SERVIZIO DI CONSERVAZIONE
DEI DOCUMENTI INFORMATICI
(software eSignum)

MANUALE DI CONSERVAZIONE

marno srl – gestioni documentali, trattamento dati e conservazione documenti informatici
via Traversa Livornese 16 – 57016 Castelnuovo della Misericordia (Livorno)
0586 744099 (telefono) – 0586 745814 (fax) – info@pec.marnonet.it – P.IVA 01111630495

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	01/09/2017	F. Costalli E. Volpato	Responsabile dello sviluppo e della manutenzione del Sistema di Conservazione Responsabile del Servizio di Conservazione
Verifica	15/09/2017	M. Ghezzo	Responsabile dei Sistemi Informativi per la Conservazione
Approvazione	02/10/2017	E. Volpato M. Volpato	Responsabile del Servizio di Conservazione Legale Rappresentante

REGISTRO DELLE VERSIONI

N°Ver/Rev/ Bozza	Data emissione	Modifiche apportate	Osservazioni
07	02/10/2017	revisione generale	//
06	08/01/2016	adeguamento agli standard di accessibilità	//
05	15/11/2014	revisione generale sulla base del nuovo template AgID	//
04	22/08/2014	revisione per conformità alle competenze minime	//
03	12/03/2014	revisione secondo le nuove regole tecniche	//
02	30/12/2013	revisione post gap analysis con l'Ente Bureau Veritas	//

INDICE DEL DOCUMENTO

1 SCOPO E AMBITO DEL DOCUMENTO 5
2 TERMINOLOGIA (GLOSSARIO E ACRONIMI) 6
2.1 Glossario 6
2.2 Acronimi 11
3 NORMATIVA E STANDARD DI RIFERIMENTO 12
3.1 Normativa di riferimento 12
3.2 Standard di riferimento 13
4 RUOLI E RESPONSABILITA' 14
5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE 18
5.1 Organigramma 18
5.2 Strutture organizzative 19
6 OGGETTI SOTTOPOSTI A CONSERVAZIONE 21
6.1 Oggetti conservati 21
6.1.1 Ambito degli oggetti inviati in conservazione 21
6.1.2 Formati utilizzati 21
6.1.3 Metadati 21
6.2 Pacchetto di versamento 21
6.3 Pacchetto di archiviazione 22
6.4 Pacchetto di distribuzione 23
7 IL PROCESSO DI CONSERVAZIONE 24
7.1 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico 24
7.1.1 Il flusso di lavoro con gli Enterprise pattern 25
7.2 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti 25
7.2.1 Verifica delle credenziali del produttore 25
7.2.2 Validazione sintattica del pacchetto di versamento 26
7.2.3 Generazione e restituzione al produttore del rapporto di presa in carico 26
7.2.4 Verifica di eventuale firma 26
7.2.5 Verifica codice IPA 27
7.2.6 Verifica presenza Virus 27
7.3 Accettazione dei PdV e generazione del rapporto di versamento di presa in carico 29
7.3.1 Flusso di accettazione 29
7.3.2 Generazione rapporto di versamento 29
7.4 Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie 30
7.5 Preparazione e gestione del pacchetto di archiviazione 30

7.6 Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione 31
7.7 Produzione di duplicati e copie informatiche 32
7.8 Scarto dei pacchetti di archiviazione 32
7.9 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori 32
8 IL SISTEMA DI CONSERVAZIONE 33
8.1 Componenti Logiche 33
8.2 Componenti Tecnologiche 36
8.3 Componenti Fisiche 37
8.3.1 Sito primario 37
8.3.2 Sito secondario di disaster recovery, certificato 22301: 38
8.4 Procedure di gestione e di evoluzione 40
8.4.1 Conduzione e manutenzione del sistema di conservazione. 40
8.4.2 Gestione e conservazione dei log (anche in accordo con l'ente Produttore) 41
8.4.3 Monitoraggio del sistema di conservazione 41
8.4.4 Change management 41
8.4.5 Verifica periodica di conformità a normativa e standard di riferimento. 42
9 MONITORAGGIO E CONTROLLI 44
9.1 Procedure di monitoraggio 44
9.1.1 Il server di log 44
9.1.2 Produzione dei log 45
9.1.3 La trasmissione dei log 45
9.1.4 Analisi dei log 45
9.1.5 Verifica funzionalità del sistema da dispositivi mobili 47
9.1.6 Specificità relative al monitoraggio 47
9.2 Verifica dell'integrità e leggibilità degli archivi 47
9.3 Soluzioni adottate in caso di anomalie 48

1 SCOPO E AMBITO DEL DOCUMENTO

Il presente manuale descrive il sistema di Conservazione per il Cliente del servizio ***esignum***, di qui innanzi denominato come il "Cliente", che intende sottoporre a conservazione, utilizzando l'apposito servizio, i propri documenti.

Il presente documento è stato redatto secondo i seguenti principi:

- **principio di Conformità**: il manuale descrive un sistema ed un processo di conservazione secondo le disposizioni normative vigenti nel tempo ivi comprese le regole tecniche ed il modello di riferimento OAIS (Open Archival Information System) standard ISO 14721:2012;
- **principio di Conformità**:il manuale fornisce una chiara spiegazione del sistema di conservazione documentale e dei processi effettivamente erogati;
- **principio di Concretezza**: il manuale è il documento che descrive il sistema di conservazione per un produttore dei documenti ben identificato, con il quale sono stati concordati tutti gli aspetti connessi alla conservazione ed alla fruizione del patrimonio informativo digitale, in conformità al modello di riferimento OAIS (Open Archival Information System) standard ISO 14721:2012;

Esso, in generale, ha lo scopo di:

- descrivere le competenze, i ruoli e le responsabilità degli attori coinvolti nel processo;
- descrivere come è stato implementato il processo di conservazione e gli aspetti operativi per arrivare alla produzione del dispositivo contenente la documentazione digitale;
- descrivere il processo di apposizione della Firma Digitale, della Marca Temporale e tutti gli aspetti procedurali inerenti la registrazione dei dispositivi sostitutivi,
- descrivere le procedure di verifica dei documenti e di gestione delle copie di sicurezza.

Il documento recepisce tutti i riferimenti legislativi di cui al punto 3.

Torna al Sommario

2 TERMINOLOGIA (GLOSSARIO E ACRONIMI)

2.1 Glossario

N.	Glossario dei termini	
[1]	***Accreditamento***	Riconoscimento, da parte di AgID, del possesso dei requisiti, in termini di qualità e sicurezza, ad un soggetto pubblico o privato, che svolge attività di conservazione
[2]	***AE***	Agenzia delle Entrate
[3]	***AgID***	Agenzia per l'Italia Digitale (già DigitPA e CNIPA)
[4]	***Archiviazione***	Processo di trattamento e gestione dei documenti di uso corrente che permette una loro classificazione (indicizzazione ed eventuale tipizzazione) ai fini della ricerca e consultazione
[5]	***Archivio Informatico***	Archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico
[6]	***Certification Authority (CA)***	Il soggetto che secondo quanto disposto dall'art. 27 del CAD presta servizi di certificazione delle firme elettroniche qualificate o che fornisce altri servizi connessi con queste ultime, quali ad esempio quello delle marche temporali
[7]	***Certificato qualificato***	Il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva
[8]	***Conservatore accreditato***	Soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, da AgID
[9]	***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
[10]	***Copia di sicurezza***	Copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell'art. 12 del DPCM 3 dicembre 2013
[11]	***Copia informatica di documento analogico/informatico***	Il documento informatico avente contenuto identico a quello del documento analogico/informatico da cui è tratto
[12]	***Dispositivo sicuro per la creazione della firma:***	I dispositivi sicuri per la generazione della firma qualificata che devono essere dotati di certificazione di sicurezza secondo l'art. 35 del CAD

N.	Glossario dei termini	
[13]	***Documento informatico***	per documento s'intende la rappresentazione informatica o analogica di atti, fatti e dati intelligibili direttamente o attraverso un processo di elaborazione elettronica
[14]	***Documento analogico***	s'intende un documento formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta (esempio: documenti cartacei), come le immagini su film (esempio: pellicole mediche, microfiches, microfilm), come le magnetizzazioni su nastro (esempio: cassette e nastri magnetici audio e video).
[15]	***Documento analogico originale***	s'intende un documento analogico che può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi
[16]	***Esibizione***	Operazione che consente di visualizzare un documento conservato e di ottenerne copia
[17]	***Fascicolo informatico***	Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'art. 41 del Codice dell'Amministrazione Digitale (D. Lgs. 7 marzo 2005, n. 82 e successive modifiche ed integrazioni)
[18]	***Fascicolo informatico***	Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'art. 41 del Codice dell'Amministrazione Digitale (D. Lgs. 7 marzo 2005, n. 82 e successive modifiche ed integrazioni)
[19]	***Firma elettronica***	L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica
[20]	***Firma elettronica avanzata***	Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati

N.	Glossario dei termini	
[21]	***Firma elettronica qualificata***	Un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma
[22]	***firma digitale***	è il risultato della procedura informatica 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.
[23]	***FTP server***	programma che permette di accettare connessioni in entrata e di comunicare con un Client attraverso il protocollo definito FTP
[24]	***funzione di hash***	é una funzione matematica che genera, a partire da una generica sequenza di simboli binari (bit), un'impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari (bit) che la generi, ed altresì risulti di fatto impossibile determinare una coppia di sequenze di simboli binari per le quali la funzione generi impronte uguali.
[25]	***Funzioni archivistiche***	Funzioni per la conservazione delle informazioni (acquisizione, archiviazione, gestione dati, accesso, distribuzione)
[26]	***Impronta***	sequenza di simboli binari di lunghezza predefinita generata mediante l'applicazione di una opportuna funzione di hash
[27]	***marca temporale***	(art. 1 DPCM) 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 rilasciata da una TSA
[28]	***OAIS***	Open Archival Information SystemStandard sviluppato dal CCSDS (Consultive Committee for data space system) nel 2002 per definire concetti, modelli e funzionalità inerenti agli archivi digitali.
[29]	***Pacchetto di Archiviazione (AIP o PdA)***	Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del DPCM 3 dicembre 2013 e secondo le modalità riportate nel manuale di conservazione .
[30]	***Pacchetto di Distribuzione (DIP o PdD)***	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta
[31]	***Pacchetto di Versamento (SIP o PdV)***	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione

N.	Glossario dei termini	
[32]	***Pacchetto Informativo***	Per pacchetto informativo si intende il 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.
[33]	***Processo di Conservazione***	Insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 9 delle regole tecniche sul sistema di conservazione
[34]	***Rapporto di Versamento***	Viene rilasciato dal sistema di conservazione, anche in automatico, successivamente alla presa in carico e alla verifica del pacchetto di versamento.
[35]	***Responsabile della Conservazione***	Soggetto, individuato dall'art. 44 del CAD e dall'art. 6, c. 5, del DPCM 3 Dicembre 2013, i cui compiti generali sono quelli di definire e attuare le politiche complessive del sistema di conservazione e di governarne la gestione con piena responsabilità ed autonomia, in relazione al modello organizzativo della conservazione adottato. Il ruolo del responsabile della conservazione, che è persona fisica inserita nell'organico del soggetto produttore dei documenti, viene stabilito dall'art. 7, c. 1, del DPCM 3 dicembre 2013. Ai sensi dell'art. 7, c. 3, del DPCM 3 Dicembre 2013, nelle PA il ruolo del responsabile della conservazione è svolto da un dirigente o, in alternativa, da un funzionario designato
[36]	***Responsabile del trattamento dei dati***	Soggetto esterno a cui è affidato il processo di conservazione che assume il ruolo di responsabile del trattamento dei dati, così come previsto dal Codice in materia di protezione dei dati personali ed espressamente richiamato dall'art. 6, punto 8) del DPCM 3 Dicembre 2013
[37]	***Responsabile del Servizio di Conservazione***	È il soggetto, interno al soggetto conservatore, cui compete la definizione e l'attuazione delle politiche complessive del sistema di conservazione, nonché il governo della gestione del sistema di conservazione.
[38]	***Responsabile della funzione archivistica di conservazione***	Soggetto persona fisica nominato responsabile della funzione archivistica di conservazione e-signum di Marno con l'assegnazione delle attività indicate nel documento dell'Agenzia per l'Italia Digitale sui profili professionali richiamati dalla Circolare 65/2014 (GU 89 del 16/04/2014)
[39]	***Responsabile del trattamento dei dati personali***	Soggetto persona fisica nominato responsabile del trattamento dei dati personali del servizio di conservazione e-signum di Marno 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)

N.	Glossario dei termini	
[40]	***Riferimento temporale***	È l'informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici da una procedura informatica.
[41]	***Scarto***	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale
[42]	***Sistema di conservazione***	Sistema di conservazione dei documenti informatici di cui all'art. 44 del Codice dell'Amministrazione Digitale (D. Lgs. 7 marzo 2005, n. 82 e successive modifiche ed integrazioni)
[43]	***Soggetto Produttore***	È la persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che dispone delle informazioni da conservare.
[44]	***SFTP server***	SSH File Transfer Protocol o SFTP è un protocollo di rete che prevede il trasferimento dei dati e funzionalità di manipolazione.
[45]	***TSA Time StampingAuthority***	Ente terzo che emette i certificati di marcatura temporale
[46]	***TSS Time Stamping Service***	Servizio di marcatura temporale che emette marche temporali utilizzando il certificato emesso da una TSA. Questo servizio deve rispettare i requisiti del RFC 3161 e il titolo IV del DPCM 13 gennaio 2004.
[48]	***Utente***	Persona fisica o giuridica che richiede accesso ai documenti presenti nel sistema di conservazione al fine di acquisire informazioni di interesse.
[49]	***Validazione temporale***	Il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi
[50]	***Versamento agli archivi di stato***	Operazione con cui il responsabile della conservazione di un organo giudiziario o amministrativo dello Stato effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali

Torna al Sommario

2.2 Acronimi

N.	Glossario degli Acronimi	
[1]	***AgID***	Agenzia per l'Italia Digitale (già DigitPA e CNIPA)
[2]	***FTP***	File Transfer Protocol
[3]	***IPA***	Indice delle Pubbliche Amministrazioni
[4]	***IPdA***	Indice del Pacchetto di Archiviazione
[5]	***IPdD***	Indice del Pacchetto di Distribuzione
[6]	***IPdV***	Indice del Pacchetto di Versamento
[7]	***OAIS***	Open Archival Information System, ISO 14721:2012
[8]	***PdD***	Pacchetto di Distribuzione
[9]	***PdV***	Pacchetto di Versamento
[10]	***RdV***	Rapporto di Versamento
[11]	***SdI***	Sistema d'Interscambio per la fatturazione elettronica PA per lo scambio di fatture e delle relative notifiche/ricevute ai sensi del DM 3 aprile 2013, n. 55
[12]	***SGSI***	Sistema di Gestione della Sicurezza delle Informazioni
[13]	***SLA***	Service Level Agreement
[14]	***OLA***	Operational Level Agreement
[15]	***TSA***	Time Stamping Authority

Torna al Sommario

3 NORMATIVA E STANDARD DI RIFERIMENTO

3.1 Normativa di riferimento

Alla data l'elenco dei principali riferimenti normativi italiani in materia, ordinati secondo il criterio della gerarchia delle fonti, è costituito da:

- Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- 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 .03.2005, n. 82.

- Regolamento europeo eIDAS 910/2014/EC del 24 luglio 2014 – Regolamento in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.

- Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 –Nuove Regole tecniche per la formazione l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici sia per i privati che per le pubbliche amministrazioni.

La normativa specifica relativa alle diverse tipologie di documenti riguardanti il contratto di erogazione del servizio di conservazione è riportata nel documento "Specificità del Contratto".

Torna al Sommario

3.2 Standard di riferimento

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

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

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

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

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

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

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

Queste informazioni devono essere riportate nell'allegato "Specificità del contratto" e devono essere periodicamente aggiornate in base agli eventuali nuovi standard adottati.

Torna al Sommario

4 RUOLI E RESPONSABILITA'

Nella tabella sottostante sono declinati i ruoli che afferiscono al Servizio di Conservazione tenendo conto delle varie figure che eventualmente si sono succedute nella gestione di uno o più ruoli; sempre all'interno della tabella sono menzionate le attività di competenza per ciascun ruolo e le deleghe previste. Non sono previste deleghe per nessuna delle figure presenti in organigramma.

ruoli	nome	attività di competenza	periodo nel ruolo	eventuali deleghe
Responsabile del servizio di conservazione	Mario Volpato	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; ha l'obbligo di archiviare e rendere disponibili, con l'impiego di procedure elaborative, relativamente ad ogni supporto di memorizzazione utilizzato, le seguenti informazioni: a) descrizione del contenuto dell'insieme dei documenti; b) estremi identificativi del Responsabile della Conservazione; c) estremi identificativi delle persone eventualmente delegate dal Responsabile della Conservazione, con l'indicazione dei compiti alle stesse assegnati; d) indicazione delle copie di sicurezza	da 01.01.99 al 31.10.14	
	Enrico Volpato		da 01.11.14 ad oggi	

ruoli	nome	attività di competenza	periodo nel ruolo	eventuali deleghe
Responsabile Sicurezza dei sistemi per la conservazione	Enrico Volpato	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 18.07.00 ad oggi	
Responsabile funzione archivistica di conservazione	Claude Sournia	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 01.01.99 ad oggi	

ruoli	nome	attività di competenza	periodo nel ruolo	eventuali deleghe
Responsabile trattamento dati personali(*anche per quanto disposto dal D.Lgs 196)*	Mario Volpato	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 01.01.99 ad oggi	
Responsabile sistemi informativi per la conservazione	Marco Ghezzo	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 01.03.00 ad oggi	

ruoli	nome	attività di competenza	periodo nel ruolo	eventuali deleghe
Responsabile sviluppo e manutenzione del sistema di conservazione	Filippo Costalli	Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione; pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione; monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione; interfaccia con l'ente produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche; gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.	da 01.10.12 ad oggi	

Torna al Sommario

5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

La struttura organizzativa dell'Azienda è schematicamente presentata nell'organigramma che segue dove sono state poste in evidenza le figure che ricoprono i ruoli per i quali è richiesto il possesso di requisiti minimi.

5.1 Organigramma

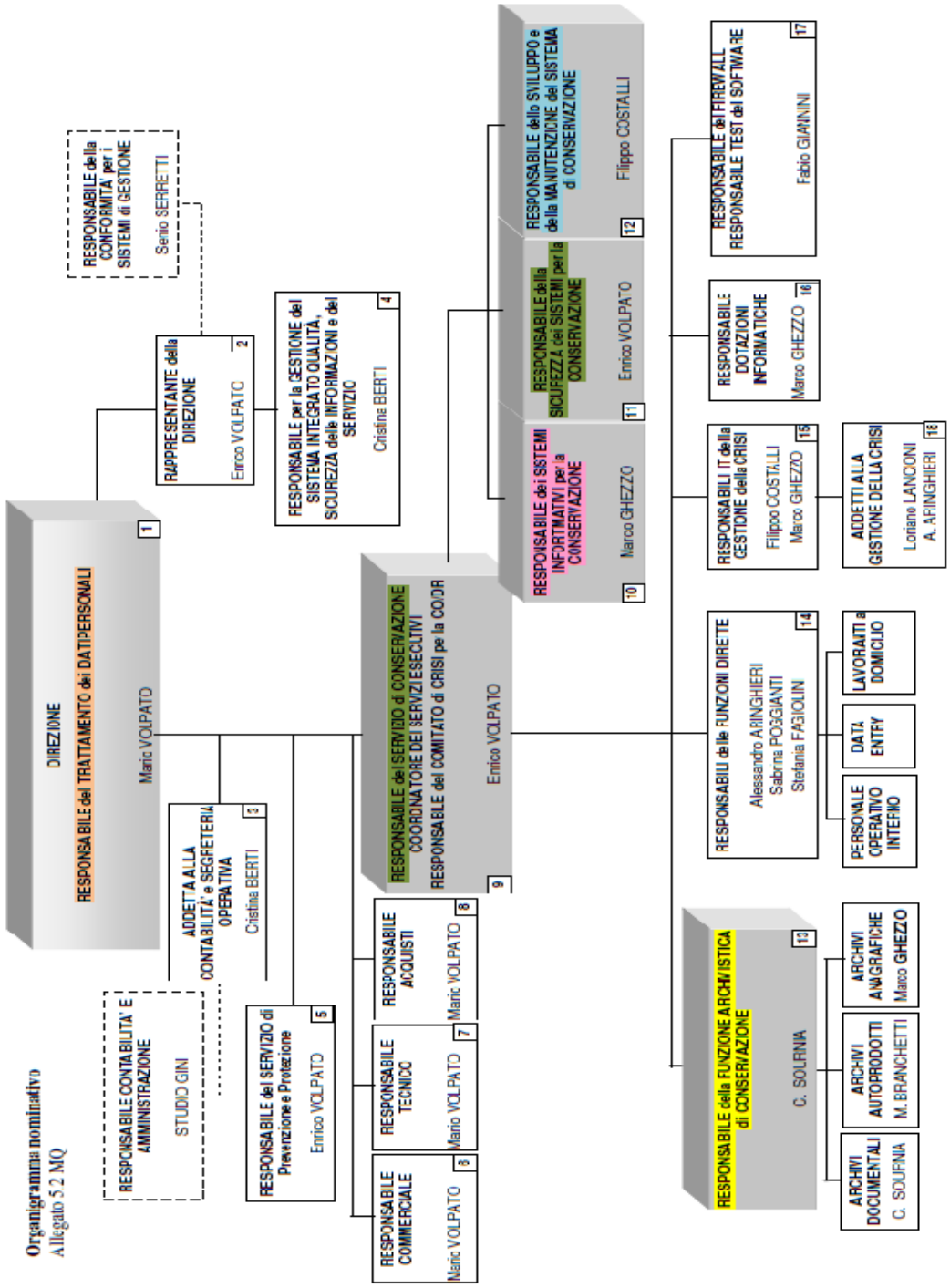

Figura 1 - Organigramma Nominativo

Torna al Sommario

5.2 Strutture organizzative

Nel processo di conservazione vengono coinvolte le funzioni aziendali con le modalità di seguito riportate:

- attività proprie di ciascun contratto di servizio di conservazione:
  - in fase di riesame dell'offerta il Responsabile del Sistema di Conservazione ne verifica il contenuto con la collaborazione del Responsabile della Funzione Archivistica; a seguito della successiva sottoscrizione del contratto ne verifica il contenuto anche in funzione di quelle che sono le specificità di contratto provvedendo a disporre i contenuti per il medesimo;
  - il Responsabile sviluppo e manutenzione del Sistema di Conservazione, a fronte della sottoscrizione di un contratto, provvede a predisporre l'acquisizione, la verifica e la gestione dei pacchetti di versamento presi in carico e alla successiva generazione del rapporto di versamento;
  - il Responsabile della Funzione Archivistica, con la collaborazione del Responsabile dello sviluppo e manutenzione del Sistema di Conservazione, provvede alla preparazione e alla gestione del pacchetto di archiviazione;
  - dopo aver validato il documento di "Specificità di Contrato", già condiviso con il cliente produttore, il Responsabile del Servizio di Conservazione si fa carico che tale documento venga correttamente recepito dal Responsabile dei Sistemi Informativi per la Conservazione che avrà cura di verificare l'efficienza degli asset di infrastruttura e la corretta esecuzione del processo, gestendo la fase di presa in carico, del controllo di coerenza, della corretta generazione del rapporto di versamento, e della preparazione e gestione dei pacchetti di archiviazione;
  - in particolare la preparazione e la gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su specifica richiesta è gestita ancora dal Responsabile dei Sistemi Informativi per la Conservazione secondo gli accordi contrattuali;
  - Il mantenimento dei documenti e dei pacchetti generati nel processo di conservazione è gestito dal Responsabile dei sistemi informativi per la conservazione e dal Responsabile dello sviluppo e della manutenzione del sistema di conservazione che garantiscono sia dal punto di vista infrastrutturale che applicativo il presidio e il controllo degli asset del servizio e quindi il corretto mantenimento dei documenti e dei pacchetti per tutto il periodo di conservazione concordato con il produttore dei documenti. Infine, scaduto il periodo di conservazione, concordato contrattualmente tra produttore dei documenti, responsabile della conservazione e Conservatore, viene avviata la procedura di Scarto concordata, con la produzione del Pacchetti di Scarto e la verbalizzazione

dello scarto e della chiusura del servizio. Prima dell'avvio dello scarto e della procedura di chiusura del Servizio, che si conclude con una verbalizzazione dell'attività, viene comunicato al produttore l'avvio dello scarto entro 30 gg al fine di fornirgli un periodo transitorio per richiedere formalmente l'estensione (prolungamento) del periodo di conservazione;

- Infine, in tutte le predette fasi del servizio di conservazione ***e-signum*** ed in generale in tutte le attività in carico ad un Conservatore è necessario garantire la Gestione dei sistemi informativi e della sicurezza a supporto del servizio; tale obiettivo viene perseguito dall'organizzazione Marno attraverso la definizione di compiti, ruoli e responsabilità come descritto nel presente manuale, attraverso verifiche ed audit periodici e tramite l'ausilio di strumenti per il controllo ed il monitoraggio. Le procedure definite all'interno del sistema di gestione della sicurezza (ISO 27001) e della qualità aziendale (ISO 9001) sono gli strumenti primari anche ai fini dell'analisi del rischio, della pianificazione e quindi ai fini dell'adozione di misure per la prevenzione, la manutenzione ed il miglioramento continuo del servizio.

- attività proprie di gestione dei sistemi informativi:
  - la conduzione e la manutenzione del sistema di conservazione è demandata al Responsabile dei Sistemi Informativi per la conservazione per quanto attiene alla gestione dell'esercizio della componenti hardware e software mentre al Responsabile dello Sviluppo e manutenzione del Sistema di Conservazione per il Coordinamento dello sviluppo e della manutenzione delle componenti;
  - il monitoraggio del sistema di conservazione inteso come l'attenzione dedicata al mantenimento del livello di sevizio (SLA) concordato con il produttore è attuato dal Responsabile dei Sistemi informativi;
  - lo change management, per quanto riguarda una possibile evoluzione tecnologica hardware e software oppure in attinenza ad eventuali migrazioni verso nuove piattaforme tecnologiche, è gestito dal Responsabile sviluppo e manutenzione;
  - l'Azienda Marno, al fine di mantenere la conformità alla normativa e agli standard di riferimento, si è sottoposta ad audit di gap analysis condotto da esperti in materia di sicurezza del sistema e, più specificatamente, di conservazione orientata in particolar modo a documenti della Pubblica Amministrazione e Società dello Stato; in aggiunta ha aderito ad un'importante Associazione di categoria (ANORC) onde poter fruire, oltre ad opportunità formative, anche a news letters sulla normativa di riferimento e su altri aspetti che possono rappresentare novità di impatto sull'attuale Sistema di Conservazione.

Torna al Sommario

6 OGGETTI SOTTOPOSTI A CONSERVAZIONE

Segue una descrizione delle tipologie degli oggetti e dei pacchetti in essi contenuti sottoposti a conservazione.

6.1 Oggetti conservati

6.1.1 Ambito degli oggetti inviati in conservazione

Attualmente vengono inviati in conservazione i documenti sanitari ed amministrativi digitalizzati dal personale Marno srl, afferenti a vari presidi ospedalieri.

Torna al Sommario

6.1.2 Formati utilizzati

Vengono accettate le tipologie di file ai sensi dell'allegato 2 al DPCM 3 dicembre 2013, recante "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":

Per i dettagli,concordati con il soggetto Produttore, si faccia riferimento a quanto descritto nell'allegato "Specificità del contratto".

Torna al Sommario

6.1.3 Metadati

I metadati dei documenti sanitari ed amministrativi riportati nel PdV sono elencati nella tabella riportata nel documento "specificità di contratto".

Torna al Sommario

6.2 Pacchetto di versamento

Una volta effettuato il processo di tipizzazione, i dati risultanti vengono inseriti nel database, andando così a completare l'intera gamma di metadati associati al fascicolo e ad ogni singolo documento digitale che la compone. Ogni singolo documento digitale è quindi corredato di una serie di informazioni che ne stabiliscono il contesto, la tipologia, la natura, la provenienza.

A questo punto il fascicolo è pronto per essere validato secondo la metodologia riportata nel documento "specificità di contratto".

- Il pacchetto di versamento consiste in un file in formato XML; questo file, auto consistente, contiene le informazioni di contenuto e di identificazione: i dati digitali risultanti dalla scansione e tutti i metadati informativi ad essi associati.

A seconda della specificità di contratto i pacchetti di versamento così prodotti vengono immessi nel sistema di conservazione secondo una delle seguenti modalità:

- Periodicamente prelevati da operatori di Marno S.r.l , copiati su supporti magnetici e portati sui sistemi di Marno per il processo di conservazione;
- Inviati tramite SFTP;
- Inviati tramite web services con protocollo HTTPS;

Lo schema XML dei pacchetti di versamento è riportato nel documento "specificità di contratto".

Torna al Sommario

6.3 Pacchetto di archiviazione

Una volta effettuata correttamente l'acquisizione dei Pacchetti di Versamento (vedi paragrafo 7.1), vengono creati i pacchetti di conservazione, secondo la sintassi prevista dalla standard UniSincro 11386. Processi automatizzati controllano periodicamente lo stato dei pacchetti di versamento, mediante analisi del rapporto di versamento, e, a partire da essi, generano per il contratto in oggetto i pacchetti di archiviazione. Ogni pacchetto di archiviazione corrisponde al singolo fascicolo adesso fascicolo informatico ed ogni foglio scansionato e tipizzato costituisce un documento informatico facente parte del fascicolo.

Il pacchetto di archiviazione è composto da:

- I metadati di ogni documento facente parte del fascicolo, nonché i metadati del fascicolo stesso. Vengono inseriti in un apposito database relazionale ridondato;
- I documenti digitali,conservati in appositi storage, consistenti in moduli NAS ridondati;
- Un Indice di conservazione del pacchetto. Tale Idc consiste in un file XML che riferisce i documenti ed i metadati, raggruppati secondo la logica stabilità in base al dominio applicativo, e strutturato secondo lo standard UniSincro 11386. Anche l'Idcviene salvato nei NAS ridondati.

Il pacchetto di archiviazione viene formato con firma sicura e marca temporale, apposta secondo l'RFC 161.

Il formato dell'Indice di conservazione segue le regole sintattiche dello standard UniSincro 11386, esteso, secondo la possibilità offerta dallo standard, con metadati peculiari del dominio applicativo dei fascicoli informatici.

Lo schema xsd relativo a tale dominio che va ad estendere UniSincro, è riportato nel documento "specificità di contratto".

I pacchetti di archiviazione sono conservati in due siti ridondati, come da manuale.

Torna al Sommario

6.4 Pacchetto di distribuzione

Il pacchetto di distribuzione è un duplicato del pacchetto di archiviazione. Il reperimento del pacchetto di distribuzione da parte di un consumatore può avvenire mediante due differenti modalità. Il sistema di conservazione è in grado di trovare e restituire gli oggetti desiderati in risposta alle richieste dell'utente: sia che si tratti di persone fisiche che, debitamente accreditate, si connettono al portale web; sia che si tratti di sistemi che, sempre previo accreditamento, si collegano al sistema in un'ottica di interoperabilità mediante web services stabiliti in fase di contratto. L'interfaccia tra il sistema di conservazione e i consumatori, indipendentemente dalla loro natura, è in grado di:

- accettare richieste semplici o complesse su gli oggetti e i loro metadati,
- indicare lo stato e la struttura degli oggetti e fornire l'informazione richiesta.
- Effettuare una ricerca puntuale accedendo al blocco di gestione dati e restituire informazioni aggregate (insieme di record);

L'utente sarà in grado di generare un pacchetto di distribuzione in base a ricerche e metodi contrattualizzati, e, dopo la verifica di congruità, può apporvi la firma digitale per conformità. Il PdD è composto come segue:

- Il file XML dell'Indice di conservazione, strutturato secondo lo standard UniSincro, contenente gli oggetti digitali ed i relativi metadati del fascicolo informatico e dei documento che ne fanno parte;
- Gli oggetti digitali;

Come detto, per ogni richiesta, il sistema verifica che l'utente abbia diritto di ricevere quello che ha richiesto e, in tal caso, autorizza il rilascio dell'informazione. Delle ricevute di transazione sono generate e conservate, a fini statistici e di controllo.

Le eventuali personalizzazioni di tali pacchetti, specifiche di un contratto, sono descritte nell'allegato "Specificità del contratto".

Torna al Sommario

7 IL PROCESSO DI CONSERVAZIONE

Descrizione generale, eventualmente corredata da schemi e rappresentazioni grafiche, delle diverse funzioni relative al processo di conservazione, quali:

- modalità di acquisizione dei pacchetti di versamento per la loro presa in carico
- verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti
- accettazione dei pacchetti di versamento e generazione del rapporto di versamento e di presa in carico
- rifiuto dei pacchetti di versamento e generazione del rapporto di versamento con evidenziazione delle anomalie
- preparazione e gestione del pacchetto di archiviazione
- preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione
- produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti
- scarto dei pacchetti di archiviazione
- predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori.
- Controlli sistematici su integrità e leggibilità
- Controlli sistematici su obsolescenza formati

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

I PdV vengono immessi nel sistema di conservazione mediante una delle tre seguenti modalità, a seconda della specificità di contratto:

- trasporto dal luogo della scansione agli uffici di Marno s.r.l. Operatori di Marno prelevano i PdV da supporto magnetico e li portano presso i locali Marno S.r.l., dove un apposito client effettua l'immissione sul PdV;
- invio tramite SFTP dal luogo di scansione ai sistemi Marno. Il collegamento FTP avviene senza nessun tipo di crittazione e questo potrebbe favorire attacchi hacker e intromissione nella visualizzazione di dati sensibili. Per questo Marno adotta SFTP, un protocollo di trasferimento file basato sul SSH (Secure Shell), un sistema di accesso sicuro e crittografato ai server remoti. A differenza del collegamento FTP e del suo omologo FTPS su certificato SSL, il collegamento SFTP avviene sulla porta 22 e non usa due canali separati per l'invio dei comandi e dei dati ed entrambi le istruzioni

vengono trasferiti lungo un'unica connessione, in pacchetti formattati e crittografati in modo speciale. In questo modo, il collegamento SFTP risulta intrinsecamente sicuro, non necessita di una doppia connessione (in quanto utilizza la stessa per dati e comandi) ed è anche più veloce del protocollo FTP/S, dato che gestisce meno dati con una semplice connessione in-line;

- invio tramite web services su HTTPS con autenticazione. L'utilizzo di una connessione HTTPS è in grado di garantire la riservatezza dei dati trasmessi criptando con SSL i messaggi scambiati con il Web service. Questo è indispensabile dato che si potrebbero trattare informazioni a cui non possiamo attribuire un carattere pubblico.

L'utilizzo di HTTPS richiede un certificato approvato da apposite autorità.

Marno si appoggia alla CA Comodo.

7.1.1 Il flusso di lavoro con gli Enterprise pattern

La funzione immissione comprende meccanismi che le permettono di confermare che i file ricevuti e i loro metadati siano completi e senza errori. Tali meccanismi sono elencati di seguito e orchestrati in un flusso di lavoro realizzato adottando gli integration pattern [IP] che permettono di organizzare e mettere in collaborazione una serie di entità specializzate in un singolo compito, orchestrandole in un workflow la cui logica può evolvere nel tempo.

L'implementazione dei pattern è stata realizzata utilizzando appositi moduli dedicati alla risoluzione di problemi legati all'integrazione ed ai flussi di lavoro. Di fatto viene utilizzata una sintassi specifica XML per definire i workflow. Risulta quindi immediato configurare le regole di routing e di mediation: in tal modo è possibile realizzare rapidamente workflow a partire da componenti presenti nel framework o sviluppati ad hoc.

Torna al Sommario

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

7.2.1 Verifica delle credenziali del produttore

Il primo controllo viene effettuato sul produttore. Nello specifico, vengono esaminati:

- L'IP della macchina che ha invocato il pacchetto di versamento. Tale IP deve essere presente in una apposita tabella detenuta dal sistema di conservazione. Questa tabella può venire alimentata in accordo con i fornitori, nel caso in cui le macchine che provano ad effettuare il versamento siano ubicate presso di loro. Le macchine che possono effettuare un versamento sono quindi tutte censite;

- Le credenziali presentate al momento del versamento. La connessione è criptata con crittografia a 256 bit ed il certificato del server rilasciato da authority certificata; il produttore deve comunque presentare username e password, queste debbono corrispondere a quelle assegnate alla macchina inviante.

Nel caso in cui i controlli di cui sopra falliscano, il pacchetto viene rifiutato con messaggio descrivente la motivazione. Il pacchetto viene comunque conservato e viene registrato che c'è stato un tentativo di versamento; tale registrazione comprende tutti i dati ed è consultabile dal proprio rapporto di versamento.

Torna al Sommario

7.2.2 Validazione sintattica del pacchetto di versamento

Gli accordi intercorrono mediante descrittori di servizi web in formato WSDL, esposti dal sistema di conservazione e approntati in fase di amministrazione con il cliente produttore. Questi descrittori variano a seconda dell'ambito applicativo e della comunità di riferimento cui i documenti si rivolgono.

In questa fase il pacchetto di versamento viene sottoposto a validazione formale mediante l'applicazione di un XML schema. Nel caso in cui la validazione sintattica fallisca, il pacchetto viene respinto al produttore con messaggio descrivente la motivazione. Il pacchetto viene comunque conservato e viene generato e registrato un rapporto di anomalia dichiarante che c'è stato un tentativo di versamento fallito a causa di un formato errato del PdV, tale registrazione comprende l'IP chiamante, il pacchetto in oggetto e la descrizione dell'errore sintattico occorso.

Torna al Sommario

7.2.3 Generazione e restituzione al produttore del rapporto di presa in carico

Una volta appurata l'identità del produttore e la correttezza del PdV,questo viene analizzato per produrre un rapporto di presa in carico, che ne dettaglia il contenuto:

- Hash del PdV;
- Mimetype del PdV;
- Lunghezza in Byte del PdV;
- Data e ora generazione del PdV;
- Numero di documenti e fascicolo che lo compongono.

Il rapporto di presa in carico viene restituito al produttore e, in base agli accordi contrattuali, viene immesso nel flusso di presa in carico.

Torna al Sommario

7.2.4 Verifica di eventuale firma

Viene effettuato il controllo della firma, nel caso in cui le specifiche di contratto prevedano che il pacchetto di versamento debba essere firmato da una persona preposta. Nel caso in cui il controllo della firma fallisca (firma assente o non rispondente), il pacchetto viene rifiutato e nel rapporto di versamento sarà possibile comprenderne la motivazione.

Il pacchetto viene conservato e viene generato e registrato un rapporto di anomalia descrivente il tentativo di versamento fallito per firma assente o non corrispondente alla persona prevista. Tale registrazione comprende l'ip chiamante, il pacchetto la descrizione del fallimento.

Torna al Sommario

7.2.5 Verifica codice IPA

In questo stadio, qualora il produttore del pacchetto di versamento fosse un ente pubblico, viene controllato il codice IPA (Indice delle Pubbliche Amministrazioni) contenuto nel pacchetto con quelli presenti in archivio. Se nessuna corrispondenza viene trovata, viene effettuato un lookup al servizio pubblico LDAP fornito da IPA presso il quale l'applicazione è registrata. In caso di ritorno positivo, il pacchetto di versamento passa allo stadio successivo.

Torna al Sommario

7.2.6 Verifica presenza Virus

Questa fase prevede il controllo di presenza di virus all'interno dei documenti contenuti nel pacchetto di versamento. Ognuno di questi (codificato in base 64) viene inviato ad un server aziendale che eroga il servizio di controllo antivirus. Il documento viene esaminato e viene tornato un responso sulla presenza o meno di virus. Il server utilizza ClamAntiVirus [ClamAV],l'antivirus open source più diffuso per sistemi operativi derivati da Unix. Il server effettua con continuità l'aggiornamento automatico del database dei virus dall'archivio centralizzato di CLAM. l database dei virus viene aggiornato anche più volte in un giorno. Il team di ClamAV aggiorna i database dei virus in maniera regolare e quasi immediatamente dopo la scoperta di un nuovo virus (o di una nuova variante). Nel caso in cui venga riscontrata la presenza di virus in almeno uno dei documenti contenuti nel pacchetto di versamento, questo viene. Il pacchetto viene comunque conservato in uno storage di quarantena e viene generato e registrato un rapporto di anomalia descrivente il tentativo di versamento fallito a causa della presenza di virus, con descrizione del virus riscontrato. Tale registrazione comprende l'ip chiamante, il pacchetto in oggetto e la descrizione del fallimento.

Torna al Sommario

Il flusso delle verifiche è illustrato nell'immagine seguente

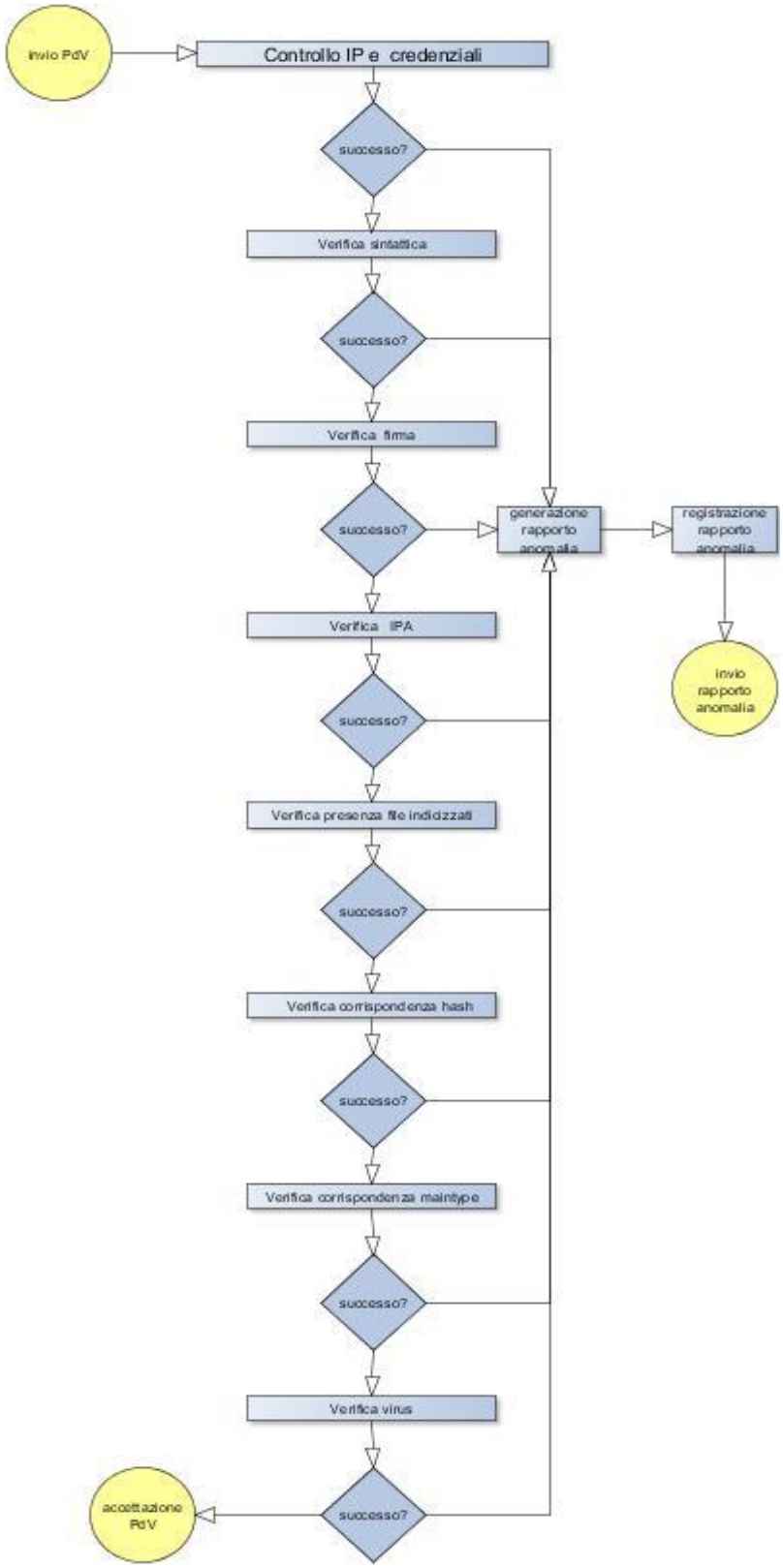

Figura 2 - flusso delle verifiche

Torna al Sommario

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

7.3.1 Flusso di accettazione

L'accettazione dei pacchetti di versamento prevede i seguenti passi:

- Lettura del pacchetto. In genere il PdV è in formato XML. Vengono adottati, per la lettura, degli appositi parserStax, che garantiscono alte performance in termini di velocità e ridotti consumi di memoria. In questo modo risulta possibile analizzare velocemente anche pacchetti composti, eventualmente, da diversi GigaByte;
- estrazione dei metadati e loro inserimento in database relazionali ridondati (come illustrato nei capitoli successivi). I metadati specifici del dominio applicativo vengono aggiunti a quelli previsti dalle regole tecniche di Agid;
- estrazione dei documenti digitali ed allocazione in appositi storage ridondati (come illustrato nei capitoli successivi);
- Calcolo dell'impronta di ogni documento;
- calcolo delle significant properties di ogni documento. Vengono estratte le proprietà significative degli oggetti digitali da conservare per rendere possibile la futura rappresentazione dell'oggetto, o una futura, eventuale, conversione in formato diverso.

Torna al Sommario

7.3.2 Generazione rapporto di versamento

Alla fine del ciclo viene effettuata in modo automatico la generazione automatica del rapporto di versamento relativo ad ogni pacchetto di versamento, univocamente identificato dal sistema di conservazione nei passi precedenti. Il rapporto di versamento viene sottoscritto con firma digitale apposta dal Responsabile del Servizio di Conservazione e inserito nel sistema di conservazione stesso;

Eventualmente viene anche effettuata generazione automatica del rapporto di anomalia, relativo ad ogni pacchetto di versamento, nel caso in cui un documento non passi correttamente attraverso il flusso descritto nel paragrafo precedente.

Viene effettuato il salvataggio sulla base dati del rapporto di versamento, cui viene associato un identificativo univoco. Questo il contenuto informativo del rapporto di versamento:

- Riferimento al PdV;
- Date e ora del trattamento del PdV;
- Riferimento ad ogni documento inserito in conservazione.

Ogni passo sopra descritto – così come ogni attività svolta all'interno del sistema di conservazione - viene registrato in appositi log, così strutturati:

- Applicativo che lo ha generato;
- IP della macchina su cui è installato l'applicativo;
- Data e ora del log;
- Nome della specifica componente dell'applicativo che lo ha generato;
- Livello di log:
- Messaggio dettagliato di log

Il messaggio cambia struttura a seconda della tipologia di attività.

I log vengono periodicamente mandati in conservazione.

Torna al Sommario

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

Nel caso di rifiuto totale o parziale di un pacchetto di versamento, viene generato, come detto, un rapporto di anomalia con il seguente contenuto informativo:

- Riferimento al PdV;
- Date e ora del trattamento del PdV;
- Motivo del rifiuto totale del PdV, oppure:
- Per ogni documento rifiutato:
  - Riferimento al documento;
  - Motivo del rifiuto;

Il rapporto di anomalia viene automaticamente sottoscritto con firma digitale apposta dal Responsabile del Servizio di Conservazione e inserito nel sistema di conservazione.

Torna al Sommario

7.5 Preparazione e gestione del pacchetto di archiviazione

Il pacchetto di archiviazione viene generato a partire dai pacchetti di versamento. La corrispondenza tra PdV e PdA varia da contratto a contratto. Uno o più pacchetti di versamento possono andare a comporre un pacchetto di archiviazione. Procedure opportunamente schedulate effettuano il controllo dei report di versamento e, a partire dal risultato di questi, generano i pacchetti di archiviazione.

I metadati applicativi vengono aggiunti ai metadati riportati dall'allegato delle regole tecniche.

Un PdA è così composto:

- Indice di conservazione;
- Documenti riferiti dall' Indice di conservazione.

L'indice di conservazione (IdC) che riassume tutto il pacchetto di archiviazione. Si tratta di un file XML strutturato secondo lo standard SinCRO 11386:2010. Successivamente alla generazione, viene firmato digitalmente e, al momento della firma, un riferimento temporale viene apposto al documento firmato sotto forma di una Marca Temporale rilasciata da una entità che garantisce una data e ora certe (TSA - Time Stamp Authority). Il sistema di conservazione di Marno implementa lo standard internazionale RFC-3161 per le marche temporali, implementato obbligatoriamente da tutte le Time Stamp Authorities italiane.

L'Indice di conservazione viene firmato dal Responsabile del Servizio di Conservazione e dal Responsabile dell'ente di competenza. In questo modo viene garantita l'integrità delle informazioni, dato che l'IdC contiene anche i checksum ed i riferimenti (oltre ai metadati applicativi) di ogni file che lo compone. L'integrità dell'IdC viene in seguito appurata periodicamente da apposite procedure schedulate.

Eventuali modificazioni rispetto alle informazioni sopra riportate, preventivamente concordate con il soggetto Produttore, saranno descritte nell'allegato "Specificità del contratto".

Torna al Sommario

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

Il pacchetto di distribuzione è un duplicato del pacchetto di archiviazione. Il pacchetto di distribuzione è così assemblato:

- Indice di Conservazione;
- Documenti digitali riferiti dall'indice di conservazione;
- Il reperimento del pacchetto di distribuzione da parte di un consumatore può avvenire mediante due differenti modalità. Il sistema di conservazione è in grado di trovare e restituire gli oggetti desiderati in risposta alle richieste dell'utente: sia che si tratti di persone fisiche che, debitamente accreditate, si connettono al portale web; sia che si tratti di sistemi che, sempre previo accreditamento, si collegano al sistema in un'ottica di interoperabilità mediante web services stabiliti in fase di contratto.

Il pacchetto di distribuzione viene generato a partire dal pacchetto di archiviazione.

Ogni consumatore accreditato può scaricare un file ISO contenente il pacchetto di distribuzione per poterlo masterizzare su supporto ottico. All'immagine ISO può essere allegato un apposito software di visualizzazione da utilizzarsi per la visualizzazione/navigazione del pacchetto.

Eventuali modificazioni rispetto alle informazioni sopra riportate, preventivamente concordate con il soggetto Produttore, saranno descritte nell'allegato "Specificità del contratto".

Torna al Sommario

7.7 Produzione di duplicati e copie informatiche

Il pubblico ufficiale può collegarsi al sistema e apporre a sua volta una firma digitale con marca temporale sul pacchetto di distribuzione. La firma entra nel sistema di conservazione insieme al log che registra tutti i passi operati dal pubblico ufficiale sul sistema.

La firma può essere apposta tramite applet, tool, mezzi concordati contrattualmente.

Torna al Sommario

7.8 Scarto dei pacchetti di archiviazione

Procedure opportunamente schedulate effettuano il controllo dei pacchetti di conservazione e, se le normative riferite al dominio applicativo interessato da un singolo PdA ne consentono lo scarto, segnalano al Responsabile del Servizio di Conservazione la possibilità di operare lo scarto del pacchetto intervenendo sull'interfaccia del sistema applicativo.

Anche in questo caso - come per ogni attività svolta all'interno del sistema di conservazione, sia essa effettuata in automatico o da utente – tale scarto viene registrato in un log gestito.

I dati del log comprendono:

- Identificativo di chi ha operato lo scarto;
- Identificativo del PdA scartato;
- Data e ora in cui lo scarto è stato effettuato.

Eventuali procedure specifiche, concordate con il soggetto Produttore, saranno descritte nell'allegato "Specificità del contratto".

Torna al Sommario

7.9 Predisposizione di misure per garantire l'interoperabilità e trasferibilità verso altri

Come descritto in precedenza, il pacchetto di distribuzione coincide col pacchetto di archiviazione eventualmente corredato da un software per la visualizzazione .Quindi abbiamo un insieme di documenti riferiti da un file XML strutturato secondo gli standard UniSincro.

L'obiettivo prioritario di UNI SInCRO e' proprio quello di definire la struttura dell'insieme dei dati a supporto del processo di conservazione. Individuando gli elementi informativi necessari all' Indice di Conservazione (il cosiddetto 'file di chiusura'), e descrivendone sia la semantica sia l'articolazione, arriva a consentire agli operatori di utilizzare una struttura-dati condivisa in modo da raggiungere un alto grado d'interoperabilità nei processi di migrazione, grazie all'adozione dello Schema XML appositamente elaborato e reso disponibile nello standard ed implementato dal sistema di conservazione di Marno.

Il sistema di conservazione è in grado, per ogni dominio applicativo trattato, di ricevere pacchetti di versamento con il formato stabilito dalla specificità di contratto e con formato identico a quello dei pacchetti di archiviazione.

Torna al Sommario

8 IL SISTEMA DI CONSERVAZIONE

In questo capitolo segue una descrizione del sistema di conservazione, comprensivo di tutte le componenti logiche, tecnologiche e fisiche seguita da una descrizione delle procedure di gestione e di evoluzione delle medesime.

8.1 Componenti Logiche

Le entità funzionali relative al Sistema di Conservazione ed al suo funzionamento possono essere riassunte nel modello OAIS sotto rappresentato.

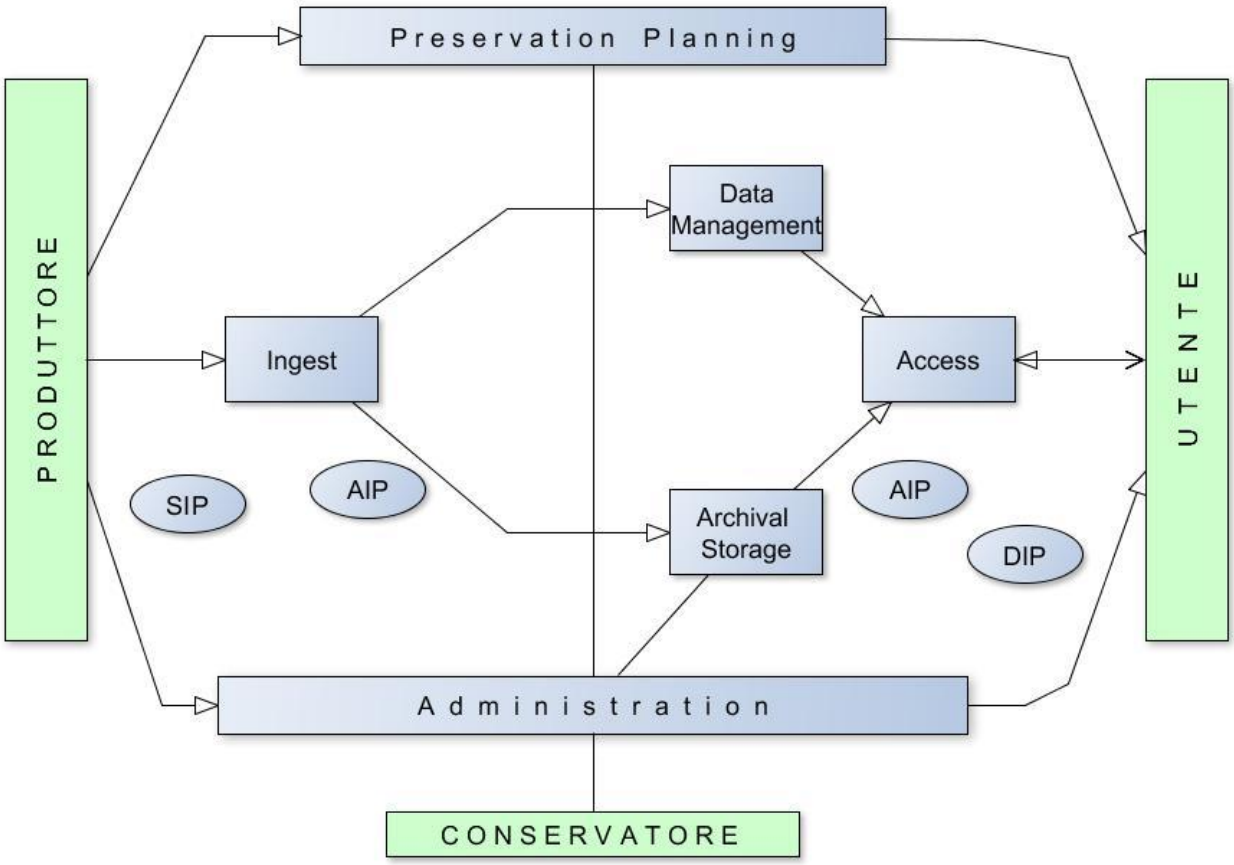

Figura 3 - Modello OAIS

La Pianificazione dell'Archiviazione si compone a) nella formulazione di raccomandazioni in relazione agli standard ed alla politica d'archiviazione a seguito degli sviluppi tecnologici, b) della sorveglianza degli sforzi fatti in materia di archiviazione, c) nella formulazione di raccomandazioni per il mantenimento della leggibilità dell'informazione stoccata e, in ultimo, d) nella pianificazione delle migrazioni e dei processi di copiatura.

La presa in carico dei dati si articola attraverso le fasi a) presa in carico dei SIP (Submission Information Package) creati dal produttore, b) dal controllo dell'integralità e dell'integrità, c) dalla trasformazione dei SIP in AIP (Archival Information Package), d) dall'estrazione dell'informazione descrittiva per la base dati di ricerca, e) dalla trasmissione degli AIP alla memoria di archivio ed infine dalla comunicazione al Data Management.

La Gestione dei Dati si compone di una prima fase relativa alla gestione delle informazioni descrittive (base dati) che identificano i fondi d'archivio ed i documenti nonché di altri dati necessari per l'utilizzazione dei materiali d'archivio e di una seconda fase che consiste nella ricezione e trattamento delle richieste (query) provenienti dall'utenza.

La parte relativa alla Memoria d'Archivio si sviluppa attraverso la conservazione e manutenzione degli AIP, alla realizzazione dei backup, al controllo regolare dell'integrità dei dati, ai meccanismi di ripristino (restore = funzione inversa di quella di backup) in caso di urgenza ed alla trasmissione degli AIP ad Access per la relativa utilizzazione.

La funzione logica di Access (esibizione) consente di a) interfacciare l'utente, b) effettuare la ricerca (query) e generare delle risposte contenenti la descrizione degli AIP e le informazioni sulla loro disponibilità, c) ricevere e trattare le richieste di dati con successiva trasformazione degli AIP in DIP (Dissemination Information Package) oltre alla fornitura dei DIP agli utenti e, in ultimo, d) la garanzia del rispetto dei diritti di accesso.

L'altra funzione di Administration (amministrazione) consente di a) effettuare il controllo dei processi globali di OAIS e delle sue relazioni esterne, b) configurare tutto l'hardware ed il software necessario e c) attribuire e gestire ogni forma di diritto di accesso.

La figura di pagina seguente rappresenta un flow chart del modello OAIS prima rappresentato.

In fase di acquisizione del pacchetto di versamento si procede ad una verifica della consistenza del pacchetto stesso e ne viene data evidenza al produttore mediante invio di specifico rapporto. Segue una verifica del pacchetto in fase di versamento che tiene conto della conformità alle specifiche contrattuali attinenti la tipologia dei documenti da conservare oltre alle modalità con cui il pacchetto viene predisposto. Il pacchetto potrà quindi essere rifiutato o versato parzialmente in funzione del buon esito dei controlli prima effettuati. Al termine delle operazioni viene generato un rapporto di versamento che contiene le informazioni relative a quanto mandiamo in conservazione.

Il modello OAIS schematizzato in figura 3 può essere rappresentato dal flusso di figura seguente:

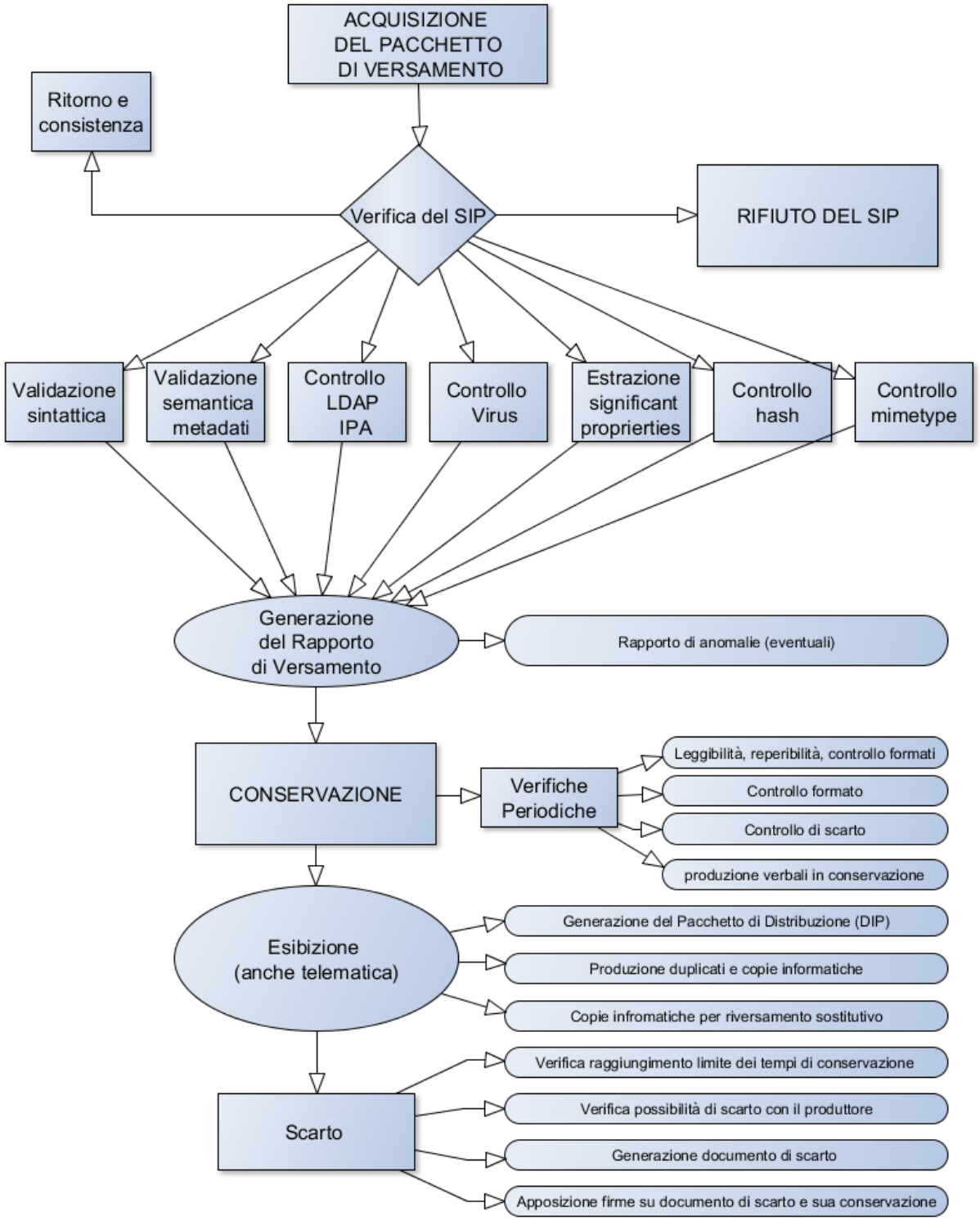

Figura 4 - Flusso OAIS

Torna al Sommario

8.2 Componenti Tecnologiche

Di seguito è illustrato la schema delle componenti tecnologiche del sistema di conservazione.

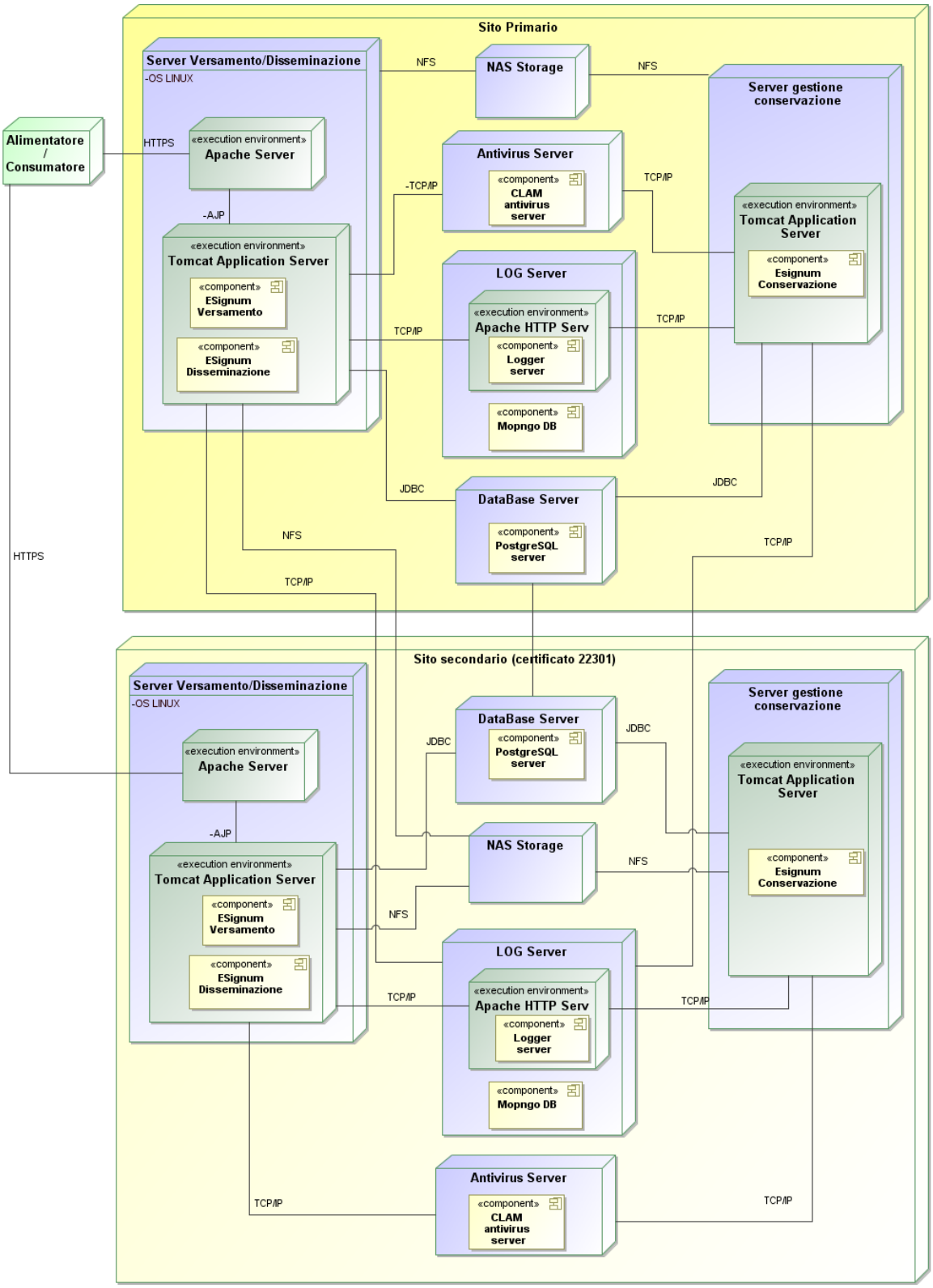

Figura 5 - Componenti Tecnologiche

Torna al Sommario

8.3 Componenti Fisiche

8.3.1 Sito primario

- Server dedicato all'alimentazione ed alla disseminazione.

  Sistema Linux contenente :

  - Apache HTTP server. Accessibile unicamente via HTTPS. Unica porta di accesso al sistema. Questo comunica via AJP con l'application server;
  - Tomcat Application Server funzionante su Oracle JDK. Contiene i moduli per l'accettazione dei pacchetti di versamento e per la disseminazione realizzati utilizzando: Java Oracle + Spring (Spring WS, Spring integration, Spring batch. Spring data).
    - Il modulo di versamento riversa i documenti binari sul *NAS Storage* primario e, in tempo reale, sul *NAS Storage* del sito di disaster recovery. Entrambi accessibili mediante il protocollo Network File System;
    - I dati vengono memorizzati con protocollo JDBC sul *Database Server* contenente RDBMS PostgreSQL;
    - Tutti i log vengono inviati in tempo reale sia al *Log Server* principale che *al Log Server* del sito di disaster recovery;
    - Ogni anomalia viene inviata ad una lista di indirizzi mail in tempo reale;
    - Ogni documento è controllato da virus mediante l'ausilio del *Antivirus server*.

- Database server

  Sistema Linux contenente motore RDBMS PostgreSQL. La macchina non è accessibile dall'esterno, non avendo un IP pubblico.

  - Il motore database è configurato per essere accessibile, tramite credenziali, solamente da un numero limitato di IP, corrispondenti a quelli degli applicativi che utilizzano i dati ed a quelli di alcuni personal di amministrazione;
  - Il motore database è configurato in maniera master-slave con quello del sito di disaster recovery. In questo modo l'allineamento dei dati avviene in tempo reale e non mediante backup schedulati, in modo da non avere perdite di dati;
  - Vengono comunque schedulati backup notturni del database.

- NAS Storage server.

  Entità di storage costituite da batterie di NAS QNAP con le seguenti caratteristiche:

  - Sistema operativo ridondante su architettura DOM per impedire l'improvvisa perdita dei dati conseguente al danneggiamento del File System. Due sistemi operativi su una Flash DOM (Disk On Module, memoria flash non volatile ad alta affidabilità) che fanno il boot di sistema alternativamente ad ogni startup. Se un system si danneggia, il NAS utilizzerà l'altro per l'avvio ed allo stesso tempo il system danneggiato verrà ripristinato da quello funzionante.

  - Avanzata gestione della configurazione RAID configurarsi in RAID livello 6, in questo modo il NAS può continuare a lavorare senza perdita di dati anche con la rottura contemporanea di due dischi.

- Log Server

  Sistema Linux contenente :

  - una piattaforma per il log centralizzato. Tutti gli applicativi inviano in tempo reale i log ai Log server in ascolto: sia a quello del sito primario, sia a quello del sito secondario. Tutti i log sono conservati in un database Elasticsearch;

  - Un cruscotto web, accessibile con credenziali, per il controllo, l'interrogazione e l'aggregazione dei log accessibili per applicativo, ip, livello di gravità etc.

- Antivirus server

  Sistema Linux contenente:

  - ClamAntiVirus (ClamAV) server. Antivirus per i sistemi operativi Unix/Linux. Utilizzato dai dagli applicativi per processare file singoli.:

    - Un demone multi-thread flessibile e scalabile effettua l'analisi dei file sottoposti;

    - Processo schedulato per l'aggiornamento automatico del database con le definizioni dei virus.

Torna al Sommario

8.3.2 Sito secondario di disaster recovery, certificato 22301:

Sito secondario di disaster recovery, certificato 22301:

- Server dedicato alla alimentazione ed alla disseminazione.

  Sistema Linux contenente :

- Apache HTTP server. Accessibile unicamente via HTTPS. Unica porta di accesso al sistema. Questo comunica via AJP con l'application server;
- TomcatApplication Server funzionante su Oracle JDK. Contiene i moduli per l'accettazione dei pacchetti di versamento e per la disseminazione, realizzati utilizzando: Java Oracle + Spring (Spring WS, Spring integration, Spring batch. Spring data). Il server si attiva solamente nel caso in cui il suo omologo nel sito primario non sia funzionante.
  - Il modulo di versamento riversa i documenti binari sul NAS Storage del sito di disaster recovery che viene acceduto mediante il protocollo Network File System;
  - I dati vengono memorizzati con protocollo JDBC sul Database Server del sito di disaster recovery contenente RDBMS PostgreSQL;
  - Tutti i log vengono inviati in tempo reale sia al Log Server principale che al Log Server del sito di disaster recovery;
  - Ogni anomalia viene inviata ad una lista di indirizzi mail in tempo reale;
  - Ogni documento è controllato da virus mediante l'ausilio del Antivirus server.

- Database server

  Sistema Linux contenente motore RDBMSPostgreSQL. La macchina non è accessibile dall'esterno, non avendo un IP pubblico.

  - Il motore database è configurato per essere accessibile, tramite credenziali, solamente da un numero limitato di IP, corrispondenti a quelli degli applicativi che utilizzano i dati, a quello del database master ed a quelli di alcuni pc di amministrazione;
  - Il motore database è configurato in maniera master-slave con quello del sito di disaster recovery. Viene aggiornato in tempo reale e non mediante backup schedulati, in modo da non avere perdita di dati;
  - Vengono comunque schedulati backup notturni del database.

- NAS Storage server.

  Entità di storage costituite da batterie di NAS QNAP con le seguenti caratteristiche:

  - Sistema operativo ridondante su architettura DOM per impedire l'improvvisa perdita dei dati conseguente al danneggiamento del File System. Due sistemi operativi su una Flash DOM (Disk On Module, memoria flash non volatile ad alta affidabilità) che fanno il boot di sistema alternativamente ad ogni startup. Se

un system si danneggia, il NAS utilizzerà l'altro per l'avvio ed allo stesso tempo il system danneggiato verrà ripristinato da quello funzionante.

- Avanzata gestione della configurazione RAID configurarsi in RAID livello 6, in questo modo il NAS può continuare a lavorare senza perdita di dati anche con la rottura contemporanea di due dischi.

- Log Server

  Sistema Linux contenente :

  - una piattaforma per il log centralizzato Tutti gli applicativi, anche quelli del sito primario, inviano in tempo reale i log al server in ascolto. Tutti i log sono conservati in un database Elasticsearch;

  - Un cruscotto web, accessibile con credenziali, per il controllo, l'interrogazione e l'aggregazione dei log. Log accessibili per applicativo, ip, livello di gravità etc.

- Antivirus server

  Sistema Linux contenente:

  - ClamAntiVirus (ClamAV) server. Antivirus per i sistemi operativi Unix/Linux. Utilizzato dai dagli applicativi per processare file singoli:

    - Un demone multi-thread flessibile e scalabile effettua l'analisi dei file sottoposti;

    - Processo schedulato per l'aggiornamento automatico del database con le definizioni dei virus.

  In caso di blocco del sito primario, subentra il sito secondario.

Torna al Sommario

8.4 Procedure di gestione e di evoluzione

Descrizione delle procedure di gestione e di evoluzione, e della relativa documentazione prevista,inerenti le componenti logiche,tecnologiche e fisiche del sistema di conservazione relativamente a:

8.4.1 Conduzione e manutenzione del sistema di conservazione.

Il Sistema di Conservazione fa parte di un contesto assai più ampio che è stato precedentemente implementato per il trattamento documentale e che si è evoluto in funzione di poter disporre di un ambiente idoneo in possesso dei requisiti richiesti dalle nuove regole tecniche; il Sistema è condotto da persone che dispongono dei requisiti necessari in termini di titoli, di esperienza maturata e di conoscenze acquisite per tale specificità; al fine di mantenere alta l'attenzione

verso qualsiasi tipo di nuova richiesta e/o implementazione cui il Sistema debba essere sottoposto, l'Azienda ha aderito all'associazione ANORC in qualità di Socio Sostenitore.

Per quanto riguarda la conduzione e la manutenzione del sistema l'Azienda ha acquisito tutte le certificazioni necessarie a garantire, nel tempo, un livello di funzionamento minimo garantito e scientificamente definito attraverso SLA (Service Level Agreement) stabilite contrattualmente ed eventuali OLA (Operational Level Agreement) concertate tra i vari gruppi operatori.

A fronte delle certificazioni prima accennate (oltre alla ISO 9001:2008 sono stati conseguiti gli schemi relativi alla ISO 20000-1:2011, alla ISO 27001:2005 e alla 22301:2012) l'Azienda ha implementato controlli relativi alla gestione della sicurezza che fanno capo al documento di Statement of applicability *(SOA versione 01 del 25 aprile 2013)* che stabilisce le modalità e la tempifica dei controlli stessi e precisamente:

- audit interni *(vedi PQS 8.1.1. Conduzione di Audit Interni)* condotti da personale esterno qualificato a garanzia dell'efficacia e dell'assenza di conflitto d'interessi;
- verifiche periodiche effettuate dai vari responsabili secondo quanto previsto alla voce "evidenze dei controlli eseguiti" nel documento SOA;
- implementazione delle azioni correttive a fronte di quanto riportato nei report rilasciati dagli enti di certificazione ed approfondimento accurato delle cause di tali rilievi;

Torna al Sommario

8.4.2 Gestione e conservazione dei log (anche in accordo con l'ente Produttore)

I log sono memorizzati all'interno del database. Ogni azione effettuata dal sistema corrisponde ad almeno un record. (Per approfondimenti sul formato dei log fare riferimento a quanto riportato nel paragrafo 9.1.4). Quotidianamente tali log vengono composti in un file XML che viene firmato dal Responsabile del Servizio della Conservazione e immesso nel sistema di conservazione.

Torna al Sommario

8.4.3 Monitoraggio del sistema di conservazione

Il monitoraggio del sistema di conservazione si concretizza nel controllo della corrispondenza tra gli hash contenuti nell'indice di conservazione e gli hash dei documenti riferiti calcolati a runtime, nel controllo delle significant properties e nella verifica dell'effettiva leggibilità dei documenti inseriti all'interno dei pacchetti di archiviazione mediante il software di visualizzazione assegnato, vedi procedura di riferimento *(PS 008 Monitoraggio in tempo reale dello stato dei Sistemi Informativi).*

Torna al Sommario

8.4.4 Change management

Al fine di garantire una continuità operativa l'Azienda ha implementato, per gli asset essenziali, altrettante BIA (Business Impact Analysis) che vengono periodicamente simulate con modalità

stabilite di volta in volta e monitorizzati gli effetti così prodotti; gli eventi configurabili in questa categoria sono, in ordine di frequenza di accadimento, i cambiamenti di software applicativo, di hardware periferico, di storage, di server ed, infine, di sistema informativo.

Ogni cambiamento viene effettuato e controllato con la regola del RFC (Request for Change) al fine di condividere e di garantire una corretta successione delle operazioni da effettuare; il tipo di RFC adottato in Azienda è il Trouble Ticketing.

Tale regola adottata è in grado di gestirne il processo ma, per una corretta evoluzione delle operazioni di change, per ciascun tipo evento, deve essere disponibile uno strumento che ne garantisca il buon fine; ed esempio, per tutti i cambiamenti attinenti alle modifiche e/o nuove implementazioni software, è stato definito un sistema di gestione in grado di mantenere il versioning del codice sorgente sviluppato. Tale metodologia consente di disporre, anche in modo condiviso, del sorgente corrispondente all'attuale versione oggetto del sw operante.

Il sistema di versionamento adottato è Subversion (http://subversion.apache.org); esso consente la completa tracciabilità cronologica delle modifiche appartate al codice sorgente, delle tipologie di modifiche e dell'indicazione del soggetto che le ha apportate. Ciascun file del progetto è dotato di una propria versione interna ed è controllato dal sistema di versionamento, vedi procedura di riferimento *(PS 006 Gestione del Change Management).*

Torna al Sommario

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

La normativa di riferimento, se pur assunta in modo volontario, risulta a tutti gli effetti come cogente, ed è inserita tra i documenti di origine esterna afferenti alla ISO 9001; come tale entra a far parte di una lista di norme i cui aggiornamenti obbediscono a precisi meccanismi definiti precedentemente e, oramai, validati.

La conformità alla normativa e agli standard di riferimento così aggiornati viene garantita da una serie di attività codificate a sistema ed, in particolare:

- attività di controllo secondo quanto previsto dal documento SOA a supporto della funzionalità del Sistema Informativo e di tutti gli altri aspetti non contemplati all'interno degli audit interni;
- audit interni secondo quanto previsto dalla ISO 20001-1:2011 per la qualità del servizio
- audit interni secondo quanto previsto dalla 22301:2012;
- audit interni secondo quanto previsto dalla 27001:2013;
- audit interni condotti secondo quanto previsto dalla check list fornita da AgID pianificati con la logica degli audit del Sistema ovvero tesi ad esaminare tutti gli aspetti almeno una volta l'anno o, più frequentemente, anche in funzione della loro criticità riscontrata in audit precedenti e/o non conformità riscontrate durante l'ultimo periodo di esercizio;

In particolare la verifica periodica della conformità legislativa piuttosto che agli standard di riferimento è dettata da quanto previsto nella procedura di riferimento del Sistema Integrato Qualità - Sicurezza - *PQS 4.2.1 Controllo Documenti del Sistema Qualità e della Sicurezza delle Informazioni e dei Documenti di Origine esterna.*

Torna al Sommario

9 MONITORAGGIO E CONTROLLI

9.1 Procedure di monitoraggio

Segue una descrizione delle procedure di monitoraggio del sistema di conservazione (comprensive dei relativi report e log) effettuate sul funzionamento del software applicativo e di sistema, nonché sulle componenti hardware, anche con l'obiettivo di valutare l'efficacia del sistema di conservazione.

9.1.1 Il server di log

Come descritto in precedenza, tutti i log vengono memorizzati all'interno del database. Ogni azione effettuata dal sistema corrisponde ad almeno un record. I log vengono inoltre inviati in tempo reale ad un server di log (anch'esso ridondato) in modo da poterne permettere la visione e l'analisi da un apposito cruscotto web.

Tutte le macchine del sistema di Log Analisi utilizzano il sistema operativo Linux della famiglia Ubuntu, in particolare il Server ricevente la versione n. 14. L'applicativo di log è GrayLog2, un software open source per la gestione log che vengono memorizzati nel database Elasticcsearch.

Si compone di:

- un server scritto in Java che accetta i messaggi syslog via TCP, UDP o AMQP e li memorizza nel database
- una piattaforma web che consente di gestire i messaggi di log dal browser web.

Il sistema di conservazione prevede quindi un server di log centralizzato ed un sistema di Analisi dei Log dinamico, scalabile e altamente portabile in grado di analizzare, in tempo reale, i messaggi che ogni componente è in grado di recapitare al server di log. Il sistema di log opera in un ambiente sincronizzato, in grado di interpretare i Log e di avvisare rapidamente gli operatori in caso di necessità.

Torna al Sommario

9.1.2 Produzione dei log

Ogni applicativo invia i messaggi di log al server. Ogni messaggio è strutturato in modo da contenete le seguenti informazioni:

- Applicativo che lo ha generato;
- IP della macchina su cui è installato l'applicativo;
- Data e ora del log;
- Nome della specifica componente dell'applicativo che lo ha generato;
- Livelli di log;
- Messaggio dettagliato di log;

I log prodotti sono di duplice natura:

- Log dei processi interni al sistema. Ogni transazione all'interno dei flussi di processo, delle verbalizzazioni delle attività e di ogni altra operazione è verbosamente loggata e registrata al fine di garantire la più completa evidenza dell'avanzamento dei processi.
- Log prodotti a seguito di interazioni con utenza, sia umana che automatizzata. Le registrazioni delle attività delle utenze umane sono puntuali per ogni step dell'interazione al fine di documentare la volontà dell'utente nelle operazioni in corso. Parimenti le registrazioni delle interazioni delle utenze automatizzate saranno verbosamente loggate.

Torna al Sommario

9.1.3 La trasmissione dei log

Il server accetta Graylog2 syslog standard tramite TCP / UDP e GELF via UDP.

Il formato dei log è il Graylog Extended Log Format(GELF) , adatto per l'invio di messaggi di log all'interno di applicazioni in modo semplice e strutturato. I log vengono anche conservati all'interno di ogni macchina che li ha generati, in appositi files di testo.

Torna al Sommario

9.1.4 Analisi dei log

Tutti i dati inviati al server di log appariranno nell'interfaccia web. E' possibile utilizzare l'interfaccia web per cercare e filtrare i dati. Una parte centrale dell'interfaccia web sono i flussi. In sostanza vengono salvate le ricerche che consentono di accedere rapidamente una visione d'insieme che è già pre-filtrata in modo che corrisponda ad esempio ad alcune parti specifiche della vostra applicazione. È inoltre possibile eseguire monitoraggio ed allarmistica sui flussi di singoli o direttamente inoltrare tutti i messaggi che vengono abbinati in un flusso ad altri endpoint.

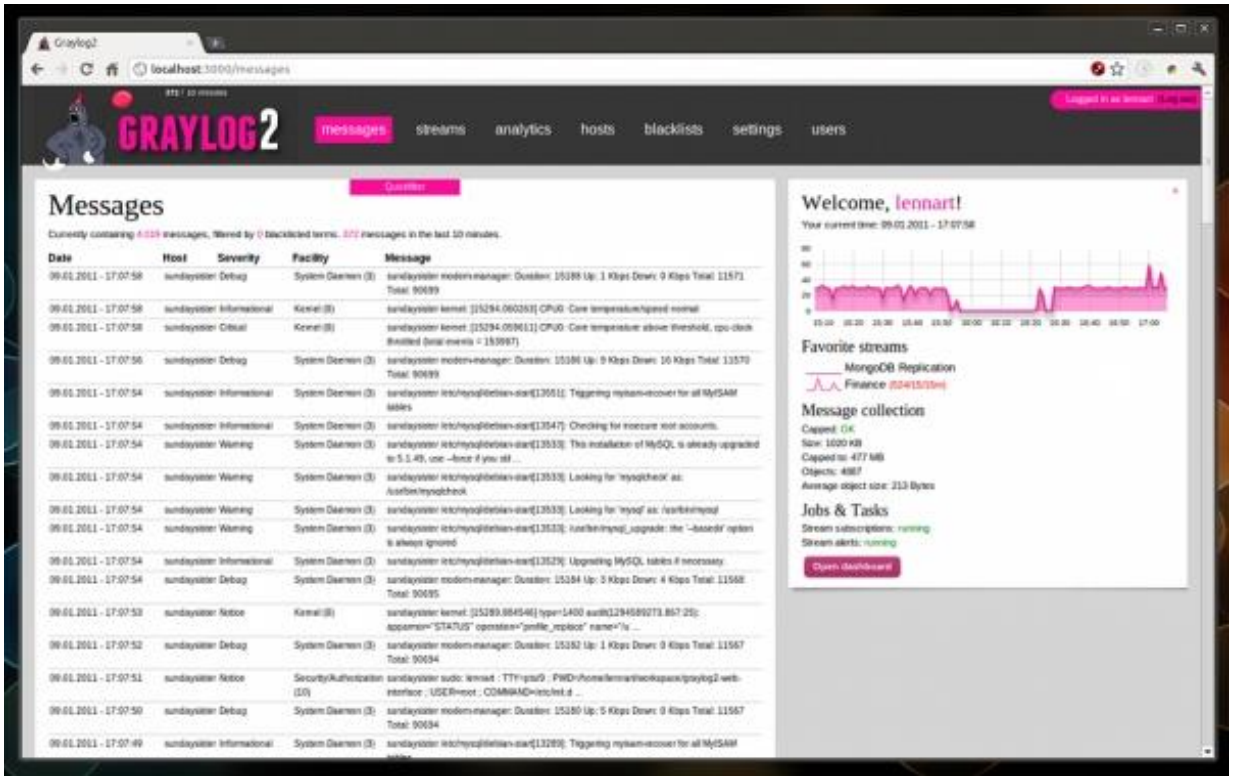

Figura 6 - visualizzazione dei log

La seguente tabella definisce i livelli dei log e i messaggi in ordine decrescente di severità.

La colonna di sinistra indica il livello di log designato e alla destra c'è una breve descrizione.

Livello	Descrizione
OFF	Il livello più alto possibile, viene usato per disattivare i log (mai in produzione)
FATAL	Errore importante che causa un prematuro termine dell'esecuzione. Questo sarà segnalato immediatamente all'operatore mediante mail
ERROR	Un errore di esecuzione o una condizione imprevista. Anche questo viene immediatamente segnalato.
WARN	Usato per ogni condizione inaspettata o anomalia di esecuzione, che però non necessariamente ha comportato un errore.
INFO	Usato per segnalare eventi di esecuzione (esempio: startup/shutdown). Deve essere segnalato ma poi non mantenuto per tanto tempo.
DEBUG	Usato nella fase di debug del programma. Viene riportato nel file di log.

La piattaforma web di analisi è in gradi di effettuare qualsiasi tipo di ricerca sui log, aggregarli e raggrupparli.

Vengono quindi resi possibili sia il monitoraggio dell'intero sistema in tempo reale che l'analisi del comportamento del sistema nel tempo. E' sufficiente disporre di una postazione con un browser web.

Torna al Sommario

9.1.5 Verifica funzionalità del sistema da dispositivi mobili

E' a disposizione degli operatori una app, realizzata dall'Azienda per applicativi mobili Android, in grado di interrogare, mediante un apposito web services, i server di versamento/disseminazione e quello di gestione, sia del sito primario che di quello di DR.

Oltre a controllare che i server rispondano sull'https, il servizio effettua un check sulla disponibilità dei database server, effettuando una query di ping, nonché dei NAS storage montati in NFS. Il risultato ritornato viene mostrato sul display. In questo modo gli operatori sono in grado di effettuare un controllo sulle funzionalità del sistema anche quando non fisicamente presenti all'interno dei siti.

Torna al Sommario

9.1.6 Specificità relative al monitoraggio

Ulteriori procedure aggiuntive richieste dal soggetto Produttore saranno descritte nell'allegato "Specificità del contratto".

Torna al Sommario

9.2 Verifica dell'integrità e leggibilità degli archivi

Verifiche periodiche sugli archivi sono effettuate da procedure schedulate che effettuano periodici controlli al fine di garantire l'integrità dei documenti conservati e la loro congruenza:

- Controllo della corrispondenza tra gli hash contenuti nell'indice di conservazione e gli hash dei documenti riferiti calcolati a runtime;
- Controllo delle significant properties;
- verifica dell'effettiva leggibilità dei documenti inseriti all'interno dei pacchetti di archiviazione, mediante il software di visualizzazione assegnato.

Le procedure in questione sono completamente automatizzate. Alla fine della procedura, che esegue il controllo su parti dell'archivio, viene generato un report con l'elenco dei pacchetti di archiviazione controllati, il risultato dei controllo, la data e l'ora in cui i controlli sono stati effettuati. Il template del verbale è definito dal Responsabile del Servizio di Conservazione e definito in sede di specifica di contratto.

Per quanto riguarda l'ultimo punto, concernete la leggibilità dei documenti, il Responsabile del Servizio di Conservazione, con cadenza annuale, verificherà 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.

Il verbale in oggetto viene inviato via mail al responsabile della Conservazione. In caso di anomalie viene inviata una mail di alert al Responsabile ed alle altre figure deputate.

Le attività svolte dalle procedure di verifica sono controllabili anche dal server di log descritto nel capitolo precedente.

Al fine di garantire il Servizio a fronte di un'eventuale obsolescenza dei formati dei documenti conservati Marno provvede a comunicare al produttore la data di scadenza del vecchio formato e il permesso ad adottarne uno disponibile - ottenuto il consenso alla migrazione, concordata nei tempi e nei metodi, Marno procede alla copia dei documenti nel nuovo formato ed alla produzione dei relativi verbali. Il produttore, da parte sua, provvederà, anche a campione, a verificare l'esito della migrazione arricchendo i verbali; ad ulteriore consenso ottenuto verranno eliminati i file originali.

Ulteriori procedure aggiuntive richieste dal soggetto Produttore saranno descritte nell'allegato "Specificità del contratto".

Torna al Sommario

9.3 Soluzioni adottate in caso di anomalie

In caso di anomalia riscontrata dai controlli del paragrafo precedente, il Responsabile del Servizio di Conservazione provvederà, utilizzando le copie di sicurezza conservate nel sito di Recovery, al corretto ripristino dell'intero archivio.

Un'apposita procedura preleva i dati dal le copie di sicurezza generate, ne verifica l'integrità, e procede nuovamente al salvataggio di tutti gli elementi (documenti digitali, indice di conservazione) sul sistema di Conservazione primario.

Il verificarsi dell'anomalia e l'esecuzione della procedura di ripristino dell'archivio sono debitamente registrati nel sistema di log.

Accordi specifici concordati con il soggetto Produttore possono essere descritti nell'allegato "Specificità del contratto".

Torna al Sommario