavori di sviluppo e test, la disponibilità al rilascio in esercizio.
Nel corso dello svolgimento dell'intervento il team di manutenzione provvederà a mantenere aggiornato il sistema centrale di gestione delle segnalazioni relativamente allo stato dell'intervento.
Il flusso operativo si articola attraverso i seguenti passi:

- a fronte dell'attivazione, il team di manutenzione provvede alla fornitura di una prima risposta immediata con una prima soluzione temporanea (by-pass seguita dalla preparazione di una correzione puntuale - PTF (*ProgramTemporary Fix*) e dall'effettuazione del test di regressione e relativi collaudi di integrazione;
- nella fase di presa in carico degli interventi viene svolta una attività di analisi volta a studiare l'impatto delle variazioni e le eventuali modifiche alla performance del sistema che ne derivano. Il responsabile di servizio/progetto di RCM Italia effettuata una prima valutazione e designa, sulla base delle competenze tecnico-funzionali necessarie, il responsabile dell'intervento e attiva il team di risorse in base agli *skill* necessari alla priorità dell'intervento richiesto ed alle disponibilità;
- il passo successivo, la definizione dell'intervento, è volto a individuare e descrivere le esigenze funzionali e gli altri vincoli espressi dall'utente, nel caso di intervento originato da una richiesta da parte degli utenti del sistema, ovvero a individuare le necessità di adeguare le funzionalità del sistema alle variazioni del contesto tecnologico/funzionale. Si procede alla definizione della soluzione più idonea, all'individuazione degli oggetti da modificare e alla definizione dei casi di test, di integrazione e di sistema, che permettono di verificare il corretto ripristino della funzionalità: viene effettuata una attività di pianificazione che ha l'obiettivo di definire le operazioni da eseguire nell'ambito dell'intervento, le dipendenze tra di esse e la loro durata individuale ed in particolare ha

ad oggetto la stima della dimensione dell'intervento, la stima dell'effort per eseguire l'intervento manutentivo ed i test di regressione ad esso associati (per ognuna delle figure professionali coinvolte), la stima della durata dell'intervento basata sulla precedente stima della quantità di lavoro necessaria;

- una volta ottenuta l'approvazione del soggetto produttore, si passa alla fase successiva di attuazione/integrazione durante la quale vengono realizzate le modifiche necessarie al software applicativo e alla struttura della base dati; vengono eseguiti i casi di test unitario del software modificato/prodotto e vengono eseguiti i casi di test di integrazione e di sistema definiti nel corso della fase precedente. Le attività di aggiornamento del software sono accompagnate da altrettanti aggiornamenti della documentazione relativa rispetto alle modifiche effettuate. Il responsabile di servizio riceve notifica automatica dell'esito positivo delle attività di test; verifica i risultati delle attività eseguite e comunica al soggetto produttore la chiusura dell'intervento e la disponibilità per il rilascio nell'ambiente di esercizio;
- si procede infine alle operazioni di collaudo di integrazione, per gli interventi che lo richiedano, ed al successivo rilascio in esercizio dell'applicazione.

Viene formalizzata la chiusura definitiva dell'intervento e registrata con l'apposito strumento di gestione interventi: la chiusura dell'intervento viene notificata al produttore e agli utenti secondo i canali di comunicazione concordati.

Torna al sommario

9. MONITORAGGIO E CONTROLLI

Il presente capitolo descrive le procedure di monitoraggio delle funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate.
(Regole tecniche: art. 8, comma 2 lettera h).

Torna al sommario

9.1 Procedure di monitoraggio

Tipo anomalia	Descrizione	Modalità di gestione
Mancata risposta al Versamento	È il caso in cui l'unità documentaria viene correttamente versata ma, per vari motivi, la risposta di avvenuta ricezione non perviene al produttore, che pertanto, erroneamente, lo reputa non versata.	Il soggetto produttore deve trasmettere nuovamente e il sistema di conservazione restituisce una risposta di esito negativo con l'indicazione che l'unità documentaria risulta già versata. Tale risposta deve essere usata dal produttore come attestazione di avvenuto versamento e l'unità documentaria deve risultare come versata.
Errori temporanei	È il caso di errori dovuti a problemi temporanei che pregiudicano il versamento, ma si presume non si ripresentino a un successivo tentativo di Versamento. Il caso più frequente è l'impossibilità temporanea di accedere alle CRL degli enti certificatori. In questi casi il sistema di conservazione dopo aver riprovato 10 volte, genera un messaggio di errore perché non riesce a completare le verifiche previste sulla validità della firma e il versamento viene quindi rifiutato impostando il processo in stato ERRV.	Il soggetto produttore deve provvedere a rinviare l'unità documentaria in un momento successivo. L'operazione potrebbe dover essere ripetuta più volte qualora il problema, seppur temporaneo, dovesse protrarsi nel tempo.
Versamenti non conformi alle regole concordate	È il caso in cui il versamento non viene accettato perché non conforme alle regole concordate (firma non valida, Formato file non previsto, file corrotto, mancanza di Metadati obbligatori, ecc.).	Il soggetto conservatore invia via e-mail una segnalazione dell'anomalia ai referenti del soggetto produttore, con i quali viene concordata la soluzione del problema.
Errori interni o dovuti a casistiche non previste o non gestite	In alcuni casi è possibile che il sistema di conservazione risponda con un messaggio di errore generico che non indica le cause dell'anomalia riscontrata in quanto dovuta a un errore interno o perché legata a una casistica non prevista, non gestita o non gestibile dal sistema di conservazione.	I referenti del soggetto produttore segnalano il problema via e-mail al soggetto conservatore, che si attiverà per la sua risoluzione.

Tabella 3 - Procedure di monitoraggio

Le anomalie vengono affrontate con diverse metodologie, secondo la natura dell'anomalia stessa e la collocazione dell'evento che l'ha generata nel processo di conservazione; quindi oltre alle procedure atte a garantire l'integrità degli archivi, esistono anche procedure atte a risolvere anomalie in altre componenti del sistema.

Le caratteristiche comuni e le specificità delle procedure di risoluzione delle anomalie dipendono da diversi fattori organizzativi e tecnologici:

- tutte le funzionalità del sistema che inseriscono o modificano dati nel Data Base e file nell'area SFTP o nel File System operano in modalità transazionale;
- il backup del Data Base assicura il *restore* all'ultima transazione completata correttamente;
- dell'Area di Upload riservata a ciascun soggetto produttore e viene effettuato backup;

Non è quindi possibile far fronte a tutte le possibili anomalie con le stesse procedure, ma sono necessarie procedure specifiche secondo la natura dell'anomalia stessa.

La tabella seguente illustra le misure adottate per risolvere eventuali anomalie, classificate in ragione della collocazione delle informazioni nell'ambito del sistema nel momento in cui si è verificata anomalia:

File System	Si effettua la restore tramite le funzioni standard del file server per tutti i file inseriti nel File system fino all'ultimo back up; per i file inseriti successivamente all'ultimo back up si eseguono opportune procedure di quadratura tra Data Base e File System, che provvedono a riportare il sistema in stato di congruenza. Le procedure di recupero debbono essere eseguite sia sul sito primario che sul secondario.
Database	Si effettua la restore tramite le funzioni standard di Oracle dal sito primario o dal sito secondario (nel caso di indisponibilità del DB primario)
Area SFTP/Upload	In caso di problemi riscontrati prima del backup, si richiede al soggetto produttore la ritrasmissione dei PdV

Tabella 4 - Misure adottate per risolvere eventuali anomalie

I servizi ed i sistemi gestiti da RCM Italia, sono controllati in modo automatico da due diversi sistemi di monitoraggio che consentono la visualizzazione e la notifica degli allarmi:

Il "Sistema Esterno" consente il controllo dei servizi erogati in rete dall'infrastruttura effettuando accessi periodici ai servizi tramite collegamento esterno in ADSL su rete internet.

Il "Sistema Interno" utilizza un Network Management System completamente gestito dagli addetti della CA che consente di mantenere il controllo della rete e dei sistemi fornendo importanti informazioni per la corretta gestione sistemistica.

La rilevazione di qualsiasi anomalia viene registrata e successivamente risolta dal personale autorizzato RCM Italia.

Tutti i controlli seguono una pianificazione stabilita dal responsabile dello sviluppo e della manutenzione dei sistemi di conservazione. Detta pianificazione viene messa in atto attraverso piattaforme e software ad hoc, in grado di eseguire controlli "terzi" in modo automatico ed inviare le eventuali notifiche al responsabile dei sistemi informativi.

Torna al sommario

9.2 Verifica dell'integrità degli archivi

La funzionalità di verifica di integrità degli archivi, permette di verificare l'integrità del documento informatico dal momento della sua conservazione, confrontando l'impronta attuale con quella contenuta nell'Indice di Conservazione. Tale funzionalità viene applicata durante il processo di conservazione subito dopo la fase di memorizzazione nel file system, e risulta poi utile, nell'assolvimento dei requisiti di verifica periodica della leggibilità dei documenti, come richiesto dalla normativa.

A ogni verifica effettuata viene generato un report in formato xml che può essere consultato da parte del responsabile del servizio di conservazione per attestare la corretta esecuzione della verifica o per diagnosticare eventuali anomalie.

Torna al sommario

9.3 Soluzioni adottate in caso di anomalie

Di seguito viene descritta la tabella dei livelli di servizio garantiti, suddivisi per attività relativa al servizio di conservazione.

ID	Attività	Livelli di servizio	% di applicazione
1	Lavorazione dei PdV ricevuti	Entro il giorno lavorativo successivo (festivi esclusi) dalla ricezione del pacchetto di versamento.	99,5% dei PdV ricevuti
2	Comunicazione eventuali anomalie in fase di versamento (Per errori strettamente riguardanti il contenuto dei file ricevuti)	Entro il giorno lavorativo successivo (festivi esclusi) dalla ricezione del pacchetto di versamento.	99,5% dei PdV ricevuti
3	Invio ai clienti della segnalazione di errori che causano il blocco dell'elaborazione dei PdV	Entro il giorno lavorativo successivo (festivi esclusi) dalla ricezione del pacchetto di versamento.	99,5% dei PdV ricevuti
4	Avvio rielaborazione dei PdV o oggetto di anomalia.	Entro il giorno lavorativo successivo (festivi esclusi) dalla risoluzione anomalia (dalla data comunicazione al Cliente).	99,5% dei PdV ricevuti
5	Risoluzione malfunzionamenti ddel servizio di CS	Presa in carico: entro 8 ore lavorative nei seguenti orari: dalle ore 9.00 alle ore 13.00 e dalle ore 14.00 alle ore 17 di ciascun giorno feriale.	N.A.
6	Disponibilità dei servizi di caricamento (upload) - Upload Manuale - Modalità SFTP - A2A (Web Services) N.B.: La disponibilità delle modalità Custom viene espressamente concordata con il Soggetto Produttore	Entro il giorno lavorativo successivo (festivi esclusi) dalla segnalazione.	99,9% su base trimestrale
7	Disponibilità del servizio di consultazione ed esibizione dei documenti conservati (interfaccia Web).	Entro il giorno lavorativo successivo (festivi esclusi) dalla ricezione del pacchetto di versamento.	99% su base trimestrale

Tabella 5 - Soluzioni adottate in caso di anomalie

Qui di seguito sono riportate le condizioni in presenza delle quali, non saranno imputabili a RCM Italia il verificarsi di eventuali disservizi:

- cause di forza maggiore e cioè eventi che, oggettivamente, impediscano al personale di RCM Italia di intervenire per eseguire le attività poste dal Contratto a carico della stessa RCM Italia (in via meramente esemplificativa e non esaustiva: scioperi e manifestazioni con blocco delle vie di

comunicazione; incidenti stradali; guerre e atti di terrorismo; catastrofi naturali quali alluvioni, tempeste, uragani etc);

- interventi straordinari da e effettuarsi con urgenza ad insindacabile giudizio di RCM Italia per evitare pericoli alla sicurezza e/o stabilità e/o riservatezza e/o integrità dei dati e/o informazioni del Cliente. L'eventuale esecuzione di tali interventi sarà comunque comunicata al Cliente a mezzo e mail inviata all'indirizzo di posta elettronica indicato in fase d'ordine con preavviso anche inferiore alle 48 ore oppure e contestualmente all'avvio delle operazioni in questione o comunque non appena possibile;
- indisponibilità o blocchi dell'Infrastruttura imputabili a:
  - errato utilizzo, errata configurazione o comandi di spegnimento, volontariamente o involontariamente e eseguiti dal cliente;
  - anomalie e malfunzionamenti dei software applicativi/gestionali fornitti i da terze parti;
  - inadempimento o violazione del Contratto imputabile al Cliente;
  - anomalia o malfunzionamento del Servizio, ovvero loro mancata o ritardata rimozione o eliminazione imputabili ad inadempimento o violazione del Contratto da parte del Cliente ovvero ad un cattivo uso del Servizio da parte sua;
  - cause che determinano l'inaccessibilità, totale o parziale, dell'Infrastruttura dal Cliente imputabili a guasti nella rete internet esterna al perimetro di RCM Italia e comunque fuori dal suo controllo (in via meramente esemplificativa guasti o problemi).

Torna al sommario