TIPO DI DOCUMENTO	MANUALE DELLA CONSERVAZIONE
PROGETTO	CONSERVAZIONE DIGITALE A NORMA
NOME CLIENTE	MEDIATICA S.P.A.
STATO DEL DOCUMENTO	**APPROVATA**
VERSIONE	**2.5**
DATA	25.03.2019

ATTIVITÀ	RESPONSABILITÀ	FIRMA	DATA
Redazione	*Adriano Ricchello*		
Verifica	Responsabile del servizio di conservazione *Stefano Di Zenzo*		
Approvazione	Responsabile del servizio di conservazione *Stefano Di Zenzo*		

MATRICE DELLE REVISIONI

Par.	Motivazioni in Sintesi
Par. 5.3.2	Inserito riferimento per gli audit interni al par. 4.8 del Piano di Sicurezza
Par.6.1	Previsto check automatico tipo documento in fase di versamento
Par. 8.3	Aggiornata versione VMWare alla 6.0.3
Par. 9	Specificati principi di separazione dei ruoli
Par. 9.1	Aggiornato riferimento al GDPR 679/2016
Par. 10	Inserito SLA di uptime del servizio

LISTA DI DISTRIBUZIONE

N° Copia	Funzione
1	Responsabile del Servizio di Conservazione
1	Privacy Manager
1	IT Manager
1	Security Manager
1	AGID

Sommario

1 SCOPO E AMBITO DEL DOCUMENTO 4
2 TERMINOLOGIA (GLOSSARIO E ACRONIMI) 6
2.1 Documenti correlati 9
3 NORMATIVA E STANDARD DI RIFERIMENTO 11
3.1 Normativa di riferimento 11
3.2 Standard di riferimento 12
4 RUOLI E RESPONSABILITA' 13
5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE 17
5.1 Organigramma 17
5.2 Strutture organizzative: attività proprie di ciascun contratto di servizio di conservazione. 17
5.2.1 Acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento; 18
5.2.2 Preparazione e gestione del pacchetto di archiviazione; 19
5.2.3 Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta. 19
5.2.4 Scarto dei pacchetti di archiviazione 20
5.2.5 Chiusura del servizio di conservazione (al termine di un contratto) 20
5.3 Strutture organizzative: attività proprie di gestione dei sistemi informativi. 20
5.3.1 Conduzione e manutenzione del sistema di conservazione 21
5.3.2 Monitoraggio del sistema di conservazione 22
5.3.3 Change management; 23
5.3.4 Verifica periodica di conformità a normativa e standard di riferimento. 24
6 OGGETTI SOTTOPOSTI A CONSERVAZIONE 26
6.1 Oggetti conservati 26
6.2 Pacchetto di versamento 27
6.2.1 Modo interattivo 28
6.2.2 Layer applicativo 28
6.2.3 Struttura del Rapporto di Versamento - RdV 29
6.3 Pacchetto di archiviazione 31
6.3.1 Struttura del Pacchetto di Archiviazione - PDA 31
6.3.2 Indice del pacchetto di archiviazione - IPdA 33
6.4 Pacchetto di distribuzione 34
7 IL PROCESSO DI CONSERVAZIONE 36
7.1 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico . 36
7.1.1 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti 37
7.1.2 Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico 38
7.1.3 Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie 39
7.1.4 Preparazione e gestione del pacchetto di archiviazione 39

7.1.5 Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione 40
7.1.6 Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti 41
7.1.7 Scarto dei pacchetti di archiviazione 41
7.1.8 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori 42
7.1.9 Cessazione del servizio 42
7.1.10 Gestione delle segnalazioni da parte dell'utente 43
8 IL SISTEMA DI CONSERVAZIONE 45
8.1 Componenti Logiche 45
8.2 Componenti Tecnologiche 47
8.3 Componenti Fisiche 48
8.4 Procedure di gestione e di evoluzione 48
9 MONITORAGGIO E CONTROLLI 49
9.1 Procedure di monitoraggio 50
9.2 Verifica dell'integrità degli archivi 51
9.3 Soluzioni adottate in caso di anomalie 51
10 Appendice A – livelli di servizio (SLA) 53

1 SCOPO E AMBITO DEL DOCUMENTO

Il presente Manuale di Conservazione identifica processi e infrastrutture del sistema di *conservazione documentale a norma* messo in atto da Mediatica S.p.A. (di seguito *Mediatica*) per la gestione dei documenti propri e dei propri clienti.

Nel documento sono definite le informazioni necessarie per la gestione del sistema di conservazione e per la definizione dei ruoli e delle interazioni con i soggetti esterni con i quali interagisce.

Viene emesso seguendo le indicazioni del documento *Schema Manuale Conservazione* emesso da Agid in data 16.1.2015.

Nel dettaglio il presente documento definisce:

- i dati dei soggetti che nel tempo hanno assunto la responsabilità del sistema di conservazione, descrivendo in modo puntuale, in caso di delega, i soggetti, le funzioni e gli ambiti oggetto della delega stessa;
- la struttura organizzativa comprensiva delle funzioni, delle responsabilità e degli obblighi dei diversi soggetti che intervengono nel processo di conservazione;
- la descrizione delle tipologie degli oggetti sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di documenti e delle eventuali eccezioni;
- la descrizione delle modalità di presa in carico di uno o più pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento;
- la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione;
- la modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;
- la descrizione del sistema di conservazione, comprensivo di tutte le componenti tecnologiche, fisiche e logiche, opportunamente documentate e delle procedure di gestione e di evoluzione delle medesime;
- la descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie;
- la descrizione delle procedure per la produzione di duplicati o copie;
- i tempi entro i quali le diverse tipologie di documenti devono essere scartate ovvero trasferite in conservazione, ove, nel caso delle pubbliche amministrazioni, non già presenti nel manuale di gestione;
- le modalità con cui viene richiesta la presenza di un pubblico ufficiale, indicando anche quali sono i casi per i quali è previsto il suo intervento;
- le normative in vigore nei luoghi dove sono conservati i documenti.

Tutti i documenti sono emessi dall'RSC in formato elettronico, firmati digitalmente e archiviati tramite Conservazione.

(Torna al Sommario)

2 TERMINOLOGIA (GLOSSARIO E ACRONIMI)

Termine/Acronimo	Definizione
Accesso	Operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici
Affidabilità	Caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico
AgID	Agenzia per l'Italia Digitale
Archivio	Complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività
Archivio informatico	Archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico
Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico
Autenticità	Caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico
Base di dati	Collezione di dati registrati e correlati tra loro
CA	Certification Authority
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
Classificazione	Attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati
Copia analogica del documento informatico	Documento analogico avente contenuto identico a quello del documento informatico da cui è tratto
Destinatario	Identifica il soggetto/sistema al quale il documento informatico è indirizzato
Documento	Per documento s'intende la rappresentazione informatica o in formato analogico di atti, fatti e dati intelligibili direttamente o attraverso un processo di elaborazione elettronica.
Documento informatico	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
Esibizione	Operazione che consente di visualizzare un documento conservato e di ottenerne copia

Termine/Acronimo	Definizione
Evidenza informatica	Una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica
Firma digitale	Il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.
Formato	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
FTP Server	Programma che permette di accettare connessioni in entrata e di comunicare con un Client attraverso il protocollo FTP
Funzione di hash	Una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
Generazione automatica di documento informatico	Formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni
Idp	Strumento per rilasciare le informazioni di identificazione di tutti i soggetti che cercano di interagire con un Sistema; ciò si ottiene tramite un modulo di autenticazione che verifica un token di sicurezza come alternativa all'autenticazione esplicita di un utente all'interno di un ambito di sicurezza.
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.
Insieme minimo di metadati del documento informatico	Complesso dei metadati, la cui struttura è descritta nell'allegato 5 del presente decreto, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta
Integrità	Insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato
Interoperabilità	Capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi
IPdA	Indice del Pacchetto di Archiviazione
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 – il presente documento

Termine/Acronimo	Definizione
Marca temporale	Una marca temporale (art. 1 DPCM [4]) è un'evidenza informatica risultato di una procedura informatica, con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi.
MC	Manuale di Conservazione
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
Pacchetto di archiviazione	Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del D.P.C.M. 3/12/2013 e secondo le modalità riportate nel presente manuale di conservazione
Pacchetto di distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta
Pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione
Pacchetto informativo	Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare
PdA	Pacchetto di Archiviazione
PdV	Pacchetto di Versamento
Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza
Piano della sicurezza del sistema di gestione informatica dei documenti	Documento, che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi nell'ambito dell'organizzazione di appartenenza
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
RC	Responsabile della Conservazione

Termine/Acronimo	Definizione
Responsabile della gestione documentale	Dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione
Responsabile della conservazione	Soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 delle regole tecniche del sistema di conservazione
Responsabile del Servizio di Conservazione	Soggetto persona fisica nominato responsabile del servizio di conservazione di Mediatica S.p.A. con l'assegnazione delle attività indicate nel documento dell'Agenzia per l'Italia Digitale sui profili professionali richiamati dalla Circolare n. 65/2014 (G.U. n. 89 del 16/04/2014)
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
Riferimento temporale	Informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici da una procedura informatica.
RSC	Responsabile del Servizio di Conservazione
Scarto	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale
Sistema di 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
TSA	Time Stamping Authority. Ente terzo che emette i certificati di marcatura Temporale
Utente	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse
VPN	Virtual Private Network. E' una rete di telecomunicazioni privata, instaurata tra soggetti che utilizzano, come infrastruttura di trasporto, un sistema di trasmissione pubblico e condiviso, come ad esempio la rete Internet.

Tabella 1 - glossario e acronimi

(Torna al Sommario)

2.1 Documenti correlati

Costituiscono parte integrante del presente documento, ma vengono emessi ed aggiornati con atti separati, i seguenti documenti:

- *Libro dei Verbali;*
- *Definizione delle classi documentali.*

Entrambi i documenti sono emessi dall'RSC in formato elettronico, firmati digitalmente e archiviati tramite Conservazione.

(Torna al Sommario)

3 NORMATIVA E STANDARD DI RIFERIMENTO

3.1 Normativa di riferimento

E' di seguito riportata la principale normativa di riferimento per l'attività di conservazione a livello nazionale, eventualmente quella a livello locale in vigore nei luoghi dove sono conservati i documenti e quella specifica relativa alle diverse tipologie di documenti riguardanti il contratto di erogazione del servizio di conservazione.

Queste informazioni sono periodicamente aggiornate in base alle eventuali modifiche della normativa.

Alla data del 16.1.2015 i principali riferimenti normativi italiani in materia, ordinati secondo il criterio della gerarchia delle fonti, sono costituiti da:

- Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- 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

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

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

Tale elenco, a cui l'attività di conservazione si riferisce, è periodicamente aggiornato in base agli eventuali nuovi standard adottati.

(Torna al Sommario)

4 RUOLI E RESPONSABILITA'

Sono di seguito indicate le attività svolte e i nominativi delle persone che ricoprono i ruoli cosi come individuati nel documento *Profili professionali*.

ruoli	nominativo	attività di competenza	periodo nel ruolo	eventuali deleghe
Responsabile del Servizio di Conservazione	Stefano Di Zenzo	- 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.	Da Gennaio 2010 ad oggi	= =
Responsabile Sicurezza dei Sistemi per la Conservazione	Alessandro Di Francesco	- Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; - segnalazione delle eventuali difformità al Responsabile del Servizio di Conservazione e individuazione e pianificazione delle necessarie azioni correttive.	Da Gennaio 2015 ad oggi	= =

ruoli	nominativo	attività di competenza	periodo nel ruolo	eventuali deleghe
Responsabile Funzione Archivistica di Conservazione	Stefano Di Zenzo	- 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.	Da Gennaio 2010 ad oggi	= =
Responsabile Trattamento Dati Personali	Adriano Ricchello	- 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 impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.	Da Gennaio 2015 ad oggi	= =

ruoli	nominativo	attività di competenza	periodo nel ruolo	eventuali deleghe
Responsabile Sistemi Informativi per la Conservazione	Paolo Bolognese	- Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione; - monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore; - segnalazione delle eventuali difformità degli SLA al Responsabile del Servizio di Conservazione e individuazione e pianificazione delle necessarie azioni correttive; - pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione; - controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del Servizio di Conservazione.	Da Dicembre 2011 ad oggi	= =
Responsabile Sviluppo e Manutenzione del Sistema di Conservazione	Paolo Bolognese	- 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	Da Dicembre 2011 ad oggi	= =

ruoli	nominativo	attività di competenza	periodo nel ruolo	eventuali deleghe
		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.		

Tabella 2 - ruoli e responsabilità

(Torna al Sommario)

5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Organigramma

Segue uno schema delle strutture organizzative coinvolte nel servizio di conservazione.

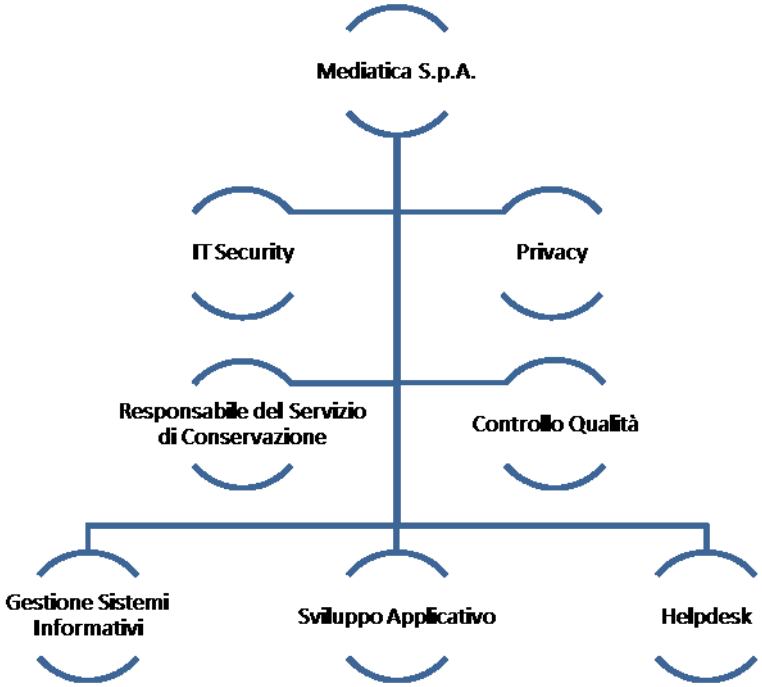

Figura 1 - organigramma

coordinati dai ruoli professionali riportati al par. 4.

(Torna al Sommario)

5.2 Strutture organizzative: attività proprie di ciascun contratto di servizio di conservazione.

L'attivazione del servizio di conservazione, a seguito della sottoscrizione di un contratto con un Cliente o per esigenze interne all'Azienda, viene autorizzata dal RSC che provvede alla necessaria configurazione della piattaforma di conservazione e all'aggiornamento degli allegati:

- *Libro dei Verbali;*
- *Definizione delle classi documentali:*
    - descrizione delle tipologie degli oggetti sottoposti a conservazione

- indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di documenti e delle eventuali eccezioni
- utenze e profilature.

RSC provvede anche a definire le modalità con cui il pacchetto di versamento viene ricevuto e a coinvolgere le strutture a supporto (Gestione Sistemi Informativi e/o Sviluppo Applicativo) per gli adeguamenti infrastrutturali e applicativi necessari.

In generale, gli interventi applicativi sono messi in atto per estrarre i documenti prima che questi vengano memorizzati nella soluzione di conservazione, senza richiedere alcuna modifica della stessa. Qualora ciò sia necessario, o per il necessario supporto durante la vita operativa della stessa, è garantita l'assistenza del fornitore della piattaforma stessa, Andxor Soluzioni Informatiche S.r.l., attraverso uno specifico contratto di supporto.

I processi di change, project e program management sono descritti nei seguenti documenti del Sistema di Gestione della Sicurezza delle Informazioni (SGSI):

- *BAI01 – Gestione dei Programmi e dei Progetti;*
- *BAI06 – Gestione del Change.*

(Torna al Sommario)

5.2.1 *Acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento;*

Per versamento si intende l'insieme di azioni finalizzate all'introduzione di uno o più documenti e dei relativi metadati nel sistema di conservazione. Nel dettaglio si possono distinguere le fasi seguenti:

1. acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico;
2. verifica che il pacchetto di versamento e gli oggetti contenuti siano coerenti con le modalità previste dal presente manuale di conservazione e con le configurazioni delle classi documentali riportate nell'allegato *Definizione delle classi documentali*;
3. il rifiuto del pacchetto di versamento, nel caso in cui le verifiche di cui al punto 2 abbiano evidenziato delle anomalie;
4. la generazione automatica del rapporto di versamento relativo al pacchetto di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo universale coordinato (UTC), e una o più impronte, calcolate sull'intero contenuto del pacchetto di versamento.

(Torna al Sommario)

5.2.2 *Preparazione e gestione del pacchetto di archiviazione;*

Il processo di conservazione consiste nella produzione di uno o più pacchetti di archiviazione e dei relativi indici del pacchetto di archiviazione.

Il processo di conservazione viene eseguito periodicamente in base alla configurazione dell'applicativo.

Il Responsabile del Servizio di Conservazione può comunque lanciare il processo di conservazione manualmente attraverso l'interfaccia ogni volta lo ritenga necessario.

La conservazione viene effettuata per ogni classe documentale che abbia una regola di conservazione valida.

Di seguito l'elenco delle attività svolte:

1. per ogni classe documentale presente viene analizzata la regola di conservazione ad essa associata. Le classi documentali per le quali la conservazione è disabilitata non vengono considerate;
2. per ogni classe documentale viene estratta la lista dei documenti da conservare in base alla regola di conservazione;
3. viene prodotto l'indice del pacchetto di archiviazione contenente i metadati di ciascun documento conservato, inclusa l'impronta. Per una descrizione dell'IPdA si veda il paragrafo seguente;
4. l'IPdA viene firmato con le credenziali di RSC o di un suo delegato e contestualmente viene apposta la marca temporale;
5. l'IPdA, l'insieme di tutti i documenti conservati e una serie di altri dati aggiuntivi vengono raggruppati nel pacchetto di archiviazione;
6. il PdA viene salvato e i suoi metadati vengono inseriti nel DB, rendendolo così consultabile e scaricabile. Per una descrizione dettagliata della struttura del PdA si veda il paragrafo 6.3.

(Torna al Sommario)

5.2.3 *Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta.*

Il sistema di conservazione consente ai soggetti autorizzati l'accesso diretto, anche da remoto, ai documenti informatici conservati.

Per esibizione si intende, dunque, l'operazione che consente a tali soggetti la visualizzazione di uno o più documenti conservati e la loro esportazione dal sistema di conservazione attraverso la produzione di un pacchetto di distribuzione selettiva.

Per una descrizione delle interfacce che permettono all'utente di effettuare l'esibizione si veda il manuale utente dell'applicativo.

(Torna al Sommario)

5.2.4 Scarto dei pacchetti di archiviazione

Superato il periodo di conservazione di un pacchetto di archiviazione (definito nella specifica classe documentale), RSC provvede a comunicare al cliente gli estremi del pacchetto pronto per essere scartato. Solo dopo approvazione formale da parte del cliente (salvo diversi accordi specifici sul servizio) procede alla eliminazione del pacchetto di archiviazione, dandone comunicazione al cliente stesso e riportando l'evento sul *Libro dei Verbali*.

(Torna al Sommario)

5.2.5 Chiusura del servizio di conservazione (al termine di un contratto)

Al termine del contratto RSC provvede alla consegna dell'insieme dei pacchetti di archiviazione con le modalità concordate per il servizio stesso che possono prevedere:

- invio immagine ISO dei pacchetti archivio;
- recupero via API/web service da parte del cliente attraverso le interfacce di interoperabilità messe a disposizione dalla piattaforma.
- altre modalità preventivamente concordate.

Solo dopo formale conferma da parte del cliente della corretta ricezione di tutti i pacchetti di archiviazione, RSC provvede alla eliminazione dell'intero archivio, aggiornando il *Libro dei Verbali* e la *Definizione delle Classi Documentali.*

Il documento DQ 8.3.6 07 Piano di Cessazione Servizi di Conservazione contiene i dettagli operativi per lo svolgimento di tale fase.

(Torna al Sommario)

5.3 Strutture organizzative: attività proprie di gestione dei sistemi informativi.

La gestione dei sistemi informativi avviene nel rispetto delle indicazioni del Sistema Qualità Aziendale certificato ISO 9001:2008 e del Sistema di Gestione della Sicurezza delle Informazioni certificato ISO 27001:2013 e costruito nel rispetto dei seguenti standard:

- ISO 27001:2013
- CoBit 5
- Itil v.3

In particolare, il processo *DSS01 - Gestione delle Operazioni* identifica l'organizzazione messa in atto per coordinare ed eseguire le attività e le procedure operative richieste per fornire i servizi IT con risorse interne ed esterne, ivi compresi l'esecuzione di procedure operative standard predefinite e le attività di monitoraggio richieste, al fine di:

- eseguire le procedure operative: manutenere ed eseguire procedure e task operativi in modo regolare ed affidabile;
- supervisionare le operazioni dei servizi IT affidati a fornitori esterni per garantire la protezione delle informazioni aziendali e l'affidabilità dei servizi erogati;
- monitorare l'infrastruttura IT ed i relativi eventi. Archiviare le informazioni necessarie per ricostruire la successione cronologica delle operazioni e delle altre attività svolte a supporto dell'operatività;
- manutenere le contromisure di protezione da eventi ambientali. Installare apparati specializzati per il controllo ed il monitoraggio dell'ambiente;
- gestire le facilities incluse energia e comunicazioni, in piena con leggi e regolamenti, requisiti tecnici e di business, specifiche del fornitore, linee guida di safety.

Nei successivi paragrafi si illustrano i processi specifici di tale gestione, nonché i ruoli e le responsabilità in gioco.

(Torna al Sommario)

5.3.1 Conduzione e manutenzione del sistema di conservazione

La conduzione e manutenzione del sistema di conservazione è in carico alla struttura di *Gestione dei Sistemi Informativi* indicata nello schema del par. 5.1.

Tale struttura provvede:

- al monitoraggio dello stato di salute di tutti i sistemi coinvolti (vedi successivo paragrafo);
- alla gestione degli incident, change e progetti evolutivi della piattaforma secondo le indicazioni dei processi del Sistema di Gestione della Sicurezza delle Informazioni:
    - *processo BAI01 – Gestione dei programmi e dei progetti* (vedi par. 5.3.3);
    - *processo BAI06 – Gestione dei change* (vedi par. 5.3.3);
    - *processo DSS02 – Gestione delle Richieste di Servizio e degli Incidenti*. Il processo prevede le seguenti attività:
        1. **definire gli schemi per la classificazione degli incidenti e delle richieste di servizio**: definire gli schemi ed i modelli per la classificazione degli incidenti e delle richieste di servizio.
        2. **Registrare, classificare e dare priorità ad incidenti e richieste di servizio**: identificare, registrare e classificare le richieste di servizio e gli incidenti, assegnando la priorità adeguata.
        3. **Verificare, approvare ed evadere le richieste di servizio**: selezionare le procedure di richiesta di servizio più appropriate ed accertare che la richiesta soddisfi i criteri definiti al punto 1. Ottenere approvazione, se richiesto, ed evadere la richiesta.

4. **Analizzare, diagnosticare e assegnare gli incidenti**: identificare e registrare le segnalazioni di incidenti valutando i sintomi descritti dall'utente, determinare le possibili cause, assegnare l'incidente per la risoluzione.
5. **Risolvere e recuperare dall'incidente**: documentare, applicare e testare le soluzioni temporanee (workaround) o definitive, ed eseguire le azioni di recupero per ripristinare il relativo servizio IT.
6. **Chiudere gli incidenti e le richieste di servizio**: verificare che le soluzioni adottate per evadere le richieste di servizio e per risolvere gli incidenti siano soddisfacenti, e chiudere il ticket.
7. **Tracciare lo stato di avanzamento e produrre la reportistica**: tracciare, analizzare e riportare regolarmente sulle attività di gestione degli incidenti e delle richieste di servizio, al fine di assicurare la presenza delle informazioni necessarie per l'analisi anche in vista di miglioramenti futuri.

(Torna al Sommario)

5.3.2 *Monitoraggio del sistema di conservazione*

Il monitoraggio del sistema di conservazione è svolto, per la parte funzionale, da RSC che provvede con cadenza annuale a controllare:

- la consistenza e l'integrità dei PdA e dell'IPdA
- l'effettiva leggibilità dei documenti inseriti all'interno dei pacchetti di archiviazione

attraverso l'esecuzione di una procedura di controllo che interesserà un adeguato campione dei pacchetti di archiviazione sottoposti a *conservazione e* la verifica che, per i formati dei file utilizzati per la conservazione dei documenti, sia disponibile sul mercato un visualizzatore aggiornato e conforme alle specifiche del singolo formato di file.

Tutte le procedure di verifica, gli eventuali interventi sul software applicativo, le modifiche delle configurazioni, l'assegnazione delle deleghe a svolgere opportune operazioni, nonché tutti gli avvenimenti importanti o ritenuti tali da RSC ai fini del corretto svolgimento del processo di conservazione saranno opportunamente tracciati sull'apposito *Libro dei Verbali*.

Il monitoraggio dello stato di salute dell'infrastruttura è gestito dallo stesso gruppo di *Gestione dei Sistemi Informativi*, attraverso il sistema di monitoraggio predisposto e presidiato h24 per 365 gg/anno (vedi par. 0 e relativi sottoparagrafi), provvedendo ad intercettare eventuali problematiche e ad avviare la relativa risoluzione secondo quanto indicato al paragrafo precedente.

Lo stesso Gruppo provvede al controllo della corretta esecuzione del backup (anche sul sito di Disaster Recovery) almeno su base giornaliera.

La pianificazione ed esecuzione degli audit interni è stata implementata con il SGSI, attraverso documenti di processi e linee guida apposite secondo le indicazioni delle ISO/IEC

27007 e TR 101 533-02. Il dettaglio del processo di audit è riportato nella procedura *MEA03-Monitoraggio Analisi e Valutazione della conformità a Requisiti Esterni.*

Tutti gli audit svolti prevedono uno stretto controllo della indipendenza degli esaminatori come da documento *Segregation-Of-Duties v.1.0* redatto nel rispetto delle indicazioni contenute nel *CISA Review Manual 2008, chapter 2, page 112.*

Il par. 4.8 del Piano di Sicurezza contiene prescrizioni di dettaglio sul Piano degli Audit Interni di Sistema.

(Torna al Sommario)

5.3.3 Change management;

Eventuali richieste di variazione della infrastruttura sistemistica o applicativa sono gestite nel rispetto del processo *BAI06 – Gestione dei change* che prevede le seguenti attività:

1. **Valutare, dare priorità ed autorizzare le richieste di cambiamento (RFC)**: valutare tutte le richieste di cambiamento per determinare l'impatto sui processi di business e sui servizi IT e per stabilire se il cambiamento possa influenzare negativamente l'ambiente operativo. Assicurare che i cambiamenti siano identificati, ordinati per priorità, suddivisi per categorie, valutati, autorizzati pianificati e messi a calendario.
2. **Gestire i cambiamenti in emergenza**: gestire con attenzione i cambiamenti effettuati in emergenza per assicurarsi che il cambiamento sia sotto controllo e che avvenga in sicurezza. Verificare che il cambiamento sia stimato in modo appropriato ed autorizzato dopo l'avvenuto cambiamento.
3. **Tenere traccia e fare report sullo stato dei cambiamenti**: definire e mantenere aggiornato un sistema per tracciare e fare report per documentare i cambiamenti rigettati, per comunicare lo stato dei cambiamenti approvati ed in corso di approvazione e di quelli completati. Assicurarsi che i cambiamenti approvati siano implementati come pianificato.
4. **Chiudere e documentare i cambiamenti**: ogni volta che un cambiamento viene implementato, deve essere aggiornata la documentazione relativa alla soluzione adottata e il manuale utente. Devono essere altresì eventualmente aggiornate le note operative che richiedano modifiche legate al cambiamento effettuato.

Le richieste evolutive più complesse, sono gestite con il processo *BAI01 – Gestione dei programmi e dei progetti* che prevede le seguenti attività:

1. **Mantenere un approccio standardizzato per la gestione dei progetti**: mantenere un approccio standard per la gestione di programmi e progetti che consenta la governance, la gestione delle review, il processo di escalation, le attività di gestione della delivery, focalizzate sul valore e il raggiungimento degli obiettivi di business (requisiti, costi, pianificazione).
2. **Avviare e lanciare i progetti**: definire e documentare la natura e l'ambito del progetto in modo da sviluppare e confermare tra le parti interessate una

comprensione comune dell'ambito del progetto e come questo è collegato agli altri progetti dentro il programma generale d'investimento dell'IT. La definizione deve essere formalmente approvata dagli sponsor di programma e di progetto.

3. **Pianificare un progetto**: costruire e mantenere un piano di progetto formale ed approvato che faccia da guida all'esecuzione ed al controllo durante l'intera vita del progetto. Gli obiettivi del progetto devono essere definiti con chiarezza e legati alla creazione e/o al miglioramento delle capacità di business.
4. **Gestire la qualità del progetto**: gestire la qualità del programma e del progetto in modo allineato con il Sistema di Gestione della Qualità in essere.
5. **Gestire il rischio del progetto**: eliminare o mitigare i rischi associati ai progetti attraverso un sistematico processo di analisi e valutazione. I rischi affrontati dalla gestione di progetti sono consolidati e registrati centralmente.
6. **Monitorare e tenere sotto controllo i progetti**: misurare le prestazioni di progetto secondo le metriche chiave come la schedulazione, la qualità, l'assorbimento delle risorse ed i costi. Identificare qualsiasi deviazione rispetto al risultato atteso. Valutare l'effetto delle deviazioni sul progetto e sul programma generale. Riportare i risultati alle parti interessate.
7. **Gestire le risorse di progetto e i work package**: gestire i work package di progetto specificando requisiti formali di autorizzazione e accettazione, assegnando e coordinando le appropriate risorse di business e dell'IT.
8. **Chiudere un progetto o una fase**: alla fine di ogni progetto o rilascio, richiedere alle parti interessate di accertare se il progetto o rilascio ha prodotto i risultati ed il valore atteso. Identificare e comunicare qualsiasi attività straordinarie richieste per raggiungere i risultati attesi del progetto e i benefici del programma, ed identificare e documentare quanto appreso per usi futuri su progetti, rilasci, e programmi.

I *change* sono presi in carico dal gruppo di *Gestione dei Sistemi Informativi* avvalendosi del supporto di:

- *Gruppo Sviluppo Applicativo*: per la manutenzione evolutiva dei sistemi di estrazione e preparazione dei dati del cliente;
- il fornitore *Andxor Soluzioni Informatiche Srl* per gli interventi evolutivi della piattaforma di conservazione.

(Torna al Sommario)

5.3.4 Verifica periodica di conformità a normativa e standard di riferimento.

La verifica periodica di conformità a normativa e standard di riferimento è eseguita da RSC in modo continuativo attraverso formazione continua, la registrazione a specifici servizi newsletter del settore e a gruppi di approfondimento.

(Torna al Sommario)

6 OGGETTI SOTTOPOSTI A CONSERVAZIONE

6.1 Oggetti conservati

Il servizio permette il trattamento e la conservazione di qualunque tipologia di documento. Il cliente che intende usufruirne, deciderà per quali tipologie documentali attivare il servizio di conservazione e, collaborerà con Mediatica nelle operazioni di definizione del relativo trattamento.

Nell'allegato *Definizione delle classi documentali* sono elencate e descritte le tipologie di documenti sottoposti a conservazione e le relative politiche di conservazione. Per ciascuna tipologia sono elencati e descritti i relativi metadati e i formati (comprensivi della relativa versione) dei file utilizzati. Quest'ultima informazione è necessaria in quanto devono essere conservati tutti i visualizzatori relativi ai formati gestiti o le modalità con cui il sistema di conservazione ne garantisce la leggibilità nel tempo. A tale proposito nello stesso documento è predisposta la tabella sotto riportata o, in alternativa, le modalità adottate per garantire la leggibilità dei formati gestiti.

Nome classe		**Descrizione**				
***		***				
Area e ufficio	*Proprietario documento*	*Periodo conservazione*	*Documenti previsti nell'anno*	*Dimension e media documenti*	*Periodicità invio conservazione*	*Periodicità chiusura PdA*
***	***	***	***	***	***	***
Elenco medatati per tipologia (stringa, data, ecc.): *** Tipo documento - esempio pdf/a: *** Periodo di transizione (se previsto): *** Dati personali critici o sensibili: No						

Tabella 3 - tabella definizione classe documentale

Anche per i fascicoli devono essere elencate e descritte le diverse tipologie e le relative politiche di conservazione. Per ciascuna tipologia devono essere elencati e descritti i relativi metadati e le strutture.

Vengono di seguito elencati i principali formati digitali supportati per la Conservazione dei documenti digitali, con riferimento ai formati scelti per la conservazione, in linea con quanto indicato nell'allegato n°2 del D.P.C.M. 3 dicembre 2013 - Regole tecniche in materia di Sistema di Conservazione:

Estensione	**Produttore**	**MIME type**	**Formato**	**Ultima Versione**	**Standard**
.pdf	Adobe	application/pdf	PDF – PDF/A	1.7	ISO 32000-1 (PDF) ISO 19005-1:2005 (vers. PDF 1.4) ISO 19005-2:2011 (vers. PDF 1.7)
.tif	Aldus Corporation in seguito acquistata da Adobe	image/tiff	TIFF	TIFF 6.0 del 1992 TIFF Supplement 2 del 2002	N.A.

Estensione	Produttore	MIME type	Formato	Ultima Versione	Standard
.jpg	Joint Photographic Experts Group	image/jpeg	JPG	2009	ISO/IEC 10918:1
.docx, .xlsx, .pptx	Microsoft	= =	Office Open XML	1.1	ISO/IEC DIS 29500:2008
.ods, .odp, .odg, .odb	OASIS	application/vnd.oasis.opendocument.text	Open Document Format	1.0	ISO/IEC 26300:2006 UNI CEI ISO/IEC 26300
.xml	W3C	application/xml text/xml	XML	= =	Specifiche pubblicate da W3C http://www.w3.org/XML/
.txt	= =	= =	TXT	= =	= =
.eml	= =	= =	Formati Messaggi di posta elettronica	= =	RFC 2822/MIME

Tabella 4 – tabella formati documentali

La piattaforma verifica in fase di versamento che la tipologia di documento ricevuta coincida con quella prevista per la classe documentale (esempio: xml, jpg, pdf). In caso contrario, provvede a scartare il documento segnalandolo all'utente.

(Torna al Sommario)

6.2 Pacchetto di versamento

Il Pacchetti di Versamento è costruito dal Produttore (opzionalmente sottoscritto con firma digitale) che provvede a trasmetterlo al sistema di conservazione con le modalità descritte nel contratto.

Il versamento può essere acquisito:

- in modalità interattiva sfruttando l'interfaccia dell'applicazione stessa (vedi par. 6.2.1);
- attraverso un layer applicativo di comunicazione predisposto ad hoc per la specifica classe documentale (vedi par. 6.2.2) che provvede ad estrarre i documenti e i metadata e a trasmetterli al sistema di gestione documentale con le opportune modalità (API).

Indipendentemente dalla modalità scelta, i metadati specifici di ciascun versamento sono memorizzati nel file di log *RdV* comprensivi del riferimento temporale specificato con riferimento al Tempo universale coordinato (UTC).

(Torna al Sommario)

6.2.1 Modo interattivo

In questo caso il versamento di un documento avviene attraverso l'interfaccia dell'applicativo che consente di selezionare il documento da versare e di specificare tutti i metadati ad esso associati per la specifica classe documentale.

La pressione del bottone `Archivia` invia all'applicativo il pacchetto di versamento, che di fatto consiste nella POST HTTP contenente il documento e tutti i suoi metadati.

In tal caso il rapporto di versamento viene salvato nella classe documentale predefinita e una parte di esso viene visualizzata in interfaccia (Figura 2).

Figura 2: Rapporto di versamento visualizzato in interfaccia

Usando la modalità interattiva viene creato un PdV e un RdV per ogni documento caricato.

(Torna al Sommario)

6.2.2 Layer applicativo

Tale versamento utilizza le API dell'applicativo che prevedono autenticazione HTTP Auth Simple (su https). Le utenze che si possono usare sono tutte quelle censite all'interno di della piattaforma stessa.

Le API da usare per il versamento sono quattro, una delle quali va usata solo in caso di errore.

1. `parcel create`: permette di aprire una sessione di versamento dando così inizio al pacchetto di versamento. L'API restituisce un identificativo del pacchetto di versamento che deve essere utilizzato nelle chiamate successive.
2. `upload document`: permette di versare un documento facente parte del pacchetto di versamento creato con la parcel create.
3. `parcel close`: chiude il pacchetto di versamento e genera il rapporto di versamento.
4. `Parcel delete`: da usare in caso di errore. Chiude il pacchetto di versamento e genera la ricevuta di versamento contenente indicazioni riguardo l'errore verificatosi. Elimina inoltre tutti i documenti facenti parte dello stesso pacchetto di versamento, rendendo così il pacchetto di versamento atomico.

Per quanto detto, l'inizio di un nuovo PdV è dichiarato dalla chiamata `parcel create` che provvede a restituire un identificativo univo del pacchetto stesso.

La successiva chiamata `upload document` provvede al caricamento di un documento nel PdV. Usata iterativamente consente il caricamento di n documenti nel PdV stesso.

La chiamata `parcel close` provvede a dichiarare la chiusura del pacchetto nel caso il caricamento non abbia evidenziato errori.

Non ci sono limiti al numero di documenti che possono comporre il PdV.

La presenza del layer applicativo descritto consente di gestire PdV fortemente customizzati attraverso la realizzazione di semplici parser a monte che trasformino il PdV ricevuto nelle tre chiamate fondamentali descritte. A titolo di esempio si possono supportare i seguenti PdV:

- file di tipo .zip con n documenti più un file di indice in formato xml a norma UNI 11386 - SInCRO;
- spool di stampa;
- ecc. ecc.

Il dettaglio della struttura del PdV è riportato negli accordi contrattuali dello specifico servizio e nel documento *Definizione delle classi documentali*.

(Torna al Sommario)

6.2.3 Struttura del Rapporto di Versamento - RdV

Il rapporto di versamento è un file XML firmato secondo lo standard XAdES da RSC o da un suo delegato.

Il suo contenuto è definito dal seguente schema XSD:

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns="http://andxor.it/tDoc/report.xsd"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    targetNamespace="http://andxor.it/tDoc/report.xsd"
    elementFormDefault="qualified">
  <xs:import namespace="http://www.w3.org/2000/09/xmldsig#"
schemaLocation="http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/xmldsig-core-
schema.xsd"/>
  <xs:attribute name="function" type="xs:NMTOKEN" default="SHA-256" />
  <xs:simpleType name="TimeInfo">
    <xs:restriction base="xs:dateTime" />
  </xs:simpleType>
  <xs:complexType name="TimeReference">
    <xs:sequence>
      <xs:element name="TimeInfo" type="TimeInfo" />
    </xs:sequence>
```

```
</xs:complexType>
<xs:complexType name="Identifier">
  <xs:simpleContent>
    <xs:extension base="xs:NMTOKEN">
      <xs:attribute name="scheme" type="xs:string" default="local" />
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
<xs:complexType name="CreatingApplication">
  <xs:sequence>
    <xs:element name="Name" type="xs:string" />
    <xs:element name="Version" type="xs:string" />
    <xs:element name="Producer" type="xs:string" />
  </xs:sequence>
</xs:complexType>
<xs:complexType name="File">
  <xs:sequence>
    <xs:element name="ID" type="xs:string" />
    <xs:element name="Path" type="xs:string" minOccurs="0" />
    <xs:element name="Hash" type="Hash" />
    <xs:element name="metadata" type="metadata" />
  </xs:sequence>
  <xs:attribute name="format" type="xs:string" use="required"/>
</xs:complexType>
<xs:complexType name="Hash">
  <xs:simpleContent>
    <xs:extension base="xs:string">
      <xs:attribute name="function" type="xs:NMTOKEN" default="SHA-1" />
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
<xs:complexType name="metadata">
  <xs:sequence>
    <xs:element name="meta" maxOccurs="unbounded">
      <xs:complexType>
        <xs:attribute name="class" type="xs:string" use="optional" />
        <xs:attribute name="name"  type="xs:string" use="required" />
        <xs:attribute name="value" type="xs:string" use="required" />
      </xs:complexType>
    </xs:element>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="SelfDescription">
  <xs:sequence>
    <xs:element name="CreatingApplication" type="CreatingApplication" />
```

```
      <xs:element name="ID" type="Identifier" />
      <xs:element name="IPdV" type="xs:string" />
      <xs:element name="company" type="xs:string" />
      <xs:element name="doctype" type="xs:string" />
      <xs:element name="TimeReference" type="TimeReference" />
      <xs:element name="Result" type="xs:string" />
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="FileGroup">
    <xs:sequence>
      <xs:element name="File" type="File" maxOccurs="unbounded" />
      <xs:element name="Extra" type="xs:string" minOccurs="0" />
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="RdV">
    <xs:sequence>
      <xs:element name="SelfDescription" type="SelfDescription" />
      <xs:element name="FileGroup" type="FileGroup" maxOccurs="unbounded" />
      <xs:element ref="ds:Signature"/>
    </xs:sequence>
  </xs:complexType>
  <xs:element name="RdV" type="RdV" />
</xs:schema>
```

Le eventuali personalizzazioni di tali pacchetti, specifiche di ogni contratto, sono descritte nell'allegato *Definizione delle classi documentali*.

(Torna al Sommario)

6.3 Pacchetto di archiviazione

6.3.1 Struttura del Pacchetto di Archiviazione - PDA

Il pacchetto di archiviazione contiene i file contenuti in uno o più pacchetti di versamento al termine del processo di conservazione.

Le tempistiche con cui sono generati i PdA sono definite nel Contratto. La generazione del PdA avviene automaticamente secondo uno scadenziario configurato attraverso l'applicazione. In alternativa può essere forzata una esecuzione manuale ove necessario.

Per motivi di comodità di gestione, in genere, il PdA contiene documenti di un solo cliente e di una sola classe documentale.

Il PdA complessivamente contiene i seguenti file:

- i documenti che devono essere conservati;

- un file XML come da Norma UNI 11386 (SInCRO) contenente l'indice dei documenti informatici da conservare (IPdA) firmato digitalmente dal Responsabile del Servizio di Conservazione e marcato temporalmente. Per i dettagli della struttura dell'IPdA si rimanda al successivo paragrafo 6.3.2

La struttura descritta fa riferimento allo standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010), che è lo standard nazionale riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione.

A titolo di esempio, un PdA conservato risulta un file 150F2667829.xml.p7m in cui il filename riporta in esadecimale l'identificativo univoco (in questo caso 1447175813161) del PdA contenuto anche al suo interno. L'univoco di per sé indica lo UNIX millitime di creazione, rappresentato anche in formato leggibile all'interno dell'XML nel nodo IdC→Process→TimeRefrence→TimeInfo (con minore precisione perché non mostra i millisecondi).

Attraverso l'applicazione, (vedi Figura 3) è possibile ricercare e visualizzare i documenti contenuti nel PdA con i relativi metadati e fare ricerche interne al PdA stesso.

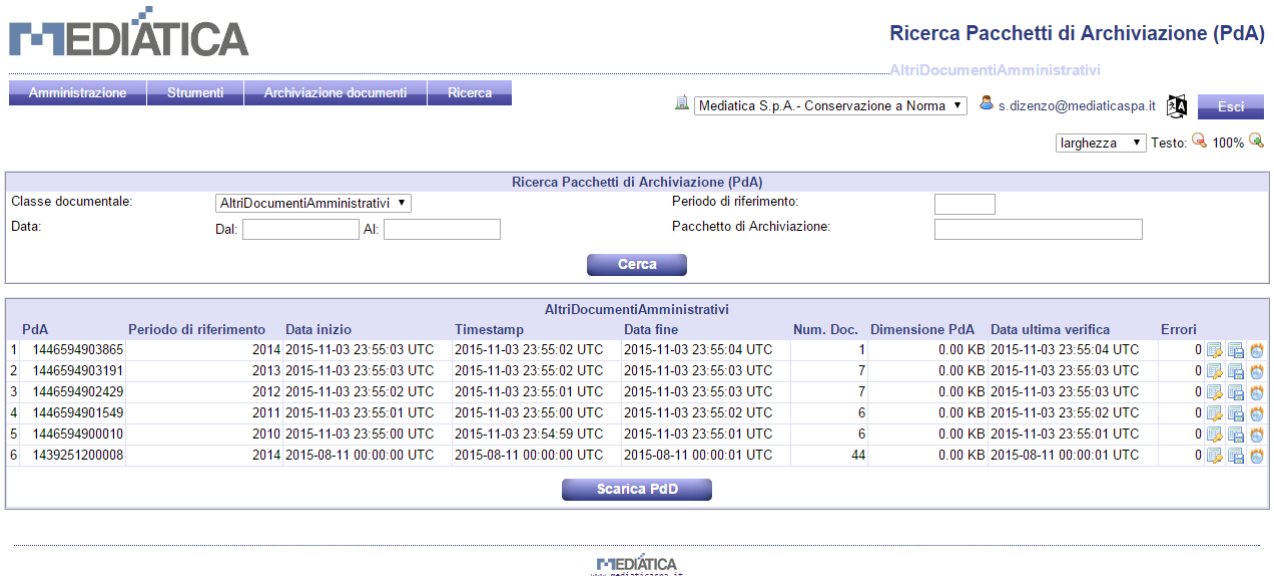

Figura 3 - Interfaccia di ricerca e visualizzazione dei PdA

Tutti gli elementi appena descritti possono, opzionalmente, essere inseriti in un unico file ISO che costituisce il pacchetto di archiviazione esportabile su qualunque supporto (ad esempio DVD).

I metadati specifici del PdA, le regole di validazione ed eventuali ulteriori personalizzazioni, specifiche di un contratto, sono riportate nell'allegato *Definizione delle classi documentali*.

(Torna al Sommario)

6.3.2 Indice del pacchetto di archiviazione - IPdA

Il file indice del PdA è un file XML creato dall'applicativo a chiusura del processo di conservazione nel rispetto dello standard SInCRO (Supporto all'Interoperabilità) nella Conservazione e nel Recupero degli Oggetti digitali - UNI 11386:2010.

Al suo interno si trovano:

- informazioni riguardanti l'azienda e il prodotto che generano l'indice;
- informazioni riguardanti l'azienda proprietaria dei documenti, per la quale viene prodotto l'indice;
- informazioni riguardanti la classe documentale e il periodo di riferimento dei documenti conservati;
- informazioni specifiche di ogni documento. In questa sezione trovano posto l'ID univoco del documento, il nome del file, la sua impronta e tutti i metadati ad esso correlati;
- informazioni riguardanti tutti i soggetti (fisici e giuridici) interessati dal processo di conservazione. In tale sezione trovano posto almeno il soggetto che appone la firma all'IPdA e l'azienda che offre il servizio di conservazione.

La struttura dell'IPdA completa delle ulteriori strutture collegate ai diversi elementi "MoreInfo" previsti dallo standard SInCRO, è di seguito illustrata (IdC coincide con IPdA e VdC coincide con PdA):

- **IdC**
  - **SelfDescription:** descrizione generale del pacchetto
    - **ID:** identificativo univoco del PdA, rappresenta lo Unix millitime dell'inizio della creazione
    - **CreatingApplication:** la descrizione del sistema che ha creato il PdA
      - **Name:** "tDoc"
      - **Version:** la release di tDoc che ha generato questo PdA
      - **Producer:** "Andxor Soluzioni Informatiche srl"
    - **MoreInfo**
      - **EmbeddedMetadata**
        - **Iotto:** riferimenti alla classe documentale a cui si riferisce questo PdA
          - **company:** nome azienda – *Mediatica S.p.A.*
          - **doctype:** nome classe documentale
          - **period:** periodo fiscale
          - **previous:** identificativo e hash SHA-256 del PdA precedente (della stessa classe documentale)
  - **VdC**
    - **ID:** lo stesso identificativo di SelfDescription→ID
  - **FileGroup:** contenitore per l'elenco di file
    - **File (uno o più):** elemento presente per ogni singolo file elencato (e suo media-type, generalmente "application/pdf")
      - **ID:** identificativo univoco del documento (sequenziale all'interno del database di tDoc)
      - **Path:** path del file all'interno del PdA (relativo alla posizione del file XML stesso)

- **Hash:** SHA-256 del file
- **MoreInfo**
  - **EmbeddedMetadata**
    - **metadata:** metadati del singolo documento
      - **meta (uno o più):** elemento nome/valore presente per ogni singolo metadato del documento

- **Process:** dati relativo al processo di creazione del PdA
  - **Agent (uno o più):** tutte le persone fisiche e giuridiche interessate nella creazione di questo PdA
    - **AgentName:** nome della persona
      - **FormalName:** nome della persona giuridica
      - **NameAndSurname:** nome della persona fisica
        - **FirstName:** nome
        - **LastName:** cognome
    - **AgentID:** partita IVA della persona giuridica o codice fiscale della persona fisica
  - **TimeReference:** riferimento temporale della creazione del PdA
    - **TimeInfo:** lo stesso istante codificato in SelfDescription→ID, ma in formato leggibile
  - **LawAndRegulations:** riferimento alla legge in corso alla creazione di questo PdA

L'indice del pacchetto di archiviazione viene firmato in modalità CAdES e marcato, pertanto all'interno del pacchetto di archiviazione sarà un file con estensione.p7m.

(Torna al Sommario)

6.4 Pacchetto di distribuzione

Il pacchetto di distribuzione (PdD), prodotto al termine del processo di esibizione, è un file in formato ZIP che comprende i seguenti elementi:

- l'insieme dei documenti ricercati attraverso l'interfaccia di esibizione suddivisi per Azienda, classe documentale e per PdA di appartenenza;
- l'insieme degli IPdA di appartenenza dei documenti ricercati
- `viewer.jar`: applicazione java che consente la visualizzazione di tutti i documenti contenuti nel pacchetto di distribuzione e dei relativi metadati.

L'applicazione consente anche di verificare le firme apposte sugli IPdA contenuti nel pacchetto e di fare ricerche interne al PdD;

- `certs`: directory contenente i certificati necessari per la verifica delle firme apposte sugli indici del pacchetto di archiviazione;
- `schemas`: directory contenente gli schemi XSD che descrivono la struttura degli indici dei pacchetti di archiviazione.
- `autorun.inf`: file contenente le istruzioni per avviare automaticamente l'applicazione viewer.jar.

- `index.txt.p7m`: file indice del PdD firmato dal Responsabile del Servizio di Conservazione o da un suo delegato secondo il formato CAdES.

Il file contiene l'elenco degli IPdA contenuti nel PdD e dei relativi hash.

Questo fa sì che il file indice fornisca garanzie di autenticità e di integrità circa gli IPdA contenuti nel pacchetto. A loro volta gli IPdA contengono l'elenco dei documenti e dei relativi hash e, essendo firmati, garantiscono l'autenticità e l'integrità di tutti i documenti contenuti nel PdD.

La presenza di un file così strutturato all'interno del PdD fornisce le stesse garanzie che fornirebbe una firma CAdES esterna al pacchetto, con il vantaggio di evitare proprio la firma esterna al PdD, che potrebbe essere tecnicamente improponibile vista la potenziale dimensione di un PdD, che potrebbe raggiungere decine o centinaia di GB.

Le eventuali personalizzazioni di tali pacchetti, specifiche di un contratto, sono descritte nell'allegato *Definizione delle classi documentali*.

(Torna al Sommario)

7 IL PROCESSO DI CONSERVAZIONE

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

Le diverse tipologie di documenti sono prodotte, formate ed emesse a cura e sotto l'esclusiva responsabilità del Produttore.

L'accesso alla piattaforma è garantito da un sistema di autenticazione nominativo.

Per garantire l'identificazione certa del soggetto che ha formato il documento, i documenti informatici posti in conservazione sono, in genere, sottoscritti con firma digitale e identificati in modo univoco e persistente. Tuttavia il Produttore ha facoltà di depositare in conservazione anche documenti informatici non sottoscritti con firma digitale purché previsto per la specifica classe documentale e nel contratto di servizio.

Sono conservati solo i formati idonei ad essere conservati a lungo termine, ai sensi della normativa vigente, rispettando i requisiti previsti di "standard aperti". La struttura dei dati per la memorizzazione nel sistema di conservazione è in grado di assicurare l'interoperabilità tra sistemi.

Tutti i documenti versati nel sistema di conservazione sono contraddistinti da un set di metadati obbligatori per il sistema definiti in fase di creazione della specifica classe documentale.

L'attività di versamento è costituita dalle seguenti operazioni:

- produzione da parte dell'Ente dei documenti nei tempi previsti dalla legge;
- eventuale predisposizione dei gruppi di caricamento composti da file contenenti tutti i documenti da conservare, avente nome file univoco e i metadati caratteristici di ciascun documento;
- caricamento singolo o massivo dei documenti attraverso le modalità indicate al par. 6.2 e relativi sottoparagrafi ad opera degli Operatori del Produttore aventi le autorizzazioni per l'accesso e caricamento dei documenti;

Altre modalità di ricezione dei pacchetti di versamento potranno essere previste e saranno regolamentate nel documento *Definizione delle classi documentali*.

La trasmissione avviene nel rispetto della riservatezza delle informazioni, normalmente attraverso una Virtual Private Network (VPN) dedicata a ciascun cliente che garantisce la crittografia dei contenuti secondo i seguenti protocolli:

- IKE: Enc 3DES, AES 256 bit; Auth MD5 , SHA1
- IPSEC: Enc 3DES, AES 128 bit, AES 256 bit; Auth MD5 , SHA1.

Eventuali variazioni o informazioni specifiche nella trasmissione sono riportate nel Contratto o nel documento *Definizione delle classi documentali*.

Il sistema di conservazione prende in carico un PdV solo dopo che tutte le sue parti sono state correttamente ricevute e dopo che si sono superati con esito positivo i relativi controlli (vedi successivo paragrafo).

La correttezza e completezza dei controlli viene ufficialmente dichiarata nella produzione del Rapporto di Versamento (RdV) che viene inviato o reso disponibile al cliente secondo le modalità previste dall'accordo contrattuale e indicate nel par. 6.2.

I log emessi (anche a seguito di verifiche periodiche) sono conservati sulla stessa piattaforma di conservazione con le modalità indicate nel presente documento.

In caso di corruzione o perdita dei dati, il ripristino del servizio e dei dati è garantito dalla specifica procedura operativa *Backup & Disaster Recovery Plan*.

(Torna al Sommario)

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

Ogni versamento da parte del Produttore deve contenere pacchetti omogenei per tipologia documentale ed Ente Produttore. La verifica relativa all'identificazione dell'Ente Produttore è eseguita mediante il controllo sulle informazioni relative alla tipologia documentale e ai dati del Soggetto Produttore. Se tali verifiche portassero a una incongruenza tra questi elementi, allora il pacchetto di versamento verrebbe rifiutato. In tal modo ci si cautela rispetto a eventuali errori di provenienza dei documenti.

Inoltre, all'atto del caricamento di un pacchetto di versamento, viene controllato il formato di ciascun file versato. Tale controllo viene svolto in automatico dal sistema che scarta documenti con formati non previsti.

Se il formato del file non dovesse essere contemplato tra quelli previsti dalla normativa vigente, (attualmente dall'allegato 2 del DPCM 3 dicembre 2013), il pacchetto di versamento viene rifiutato, salvo indicazioni esplicite contenute nel Contratto.

Il sistema prevede che in fase di acquisizione del pacchetto di versamento venga verificata la presenza dei metadati obbligatori specifici per la classe documentale ed, eventualmente, il rispetto di regole specifiche sulle proprietà dei metadati stessi (formato, sequenzialità, ecc.). Tali regole possono essere fortemente personalizzate attraverso la definizione di specifiche *espressioni regolari*.

I controlli complessivamente eseguiti su un PdV risultano:

- identificazione certa del soggetto che ha formato il documento e del relativo ente produttore attraverso la verifica delle autorizzazioni/credenziali dell'utente versante e dei suoi eventuali incaricati/delegati ad effettuare il versamento. In caso di esito negativo il sistema rifiuta il versamento. L'accesso alla piattaforma, inoltre, è a monte filtrato da una Virtual Private Network dedicata fra il produttore e Mediatica S.p.A.
- controllo formale dei documenti. In particolare viene verificato che siano tutti di formato omogeneo e valido per una delle Classi Documentali registrate a sistema. In caso di esito negativo il sistema rifiuta il versamento;
- controllo sul MIME Type. Il sistema verifica che il MIME type dichiarato per la classe documentale coincida con il MIME type effettivo del documento caricato. In caso di esito negativo il sistema rifiuta il versamento;

- controllo sulla consistenza dei metadati presenti in base alle regole impostate per la specifica classe documentale. In caso di esito negativo il sistema rifiuta il tentativo versamento;
- eventuali controlli supplementari definiti nel Contratto.

Eventuali problemi che pregiudichino l'emissione del RdV sono segnalati nel file di log che fa parte di una specifica classe documentale (Log) appartenente all'Azienda root e sottoposti a conservazione automatica.

Tutti i RdV emessi fanno parte di una specifica classe documentale (RdV) appartenente all'azienda root e sottoposti a conservazione automatica. Esso è sempre consultabile dal Produttore o trasmesso su richiesta di quest'ultimo.

La gestione degli esiti negativi è formalizzata nel Contratto.

(Torna al Sommario)

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

Nel caso in cui tutte le verifiche in fase di versamento siano andate a buon fine, il sistema provvede a memorizzare ed indicizzare i documenti e a produrre un *Rapporto di Versamento*. La struttura del *Rapporto di Versamento* è indicata al par. 6.2.3.

Il rapporto di versamento contiene il riferimento temporale, specificato con riferimento al Tempo universale coordinato (UTC).

Nel caso di versamento interattivo (vedi par. 6.2.1) i dati del pacchetto di versamento sono confermati attraverso una specifica schermata (vedi Figura 2) e, opzionalmente, trasmessi per email.

La restituzione della *hash* permette la verifica da parte del Produttore della corrispondenza del documento preso in carico con quello inviato. Il *Rapporto di Versamento* costituisce il documento di controllo e di presa di responsabilità del Responsabile del Servizio di Conservazione verso il Produttore, in quanto viene garantita la conservazione di tutti e soli i documenti per i quali viene emesso il *Rapporto di Versamento*.

Il Rapporto di Versamento viene salvato in una classe documentale predefinita appartenente alla società `root`: la classe RdV. Tale classe è sottoposta al processo di conservazione e presenta i seguenti metadati:

1. N. documenti: numero di documenti presenti nel pacchetto di versamento;
2. Data creazione: data di creazione del rapporto di versamento;
3. ID: identificativo univoco del pacchetto di versamento;
4. Nome file: nome del file XML rappresentante il pacchetto di versamento;
5. Azienda: azienda proprietaria del PDA;
6. Classe documentale: classe documentale dei documenti contenuti nel PDA;
7. Utente: utente che ha effettuato il versamento;
8. Esito versamento: esito del versamento;

9. Note: il metadato è opzionale e contiene eventuali note relative al processo di versamento.

(Torna al Sommario)

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

Il rifiuto del pacchetto di versamento avviene quando il pacchetto risulta non conforme alle specifiche previste per la classe documentale di appartenenza, ad esempio:

- metadati non completi;
- quando un documento contenuto nel pacchetto non supera una delle verifiche descritte nel paragrafo precedente.

In caso di rifiuto, il Sistema restituisce al Produttore l'elenco degli errori riscontrati e le relative causali. La modalità con cui si restituisce al Produttore il messaggio di rifiuto del pacchetto di versamento, dipende dalla modalità di caricamento dello stesso:

- in caso di caricamento del pacchetto di versamento in modo interattivo (vedi par. 6.2.1) mediante interfaccia utente via browser, il messaggio di rifiuto appare a video contendo tutte le informazioni di cui sopra;
- in caso di caricamento massivo da layer applicativo (vedi par. 6.2.2), il messaggio di rifiuto viene trasmesso in risposta alla chiamata di tipo web service di caricamento del documento.
- Il messaggio di rifiuto non viene sottoposto a conservazione digitale, ma tutte le informazioni di tracciatura dell'operazione sono registrate nei log di sistema, corredati dal riferimento temporale specificato con riferimento al Tempo universale coordinato (UTC) per ciascuna di esse. Il log di sistema viene conservato.

(Torna al Sommario)

7.1.4 Preparazione e gestione del pacchetto di archiviazione

Completata la presa in carico del Pacchetto di Versamento, viene generato il Pacchetto di Archiviazione, come descritto al par. 6.3 e relativi sottoparagrafi. La frequenza con cui vengono creati i pacchetti di archiviazione è stabilita in sede contrattuale con il produttore dei documenti e riportata nel documento *Definizione delle classi documentali*.

L'insieme dei documenti appartenenti ad un pacchetto di archiviazione è sempre omogeneo per tipologia di documenti contenuti al suo interno.

Il PdA è firmato digitalmente dal Responsabile del Servizio di Conservazione e marcato temporalmente. Ogni indice è univocamente identificato all'interno del sistema.

Per quanto riguarda la descrizione delle procedure di ripristino in caso di corruzione o perdita dei dati si rimanda al paragrafo 9.2.

In generale il processo di conservazione non prevede l'utilizzo della crittografia degli oggetti conservati al fine di non alterare in alcun modo il documento inviato in conservazione.

Nessuna operazione di modifica è consentita a livello applicativo sul pacchetto di archiviazione posto in conservazione. Anche le credenziali amministrative non consentono tale operazione.

E' possibile esclusivamente procedere ad uno scarto con le modalità indicate al par.7.1.7. Le operazioni di scarto sono registrate nel Libro dei Verbali a cura di RSC e nei file di log (posti anch'essi in conservazione) in modo automatico dal sistema.

(Torna al Sommario)

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

La struttura del Pacchetto di Distribuzione è riportata al par. 6.4.

I documenti sono ricercabili tramite opportune funzioni di ricerca messe a disposizione dall'applicazione di conservazione che permettono applicare filtri su tutti i metadati presenti nonché sulla data di caricamento.

L'accesso al sistema in modalità di consultazione è garantito agli Utenti opportunamente autorizzati, limitatamente agli archivi del Produttore di appartenenza e in base agli accordi contrattuali con esso intercorsi. È quindi disponibile al conservatore e all'utente la funzionalità di esportazione di pacchetti e relativi indici, attraverso la quale è possibile scaricare un file .iso contenente il file indice dei pacchetti, i documenti conservati e le evidenze della conservazione (firme e marche temporali), nonché un visualizzatore.

Per garantire la fruibilità nel tempo dei documenti conservati, il sistema di conservazione prevede la gestione di una libreria di visualizzatori associata alle tipologie documentarie e ai singoli documenti.

Mediatica mette a disposizione un riferimento telefonico, email e fax (Single Point of Contact) per la gestione delle eventuali segnalazioni di errore da parte dell'utente anche dovuti ad errori di trasmissione. Un operatore di helpdesk provvede a registrare su una piattaforma di troubleticketing la richiesta, cui viene attribuito un numero univoco ed una priorità. Lo stesso operatore prova a risolvere autonomamente la segnalazione (primo livello) o ad inoltrarla ai gruppi di risoluzione specialistici (secondo livello). In qualunque momento è possibile consultare la segnalazione, tutte le comunicazioni ad essa correlate e le azioni svolte dai diversi gruppi di lavoro. Ulteriori dettagli nelle modalità di erogazione del servizio di helpdesk sono definite nel Contratto.

Mediatica non può veicolare informazioni o documenti relative al sistema di conservazione per email o altri canali, ma mette l'utente in condizioni di recuperare in autonomia tali informazioni attraverso l'interfaccia applicativa.

(Torna al Sommario)

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

Su richiesta degli utenti è possibile produrre delle estrazioni di documenti dall'archivio dell'Ente di appartenenza da riversare su altro supporto. La memorizzazione su altro supporto è a carico dell'utente che ha estratto i documenti.

Laddove si voglia cambiare il formato di un documento conservato per far fronte a problematiche di obsolescenza tecnologica delle applicazioni di visualizzazione dei documenti, è possibile ricorrere al riversamento di un documento creando un nuovo documento in altro formato e versandolo nel sistema con le stesse modalità previste per il documento originario. Tale operazione richiede un intervento del Responsabile della Funzione Archivistica di Conservazione, che al termine del riversamento deve apporre la propria firma all'insieme dei documenti riversati (pacchetto di archiviazione) in modo analogo a quanto previsto per la conservazione. Il nuovo documento mantiene i riferimenti al documento originario.

Durante l'erogazione del servizio può essere necessario l'intervento di un pubblico ufficiale per:

- attestare la conformità di una copia informatica di documento informatico conservato;
- attestare la conformità di una copia analogica di un documento informatico conservato;
- attestare la conformità di una copia informatica di un documento informatico conservato in caso di migrazione (cambio di formato del documento medesimo).

Qualora applicabile, può essere concordato con il Produttore e indicato nelle *Definizione delle classi documentali* specifiche modalità di coinvolgimento del pubblico ufficiale.

(Torna al Sommario)

7.1.7 Scarto dei pacchetti di archiviazione

L'attività di scarto viene gestita sul sistema dal Responsabile della Funzione Archivistica o suoi delegati con le seguenti modalità:

- con cadenza annuale (o diversamente definito per classe documentale) si procede all'estrazione della lista dei documenti scaduti (con data di conservazione antecedente il periodo maggiore della retention per la classe documentale)
- la lista prodotta viene sottoposta all'attenzione del Produttore, che ha il compito di segnalare eventuali documenti per i quali si rende necessaria la conservazione oltre il periodo di conservazione standard;
- il Responsabile della Funzione Archivistica di Conservazione o suo delegato procede a modificare sul sistema di conservazione il tempo di conservazione prolungandone la durata;
- la lista emendata da tali eccezioni viene firmata dal Responsabile del Servizio di Conservazione e dal Produttore e archiviata come lista di scarto;

- i documenti oggetto della lista di scarto vengono eliminati dal sistema.

Per i documenti che necessitano di un periodo di conservazione superiore ai 20 anni, si prevedono le seguenti attività di mantenimento dell'archivio, sotto la responsabilità del Responsabile della Funzione Archivistica di Conservazione:

- monitoraggio e aggiornamento delle scadenze delle marche temporali: poiché le marche temporali apposte dal processo di conservazione hanno validità di 20 anni, occorre monitorare la scadenza delle marche apposte sui pacchetti di archiviazione e apporre nuove marche a quelle in scadenza.

Procedure specifiche concordate con il soggetto Produttore possono essere descritte nell'allegato *Definizione delle classi documentali*.

Nel caso 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.

(Torna al Sommario)

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

Sono disponibili le interfacce applicative per poter operare l'estrazione dei documenti tramite applicazione esterna. Il sistema di conservazione è in grado di accettare il versamento di pacchetti strutturati secondo lo standard UNI 11386:2010, in accordo con quanto definito dalla normativa vigente (attualmente l'Allegato 4 delle Regole tecniche). Allo stesso modo, il sistema è in grado di versare ad altri sistemi di conservazione pacchetti e indici secondo la medesima struttura, trasformando i pacchetti di archiviazione in opportuni pacchetti di distribuzione.

(Torna al Sommario)

7.1.9 Cessazione del servizio

In caso di cessazione del servizio verso un Produttore, per naturale scadenza della durata del contratto o nei casi di risoluzione o recesso per qualsivoglia motivo occorso:

- cessa di avere efficacia la nomina di Mediatica S.p.A. a Responsabile del Servizio di Conservazione;
- Mediatica S.p.A. provvede a riconsegnare al Produttore i documenti conservati presso i propri archivi, completi dei pacchetti di archiviazione, e a redigere un apposito verbale di consegna che verrà sottoscritto per accettazione dal Produttore;
- Mediatica S.p.A. si impegna a non comunicare e/o diffondere e/o comunque utilizzare ulteriormente i documenti oggetto del verbale di consegna, ovvero a conservare copia degli stessi, salva la possibilità prevista di produzione e consegna di supporti informatici;

- Mediatica S.p.A. si impegna a distruggere i documenti oggetto del verbale di consegna dai propri supporti. Il Produttore può richiedere la produzione e la consegna dei supporti informatici contenenti tutti i documenti trasmessi con almeno 30 giorni di anticipo rispetto all'eventuale data di cessazione del Servizio. All'atto della consegna il Produttore rilascia specifica ricevuta, sottoscrivendo la copia dell'elenco dei documenti (verbale di consegna), che rimane a Mediatica S.p.A. Entro 15 giorni lavorativi successivi alla consegna del materiale il Produttore deve procedere a verificare la leggibilità del contenuto dei supporti: tutte le contestazioni direttamente/indirettamente connesse alla verificabilità dei contenuti dei supporti che non siano state effettuate formalmente nel termine di 15 giorni dalla consegna non potranno essere più formulate dal Produttore. In ogni caso, decorso il termine di cui sopra senza che il Produttore abbia svolto alcuna attività, tutto il materiale consegnato e di cui all'elenco trasmesso si intende da lui accettato senza riserve. Per tutto il periodo fino allo scadere del termine Mediatica S.p.A. trattiene una copia di tutto quanto consegnato al Produttore. Soltanto allo scadere del termine dei 15 giorni e nell'eventualità di cessazione del Servizio, avviene l'eliminazione della copia fino a quel momento trattenuta.

(Torna al Sommario)

7.1.10 Gestione delle segnalazioni da parte dell'utente

Tutte le segnalazioni da parte dell'utente relativamente al servizio di conservazione sono tracciate da una piattaforma di troubleticketing che provvede a:

- memorizzare la richiesta e assegnarle un numero univoco progressivo;
- veicolare la richiesta al gruppo di lavoro più idoneo;
- tenere traccia di tutte le comunicazioni che seguono in ingresso e uscita su quella specifica richiesta;
- tenere costantemente aggiornato l'utente sullo stato di avanzamento;
- procedere alla chiusura della richiesta con validazione della sua risoluzione con l'utente finale.

Tutte le attività sono gestite dal gruppo di *IT Helpdesk* e *System Management* di Mediatica S.p.A.

Le segnalazioni si possono riferire, a titolo puramente indicativo a:

- errori di rifiuto del pacchetto di versamento;
- errori nella trasmissione;
- errori della piattaforma errore da parte dell'utente (anche a seguito di errori di trasmissione) vengono gestite formalmente;
- richieste di informazioni.

Con l'eccezione delle sole richieste di informazioni, ogni segnalazione di errore attiva i formalismi delle procedure di *incident management* formalizzate nelle procedure del Sistema di Gestione della Sicurezza delle Informazioni di Mediatica S.p.A. predisposto e certificato secondo le norme ISO 27001:2013.

(Torna al Sommario)

8 IL SISTEMA DI CONSERVAZIONE

8.1 Componenti Logiche

La soluzione applicativa per gestire il processo di conservazione è prodotta dalla Andxor Soluzioni Informatiche con il nome commerciale di tDoc.

tDoc consente la conservazione di qualsiasi tipologia di documentazione digitale garantendone, dal momento della presa in carico, le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità.

Le principali funzionalità di tDoc sono:

- definizione automatizzata delle classi documentali
- definizione automatizzata delle tempistiche di conservazione
- acquisizione documenti da altre applicazioni (Sistemi di scansione/ECM)
- gestione metadati ad essi associati
- apposizione e verifica di firme digitali qualificate e firme elettroniche avanzate
- apposizione e verifica di marcature temporali
- archiviazione con link logici tra documenti
- archiviazione di documenti master e relativi allegati
- ricerca, visualizzazione ed esibizione dei documenti
- possibilità di definire la gestione avanzata dell'anagrafica, che consente di rispecchiare modelli organizzativi complessi;
- rispetta i requisiti di interoperabilità e le altre condizioni indicate da AgID per i conservatori accreditati.

La successiva figura illustra lo schema logico del sistema:

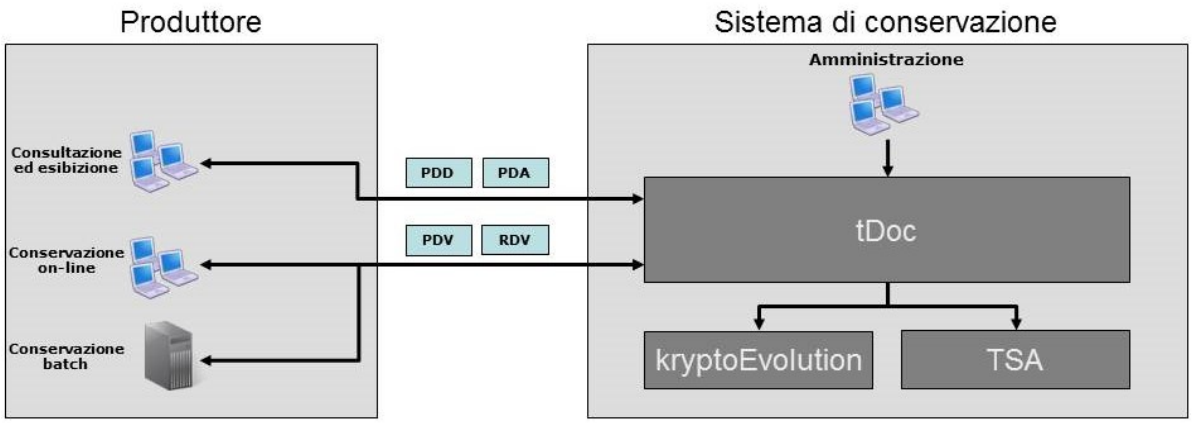

Figura 4: Schema generale di tDoc

- **kryptoEvolution**: HSM di Andxor Soluzioni Informatiche utilizzato per l'apposizione delle firme digitali in fase di creazione dei pacchetti di archiviazione o di caricamento dei documenti. Può essere utilizzato anche per firmare i documenti durante la fase di versamento;
- **TSA**: la Time Stamping Authority certificata, alla quale vengono richieste le marche temporali incluse nei pacchetti di archiviazione. Può essere utilizzata anche per marcare le firme apposte durante la fase di versamento.

La Figura 5 mostra uno schema più dettagliato di tDoc nel quale si vedono le diverse componenti interne:

- **DB**: Il data base è il repository della configurazione di tDoc (aziende, utenti, classi documentali, ecc.) e di tutti i metadati relativi ai documenti. Il database è MySQL.

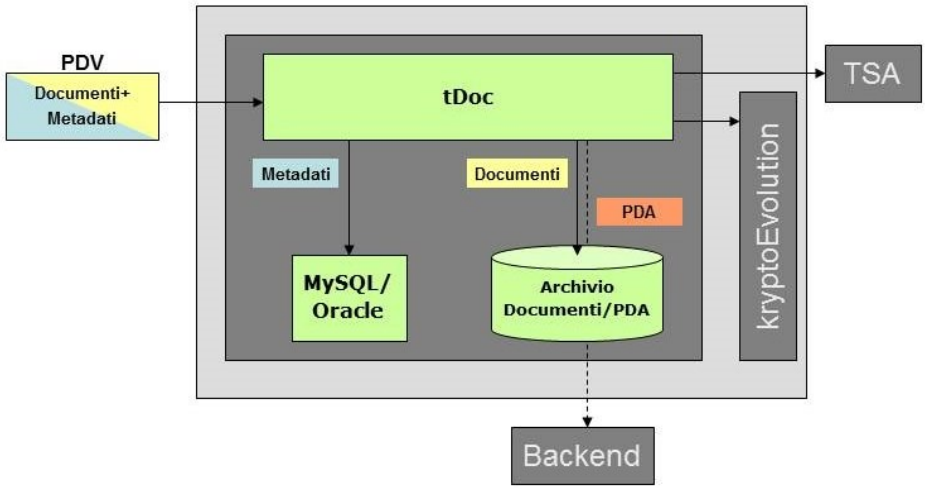

Figura 5: Schema di tDoc

- **Archivio**: nell'archivio vengono salvati i documenti e i PDA. L'archivio è configurato in uno Starage Area Network (SAN).
- **Back end**: è il repository dove viene conservato il backup dell'archivio.
- **tDoc**: è l'applicazione che svolge il lavoro di archiviazione e conservazione interfacciandosi con le altre componenti appena descritte.

(Torna al Sommario)

8.2 Componenti Tecnologiche

L'intera piattaforma applicativa è ospitata su server virtuali in una infrastruttura VMWare ESX in grado di garantire alta affidabilità e backup dei server e dei dati sullo stesso sito e su un sito di Disaster Recovery.

L'alta affidabilità è garantita dalle tecnologie VMWare High Availability , VMWare VMotion e VMWare Storage VMotion.

Malfunzionamenti hardware dell'host ospitante (ESX server) vengono prontamente intercettate e la piattaforma provvede alla istantanea migrazione dei server coinvolti su un host alternativo (vedi figura a seguire).

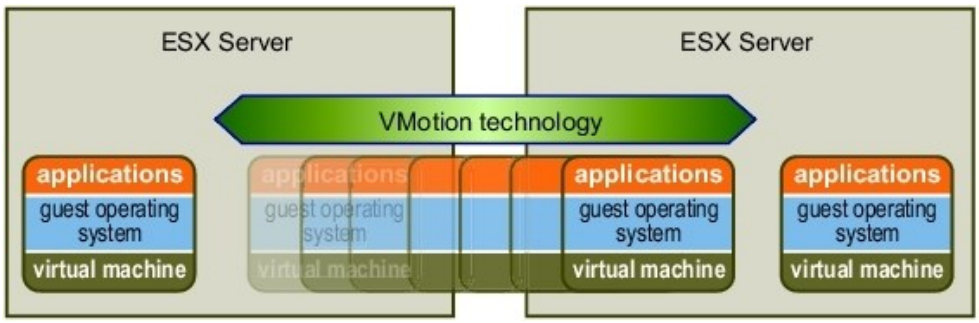

Figura 6 - tecnologia VMotion di VMWare

La stessa tecnologia replica l'intero server virtuale e i dati del repository su un Network Area Storage (NAS) presso lo stesso Datacenter nonché presso il sito di Disaster Recovery (presso la sede di Roma) con frequenza almeno giornaliera.

Tale soluzione consente di procedere al ripristino delle piene funzionalità in caso di indisponibilità totale dei sistemi o del datacenter entro gli obiettivi di RTO e RPO indicati nel Piano della Sicurezza del Servizio di Conservazione.

A monte dei sistemi descritti, la connettività verso l'esterno è gestita attraverso un firewall Sophos su cui sono attestate le Virtual Private Network (VPN) di ciascun cliente. Nessun contatto diretto con la rete pubblica (Internet) è possibile da parte del server di conservazione, mentre il collegamento con il cliente è filtrato consentendo il traffico solo sulle porte strettamente necessarie per il servizio: http, https.

La continuità elettrica è garantita da due collegamenti indipendenti al quadro per ciascun apparato, nonché da un UPS e da un gruppo elettrogeno che garantiscono un intervento "zero time" in caso di blackout (anche di lungo periodo) o disturbo sulla rete elettrica.

(Torna al Sommario)

8.3 Componenti Fisiche

Quanto illustrato nei precedenti paragrafi è ospitato sulle seguenti componenti fisiche e virtuali:

Server	Tipo	RAM	Storage	CPU	OS
tDoc Server	Virtual Machine su ambiente VMWare ESX	2 Gb	100 Gb	1 vCPU	Ubuntu
Host tDoc Server	Fujitsu Primergy RX200 S6	20 Gb	300 GB	4x Intel Xeon CPU E5620 2.40GHz	VMWare ESXi
Repository	Fujitsu Eternus DX90 S2	HA Dual Controller HA Dual FO Switch HA Dual PSU	7 TB complessivi 2 volumi RAID 5	N.A.	Proprietario Fujitsu
NAS (backup)	Fujitsu CELVIN Q800	N.A.	4 TB	N.A.	Proprietario Fujitsu
Host Disaster Recovery	Fujitsu Primergy	2 GB	30 GB + 480 GB	1	VMWare ESXi
Server Logico Disaster Recovery	Virtual Machine su ambiente VMWare ESX	2 Gb	100 Gb	1 vCPU	Ubuntu
Repository Disaster Recovery	Sulla Virtual Machine	2 GB	480 GB scalabile in modo dinamico	2,80 GHz	N.A.

Tabella 5 - componenti del sistema di conservazione

Tutte le infrastrutture indicate in tabella sono tenute costantemente aggiornate e sono presenti in una versione supportata dal produttore.

(Torna al Sommario)

8.4 Procedure di gestione e di evoluzione

Il servizio è gestito in modo conforme alle indicazioni del Sistema di Qualità aziendale ed al Sistema di Gestione della Sicurezza delle Informazioni per gli specifici processi che comprendono tutto il ciclo del servizio, al fine di garantire il raggiungimento degli SLA concordati contrattualmente con i clienti.

(Torna al Sommario)

9 MONITORAGGIO E CONTROLLI

Tutte le attività di audit sono svolte nel rispetto del principio di segregazione dei ruoli per cui controllato e controllore non coincidono e si escludono conflitti d'interesse nelle specifiche attività.

Segue una tabella riassuntiva di tale logica:

Exhibit 2.9—Segregation of Duties Control Matrix

	Control Group	Systems Analyst	Application Programmer	Help Desk and Support Manager	End User	Data Entry	Computer Operator	Database Administrator	Network Administrator	Systems Administrator	Security Administrator	Systems Programmer	Quality Assurance
Control Group		X	X	X		X	X	X	X	X		X	
Systems Analyst	X			X	X		X				X		X
Application Programmer	X			X	X	X	X	X	X	X	X	X	X
Help Desk and Support Manager	X	X	X		X	X		X	X	X		X	
End User		X	X	X			X	X	X			X	X
Data Entry	X		X	X			X	X	X	X	X	X	
Computer Operator	X	X	X		X	X		X	X	X	X	X	
Database Administrator	X		X	X	X	X	X		X	X		X	
Network Administrator	X		X	X	X	X	X	X					
System Administrator	X		X	X		X	X	X				X	
Security Administrator		X	X			X	X					X	
Systems Programmer	X		X	X	X	X	X	X		X	X		X
Quality Assurance		X	X		X							X	

X—Combination of these functions may create a potential control weakness.

Figura 7 - logiche di separazione dei ruoli

9.1 Procedure di monitoraggio

Il monitoraggio sul funzionamento del software applicativo e dei sistemi che erogano il servizio di conservazione è eseguito nel rispetto del documento *DSS01 02 - Politiche per il logging e monitoring*.

Il fine è quello di garantire la costante operatività dei sistemi e degli applicativi o di intercettare nel modo più proattivo/reattivo possibile eventuali anomalie.

Il monitoraggio messo in atto si pone l'obiettivo di minimizzare i seguenti rischi:

- mancanza di alimentazione elettrica
- guasti su apparati di telecomunicazione
- manomissione di hardware
- manomissione di software
- malfunzionamenti su apparati
- saturazione dei sistemi
- malfunzionamenti software
- mtilizzo non autorizzato dei sistemi
- perdita di dati
- utilizzo illegale dei diritti amministrativi

attraverso l'uso di piattaforme specifiche:

- sistema di *Log Management* per la gestione dei log degli amministratori di sistema secondo le prescrizioni del GDPR 2016/679 in materia di data protection:
  - ID utente
  - data e ora dell'evento
  - identità terminale (ad esempio nome e / o indirizzo IP)
  - informazioni relative all'evento (messaggio o codice)
  - indicazione se si tratta di un evento terminato con successo o con insuccesso.
- piattaforma di monitoraggio per il controllo costante dello stato dei sistemi:
  - utilizzo delle risorse di sistema (CPU, memoria , disco) oltre le soglie stabilite di attenzione (warning) e allarme, normalmente identificate rispettivamente in >70% e >90%;
  - stato del dispositivo;
  - stato dei servizi erogati dal dispositivo;
- i sistemi di *firewall* e *intrusion detection* per quanto riguarda le minacce relative alla difesa perimetrale:
  - tutte le richieste di autenticazione sul firewall (eseguite con successo e non);
  - tutte le richieste di sessione di VPN (riuscite e non);
  - tutti i pacchetti negati da regole specifiche e dalla regola "default deny";
  - tutti i pacchetti la cui destinazione è il firewall stesso (gestione del traffico firewall).

Le infrastrutture di registrazione dei log e del monitoraggio sono protette contro le minacce intenzionali e accidentali, in particolare:

- i file di registro non possono essere modificati o eliminati per nascondere abusi;

- tutte le modifiche alle voci di log sono registrate;
- le limitazioni alle dimensioni dei file di logs non possono portare alla perdita degli stessi per sovrascrittura o cancellazione.

I file di log e le infrastrutture di registrazione sono protetti in modo che solo gli amministratori autorizzati possano avere accesso e che nessun utente possa cancellare o alterarli.

Una infrastruttura operante h24 presso la sede di Mediatica S.p.A. garantisce la costante e tempestiva rilevazione di ogni anomali rilevata dai sistemi di log monitoraggio, nonché il più tempestivo intervento tecnico.

(Torna al Sommario)

9.2 Verifica dell'integrità degli archivi

Per quanto riguarda la verifica dell'integrità dei documenti, l'attività viene compiuta direttamente dalla Storage Area Network, che provvede alla gestione ridondata delle informazioni con tecnologia di Stripe 5. In questo modo la failure fisica di un disco (o di parte di esso) non pregiudica l'integrità delle informazioni che viene recuperata dai dischi residui e ricostruita con assoluta certezza.

Ogni volta che il Sistema riscontra una non conformità in merito alla leggibilità o all'integrità di un documento memorizzato, traccia in opportuni file di log l'esito negativo della verifica di leggibilità e integrità e procede alla rigenerazione del documento a partire dalla copia ancora integra.

Su base almeno giornaliera, inoltre, si procede al backup di tutte le informazioni sul dispositivo NAS e su sito remoto di Disaster Recovery, come dettagliato nel documento "Piano di schedulazione e dei backup".

Con cadenza almeno annuale, RSC provvede alla verifica manuale della corretta visualizzazione dei documenti conservati, selezionando almeno un documento per ciascuna classe documentale gestita.

(Torna al Sommario)

9.3 Soluzioni adottate in caso di anomalie

In caso di anomalie si interviene in modo adeguato allo specifico problema:

- problemi nella trasmissione del pacchetto di versamento: si procede alla gestione dell'incident come previsto dai processi di Sistema Qualità. A valle della risoluzione del problema si segnala al Produttore di reinviare i dati;

- versamenti non conformi: nel caso il pacchetto di versamento non superi le verifiche di consistenza, si procede a segnalare al Produttore il problema e a richiedere la correzione del pacchetto stesso;
- altri errori non previsti: si procede alla gestione dell'incident come previsto dai processi di Sistema Qualità. A valle della risoluzione del problema si segnala al Produttore di reinviare i dati se necessario.

Gli errori non dipendenti da errori del produttore sono registrati *Libro dei Verbali*.

(Torna al Sommario)

10 Appendice A – livelli di servizio (SLA)

Di seguito si descrivono i livelli di servizio che si garantiscono nell'espletamento del servizio, salvo indicazioni specifiche riportate nel documento *Definizione delle classi documentali*.

Attività		Livelli di servizio	Note
1	Disponibilità dei servizi	>99%	Tempo di uptime rilevato trimestrale. Sono esclusi gli interventi di manutenzione straordinari preventivamente comunicati ai clienti (e normalmente svolti fuori dall'Orario di Ufficio).
2	Tempistiche di lavorazione dei flussi documentali ricevuti: archiviazione dei documenti e inoltro degli stessi al processo di conservazione.	< 1 gg. lavorativo dalla data di ricezione.	99% di ciascun flusso ricevuto contenente un numero di documenti minore o uguale a 2.000.
3	Segnalazione della presenza di anomalie nei flussi documentali ricevuti.	Comunicazione via email entro 1 gg. lavorativo dalla ricezione.	99% dei flussi documentali standard inviati.
4	Modalità e tempistiche di rendicontazione degli esiti del processo di Conservazione dei singoli flussi documentali	Generazione dei file esiti e messa a disposizione entro il giorno lavorativo successivo alla data di ricezione del flusso documentale.	99% di ciascun flusso ricevuto contenente un numero di documenti minore o uguale a 2.000.
5	Modalità e tempistiche di archiviazione elettronica dei documenti	Archiviazione dei documenti tale da consentirne la ricerca on-line (ad evento), secondo le chiavi di ricerca concordate, entro il giorno lavorativo successivo alla data di ricezione del flusso documentale.	99% di ciascun flusso ricevuto contenente un numero di documenti minore o uguale a 1.000.
6	Backup dell'archivio documentale	Almeno una volta al giorno	100% dei casi

Tabella 6 - livelli di servizio

(Torna al Sommario)